Entscheide und Fragen zum Datenschutz, insbesondere im Versicherungsbereich

Nando Stauffer von May* / Sonia Lehner**

Das Schweizer Datenschutzrecht orientiert sich stark an der europäischen Datenschutz-Grundverordnung. In der EU werden beinahe täglich neue Entscheide gefällt sowie Merkblätter veröffentlicht. Auch in der Schweiz liegen erste Entscheide zum revidierten Datenschutzgesetz vor und der Tätigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten wird vermehrt Beachtung geschenkt. Der vorliegende Beitrag geht auf neueste Entwicklungen und Praxisfragen in den Bereichen Datensicherheit, Bekanntgabe von besonders schützenswerten Personendaten an Dritte, Informationspflicht, Auskunftsbegehren, Bussen und Auftragsbearbeitung ein, jeweils mit einem Fokus auf die Versicherungsbranche.

Le droit de la protection des données suisse s'inspire fortement du règlement européen sur la protection des données (RGPD). Au sein de l'Union européenne, de nouvelles décisions sont rendues et des fiches informatives sont publiées presque quotidiennement en la matière. En Suisse, l'on dispose également des premières décisions prises en application de la nouvelle loi fédérale sur la protection des données (LPD) et l'activité du préposé fédéral à la protection des données et à la transparence suscite de plus en plus d'intérêt. La présente contribution s'intéresse aux développements récents et aux questions pratiques dans les domaines de la sécurité des données, de la communication de données sensibles à des tiers, du devoir d'information, des demandes d'accès, des amendes ainsi que de la sous-traitance en mettant l'accent sur le secteur de l'assurance.

I. Einleitung

Nahezu jeder Versicherer kennt die nachfolgenden Situationen: Nachdem die Leistungspflicht abgelehnt wird, fliegt ein Auskunftsbegehren ins Haus. Oder mit Geschäftspartnern diskutiert «Legal» oder «Compliance», ob der Partner nun Auftragsbearbeiter, gemeinsam Verantwortlicher oder eigenständiger Verantwortlicher ist und ob man diesem Personendaten bekanntgeben darf. Bei der Datensicherheit verlässt sich der Versicherer auf seine IT-Abteilung und wenn etwas schiefläuft, kommt die Frage, ob die Verletzung der Datensicherheit (sog. *Data Breach*) gemeldet werden muss. Versicherungsnehmer wünschen entsprechenden Cyber-Schutz und hätten am liebsten auch Bussen für Datenschutzverletzungen versichert. Der vorliegende Beitrag will auf einige der sich für Versicherer stellenden Fragen Antworten geben und erste Entscheide präsentieren.

II. Datensicherheit und *Data Breach*

A. Gesetzliche Regelung

Das Schweizer Datenschutzgesetz (DSG) verpflichtet den Verantwortlichen und die Auftragsbearbeiter, durch technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten.[1] Die europäische Datenschutz-Grundverordnung (DSGVO) enthält eine ähnliche Bestimmung,[2] die den Verantwortlichen und den Auftragsverarbeiter anweist, geeignete technische und organisatorische Massnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu erreichen. Diese Bestimmung beinhaltet darüber hinaus eine exemplarische Liste von Massnahmen. In der Schweiz hat der Bundesrat die notwendigen Massnahmen in der Datenschutzverordnung präzisiert.[3] Diese Anforderungen gehen teilweise sehr weit und es ist fraglich, inwiefern diese noch durch die Delegationsnorm im DSG gedeckt sind.[4] Die Frage ist indes eher akademischer Natur, da den meisten Artikeln nur programmatischer Charakter zukom-

* Dr. iur., Rechtsanwalt, Partner bei gbf Rechtsanwälte AG, von 2016 bis 2019 Datenschutzbeauftragter eines Erst- und eines Rückversicherers.
** MLaw, *Greffière* bei der Staatsanwaltschaft des Kantons Waadt.

1 Art. 8 Abs. 1 DSG.
2 Art. 32 DSGVO.
3 Art. 1 ff. DSV.
4 Nach Art. 164 und Art. 182 BV sind alle wichtigen Rechtssätze in Form des Bundesgesetzes, d.h. durch das Parlament unter Referendumsvorbehalt, zu erlassen (formelles Legalitätsprinzip; Gesetzesvorbehalt im Sinne eines Vorbehalts des formellen Gesetzes). In diesem Sinne muss der Gesetzgeber nach der sog. Wesentlichkeitstheorie das Wichtige selber festlegen. Namentlich die Auferlegung von Leistungspflichten, wie auch die Festlegung der Rechte und Pflichten unter Privaten, bedürfen eines Entscheides durch den Gesetzgeber. Die Verordnungsstufe genügt hierfür nicht (vgl. Nando Stauffer von May, Regionale Aufgabenerfüllung und demokratische Rechte, Diss. Bern 2018, N 182–192).

men dürfte und diese kaum justiziabel sind.[5] Dies ist insoweit problematisch, als mit Busse bis zu 250'000 Franken bestraft wird, wer vorsätzlich die Mindestanforderungen an die Datensicherheit, die der Bundesrat erlassen hat, nicht einhält.[6] Dazu gibt es nun aber einen klärenden Entscheid eines Genfer Gerichts:

B. Entscheid betr. Genfer Klinik

Im fraglichen Entscheid der strafrechtlichen Rekurskammer des *Cour de Justice* Genfs[7] ging es darum, dass eine Patientin von ihrem Psychiater bzw. der diesbezüglichen Klinik wissen wollte, ob ihre medizinischen Daten von einer Schulkollegin, welche in der Buchhaltung der Klinik tätig war, bearbeitet wurden. Die Klinik hatte die Zugriffe protokolliert und teilte mit, dass die Schulkollegin am 7. Juli 2023 um 13.30 Uhr während rund dreissig Sekunden die medizinische Akte konsultierte. Welchen Inhalt die Buchhalterin genau konsultierte, konnte hingegen mangels Aufzeichnung durch die Software nicht eruiert werden. Als Mitarbeiterin in der Rechnungsabteilung hatte sie grundsätzlich Zugang zu den gesamten Krankenakten der Patienten, da sie für die Rechnungsstellung wissen musste, welche medizinischen Leistungen erbracht worden waren. Immerhin hätten die Ärzte die Möglichkeit gehabt, den Zugriff auf bestimmte Benutzer zu beschränken oder sogar ganz zu sperren, wovon aber offenbar kein Gebrauch gemacht worden ist. Die betroffene Person machte u.a. geltend, dass der Zugriff der Buchhaltung auf jene Daten hätte beschränkt werden müssen, welche für die Zahlungsabwicklung erforderlich sind, nicht aber auf die gesamte Patientenakte.

Das Genfer Strafgericht verweist auf die in der Lehre geäusserte Kritik, wonach unter dem Gesichtspunkt des Grundsatzes «nullum crimen, nulla poena sine lege» die Verletzung der wenig klaren und präzisen Bestimmungen der Datenschutzverordnung kaum je eine Strafbarkeit begründen dürfte. Der mangelnden Präzision sei dadurch zu begegnen, dass nur in schweren oder offensichtlichen Fällen eine Strafbarkeit in Frage komme, wobei der mangelnden Klarheit der Norm dadurch Rechnung getragen werde, in dem nur die vorsätzliche Begehung strafbar sei, nicht aber die fahrlässige.[8]

Im vorliegenden Fall liege ein objektiver Grund (Rechnungsstellung) für den Zugriff auf die medizinische Akte vor, die Buchhaltung unterliege der ärztlichen Schweigepflicht und die Frage, wie umfangreich der Zugriff der Buchhaltung gewährt werden dürfe, sei letztlich eine zivilrechtliche Verhältnismässigkeitsfrage. Eine schwere oder offensichtliche Verletzung der Datensicherheit liege angesichts dessen nicht vor;[9] entsprechend wurde keine Strafe ausgesprochen. In der EU unter DGSVO demgegenüber wurden wegen Verletzung der Datensicherheit schon unzählige Bussen verteilt, wie die nachfolgenden Beispiele aus der Versicherungswelt verdeutlichen.

C. Entscheid betr. Online-Autoversicherungsvermittlung

Am 18. Juli 2019 hat die *Commission Nationale de l'Informatique et des Libertés* (CNIL) einen Versicherungsvermittler für Autoversicherungen mit einer Busse von 180'000 Euro bestraft.[10] Im Rahmen seiner Geschäftstätigkeit betrieb der Vermittler eine Website, auf der Interessenten Angebote anfordern oder Autoversicherungen abschliessen konnten. Im Juli 2018 wurde die CNIL durch einen Kunden des Unternehmens informiert, dass er ohne Authentifizierungsverfahren auf die Daten anderer Kunden zugreifen konnte. Es wurde festgestellt, dass bei einer Suchanfrage mit der Suchmaschine «Duckduckgo» mit gewissen Suchbegriffen der direkte Zugang zu Kundendaten möglich war. Ausserdem konnten die Kunden, wenn sie in ihrem persönlichen Konto eingeloggt waren, durch Änderung der URL auf die Kundenkonten anderer Personen zugreifen.

Erschwerend kam hinzu, dass die Kunden sich online in ihr persönliches Konto durch Kundennummer und Geburtsdatum anmelden konnten, wobei die zweite Angabe als Passwort galt. Es wurden keine zusätzlichen Sicherheitsmassnahmen ergriffen und insbesondere kein anderes Passwort verlangt. Die CNIL wies darauf hin, dass ein starkes Passwort mindestens zwölf Zeichen lang sein und mindestens einen Grossbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten müsse. Alternativ kann ein robustes Passwort auch mindestens acht Zeichen lang sein, drei dieser vier Sonderzeichen beinhalten und von einer zusätzlichen Sicherheitsmassnahme begleitet sein (z.B. Sperrung des Kontos nach mehreren Fehlversuchen). Ein Geburtsdatum erfüllt diese Bedingungen offensichtlich nicht.

Im vorliegenden Fall wurde festgestellt, dass der Versicherungsvermittler es unterlassen hatte, elementare

[5] Siehe dazu Hannes Meyle/Anne-Sophie Morand/David Vasella, DSG: keine Mindestanforderungen an die Datensicherheit, keine entsprechende Strafbarkeit, weitere Anmerkungen, 19. September 2022, Internet: https://datenrecht.ch/dsv-keine-mindestanforderungen-an-die-datensicherheit-keine-entsprechende-strafbarkeit-weitere-anmerkungen/ (Abruf 9.10.2025) und David Vasella, Zum Entwurf der revidierten VDSG: eine verpasste Chance, 17. Juli 2021, Internet: https://datenrecht.ch/zum-entwurf-der-revidierten-vdsg-eine-verpasste-chance/ (Abruf 9.10.2025).

[6] Art. 61 lit. c DSG.

[7] Cour de Justice, Chambre pénale de recours, Arrêt du 26 mars 2025, P/9589/2024 ACPR/239/2025.

[8] Erwägung 2.3, letzter Absatz.

[9] Erwägung 2.4.

[10] *Commission Nationale de l'Informatique et des Libertés* (CNIL), SAN-2019-007 vom 18. Juli 2019.

Sicherheitsmassnahmen im Vorfeld der Entwicklung der Website zu ergreifen. In der Gesamtheit der Verfehlungen des Versicherungsvermittlers dürfte hier vor dem Hintergrund des vorzitierten Genfer Entscheids auch in der Schweiz eine Busse in Frage kommen.

D. Entscheid betr. Medizinische Begutachtung

Die *Agencia Española de Protección de Datos* (AEPD) hatte einen Fall zu beurteilen, in dem eine Person mehrmals Zustimmungen für medizinische Begutachtungen von Dritten, die sie nicht kannte, per E-Mail zugestellt erhalten hatte.[11] Obwohl sie diese E-Mails jeweils dem Kundendienst der Versicherung meldete, wurde das Problem nicht gelöst und die Person bekam weiterhin solche E-Mails.

Der Versicherung wird vorgeworfen, die Grundsätze für die Verarbeitung personenbezogener Daten, die Sicherheit der Verarbeitung und die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde verletzt zu haben.[12] Aus dem durchgeführten Verfahren ergeben sich zahlreiche Anhaltspunkte dafür, dass die Versicherung nicht genügend technische und organisatorische Massnahmen ergriffen hat, um den Schutz der Gesundheitsdaten zu gewährleisten. Die AEPD hebt auch hervor, dass Mitarbeiter von zwei verschiedenen Managern denselben Fehler gemacht hätten, was darauf hinweise, dass es sich nicht um ein menschliches Versagen, sondern um eine fehlerhafte Konfiguration von Seiten des Verantwortlichen handle. Ferner hat die Versicherung die Verletzung des Datenschutzes nicht innerhalb von 72 Stunden der Aufsichtsbehörde gemeldet, ohne dafür einen triftigen Grund zu nennen, was zudem eine Verletzung der Meldepflicht darstellt.

Die AEPD hat die Versicherung zu einer Busse von insgesamt 220’000 Euro verurteilt.

E. Entscheid betr. Sicherheitsmassnahmen beim Auftragsbearbeiter & Schlussbericht des EDÖB in Sachen Xplain

Ein im Entscheid[13] leider nicht näher beschriebener Vorfall führte zu einer Veröffentlichung von Personendaten von Versicherungsnehmern der ZURICH INSURANCE PLC SUCURSAL EN ESPAÑA in Internetforen. Der für den Vorfall verantwortliche Auftragsbearbeiter, ein Anbieter technologischer Infrastrukturen, wurde mit 80’000 Euro gebüsst, u.a. da festgestellt worden ist, dass er im Zeitpunkt der Verletzung der Datensicherheit über keine ausreichenden, dem Risiko angemessenen Sicherheitsmassnahmen getroffen hatte. Der Auftragsbearbeiter wurde offenbar nicht direkt vom Versicherer beigezogen, sondern vom katalonischen Automobilklub (REIAL AUTOMÒBIL CLUB DE CATALUNYA), welcher mit GACM SEGUROS GENERALES, COMPAÑÍA DE SEGUROS Y REASEGUROS S.A.U. (GACM) vertraglich verbunden war.

Der Fall zeigt auf, dass das Hauptrisiko beim Beizug von Auftragsbearbeitern oftmals in der Datensicherheit liegt. Folgerichtig legt der Schweizer Gesetzgeber hierauf besonderes Gewicht, wenn er folgendes vorschreibt: «Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.»[14]

Auch der Ransomware-Angriff auf Xplain zeigt die Wichtigkeit der Datensicherheit beim Auftragsbearbeiter auf: «Im Mai 2023 ereignete sich ein Ransomware-Vorfall auf das Unternehmen Xplain AG […]. Xplain ist ein Informatik-Dienstleister verschiedener Bundesorgane [u.a. für das Bundesamt für Polizei fedpol und das Bundesamt für Zoll und Grenzsicherheit BAZG] und Kantone im Bereich der öffentlichen Sicherheit. Der Vorfall hat zum Abfluss erheblicher Datenmengen geführt, die auf den Systemen von Xplain gespeichert waren. Die Daten wurden in der Folge in Tranchen im Darknet veröffentlicht.»[15] Vom Vorfall waren auch Daten betroffen, die längstens nicht mehr benötigt worden sind und hätten gelöscht werden müssen. Es ist deshalb zentral, dass nicht mehr benötigte Personendaten gelöscht werden und Verantwortliche ein – mindestens implizites, gelebtes – Löschkonzept haben und dieses auch vom Auftragsbearbeiter eingehalten wird, der ansonsten riskiert, selbst Verantwortlicher zu werden.[16] Damit ein Löschkonzept erstellt und überhaupt angemessene technische und organisatorische Massnahmen getroffen werden können, müssen der Verantwortliche wie auch der Auftragsbearbeiter eine Übersicht über die Personendaten, die er bearbeitet, haben, was im vorliegenden Fall bei Xplain offensichtlich fehlte.[17] Eine solche Übersicht stellt das Bearbeitungsverzeichnis dar, welches unseres Erachtens jedenfalls rudimentär auch von Unternehmen geführt werden sollte, welche dazu nicht verpflichtet sind.[18] Im Übrigen hält der EDÖB zurecht fest, dass der Verantwortliche durchaus auch auf die Datensicherheit des Auftragsbearbeiters vertrauen darf: «Sofern der

[11] AEPD, Exp. N° PS/00080/2022 vom 3. Mai 2022.
[12] D.h. Art. 5 Abs. 1 lit. f, Art. 32 und Art. 33 DSGVO.
[13] AEPD, Exp. N° EXP202102640 vom 8. August 2022.
[14] Art. 9 Abs. 2 DSG. Der weniger fokussierte Art. 28 DSGVO sieht diese Verpflichtung des Verantwortlichen ebenfalls vor (insb. Art. 28 Abs. 3 lit. c DSGVO), s.a. Schlussbericht und Empfehlungen des EDÖB vom 25. April 2024 in Sachen Xplain AG, N 90 f.
[15] Schlussbericht und Empfehlungen des EDÖB vom 25. April 2024 in Sachen fedpol, N 1.
[16] Schlussbericht i.S. Xplain AG (FN 14), N 119 f., 140, 143 sowie Empfehlung 10.
[17] Schlussbericht i.S. Xplain AG (FN 14), N 133.
[18] S.a. Art. 12 DSG und Art. 24 DSV.

Auftragnehmer selbst dem aDSG untersteht, kann der Verantwortliche davon ausgehen, dass die technischen und organisatorischen Massnahmen der Datensicherheit […] angemessen erfüllt sind […]. Der Verantwortliche ist deshalb verpflichtet, den Auftragsbearbeiter sorgfältig auszuwählen, zu instruieren und soweit nötig zu überwachen.»[19]

F. Entscheid betr. Screenshot

Im vorliegenden Fall aus Spanien bekam eine Versicherungsnehmerin eine E-Mail von ihrem Ex-Partner, in dessen Anhang sich ein Dokument mit den Einzelheiten der von ihr abgeschlossenen Fahrzeugversicherung befand.[20] Eine Mitarbeiterin der Versicherungsgesellschaft hatte aus dem System einen Screenshot gemacht und diesen dem Ex-Partner der Versicherten, mit dem sie eine freundschaftliche Beziehung unterhielt, weitergeleitet.

Die Versicherung war in der Lage, aufzuzeigen, dass die Mitarbeiterin berechtigt war, auf die Daten zuzugreifen und dass sie über ihre Pflichten bezüglich Datenschutzes informiert wurde (inklusive interne Ausbildungen im Bereich Datenschutz und interne Weisungen). Die Versicherung verfügte jedoch über kein System, dass die Rückverfolgbarkeit des Datenzugriffs ermöglichte und somit unberechtigte Zugriffe protokollierte. Dazu kommt, dass in diesem Fall ein *Screenshot* gemacht wurde, obwohl es Anwendungen gibt, die die Aufnahme von Screenshots unterbinden.

Die *Agencia Española de Protección de Datos* erwägt, dass die beklagte Versicherung nicht genügend Sicherheitsmassnahmen vorgenommen hat und verurteilt sie deswegen zu einer Busse von 200'000 Euro.

Während hier die fehlende Protokollierung auch unter Schweizer Recht problematisch wäre, scheint uns das fehlende Unterbinden von *Screenshots* kaum busswürdig. Auch wenn eine Anwendung zur Unterbindung von *Screenshots* eingesetzt würde, wäre es immer noch möglich, ein Foto mit dem Mobiltelefon zu machen, was zum selben Ergebnis führen würde und kaum verhindert werden kann. Um dieses Risiko zu vermeiden, müsste man die Mitarbeiter ständig überwachen, was nicht verhältnismässig ist und gegen die Rechtsprechung des EGMR verstösst.[21]

G. Entscheid betr. E-Mail-Versand

Im November 2018 schickte eine Mitarbeiterin einer Versicherung aus Versehen eine E-Mail an den falschen Empfänger. Die E-Mail enthielt den Familiennamen, das Geschlecht und Gesundheitsdaten der betroffenen Person. Zwanzig Tage später machte die Mitarbeiterin den gleichen Fehler noch einmal, worauf hin die betroffene Person sich an die *Commission nationale pour la protection des données luxembourgeoise* (CNPD) wandte.[22]

Die CNPD stellt fest, dass die Versicherung keine Dokumentation über die Verletzungen des Datenschutzes führt, wie dies die DSGVO vorschreibt.[23] Die Versicherung argumentiert, dass die gesendeten Daten es nicht erlauben, die betroffene Person zu identifizieren, weshalb es sich nicht um personenbezogene Daten handle. Die CNPD erinnert daran, dass der Begriff «personenbezogene Daten» weit auszulegen ist und die Daten im vorliegenden Fall zumindest indirekt erlauben, die betroffene Person zu identifizieren. Aus diesem Grund hätte die Versicherung dieses Ereignis dokumentieren müssen.

Darüber hinaus stellt die CNPD fest, dass das Versicherungsunternehmen die Datenschutzverletzung der Aufsichtsbehörde[24] und der versicherten Person[25] hätte melden müssen, wobei vorliegend nur letzteres erfolgt sei und dabei aber nicht sämtliche vorgeschriebenen Informationen mitgeteilt worden seien und auch die gesetzliche Frist nicht eingehalten worden sei.

Obwohl die versicherte Person dem Versenden ihrer Daten per E-Mail zugestimmt hatte, bemängelte die CNPD weiter, dass das Versicherungsunternehmen keine geeigneten technischen und organisatorischen Massnahmen ergriffen habe (bspw. Verschlüsselung), um das mit dem E-Mail-Versand verbundene Risiko zu kontrollieren, was aufgrund der enthaltenen, besonders schützenswerten Personendaten erforderlich sei.

Die Versicherung wurde zur Zahlung einer Busse von 135'000 Euro verpflichtet.

In der Schweiz dürfte dieser Vorfall weder die Schwelle der Meldepflicht an den eidgenössischen Datenschutzbeauftragten noch eine Mitteilungspflicht an die betroffene Person begründen, da dieser nur eine Person betraf und kaum zu erwarten war, dass der Empfänger die betroffene Person identifizieren kann. Eine Busse käme ebenfalls nicht in Betracht, da u.E. in den aller-

[19] Hervorhebung hinzugefügt; Schlussbericht und Empfehlungen des EDÖB vom 25. April 2024 in Sachen BAZG, N 82; Vasella, EDÖB: Schlussberichte i.S. Xplain, fedpol und BAZG, datenrecht.ch vom 12.05.2024.

[20] AEPD, Exp. N° EXP202213514 vom 21. Mai 2024.

[21] Urteil des Europäischen Gerichtshofs für Menschenrechte (EGMR), Bărbulescu gegen Rumänien, Application no. 61496/08, vom 5. September 2017.

[22] CNPD, délibération n° 31FR/2021 vom 5. August 2021. Siehe dazu auch Célian Hirsch, Deux courriels au mauvais destinataire peuvent coûter cher, 21. Oktober 2021, Internet: www.swissprivacy.law/96 (Abruf 9.10.25).

[23] Art. 33 Abs. 5 DSGVO.

[24] Art. 33 Abs. 1 DSGVO.

[25] Art. 34 Abs. 1 DSGVO.

meisten Fällen keine weitergehende, als die ohnehin meist bestehende Transportverschlüsselung verlangt werden kann. Bezeichnenderweise bleiben die Behörden denn oftmals auch vage, wenn es darum geht, die geforderte Verschlüsselung genauer zu definieren.

H. Data Breach Notice

Verletzungen der Datensicherheit («Data Breach»), d.h. eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden,[26] müssen dem EDÖB so rasch als möglich gemeldet werden, wenn diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen.[27] Der EDÖB stellt hierfür ein Online-Formular zur Verfügung; sogar auf Englisch, wobei die Übersetzung nicht durchwegs geglückt ist.[28] Der Verantwortliche muss auch die betroffene Person informieren, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.[29] Ähnliche Regelungen sieht auch die DSGVO vor.[30] Versicherer haben überdies der FINMA bei Cyber-Attacken innert 24 Stunden ab deren Entdeckung eine Erstmeldung zu erstatten.[31] Der Vorfall dürfte ferner in der Regel dem Bundesamt für Cybersicherheit gemeldet werden müssen.[32] Zu beachten ist insb., dass der Versicherer auch für ausgelagerte Tätigkeiten und entsprechend bei Verletzungen der Datensicherheit beim Outsourcing-Partner meldepflichtig sein kann.[33] Dies gilt ganz grundsätzlich auch datenschutzrechtlich bei der Auftragsbearbeitung, so dass der Auftragsbearbeiter den Verantwortlichen über Verletzungen der Datensicherheit zu orientieren hat,[34] der dann wiederum ggf. den EDÖB und/oder die betroffene Person informieren muss.

III. Bekanntgabe von besonders schützenswerten Personendaten an Dritte

A. Einleitung und gesetzliche Regelung

Wenn die Compliance-Abteilung das Wort «Gesundheitsdaten» hört, ist meist das Einwilligungsformular nicht weit entfernt. Während die Erlaubnis bzw. letztlich die Vollmacht, Gesundheitsdaten bei Dritten (wie Ärzten oder anderen Versicherern) zu beschaffen, sicherlich sinnvoll ist, scheint die Einwilligung, Personendaten bekanntgeben zu dürfen, von Versicherern bisweilen unnötigerweise eingeholt zu werden. So kann es vorkommen, dass ein Schadenbearbeiter eines Haftpflichtversicherers von der geschädigten Person die Einwilligung einverlangt (bzw. nach Compliance-Vorgaben einverlangen muss), Personendaten des Geschädigten dem eigenen Rechtsanwalt weitergeben zu dürfen, damit dieser dem Haftpflichtversicherer eine Einschätzung der Rechtslage und Prüfung des Anspruchs des Geschädigten geben kann. Der Geschädigte bzw. dessen Anwalt wird so letztlich in die Lage versetzt, den Gegenanwalt (jenen des Haftpflichtversicherers) auszuwählen, indem er die Einwilligung nach Gusto erteilt oder nicht. Mit Datenschutz hat dies nicht mehr viel zu tun.

Sowohl im Schweizer als auch im europäischen Datenschutzrecht stellt die Übermittlung von personenbezogenen Daten an Dritte eine Datenbearbeitung dar.[35] Die EU geht grundsätzlich von einem Verbot der Datenverarbeitung aus, sofern nicht eine Rechtsgrundlage die Verarbeitung erlaubt. Sind besonders schützenswerte Personendaten betroffen, ist das grundsätzliche Verbot der Datenverarbeitung und Bekanntgabe besonders strikt. Zulässig ist die Verarbeitung (inkl. Bekanntgabe) nur noch in wenigen abschliessend geregelten Situationen, insb. bei ausdrücklicher Einwilligung der betroffenen Person für einen oder mehrere festgelegte Zwecke oder wenn die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.[36] Bezüglich des Erlaubnistatbestands der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen kann präzisiert werden, dass unerheblich ist, ob es sich um ein gerichtliches, aussergerichtliches oder um ein Verwaltungsverfahren handelt.[37] Der Begriff «Rechtsansprüche» ist weit auszulegen und erfasst sowohl öffentlich-rechtliche als auch privatrechtliche Rechtspositionen.[38] Der Erlaubnistatbestand kann insb. auch bei der Übermittlung von Gesundheitsdaten durch Privatversicherer zur Anwendung kommen[39] und gilt auch für Rechtsanwälte.[40]

26 Art. 5 lit. h DSG.
27 Art. 24 Abs. 1 DSG; s.a. Leitfaden des EDÖB betreffend die Meldung von Datensicherheitsverletzungen und Informationen der Betroffenen nach Art. 24 DSG, 6. Februar 2025.
28 Internet: https://databreach.edoeb.admin.ch/report (Abruf 9.10.2025), wo bspw. «senden» am Schluss des Formulars mit «save» übersetzt wird, so dass dem englisch sprachigen Nutzer dann nicht bewusst wird, dass das Formular bereits abgeschickt wird.
29 Art. 24 Abs. 3 DSG.
30 Art. 33 f. DSGVO.
31 FINMA-Aufsichtsmitteilung 03/2024, Ziff. 3, auf Grundlage der Aufsichtsmitteilung 05/2020 sowie letztlich Art. 29 Abs. 2 FINMAG.
32 Art. 74b Abs. 1 lit. e bzw. Art. 74a ff. ISG.
33 FINMA-Aufsichtsmitteilung 03/2024, Ziff. 3.
34 Art. 24 Abs. 3 DSG.
35 Art. 5 lit. d und e DSG bzw. Art. 4 Abs. 2 DSGVO.
36 Art. 9 Abs. 2 lit. a und lit. f DSGVO. Bei letzterem handelt es sich um einen Sonderfall des allgemeinen Erlaubnistatbestands des berechtigten Interesses (Alexander Schiff, in: Eugen Ehmann/Martin Selmayr (Hrsg.), Datenschutz-Grundverordnung, 3. Auflage, München 2024, Art. 9 N 48).
37 Erwägungsgrund 52, Satz 3, DSGVO; Thomas Petri, in: Spiros Simitis/Gerrit Hornung/Indra Spiecker (Hrsg.), Datenschutzrecht Nomos-Kommentar, 2. Auflage, 2025, Art. 9 N 63; Schiff (FN 36), Art. 9 N 48.
38 Andreas Jaspers/Rolf Schwartmann/Robin L. Mühlenbeck, in: Rolf Schwartmann/Andreas Jaspers/Gregor Thüsing/Dieter Kugelmann (Hrsg.), DS-GVO/BDSG, Art. 9 N 171.
39 Jaspers/Schwartmann/Mühlenbeck (FN 38), Art. 9 N 174.
40 Cécile De Terwangne/Karen Rosier, Le règlement générale sur la protection des données (RGPD/GDPR), 2018, 280.

Unter dem schweizerischen Datenschutzgesetz ist eine Bekanntgabe von Personendaten an Dritte grundsätzlich erlaubt, solange dadurch nicht die Persönlichkeit der betroffenen Personen widerrechtlich verletzt wird.[41] Gemäss DSG liegt aber eine Persönlichkeitsverletzung vor, wenn besonders schützenswerte Personendaten Dritten bekanntgegeben werden.[42] Als Dritte gelten eigenständige Verantwortliche, wie eben Rechtsanwälte,[43] nicht aber Auftragsbearbeiter.[44] Eine Persönlichkeitsverletzung ist indes nur dann widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.[45] Die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen wird nicht explizit als Rechtfertigungsgrund genannt. Sofern es um vertragliche Ansprüche geht, kann deren Geltendmachung oder Abwehr unter den explizit genannten Rechtfertigungsgrund der Vertragsabwicklung fallen.[46] Ansonsten erfolgt die Interessenabwägung im Rahmen der Generalklausel. Es gilt das private Interesse an der Bekanntgabe von besonders schützenswerten Personendaten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen jenem der betroffenen Person gegenüberzustellen, wobei u.E. das Interesse an der Bekanntgabe zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen in der Regel überwiegen dürfte.

B. Entscheid betr. Stellung des Rechtsanwalts

Im vorliegenden Fall[47] geht es um einen Spieler, der an zwei verschiedenen Online-Glücksspielen teilnimmt und seinen Einsatz verliert. Zuerst spielt er ein Online-Glücksspiel auf einer Website, die dem Unternehmen B gehört. Nachdem er seinen Einsatz verlor, behauptet er, das Glückspielangebot des Unternehmens B sei in Österreich illegal, woraufhin das Unternehmen B ihm seinen Einsatz zurückerstattet. Der Spieler meldet sich danach auf einer anderen Online-Glücksspiel-Website an, die dem Unternehmen C gehört. Auch hier verliert er seinen Einsatz und verlangt die Rückerstattung seines Geldes, wobei er sich erneut auf die Illegalität des Angebots beruft. Da das Unternehmen C seiner Forderung nicht nachkommt, klagt der Spieler es vor Gericht ein.

Das Unternehmen B teilt dem Unternehmen C, welches zur selben Unternehmensgruppe gehört, die Informationen über das Verhalten des Spielers mit. Der Anwalt des Unternehmens C nutzt dieses Wissen und erwirkt, dass die Forderung des Spielers wegen Rechtsmissbrauchs abgewiesen wird. Der Spieler wendet sich an die österreichische Datenschutzbehörde und führt aus, dass das Unternehmen B seine personenbezogenen Daten weder dem Unternehmen C noch dessen Anwalt hätte übermitteln dürfen. Die österreichische Datenschutzbehörde muss nun entscheiden, ob die von Unternehmen C beauftragte Anwaltskanzlei die personenbezogenen Daten des Spielers im Rahmen des Zivilverfahrens verwenden durfte.

Zur Stellung des Anwalts im Datenschutz führt die Behörde zutreffend aus:

> *«Zunächst ist festzuhalten, dass Rechtsanwälte, Rechtsanwalts-Gesellschaften eingeschlossen, regelmäßig als für die Verarbeitung Verantwortliche tätig werden, wenn sie Daten für den Zweck der Vertretung ihrer Mandanten verarbeiten. Sie handeln dabei zwar unter Vollmacht und sind damit nach außen berechtigt, für ihre Mandanten rechtlich bindende Erklärungen abzugeben, die Entscheidung, welche Daten dritter Personen für die Erfüllung des Mandats zu verarbeiten sind, wird dabei aber, vorbehaltlich eines Beweises für das Gegenteil, vom Rechtsanwalt ohne Weisung des Mandanten getroffen. Jedes andere Verständnis der in Frage kommenden Rollen des Verantwortlichen […] oder Auftragsverarbeiters […] wäre mit der Selbständigkeit eines Rechtsanwalts in Fragen der Berufsausübung unvereinbar […].»*

Die Behörde hält in Bezug auf die hier für uns relevante Frage, der Rechtsgrundlage für die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen fest, dass die diesbezügliche Bestimmung auch unabhängig vom Vorliegen besonders schützenswerter Personendaten als Erlaubnistatbestand in Frage komme und insoweit dann keine Einwilligung erforderlich sei. Der Tatbestand umfasse auch den «Zugang zu Beweismitteln und das Recht auf ein Vorbringen von Tatsachen» und begründet soweit ein berechtigtes Interesse. Der Beschwerdeführer war nicht in der Lage, nachzuweisen, dass sein Interesse

[41] Art. 30 Abs. 1 DSG; Christophe Hensler, Enquête contre Digitec Galaxus, les recommandations du Préposé sont justifiables, mais sont-elles justes?, 13. Mai 2024, Internet: https://www.swissprivacy.law/299 (Abruf 9.10.25), Ziffer III/4.

[42] Art. 30 Abs. 2 lit. c DSG.

[43] S.a. European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021, N 27.

[44] David Rosenthal, Das neue Datenschutzgesetz, Jusletter 16. November 2020, 24. Der Auftragsbearbeiter gehört zum Kontrollbereich des Verantwortlichen (OFK 2023 DSG-Steiner/Laux, Art. 30 N 28).

[45] Art. 31 Abs. 1 DSG.

[46] Art. 31 Abs. 2 lit. a DSG; s.a. BSK DSG-Rampini/Harasgama, Art. 31 N 31, in: Gabor-Paul Blechta/David Vasella (Hrsg.), Datenschutzgesetz, Basler Kommentar, 4. A., Basel 2024 (zit. BSK DSG-Verfasser); die Notwendigkeit, Beweise für einen Prozess zu sammeln, ist ferner ebenfalls anerkannt und bspw. auch von Art. 328b OR gedeckt (Pärli, BGer 4A_518/2020: Rechtswidrige Beschaffung von Arbeitnehmerpersonendaten, Jusletter 14. Februar 2022, 9).

[47] Entscheid DSB-D124.3420 der österreichischen Datenschutzbehörde vom 22. Februar 2022. S.a. David Dias Matos, Intérêt légitime de l'avocat au traitement de données dans une procédure judiciaire, vom 9. Oktober 2022, Internet: https://swissprivacy.law/177 (Abruf 9.10.2025).

an der Privatsphäre überwiegt. Die Bekanntgabe von B and C und deren Anwalt erfolgte deshalb rechtmässig.

C. Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft und Bekanntgabe an den Rechtsanwalt

Um zur einleitenden Frage zurückzukommen, ob ein Versicherer einem externen Rechtsanwalt ohne Zustimmung der betroffenen Person (Versicherte, Geschädigte etc.) Gesundheitsdaten übermitteln darf, werfen wir einen Blick in die Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft.[48] Der Gesamtverband der deutschen Versicherer hält zu diesen Verhaltensregeln als Vorbemerkung folgendes fest:

> «Datenschutzaufsichtsbehörden und der Verbraucherzentrale Bundesverband (vzbv) waren in die Ausarbeitung der Selbstverpflichtung beratend eingebunden. Die unabhängigen Datenschutzbehörden des Bundes und der Länder haben bestätigt, dass Unternehmen, die die Verhaltensregeln anwenden, sicherstellen, dass die Vorgaben der Datenschutz-Grundverordnung für die Versicherungswirtschaft branchenspezifisch konkretisiert werden.»[49]

Art. 6 Abs. 2 der Verhaltensregeln behandelt die Prüfung von Ansprüchen Versicherter und Geschädigter:

> «Die Verarbeitung besonderer Kategorien personenbezogener Daten auf gesetzlicher Grundlage ist zulässig, insbesondere wenn es zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Das gilt beispielsweise für die Prüfung und Abwicklung der Ansprüche von Versicherten sowie von Geschädigten in der Haftpflichtversicherung.»

Art. 6 Abs. 3 der Verhaltensregeln beschlägt den Regress:

> «Darüber hinaus kann die Verarbeitung von Gesundheitsdaten betroffener Personen ohne deren Einwilligung erfolgen zur Geltendmachung, Prüfung und Abwicklung von gesetzlich geregelten Regressforderungen einerseits des Unternehmens oder andererseits eines Dritten, der gegenüber den betroffenen Personen eine Leistung erbracht hat, wie beispielsweise zur Prüfung und Abwicklung der Regressforderungen eines Sozialversicherungsträgers, Arbeitgebers oder privaten Krankenversicherers.»

Die Regeln von Art. 6 sollen im Übrigen auch für die Übermittlung von Gesundheitsdaten an Rückversicherer gelten.[50] Gerade wenn es um Personendaten des Versicherungsnehmers bzw. der Versicherten geht, ist unseres Erachtens eine Bekanntgabe auch von Gesundheitsdaten an Mitversicherer, Rückversicherer und im Rahmen eines Regresses durch die Abwicklung des Versicherungsvertrags gerechtfertigt, da sowohl der Regress als auch die Rückversicherung letztlich zu einem Versicherungsvertrag gehören. Art. 22 der Verhaltensregeln stellt sodann für die Übermittlung an externe Dienstleister, die keine Auftragsbearbeiter sind, weitere Voraussetzungen auf, wobei Rechtsanwälte, Steuerberater und Wirtschaftsprüfung im Rahmen Ihrer Aufgabenerfüllung davon ausgenommen sind.[51] Ferner wird festgehalten, was schon die DSGVO letztlich sagt, dass besondere Arten personenbezogener Daten von externen Dienstleistern nur verarbeitet werden dürfen, wenn die betroffene Person eingewilligt hat oder eine gesetzliche Grundlage vorliegt,[52] womit wir wieder bei der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen nach Art. 9 Abs. 2 lit. f DSGVO sind.

Gestützt auf die Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft sind somit Datenbekanntgaben an Rechtsanwälte erlaubt, wenn der Anwalt für die Versicherung die Prüfung und Abwicklung der Ansprüche von Versicherten sowie von Geschädigten in der Haftpflichtversicherung übernimmt oder er für den Versicherer Regeresse behandelt. Nach der DSGVO dürfte es demgegenüber nicht ohne Einwilligung zulässig sein, wenn dem Rechtsanwalt Gesundheitsdaten übermittelt werden, um die Vertragsgestaltung zu übernehmen oder Gesundheitsfragebögen zu verfassen. Wenngleich solche Dokumente dann Grundlage für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen sein können, ist doch ein gerichtliches oder aussergerichtliches Verfahren im Zeitpunkt der Vertragsgestaltung noch in weiter Ferne. Sobald aber ein Versicherter oder Geschädigter einen Anspruch stellt, greift Art. 9 Abs. 2 lit. f DSGVO. Natürlich sind dem Anwalt nur jene Personendaten zu übermitteln, die für die Prüfung und Abwicklung erforderlich sind, wobei man hier nicht allzu streng ist. Auch wird man einem Versicherer kaum vorwerfen können, dass der Beizug eines Anwalts nicht erforderlich sei, weil der Versicherer selbst auch Schadenbearbeiter mit juristischer Ausbildung habe. Es liegt hier nicht an der Datenschutzbehörde oder dem Gericht und schon gar nicht an der betroffenen Person (i.d.R. die Gegenseite) sich anzumassen, wann der Beizug eines Spezialisten notwendig ist und wann nicht. Im Hin-

[48] Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft, Stand 29.6.2018.

[49] Internet: https://www.gdv.de/gdv/service/datenschutzkodex (Abruf 9.10.2025).

[50] Art. 17 Abs. 4 der Verhaltensregeln (FN 48).

[51] Art. 22 Abs. 9 der Verhaltensregeln (FN 48).

[52] Art. 22 Abs. 10 der Verhaltensregeln (FN 48).

blick auf ein gerichtliches Verfahren, für welches dann ohnehin ein Anwalt beigezogen wird, kann es Sinn machen, diesen schon frühzeitig einzubeziehen. Auch kann sein Spezialwissen erforderlich oder auch für eine Zweitmeinung im Rahmen der Prüfung dienlich sein. Die Interessen der betroffenen Personen müssen dabei denn auch nicht beeinträchtigt werden, kann es doch bspw. auch im Interesse des Geschädigten liegen, dass der externe Anwalt den Fall evtl. zügiger, kompetenter oder neutraler behandelt, wenngleich es wohl auch Anwälte gibt, die es lieber auf ein gerichtliches Verfahren ankommen lassen. Mit Datenschutz hat dies indes nichts zu tun. Wann ein Versicherer den Rechtsanwalt für die Prüfung von Ansprüchen beizieht, ist einzig und allein der Entscheid des Versicherers und eine diesbezügliche Notwendigkeit ist unseres Erachten nach Art. 9 Abs. 2 lit. f DSGVO nicht zu prüfen, solange man im vorstehend definierten Zweck bleibt.

D. Bekanntgabe besonders schützenswerter Personendaten an den Rechtsanwalt unter Schweizer Recht

Nachdem Art. 9 DSGVO einschränkender formuliert ist als Art. 30 f. DSG, kann festgehalten werden, dass die in der EU erlaubten Bekanntgaben auch in der Schweiz erlaubt sind. Da das DSG keinen bestimmten Rechtfertigungsgrund verlangt und die Interessenabwägung im Rahmen der Generalklausel erfolgt, sind sogar weitergehende Datenbekanntgaben ohne Einwilligung möglich, sofern die Interessen des Versicherers jene der betroffenen Person überwiegen. Es kann so auch auf die Art von Gesundheitsdaten darauf ankommen, dürfte doch bspw. das Interesse der betroffenen Person an der Geheimhaltung ihrer Zahnarztdaten in der Regel geringer sein als jenes in Bezug auf das Patientendossier ihres Psychiaters. Für die Interessenabwägung ist auch relevant, wofür die Gesundheitsdaten verwendet werden (bspw. bei Allergien).[53]

In Bezug auf die Bekanntgabe an einen Rechtsanwalt kann ferner mit dem Normzweck der Bekanntgabe besonders schützenswerter Personendaten argumentiert werden. Es soll «eine Weitergabe besonders schützenswerter Daten an Dritte durch höhere Hürden erschwert» werden «und so kein unkontrolliertes Herausbrechen der Daten aus dem eigenen Kontrollbereich des Verantwortlichen möglich» sein.[54] Wenngleich der Rechtsanwalt ein Dritter und eigenständiger Verantwortlicher ist, liegt aufgrund des Anwaltsgeheimnisses[55] kein «unkontrolliertes Herausbrechen» und somit u.E. auch keine Persönlichkeitsverletzung vor.

Der EDÖB hat – allerdings in einem nicht mehr online verfügbaren Merkblatt aus dem Jahre 2009 – befunden, dass ein Haftpflichtversicherer grundsätzlich Gutachten über eine geschädigte Person durch einen externen Gutachter erstellen lassen könne und er dafür keine Zustimmung der betroffenen Person bedürfe.[56] Diese Auffassung ist im Lichte des Vorstehenden korrekt. Der EDÖB scheint – ohne dies explizit zu nennen – indes im Merkblatt irrigerweise davon auszugehen, dass dieser externe Gutachter – Arzt, Ingenieur, Biomechaniker oder Betriebswirtschafter – Auftragsbearbeiter sei.[57] Er nimmt in Bezug auf die Bekanntgabe aber trotzdem eine (korrekte) Interessenabwägung vor: «Im Falle des Haftpflichtversicherers muss das Interesse der Versichertengemeinschaft, die Forderung einer geschädigten Person einer umfassenden Prüfung zu unterziehen, um die Berechtigung und den Umfang der geschuldeten Leistung festzustellen, als ein ausreichendes privates Interesse betrachtet werden, welches das Bearbeiten der Personendaten der geschädigten Person rechtfertigt.»[58]

Im vorzitierten Merkblatt führt der EDÖB ferner aus, dass der Haftpflichtversicherer die betroffene Person darüber informieren müsse, dass ihre Personendaten für das Erstellen eines Gutachtens auch an einen externen Gutachter übergeben werden können. Die Information erfolge dabei in der Regel bei der Anforderung der Personendaten durch den Haftpflichtversicherer, spätestens aber zum Zeitpunkt der Übergabe der Personendaten an den externen Gutachter.[59] Sofern damit eine allgemeine Information – bspw. Hinweis auf die Datenschutzerklärung auf der Website, welche die Weitergabe von Gesundheitsdaten an externe Gutachter zwecks Begutachtung nennt – gemeint ist, scheint dies zutreffend. Der die Daten empfangende Arzt oder Anwalt demgegenüber unterliegt keiner Informationspflicht.[60] Im Hinblick an die Datenbekanntgabe an den eigenen Rechtsanwalt entfällt unseres Erachtens die Informationspflicht des Haftpflichtversicherers gänzlich, da es dem Schutzzweck des Anwaltsgeheimnisses widerspricht, die Gegenpartei informieren zu müssen. Wenn der Anwalt nicht informieren darf,[61] kann nicht von dessen Mandanten verlangt werden, dass er infor-

53 OFK 2023 DSG-Steiner/Laux, Art. 30 N 34.
54 OFK 2023 DSG-Steiner/Laux, Art. 30 N 26.
55 Art. 13 BGFA; Art. 321 StGB.
56 EDÖB, Einholen von Gutachten durch Haftpflichtversicherer vom 15.12.2009; ehemals erhältlich unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/merkblaetter/einholen-von-gutachten-durch-haftpflichtversicherer.html.
57 Wortwörtlich schreibt der EDÖB: «Bearbeitet der Gutachter die Personendaten nur für die Zwecke des Haftpflichtversicherers, kommt es zu einer gesetzlichen Privilegierung der beiden Akteure. Für den Gutachter gelten die gleichen Rechtfertigungsgründe wie für den Haftpflichtversicherer.»
58 EDÖB, Einholen von Gutachten durch Haftpflichtversicherer (FN 56).
59 EDÖB, Einholen von Gutachten durch Haftpflichtversicherer (FN 56).
60 Art. 20 Abs. 1 lit. c DSG.
61 OFK 2023 DSG-Bieri/Powell, Art. 20 N 13.

miert. Ein allgemeiner Hinweis in der Datenschutzerklärung auf der Website des Haftpflichtversicherers, wonach Gesundheitsdaten an Rechtsanwälte zur Prüfung von Ansprüchen weitergeleitet werden können, schadet aber freilich nicht.

E. Wenn der Versicherer als Bundesorgan gilt

Einem grundsätzlich anderen Prinzip unterliegt die Krankenversicherung nach KVG, die obligatorische Unfallversicherung sowie die obligatorische berufliche Vorsorge. Hier gelten die Unfallversicherer sowie Kranken- bzw. Pensionskassen als Bundesorgane und als solche dürfen sie Gesundheitsdaten grundsätzlich nur bearbeiten, wenn hierfür eine formell-gesetzliche Grundlage besteht oder ausnahmeweise die Einwilligung eingeholt worden ist.[62]

F. Der Fall «Groupe Mutuel» – Austausch innerhalb der Gruppe

Die vorbeschriebene Rechtslage schränkt entsprechend auch den Informationsaustausch innerhalb der Versicherungsgruppe ein, wenn die Tätigkeit einer Gruppengesellschaft in Erfüllung einer Bundesaufgabe erfolgt. Das Bundesgericht hat entsprechend folgendes festgehalten:[63]

«Ohne Zustimmung der betroffenen versicherten Person ist ein Informationsaustausch zwischen einer Krankenkasse (Krankentaggeldversicherung nach KVG) und einer privaten Zusatzversicherung – auch wenn beide der gleichen Versicherungsgruppe angehören und über eine gemeinsame Organisation verfügen – nicht erlaubt.»

Im fraglichen Entscheid war dies indes für den Versicherer nicht nachteilig. Die Versicherte versuchte im Zusammenhang mit einer im Gesundheitsfragebogen nicht angegebenen Vorerkrankung das diesbezügliche Wissen der einen Gruppengesellschaft, der anderen anzurechnen, so dass diese keinen rückwirkenden Gesundheitsvorbehalt mehr hätte anbringen dürfen. Dem war vor Bundesgericht aber kein Erfolg beschieden, vielmehr hielt das oberste Gericht fest:

> «Die Krankenversicherung konnte und durfte daher keine Kenntnis haben von der Verletzung der Anzeigepflicht bei Abschluss einer freiwilligen Krankentaggeldversicherung nach KVG, selbst wenn die private Versicherung die nicht angezeigten Tatsachen gekannt hatte.» [64]

G. Der Fall «Helsana» – Anforderungen an die Einwilligung

Im sog. Helsana-Entscheid[65] hatte das Bundesverwaltungsgericht ebenfalls einen Fall einer Versicherungsgruppe mit Zusatz- und Krankenversicherer zu beurteilen, in welchem tatsächlich eine Datenbekanntgabe erfolgte und hierfür auch die Einwilligung eingeholt worden war. Indes waren nach Ansicht des Gerichts die Voraussetzung an eine gültige Einwilligung nicht erfüllt. In der Tat bedarf es für die Gültigkeit einer Einwilligung mehr als bloss der Zustimmung. Eine Einwilligung ist nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird.[66] Stehen besonders schützenswerte Personendaten zur Bearbeitung, muss die Einwilligung ausdrücklich erfolgen.[67] Das Krankenversicherungsgesetz verlangt überdies, dass die Einwilligung schriftlich erteilt wird, sofern dies nicht unmöglich ist und diesfalls die Einwilligung nach den Umständen als im Interesse der versicherten Person vorausgesetzt werden darf.[68] Das Bundesverwaltungsgericht interpretiert hier die Schriftlichkeit im Sinne von Art. 14 OR,[69] d.h. eigenhändig oder mit zugelassener qualifizierter elektronischer Signatur. Bei näherer Betrachtung hält diese Auslegung indes nicht stand, ein Nachweis in Textform (ohne Unterschriftserfordernis) genügt unseres Erachtens.[70]

Laut Bundesverwaltungsgericht erfolgte die Einwilligung – entgegen der Ansicht des EDÖB – freiwillig, obwohl ohne Einwilligung die Teilnahme am Bonusprogramm der Zusatzversicherung unmöglich war und somit keine geldwerten Vorteile erlangt werden konnten.[71]

Hingegen sei die Einwilligung nicht nach angemessener Information erteilt worden: «Die Klausel enthält keine einschränkenden Verweise auf den Zweck der Datenbearbeitung oder andere Bestimmungen, sondern ist breit und ohne Einschränkungen formuliert. Die Beklagte holt damit eine über den notwendigen Zweck der Datenbearbeitung hinausgehende Einwilligung ein. Erschwerend kommt hinzu, dass sich die Einwilligung, auf mehrere Bestimmungen verteilt, in den umfangreichen Nutzungs- und Datenschutzbestimmungen befindet, welche die Teilnehmerinnen und Teilnehmer

[62] Art. 34 DSG; BGE 149 V 29 E. 5.3.2; Schweizer Pensionskassenverband, ASIP, Fachmitteilung Nr. 130 vom 11. April 2022, Ziffer 4; Simone Emmel, Art. 85a N 2, in: Marc Hürzeler/Hans-Ulrich Stauffer (Hrsg.), Berufliche Vorsorge, Basler Kommentar, Basel 2021.

[63] BGE 149 V 29 Regeste.

[64] BGE 149 V 29 Regeste.

[65] Urteil des Bundesverwaltungsgerichts, A-3548/2018 vom 19. März 2019.

[66] Art. 6 Abs. 6 DSG.

[67] Art. 6 Abs. 7 lit. a DSG.

[68] Art. 84a Abs. 5 lit. b KVG.

[69] Urteil des Bundesverwaltungsgerichts, A-3548/2018 vom 19. März 2019, E. 4.8.4.

[70] Eingehend dazu: Bühlmann/Schüepp, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, Jusletter 15. März 2021, 40 ff.

[71] Urteil des Bundesverwaltungsgerichts, A-3548/2018 vom 19. März 2019, E. 4.7.

durch Anklicken einer Schaltfläche in der Helsana+-App genehmigen. Dieses Vorgehen erschwert es den Teilnehmerinnen und Teilnehmern, zu erkennen, in welche Datenbearbeitungen sie einwilligen. Aus diesen Gründen entspricht die Einwilligung nicht den Voraussetzungen einer angemessenen Information für die Gültigkeit einer Einwilligung.»[72] Das Bundesverwaltungsgericht beurteilte dementsprechend einen Teil der Datenbearbeitung im Rahmen von Helsana+ als rechtswidrig. Das Vorstehende erinnert an viele Datenschutzerklärungen, die sehr umfassend sind und doch vage bleiben, bei denen man am Schluss nicht weiss, welche Daten, nun zu welchem Zweck bearbeitet werden und die einem durch den schieren Umfang letztlich vom Lesen abhalten. Sofern der Entscheid des Bundesverwaltungsgerichts dies kritisiert und verlangt, dass bei der Information in Bezug auf die Einwilligung eben konkret und prägnant im Hinblick auf die Bearbeitung im Zusammenhang mit der Einwilligung informiert wird, verdient er Zustimmung.[73]

IV. Informationspflicht

A. Gesetzliche Regelung im DSG

Der Verantwortliche muss die betroffene Person angemessen über die Beschaffung von Personendaten informieren. Konkret muss er jene Informationen mitteilen, die erforderlich sind, damit sie ihre Rechte gemäss DSG geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Mindestens sind dies die Identität und die Kontaktdaten des Verantwortlichen, der Bearbeitungszweck, die Empfänger bzw. Kategorien von Empfängern, denen Personendaten bekanntgegeben werden, und ggf. der Staat, in welchem die Personendaten bekanntgegeben werden, sowie ggf. die Garantien, falls der Staat keinen angemessenen Schutz gewährleistet. Werden die Daten nicht bei der betroffenen Person beschafft, so sind ihr zudem die Kategorien der bearbeiteten Personendaten mitzuteilen.[74] In Bezug auf die Bekanntgabe ins Ausland ist noch anzumerken, dass diese jegliche Übermittlung umfasst, auch solche an Auftragsbearbeiter oder Mitarbeiter.[75] Die Informationspflicht entfällt u.a., wenn die betroffene Person bereits über die entsprechenden Informationen verfügt, wenn die Bearbeitung gesetzlich vorgesehen ist und wenn es sich beim Verantwortlichen um eine private Person, die gesetzlich zur Geheimhaltung verpflichtet ist, handelt.[76] Eine detailliertere Informationspflicht mit weniger Ausnahmen sieht auch die DSGVO vor.[77]

B. Gesetzliche Regelung im VVG

Das Versicherungsvertragsgesetz verlangt ebenfalls eine Information über die Datenbearbeitung, «einschliesslich Zweck und Art der Datenbank sowie Empfänger und Aufbewahrung der Daten».[78] Rein akademisch ist wohl die Frage, ob diese Information auch erbracht werden muss, wenn eine solche nach DSG nicht notwendig ist, bspw. weil der Versicherungsnehmer diese schon hat. Der Versicherer wird das Informationsblatt automatisch immer zur Verfügung stellen. Interessant sind hingegen jene Punkte, die nach DSG nicht vorgeschrieben sind, nämlich die «Art der Datenbank» und die «Aufbewahrung der Daten». Ersteres, in der früheren Version noch «Art der Datensammlung» genannt, war und ist eine wenig sinnvolle Information. Microsoft definiert und erläutert den Begriff Datenbank wie folgt: «Gemäß der grundlegendsten Definition ist eine Datenbank eine Sammlung miteinander verknüpfter Informationen. Wenn Sie eine Einkaufsliste auf ein Stück Papier schreiben, erstellen Sie im Grunde eine kleine analoge Datenbank. Was ist eine Datenbank jedoch im Informatikbereich? In diesem Kontext wird eine «Datenbank» als Sammlung von Informationen definiert, die als Daten auf einem Computersystem gespeichert werden, […]. Datenbanken werden zum Speichern und Organisieren von Daten verwendet, um die Verwaltung und den Zugriff zu vereinfachen. Wenn eine Sammlung von Daten wächst und komplexer wird, wird es immer schwieriger, diese Daten organisiert, zugänglich und sicher zu halten. Daher verwenden Sie Datenbank-Managementsysteme, die Datenbankverwaltungstools umfassen, um dies zu vereinfachen.»[79] Über die Art einer solchen Datenbank, von denen ein Versicherer wohl mehr als eine hat, soll nun informiert werden. Soll erklärt werden, auf welchem Computersystem diese gespeichert ist? Wie die Software heisst? Ist die Grösse der Datenbank oder der Hardware anzugeben? Das macht alles wenig Sinn; vielmehr hätte der Begriff der «Datensammlung», welcher aus dem früheren DSG stammt, ersatzlos gelöscht werden sollen. Es sind unseres Erachtens jene Informationen zu erteilen, die das DSG vorschreibt. Hinzu kommt einzig die «Aufbewahrung der Daten», womit namentlich die Dauer der Aufbewahrung gemeint ist.[80] Letztlich sind hier die Angaben gemeint, die man auch im

[72] Urteil des Bundesverwaltungsgerichts, A-3548/2018 vom 19. März 2019, E. 4.8.4.

[73] Siehe dazu auch Ziff. 4.4. Ansonsten kann die etwas dürftige Entscheidungsbegründung freilich durchaus kritisiert werden (s. dazu Bühlmann/Schüepp [FN 70] 17 ff.).

[74] Art. 19 DSG.

[75] BSK DSG-Rampini/Harasgama (FN 46), Art. 16 N 26.

[76] Art. 20 Abs. 1 lit. a–c DSG.

[77] Art. 12 ff. DSGVO.

[78] Art. 3 Abs. 1 lit. g VVG.

[79] Internet: https://azure.microsoft.com/de-de/resources/cloud-computing-dictionary/what-are-databases (Abruf 9.10.2025).

[80] BSK VVG-Kuhn/Körner, Art. 3 N 33, in: Pascal Grolimund/Leander Loacker/Anton K. Schnyder (Hrsg.), Versicherungsvertragsgesetz, Basler Kommentar, 2. A., Basel 2023, welche auch noch Angaben über die Art der Aufbewahrung verlangen, was aber nicht erforderlich sein dürfte.

Rahmen eines Auskunftsbegehrens DSG erhalten würde, nämlich «die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer».

Die Informationspflicht wird in aller Regel dadurch erfüllt werden, in dem auf der Website gut auffindbar eine oder mehrere Datenschutzerklärungen (bspw. Datenschutzerklärung für die Website, Datenschutzerklärung für Versicherungsverträge, etc.) zur Verfügung gestellt werden. Vasella hält diesbezüglich zurecht fest: «Das Internet ist ausreichend verbreitet».[81] Gegenüber dem Versicherungsnehmer sind im Merkblatt nach Art. 3 VVG, welches sich auch im Internet befinden kann, zusätzlich Kurzinformationen zur Datenbearbeitung notwendig; für weiterführende oder detailliertere Informationen kann das Merkblatt auf die Datenschutzerklärung auf der Website verweisen.

C. Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies

In Bezug auf Cookies gilt es die Rechtslage für das Setzen von Cookies, d.h. das Zugreifen auf das Endgerät des Website-Besuchers, darzustellen, bevor wir zur eigentlichen Bearbeitung von Personendaten kommen. Für das Setzen von Cookies verlangt das Schweizer Fernmeldegesetz eine Information über die Bearbeitung mittels Cookies, deren Zweck und das Ablehnungsrecht.[82] Diese Information kann nach herrschender Lehre auch bloss in der Datenschutzerklärung erfolgen, so dass kein Cookie-Banner notwendig ist.[83] Nichtzutreffend ist deshalb die Ansicht des EDÖB, wonach der Verantwortliche das Widerspruchsrecht gegen den Einsatz nicht notwendiger Cookies auf der Webseite an prominenter Stelle anzeigen müsse, sodass die Möglichkeit eines Opt-out für Benutzende, sowohl beim ersten, wie auch bei den nachfolgenden Besuchen leicht erkannt und mit wenigen Klicks angewählt und ausgeübt werden könne.[84] Jeder Benutzer kann selbst durch Browser-Einstellung das Setzen nicht notwendiger Cookies unterbinden.[85]

In der EU schreibt die ePrivacy-Richtlinie eine Information vor, wobei für nicht unbedingt erforderliche Cookies eine Einwilligung einzuholen ist.[86] Die Einwilligung in das blosse Setzen von Cookies stellt dabei nicht per se auch eine Einwilligung in die Bearbeitung von Personendaten dar, was beim Verfassen der Einwilligungserklärung zu berücksichtigen ist.[87]

In Bezug auf die Bearbeitung von Personendaten – sofern diese durch Cookies oder ähnliche Technologien überhaupt ermöglicht wird[88] – gilt in der Schweiz, dass diese grundsätzlich erlaubt ist. In der Schweiz ist nur dann eine Einwilligung notwendig, wenn aus der Bearbeitung ansonsten eine Persönlichkeitsverletzung resultiert. Dies wäre bspw. der Fall, wenn auf medizinischen Websites oder Applikationen ausnahmsweise besonders schützenswerte Personendaten bekanntgeben würden, oder wenn Personendaten in unsichere Drittstaaten gehen, ohne dass ein ausreichender Schutz vereinbart worden ist. Dies hat bisher dazu geführt, dass in den allermeisten Fällen keine Einwilligung und auch kein Cookie-Banner notwendig war. Diese, unseres Erachtens noch immer zutreffende Auffassung, ist durch zwei Punkte ins Wanken geraten:

Nach dem Grundsatz von *Privacy by Default*, wonach der Verantwortliche verpflichtet ist, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit nicht die betroffene Person zu etwas anderem einwilligt,[89] sollte nach mehreren Verlautbarungen für nicht zwingend notwendige Cookies die Zustimmung eingeholt werden müssen. Rosenthal hält diesbezüglich aber zurecht fest, dass dieser Grundsatz nur greift, wenn dem Benutzer eine Wahlmöglichkeit belassen wird.[90]

Der zweite Punkt scheint prima Vista etwas weithergeholt. Fühlen Sie sich durch Cookies in Ihrer Persönlichkeit verletzt? Wohlverstanden, wir meinen hier die Cookies, nicht die nervigen Cookie-Banner. Wahrscheinlich werden die meisten mit einem Nein ant-

[81] Vasella, Zu den Anforderungen an die Erfüllung der Informationspflicht nach dem revDSG, 28. Oktober 2022, Internet: https://datenrecht.ch/zu-den-anforderungen-an-die-erfuellung-der-informationspflicht-nach-dem-revdsg (Abruf 9.10.2025).

[82] Art. 45c FMG.

[83] Hensler (FN 41), Ziffer III/1. Inwieweit diese Information gehen muss ist freilich umstritten, s. bspw. Schlussbericht vom 15. April 2024 des EDÖB in Sachen Digitec Galaxus AG, Empfehlung 1, vs. Vasella, EDÖB i.S. Digitec Galaxus: Sehr strenge Transparenzanforderungen, aber Gastkauf nicht zwingend, 17. April 2024; Internet: https://datenrecht.ch/edoeb-i-s-digitec-galaxus-sehr-strenge-transparenzanforderungen-aber-gastkauf-nicht-zwingend/ (Abruf 9.10.2025).

[84] Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien vom 22. Januar 2025, Ziff. 3.9. Einen Cookie-Banner verlangt aber auch der EDÖB nicht zwingend, s.a. Schlussbericht i.S. Digitec Galaxus AG (FN 83), N 44.

[85] Vasella, EDÖB: Leitlinien zu Cookies und ähnlichen Technologien, 29. Januar 2025; Internet: https://datenrecht.ch/edoeb-leitlinien-zu-cookies-und-aehnlichen-technologien/ (Abruf 9.10.2025), spricht diesbezüglich vom «technischen Widerspruchsrecht».

[86] Art. 5 Abs. 3 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

[87] Datenschutz-Guru, Datenschutz-Tipps 22/2020: Ein kleiner Tipp für Cookie-Banner.

[88] Zum teilweise falsch verstandenen Begriff der Personendaten, s. Vasella, EDÖB: Leitlinien zu Cookies (FN 85).

[89] Art. 7 Abs. 3 DSG.

[90] Rosenthal (FN 44), 22 ; Steiger, Neues Datenschutzgesetz verlangt keine Cookie-Banner in der Schweiz, 6. Februar 2023, Internet: https://steigerlegal.ch/2023/02/06/cookie-banner-neues-datenschutzgesetz-schweiz (Abruf 9.10.2025); Vasella, EDÖB: Leitlinien zu Cookies (FN 85).

worten, trotzdem erblickt der EDÖB im Einsatz von Cookies, es sei denn diese seien technisch zwingend notwendig oder dienten der informationstechnischen Sicherheit,[91] eine Persönlichkeitsverletzung. Juristisch begründet der EÖDB dies wie folgt: «Nebst den notwendigen Cookies werden oft solche verwendet, die für den sicheren technischen Betrieb einer Applikation nicht erforderlich sind, aber z.B. dazu dienen, das Erlebnis der Nutzenden beim Surfen auf der Webseite zu optimieren (sog. funktionale oder Komfort Cookies). Der Einsatz solcher Cookies kollidiert, da er über das notwendige Mass hinausgeht, mit dem datenschutzrechtlichen Grundsatz der Verhältnismässigkeit nach Art. 6 Abs. 2 DSG. Werden Personendaten von einem privaten Verantwortlichen entgegen den allgemeinen Bearbeitungsgrundsätzen nach Art. 6 und 8 DSG bearbeitet, verletzt diese Bearbeitung gemäss Art. 30 Abs. 2 lit. a DSG die Persönlichkeit der davon betroffenen Personen.»[92] Et voilà, schon sind Sie in der Persönlichkeit verletzt. Ein raffinierter Trick gegen jegliches Bauchgefühl, der nur funktioniert, wenn man – wie der EDÖB – bei der Verhältnismässigkeit übertrieben streng ist und schlimmer noch, sich anmasst, zu entscheiden, zu welchen Zwecken (technische Sicherheit ja, Komfort nein) Datenbearbeitungen stattfinden dürfen. Der Verantwortliche bestimmt die Zwecke, nicht der Gesetzgeber und schon gar nicht irgendeine Behörde. Vasella hält zurecht fest, dass es dem Verantwortlichen freistehe, die Zwecke seiner Website selbst zu bestimmen und wenn diese Zwecke den weiteren Einsatz von Cookies erheischen, kann dies in Bezug auf diese Zwecke zulässig und verhältnismässig sein.[93] Der EDÖB hat auf die berechtigte Kritik reagiert und am 6. Oktober 2025 eine aktualisierte Version (Version 1.1) seines Leitfadens publiziert, in welcher er nun immerhin festhält (Ziffer 3.5.2): «Welche Cookies und ähnliche Technologien zur Gewährleistung der funktionalen Durchführbarkeit der gewünschten Bearbeitung technisch notwendig sind, hängt vom Verwendungszweck ab, welchen der Verantwortliche mit einer konkreten Datenbearbeitung verfolgt, und kann nicht pauschal beantwortet werden. Ob Datenbearbeitungen mittels Cookies oder ähnliche Technologien für einen bestimmten Zweck geeignet, erforderlich und zumutbar sind, ergibt sich aus einer Würdigung der konkreten Umstände des Einzelfalls.»

Wir sind persönlich auch der Ansicht, dass es erstens – im Hinblick auf das FMG – unhöflich ist, fremden Personen einfach Cookies in den Ofen bzw. das Endgerät zu setzen, wenn dies nicht notwendig ist. Zweitens ist eine gestützt darauf erfolgte Bearbeitung von Personendaten (wenn denn überhaupt wirklich Personendaten vorliegen) in vielen Fällen ebenfalls wenig besucherfreundlich, so dass wir regelmässig empfehlen, auf solche Cookies und ähnliche Technologien zu verzichten. In den meisten Fällen wird deren Nutzen u.E. ohnehin überschätzt. Trotzdem denken wir, dass die allerwenigsten Cookies wirklich ernsthaft geeignet sind, unsere Persönlichkeit zu verletzen und es letztlich eben jedem Website-Betreiber überlassen ist, die Zwecke seiner Website zu definieren. Wünschenswert wäre es, die Betreiber würden sich mit den Zwecken und dem Einsatz von Cookies und ähnlichen Technologien auch ernsthaft auseinandersetzen, anstatt mehr oder weniger gedankenlos irgendwelchen Leitlinien zu folgen und einen Cookie-Banner zu setzen.

Im Übrigen könnte eine allfällige Persönlichkeitsverletzung nicht nur durch eine Einwilligung, sondern ggf. auch durch ein überwiegendes privates Interesse gerechtfertigt sein. Auch der EDÖB anerkennt, dass private Verantwortliche im Rahmen einer Interessenabwägung prüfen können, ob die mittels Cookies durchgeführten Datenbearbeitungen durch überwiegende private Interessen gerechtfertigt werden können.[94]

Es bleibt somit dabei, dass ein Cookie-Banner nur notwendig ist, wenn ausnahmsweise eine Einwilligung eingeholt werden muss.

Erfreulich ist die Mitteilung des EDÖB, dass bei der **«Einbindung von Drittdiensten oder bei einer Auftragsdatenbearbeitung»** der «Webseitenbetreiber für detaillierte Informationen auf weiterführende Informationen beim Drittdienst resp. Auftragsdatenbearbeiter verweisen» kann.[95] Dies erleichtert, die eigene Datenschutzerklärung aktuell zu halten, zumal der Website-Betreiber sich letztlich ja ohnehin auf die vom Drittdienstleister erhaltenen Informationen verlassen muss. Wenig hilfreich ist demgegenüber, wenn der EDÖB beim Einsatz von *Social Media Plug-in* eine gemeinsame Verantwortung für den Prozess der Datenbeschaf-

[91] Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies (FN 84), Ziff. 3.5.2.

[92] Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies (FN 84), Ziff. 3.6.

[93] Vasella, EDÖB: Leitlinien zu Cookies (FN 85).

[94] Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies (FN 84), Ziff. 3.6. «Ob die privaten Interessen des Datenbearbeiters eine konkrete Persönlichkeitsverletzung überwiegen und so zu rechtfertigen vermögen, hängt von der Abwägung der Interessen des Verantwortlichen und der betroffenen Person im Einzelfall ab. Betreiber von Webseiten müssen also zunächst prüfen, welche privaten Interessen, die von ihnen jenseits der Grenzen des Verhältnismässigkeitsprinzips eingesetzten Cookies oder ähnlichen Technologien bedienen, welchen Nutzen und welche Nachteile sie für die Betroffenen haben und wie schwer die sich aus den Nachteilen ergebende Verletzung der Persönlichkeit der Betroffenen wiegt. Anschliessend gilt es abzuwägen, ob die Verletzung den Betroffenen zumutbar ist, sodass die privaten Interessen der Webseitenbetreiber überwiegen. In die Abwägung einbezogen werden müssen Elemente wie die Speicherdauer der mit Cookies erhobenen Informationen oder allfällige Datenbekanntgaben an Dritte» (Ziff. 3.7).

[95] Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies (FN 84), Ziff. 3.3.1 in fine.

fung des *Social Media*-Anbieters «mittels der Webseite» annimmt.[96] Falsch ist, wenn der EDÖB eine über diese Datenbeschaffung hinausgehende Verantwortlichkeit des Website-Betreibers für die Datenbearbeitung durch den Social Media-Anbieter behauptet.[97] Hierfür fehlt jegliche Rechtsgrundlage.[98] Es genügt, wenn der Website-Betreiber auch hier über die Datenbearbeitung bzw. Bekanntgabe an den Dritten informiert und ggf. auf die detaillierten Informationen beim *Social Media*-Anbieter verweist.

D. Schlussbericht des EDÖB in Sachen Digitec Galaxus – präzise & verständliche Information

Grundsätzlich ist unbestritten, dass die betroffene Person der Datenschutzerklärung nicht zustimmen muss. Vielmehr ist die Erteilung einer Information grundsätzlich ein einseitiger Akt. Der betroffenen Person steht es frei, die erhaltenen Informationen zur Kenntnis zu nehmen oder diese zu ignorieren. Digitec Galaxus AG holt von Ihren Kunden dennoch folgende Zustimmung ein: «Ja, **ich stimme der in der Datenschutzerklärung umschriebenen Bearbeitung sämtlicher meiner Personendaten zu**. Dies umfasst die Bearbeitung sämtlicher meiner Personendaten, insbesondere zum Zweck der Analyse des Kundenverhaltens und des Direktmarketings durch alle Unternehmen der Migros-Gruppe.»[99] Der EDÖB gibt die diesbezügliche Erläuterung von Digitec Galaxus AG wie folgt wieder: «Gemäss der Digitec Galaxus AG soll dieses Verfahren nicht so verstanden werden, dass die Durchführung gewisser in der Datenschutzerklärung beschriebenen Datenbearbeitungen nur aufgrund dieser Zustimmung erlaubt wären, sondern lediglich als eine kundenfreundliche Massnahme, die dazu dient, den Kunden den Gegenstand der möglichen Datenbearbeitungen durch die Digitec Galaxus AG zu verdeutlichen:»[100] Etwas überraschend bewertet der EDÖB dieses (unnötige) Einholen einer Zustimmung wie folgt: «Dass bei der Registrierung aufgefordert wird, durch das Ankreuzen Kenntnis von der Datenschutzerklärung zu nehmen, kann als Zeichen einer aktiven Information angesehen werden, was […] zu begrüssen ist. Die Information wird folglich durch die Digitec Galaxus AG ausdrücklich bereitgestellt.»[101] Der letzte Satz ergibt weder sprachlich noch inhaltlich Sinn. An der Bereitstellung durch den Verantwortlichen als einseitigen Akt ändert sich nichts, wenn die betroffene Person danach ein Kontrollkästchen ankreuzen muss. Die Zustimmung will Digitec Galaxus AG und auch der EDÖB nicht so verstanden wissen, dass die Datenbearbeitung auf Grundlage der Einwilligung im Sinne des DSG erfolge. Auch wäre eine derart pauschale Einwilligung gar nicht zulässig.[102] Bereits die Tatsache, dass Digitec Galaxus AG sich erklären muss, was die Zustimmung denn genau bedeuten solle und der EDÖB festhalten muss, dass es sich nicht um eine Einwilligung handle, zeigt, dass nicht «in präziser, transparenter, verständlicher und leicht zugänglicher Form»[103] informiert worden ist. Es ist wahrscheinlich, dass hier mehrere Kunden denken, es werde ihre Einwilligung nach DSG eingeholt und sie könnten diese dann widerrufen,[104] woraufhin die Datenbearbeitung stoppen würde. Ein solcher Widerruf der Einwilligung wäre dann als Widerspruch gegen die Datenbearbeitung zu behandeln, woraufhin der Verantwortliche, wenn er die Bearbeitung fortführen möchte, einen Rechtfertigungsgrund geltend machen müsste. Beim Einholen der Einwilligung ist diese typischerweise der Rechtfertigungsgrund, weshalb beim Widerruf die betroffene Person davon ausgehen kann, dass die Bearbeitung dann stoppt. Wird nun aber eine gesetzliche Pflicht oder ein überwiegendes privates Interesse vorgetragen, kommt sich die betroffene Person

96 Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies (FN 84), Ziff. 3.2.2.: «Werden beispielsweise Social Plug-Ins von Plattformen wie Facebook, X oder Instagram oder Videos von Plattformen wie YouTube eingebunden, können Webseitenbetreiber gewisse Funktionalitäten von sozialen Netzwerken auf ihren eigenen Webseiten nutzen. Durch die Einbindung von Drittprodukten wird der Browser des Besuchers der betreffenden Webseite veranlasst, Inhalte des Anbieters anzufordern und hierzu Personendaten des Besuchers an den Drittanbieter zu übermitteln. In dieser Konstellation der eingebetteten Dienste, bearbeiten Dritte die beschafften Personendaten zu eigenen Zwecken und damit in eigenen Interessen. […] Der Dritte ist zunächst für seine Datenbearbeitung verantwortlich, da er aus Eigeninteresse auf die Bearbeitung von personenbezogenen Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Bearbeitung mitwirkt. Der Webseiteninhaber wiederum ermöglicht die Datenbeschaffung des Dritten erst mit der Einbindung des Drittdienstes auf seiner Webseite (Mittel), auch wenn er auf die nachgelagerte Datenbearbeitung keinen oder nur geringen Einfluss hat. Daraus folgt, dass für den Prozess der Datenbeschaffung des Dritten […] mittels der Webseite von einer gemeinsamen oder geteilten Verantwortlichkeit auszugehen ist. Da der Webseitenbetreiber die Kontrolle darüber hat, welche Drittdienste eingebaut werden, kann er nicht davon ausgehen, dass seine Verantwortung dort aufhört, wo die Nutzungsbedingungen der Dritten gelten. Er trägt die Verantwortung, die Internetseite datenschutzkonform zu gestalten. Er muss sich folglich über die Datenbearbeitung der eingebundenen Drittdienste in Kenntnis setzen und sicherstellen, dass die Anforderungen des Gesetzes eingehalten werden. Namentlich hat der Webseitenbetreiber sicher zu stellen, dass gegenüber den betroffenen Webseitenbesuchern sämtliche Informationspflichten erfüllt werden.»

97 Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies (FN 84), Ziff. 3.2.2.

98 Vasella, EDÖB: Leitlinien zu Cookies (FN 85).

99 Schlussbericht i.S. Digitec Galaxus AG (FN 83), N 18.

100 Schlussbericht i.S. Digitec Galaxus AG (FN 83), N 20.

101 Schlussbericht i.S. Digitec Galaxus AG (FN 83), N 103.

102 Art. 6 Abs. 6 DSG; Schlussbericht i.S. Sachen Digitec Galaxus AG (FN 83), N 141.

103 Art. 13 DSV.

104 Zum Widerruf der Einwilligung s. Schlussbericht i.S. Digitec Galaxus AG (FN 83), N 101, und Vasella, Schlussbericht und Empfehlungen i.S. Once Dating, vom 19. Juni 2006, Internet: https://datenrecht.ch/edoeb-schlussbericht-und-empfehlungen-is-once-dating (Abruf 9.10.2025).

überlistet oder getäuscht vor, weil es die Einwilligung bzw. Zustimmung gar nicht braucht. Auch deshalb ist auf die Zustimmung zur Datenschutzerklärung zu verzichten.

Erfreulich ist sodann aber folgende Kritik des EDÖB: «Vorliegend umschreibt die Digitec Galaxus AG zwar die Zwecke, die gesammelten Personendaten und an wen diese bekanntgegeben werden, allerdings ist nicht ersichtlich, **welche Personendaten konkret zu welchen Zwecken bearbeitet und welche Personendaten konkret an welche Unternehmen weitergegeben werden**. Ziff. 7 der Datenschutzerklärung erweckt den Anschein, als würden sämtliche dort aufgelisteten Daten für sämtliche Zwecke verwendet und damit an sämtliche in Ziff. 9 umschriebenen Dritten bekanntgegeben werden. Für betroffene Personen muss jedoch ersichtlich sein, welche Personendaten konkret zu welchen Zwecken bearbeitet werden. Ist dies für die betroffene Person nicht klar, kann sie keine bewussten Entscheidungen über ihr informationelles Selbstbestimmungsrecht treffen. Ausserdem ist es bspw. nicht möglich, die Erforderlichkeit eines Eingriffs zu beurteilen oder die Einhaltung der Grundsätze der Speicherbegrenzung und der Datenrichtigkeit. In diesem Sinne sind die Informationen, die bereitgestellt werden, für den Nutzer oder die Nutzerin nicht eindeutig und klar. Sie erlaubt es den betroffenen Personen nicht, sich einen Überblick über die tatsächlich durchgeführten Datenbearbeitungen zu verschaffen. Verantwortliche haben in ihrer Datenschutzerklärung klar und erkennbar zu umschreiben, welche Personendaten zu welchem Zweck bearbeitet und an wen diese weitergegeben werden. Folglich erachten wir die Informationen in der Datenschutzrichtlinie als ungenügend hinsichtlich des Transparenzgebots nach Art. 4 Abs. 4 DSG.»[105] Die Lehre kritisiert den EDÖB mit dem Argument, dass es für die Wahrung der Betroffenenrechte nicht immer notwendig sei, zu wissen, welches Personendatum nun genau für welchen Zweck bearbeitet werde. Vielmehr seien die Zwecke zentral. Dies erlaube dann auch, später flexibel gewisse Personendaten auch für andere, bereits genannte Zwecke zu verwenden.[106] Der EDÖB habe auch gar keine gesetzliche Grundlage, um eine Zuordnung von Daten und Zwecken zu verlangen.[107] Wie bereits erwähnt, hat die Information «in präziser, transparenter, verständlicher und leicht zugänglicher Form»[108] zu erfolgen. Können keine Verknüpfungen zwischen den Daten und den damit verfolgten Zwecken und Bekanntgaben gemacht werden, ist die Information wenig präzise und auch wenig transparent. Sie verstösst somit gegen die Datenschutzverordnung, in vielen Fällen auch gegen das Datenschutzgesetz. Es sind diejenigen Informationen mitzuteilen, die erforderlich sind, damit die betroffene Person ihre Rechte gemäss DSG geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist.[109] Es ist bspw. sehr wohl relevant, ob unsere Telefonnummer oder unsere E-Mail für Direktmarketing verwendet werden. Auch ist uns wichtig zu wissen, ob unsere Patientenakte oder unsere Kreditkartendaten dem Spezialisten, an den mich mein Hausarzt überweist, übermittelt werden. Es ist diesbezüglich auch zentral, zu wissen, dass die Patientenakte an den Spezialisten geht und dass die Kreditkartendaten an die Bank oder Zahlungsverarbeiter gehen und nicht umgekehrt. Eine Zuordnung ist in vielen, wohl nicht in allen Fällen wichtig und erforderlich.

Auch unter der DSGVO sind konkrete Zuordnungen notwendig, so führt die irische Datenschutzaufsichtsbehörde betr. Facebook's Datenschutzerklärung folgendes aus: «what Article 13 does clearly require is that the purposes and legal bases must be specified in respect of the intended processing. Purposes and legal bases cannot simply be cited in the abstract and detached from the personal data processing they concern.»[110] Und weiter: «In that information, there should be a clear link between the specified category/categories of data, the purpose(s) of the specified operation(s), and the legal basis being relied on to support the specified operation(s).»[111] Vage Ausführungen und unnötige Wiederholungen sind zu vermeiden, damit sich die betroffene Person ein klares Bild machen kann: «When all of the available information has been accessed, it becomes apparent that the texts provided are variations of each other, in that they re-iterate the goals and objectives of Facebook in carrying out data processing (for example, personalisation, communication, analytics, product improvement, etc.) rather than elaborating on this or providing information concerning processing operations. This approach lacks clarity and concision, and makes it difficult for the user to access meaningful information as to the processing operations that will be grounded on Article 6(1)(b) GDPR or on other legal bases. In my view, insufficient detail has been provided in relation to the processing operations carried out both in general and on the basis of Article 6(1)(b) GDPR specifically. Such an approach deprives the user of meaningful information and further risks causing significant confusion as to what legal basis will be relied upon to ground a specific process-

105 Schlussbericht i.S. Digitec Galaxus AG (FN 83), N 107 f.
106 Hensler (FN 41), Ziffer III/2.
107 Vasella (FN 83).
108 Art. 13 DSV.
109 Art. 19 Abs. 2 DSG.
110 Entscheid der irischen *Data Protection Commission* vom 31. Dezember 2022, DPC Inquiry Reference: IN-18-5-5, betreffend Meta Platforms Ireland Limited (ehemals Facebook Ireland Limited) im Hinblick auf Facebook, N 5.29.
111 Entscheid der irischen *Data Protection Commission* (FN 110), N 5.41.

ing operation.»[112] Zusammenfassend: «Put simply, it is impossible to identify what processing operations will be carried out in order to fulfil the objectives that are repeated throughout the documents and the legal basis for such operations. In the absence of such information, the user is left to guess as to what processing is carried out on what data, on foot of the specified lawful bases, in order to fulfil these objectives. For the reasons set out above in relation to the correct interpretation of Article 13(1)(c) GDPR, this is insufficient information.»[113]

Oftmals wünschen Verantwortliche, dass sie in der Datenschutzerklärung gewisse in Zukunft evtl. anstehende Bearbeitungsvorgänge aufführen können, um die Datenschutzerklärung nicht ändern zu müssen und natürlich auch, um die bisher gesammelten Personendaten dann auch für diese zukünftigen Zwecke nutzen zu dürfen, ohne nochmals darüber informieren zu müssen. Der EDÖB weist dieses Anliegen grundsätzlich zurück: «Eine betroffene Person vertraut nach Treu und Glauben darauf, dass die Informationen in der Datenschutzerklärung zutreffen. Wird dem Ansatz von der Digitec Galaxus AG gefolgt, können Verantwortliche eine Datenschutzerklärung verfassen, welche jegliche Datenbearbeitungen auf Vorrat miteinbeziehen. **Eine Datenschutzerklärung mit Datenbearbeitungen «auf Vorrat»** lässt die betroffenen Personen im Unwissen. Ihnen wäre es nicht mehr möglich, Datenbearbeitungen, die tatsächlich erfolgen, von denjenigen, die möglicherweise in Zukunft eintreten können, abzugrenzen. Die betroffenen Personen sind sich über die Datenbeschaffung und ihre wesentlichen Rahmenbedingungen nicht mehr im Klaren. Sie müssten in einem ersten Schritt vom Verantwortlichen oder der Verantwortlichen wissen, welche Datenbearbeitungen tatsächlich erfolgen und könnten erst in einem zweiten Schritt ihre Betroffenenrechte ausüben. Die betroffenen Personen dürfen nach Treu und Glauben damit rechnen, dass die Datenbearbeitungen, welche in der Datenschutzerklärung umschrieben werden, auch tatsächlich erfolgen. Das Verhalten von der Digitec Galaxus AG verstösst gegen den Grundsatz von Treu und Glauben und stellt eine Verletzung des Transparenzgrundsatzes dar, die zu einer Persönlichkeitsverletzung gemäss Art. 12 Abs. 2 lit. a DSG führt. Wenn kein Rechtfertigungsgrund vorliegt, ist diese Persönlichkeitsverletzung widerrechtlich».[114] Mit dem letzten Satz lässt der EDÖB eine Hintertür geöffnet. Es sind Situationen denkbar, wo der Verantwortliche ein überwiegendes privates Interesse hat, einen Bearbeitungsvorgang, der erst angedacht ist und mutmasslich später umgesetzt wird, bereits in die Datenschutzerklärung aufzunehmen, damit er der diesbezüglichen Informationspflicht bereits nachgekommen ist. Dies dürfte aber nur in wenigen, bereits relativ konkreten Situationen in Frage kommen. Die Auffassung des EDÖB wird in der Lehre kritisiert.[115] Richtig ist wohl die Feststellung, dass – soweit dies einen gewissen Umfang nicht überschreitet – auch über in Zukunft beabsichtigte Datenbearbeitungen informiert werden kann, wenn diese explizit auch so gekennzeichnet werden.[116] Wenig überzeugend ist hingegen das Argument, dass die nach Aufnahme der ursprünglich nur beabsichtigten Bearbeitung revidierte Datenschutzerklärung dann ohnehin wohl niemand lesen werde und wenn es jemanden interessiere, diese Person ja ein Auskunftsbegehren stellen könne.[117] Bereits die erste Datenschutzerklärung liest kaum jemand, so dass man mit diesem Argument die Informationspflicht gleich ganz fallen lassen könnte. Vielmehr ist diese aber ein, wenn nicht der zentrale Punkt des Datenschutzes. Sie ermöglicht es der betroffenen Person, sich zu informieren, wenn sie denn will, ohne grossen Aufwand und ohne jemanden hierfür zuerst anfragen zu müssen. Ob und ggf. welche Rechte die betroffene Person dann geltend machen will, kann sie anschliessend autonom entscheiden. Für die digitale Selbstbestimmung ist die Informationspflicht somit zentraler Ausgangspunkt.

Der EDÖB empfiehlt Digitec Galaxus AG, unmissverständlich darüber zu informieren, **«welche Bearbeitungen zu Persönlichkeitsverletzungen führen und auf welche Gründe sich die Digitec Galaxus AG zu deren Rechtfertigung beruft»**.[118] Es ist unklar, auf welche Rechtsgrundlage sich der EDÖB hier genau beruft. Hensler leitet dies aus der Notwendigkeit für die Geltendmachung der Rechte der betroffenen Person ab, da diese Angaben je nach Art der Personendaten sowie Art und Umfang der Bearbeitung relevant seien, um die Rechtmässigkeit der Bearbeitung beurteilen zu können.[119] Vasella hingegen macht geltend, der Gesetzgeber hätte sich gegen eine Pflicht zur Information über die Rechtsgrundlagen entschieden, weshalb der EDÖB ohne Rechtsgrundlage diese Empfehlung ausgesprochen habe.[120] Die Beurteilung der Rechtmässigkeit ist eine Rechtsfrage, ebenso die Frage, ob eine Persönlichkeitsverletzung vorliegt. Die betroffene Person kann sich hierzu unabhängig vom Verantwortlichen eine Meinung bilden und ist in Bezug auf diese beiden Punkte nicht auf Informationen angewiesen, wenn ihr wie vorstehend dargelegt und

112 Entscheid der irischen *Data Protection Commission* (FN 110), N 5.60.
113 Entscheid der irischen *Data Protection Commission* (FN 110), N 5.64.
114 Schlussbericht i.S. Digitec Galaxus AG (FN 83), N 118 f.
115 S.a. Vasella (FN 83).
116 Hensler (FN 41), Ziffer III/3.
117 Hensler (FN 41), Ziffer III/3.
118 Schlussbericht i.S. Digitec Galaxus AG (FN 83), Empfehlung 5.
119 Hensler (FN 41), Ziffer III/4.
120 Vasella (FN 83).

vom EDÖB zurecht gefordert die ausreichend präzisen Informationen gegeben werden. Einzig fraglich kann deshalb sein, ob der Verantwortliche die Rechtfertigungsgründe nennen muss, auf die er sich berufen will. Hier wiederum sind wir im Bereich des Sachverhalts. Diese Rechtfertigungsgründe ergeben sich indes in aller Regel entweder aus dem Bearbeitungszweck (bspw. Bonitätsprüfung) oder aus dem Gesetz («durch Gesetz gerechtfertigt») oder sind der betroffenen Person ohnehin bekannt («Abwicklung eines Vertrags» oder erteilte Einwilligung). Hier eine Informationspflicht zu verlangen, obwohl der Gesetzgeber dies so nicht explizit gefordert hat, scheint uns zu weit zu gehen. Die Frage nach einer Persönlichkeitsverletzung, deren Rechtfertigung und diesbezüglicher Interessenabwägung ist letztlich eine Frage, die nicht bereits in der Datenschutzerklärung und u.E. auch nicht in der Auskunftserteilung zu beantworten ist, sondern später geklärt werden muss, wenn die betroffene Person mit der Bearbeitung ihrer Personendaten zu einem bestimmten Zweck nicht einverstanden ist. Wir befinden uns dann im kontradiktorischen Verfahren und nicht mehr in der einseitigen Informationserteilung. Dies deckt sich mit dem Grundsatz des Schweizer DSG, wonach eine Datenbearbeitung grundsätzlich erlaubt ist. Eine Persönlichkeitsverletzung muss entsprechend behauptet werden, bevor dann der Rechtfertigungsgrund vorgetragen wird. Dies will nicht heissen, dass der Verantwortliche sich nicht zu Beginn über die Rechtfertigungsgründe vergewissern muss, er muss diese nur nicht vorsorglich schon bekanntgeben, solange niemand konkret eine Persönlichkeitsverletzung behauptet.

E. Schlussbericht des EDÖB in Sachen Once Dating – Information über Empfänger & Auslandtransfer

Der Verantwortliche muss die betroffene Person über die **Empfänger** oder die Kategorien von Empfängern von Personendaten informieren.[121] Der EDÖB schreibt diesbezüglich in Bezug auf einige grundsätzlich als Auftragsbearbeiter eingesetzte Dienstleister was folgt: «Gemäss unserer Abklärung behalten sich einige Dienstleister der Once Dating AG das Recht vor, die ihnen durch die Once Dating AG bereitgestellten Daten zu eigenen Zwecken zu nutzen. Diese sind: Facebook, Google, Sendgrid, Looker, Vonage und Paypal. […]. Dies bedeutet, dass die Once Dating AG Daten an Dritte bekanntgibt, die diese nicht nur in ihrem Auftrag bearbeiten, sondern zum Teil auch in eigener Verantwortung. Aufgrund der Tatsache, dass diese Empfänger die Daten nicht ausschliesslich im Auftrag der Once Dating AG bearbeiten, ist der Begriff «Dienstleister der Once» nicht zutreffend, um diese Kategorie von Datenempfängern zu beschreiben. Immer wenn die Empfänger Personendaten in eigener Verantwortung bearbeiten, gelten diese als Dritte, nicht aber als reine Dienstleister bzw. Auftragnehmer.»[122] Vasella kritisiert zurecht, dass erstens der Begriff «Dienstleister» nicht mit Auftragsbearbeiter gleichgesetzt werden kann, dieser vielmehr – ebenso wie Auftragnehmer – diesbezüglich neutral sei und damit auch Verantwortliche gemeint sein könnten. Auch ist es nicht notwendig, in der Datenschutzerklärung eine rechtliche Qualifikation zwischen Auftragsbearbeiter und Verantwortlicher vorzunehmen, es genüge die Empfänger, wozu sowohl Auftragsbearbeiter als auch Verantwortliche zählen, zu benennen.[123]

Werden die Personendaten ins Ausland bekanntgegeben, so ist über den betreffenden Staat und ggf. die Garantien nach Artikel 16 Absatz 2 oder die Anwendung einer Ausnahme nach Artikel 17 zu informieren.[124] Der EDÖB erachtet eine allgemeine Aussage über die Verwendung von «EU-Standardvertragsklauseln oder anderen geeigneten Schutzklauseln, um den Datenübertragungen einen festen Rahmen zu verleihen und die Geheimhaltung und Sicherheit der Daten abzusichern», für nicht genügend. Gemäss dem Erwägungsgrund 4 der neuen europäischen Standardvertragsklauseln müsse die Information einen Verweis auf die angemessenen Garantien und die Möglichkeiten, wie eine Kopie von ihnen eingeholt werden könne, oder wo sie verfügbar sind, umfassen.[125] Nach Auffassung von Vasella, sollte es genügen, wenn der Verantwortliche in der Datenschutzerklärung darauf hinweist, dass er in der Regel mit den Standardvertragsklauseln arbeitet. Auch legt er nachvollziehbar dar, weshalb der vom EDÖB zitierte Erwägungsgrund 4 in der Schweiz nicht anwendbar ist, weshalb auch eine Information über das Recht, eine Kopie der Klauseln zu erhalten, unter dem DSG nicht erforderlich sei.[126] Nach hier vertretener Ansicht ist für jede Empfängerin bzw. jede Empfängerkategorie anzugeben, mit welchen Garantien gearbeitet wird. Letztlich muss die betroffene Person erkennen können, welche Personendaten an welchen Empfänger (oder Empfängerkategorie) geht und unter welchen Sicherheitsgarantien. Bei einer Empfängerkategorie (bspw. Rückversicherer) genügt es, wenn angeben wird, dass in der Regel mit EU-Standardvertragsklauseln, ausnahmsweise mit anderen Datenschutzklauseln, die dem EDÖB vorgängig mitgeteilt wurden, gearbeitet wird. Diese Ungenauigkeit ist hinzunehmen,

[121] Art. 19 Abs. 2 lit. c DSG.

[122] Schlussbericht vom 3. März 2023 des EDÖB in Sachen Digitec Galaxus AG, N 95 f.

[123] Vasella, Schlussbericht (FN 104).

[124] Art. 19 Abs. 4 DSG.

[125] Schlussbericht i.S. Digitec Galaxus AG (FN 122), N 98.

[126] Vasella, Schlussbericht (FN 104).

da diese damit zusammenhängt, dass es genügt, nur «Kategorien von Empfängern» anzugeben.

F. Datenschutzerklärung für den EU-Raum und darüber hinaus

Die österreichische Datenschutzbehörde hatte im Sommer 2019 eine Datenschutzerklärung eines Schweizer Unternehmens im Hinblick auf deren Anwendung unter Geltung der DSGVO zu beurteilen.[127] Die Datenschutzerklärung wurde sogar mit Verweisen auf die DSGVO formuliert, allerding mehr schlecht als recht, worauf hier nicht im Detail eingegangen wird. Der Verantwortliche hatte bei den Kontaktangaben den Namen des «Datenschutzverantwortlichen» angegeben. Dies entspricht der Terminologie des Schweizer Datenschutzgesetzes vom 19. Juni 1992[128] für den Datenschutzberater (aktuelles DSG[129]) bzw. Datenschutzbeauftragten (DSGVO[130]). Der österreichischen Datenschutzbehörde war dieser Begriff aber «fremd»: «Davon ausgehend ist unklar, ob es sich bei dem seitens der Beschwerdegegnerin ins Treffen geführten ‹Datenschutzverantwortlichen› um eine Art interne Ansprechstelle bei der Beschwerdegegnerin handelt, oder um einen Datenschutzbeauftragten iSd Art. 37 ff DSGVO. Aus Sicht des Beschwerdeführers […] hätte es sich auch um den Vertreter gemäß Art. 27 DSGVO handeln können. Unter Berücksichtigung des in Art. 12 Abs. 1 verankerten Präzisions- und Verständlichkeitsgebots ist die Beschwerdegegnerin daher angehalten, hinreichend verständliche und präzise Informationen im Hinblick auf den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters mitzuteilen, wobei insbesondere zu erläutern ist, was unter dem Begriff ‹Datenschutzverantwortliche› zu verstehen ist.»[131] Folgt man der Auffassung der Datenschutzbehörde, so sind Datenschutzerklärungen für jedes Land gesondert zu formulieren, um die lokale Terminologie zu treffen. Während Versicherer in aller Regel ohnehin pro Land eine oder mehrere separate Datenschutzerklärungen verwenden, ist dies für global tätige Startups eine Zumutung. In der Praxis hatte man sich auch in der Versicherungswelt (insb. Rückversicherer) oft damit begnügt, bspw. die Begriffe der DSGVO zu verwenden und zu definieren, dass die Begriffe jene Bedeutung haben, die Ihnen nach der DSGVO zukommt. Doch auch dies ist natürlich wenig hilfreich, da ein Datenschutzbeauftragter nach DSGVO rechtlich nicht dasselbe ist wie der Datenschutzberater. Auch der Hinweis, dass Begriffe dann nach lokalem anwendbaren Datenschutzrecht verstanden werden sollen, hilft nur bedingt, wird in aussereuropäischen Erlassen es wohl auch Funktionen geben, die sich nicht einem Begriff in der DSGVO zuordnen lassen. Zudem müsste der Verantwortliche sich dann auch vergewissern, ob er bspw. mit der Art und Weise, wie er den Datenschutzberater ernannt hat, und mit den Kompetenzen, die er ihm gewährt, den Anforderungen des lokal anwendbaren Datenschutzrechts nachgekommen ist. Es wäre insgesamt wünschenswert, wenn Behörden und Gerichte hier Augenmass walten liessen und dem internationalen Kontext und den Möglichkeiten eines Unternehmens im Rahmen der Verhältnismässigkeit Rechnung tragen würden. Von Versicherern und auch von Versicherungsvermittlern kann und darf man aber erwarten, dass sie die lokalen Gesetze inkl. Terminologie einhalten, wenn sie im betreffenden Land eine Zulassung oder Registrierung haben.

V. Auskunftsbegehren

A. Gesetzliche Regelung

Jede Person hat das Recht, vom Verantwortlichen Auskunft darüber verlangen zu können, ob Personendaten über sie verarbeitet werden und ggf. auf gewisse Mindestinformationen hierüber.[132] Der Verantwortliche kann die Auskunft verweigern, einschränken oder aufschieben, u.a. wenn ein Gesetz im formellen Sinn dies vorsieht, wenn dies aufgrund überwiegender Interessen Dritter erforderlich ist oder wenn das Auskunftsrecht offensichtlich unbegründet ist.[133] In der EU sind Einschränkungen restriktiver geregelt.[134]

B. Rechtsmissbrauch

Das Auskunftsrecht gilt unter Vorbehalt des offenbaren Rechtsmissbrauchs gemäss Art. 2 Abs. 2 ZGB. Ob das Auskunftsrecht missbräuchlich ausgeübt wird, ist stets von den Umständen des Einzelfalls abhängig (siehe BGE 138 III 432). Rechtsmissbrauch wird bei zweckwidriger Verwendung eines Rechtsinstituts zur Verwirklichung von Interessen, die dieses Institut nicht schützen will, angenommen. Grundsätzlich kann das Auskunftsrecht ohne Nachweis eines Interesses geltend gemacht werden. Rechtsmissbrauch fällt in Betracht, wenn das Auskunftsrecht zu datenschutzwidrigen Zwecken eingesetzt wird. In BGE 138 III 425 hat das Bundesgericht festgehalten, dass unter Vorbehalt einer rechtmissbräuchlichen Ausübung das Auskunftsrechts auch zur Vorbereitung eines Zivilprozesses geltend gemacht werden kann.

127 Entscheid der österreichischen Datenschutzbehörde vom 22. August 2019, DSB-D130.206/0006-DSB/2019.
128 Art. 11a Abs. 5 und 6 aDSG.
129 Art. 10 DSG.
130 Art. 37 DSGVO.
131 Entscheid der österreichischen Datenschutzbehörde vom 22. August 2019, DSB-D130.206/0006-DSB/2019, E D/4a.
132 Art. 25 DSG bzw. Art. 15 DSGVO.
133 Art. 26 DSG.
134 Art. 23 DSGVO.

C. Entscheid betr. Einsicht in Observationsunterlagen

Im vorliegenden Fall[135] verlangte ein Geschädigter Einsicht in die von der Versicherung eingeholten Observationsunterlagen. Diese entgegnete, dass der Geschädigte nichts Neues über sich selbst erfahre; auch stimme doch das Observationsmaterial mit den tatsächlichen Gegebenheiten überein. Das erste Argument ist in Bezug auf das datenschutzrechtliche Auskunftsrecht irrelevant, geht es doch darum, dass die betroffene Person weiss, welche Daten der Verantwortliche über sie bearbeitet; und nicht darum, etwas Neues zu erfahren. Auch das zweite Argument ist für sich wenig hilfreich, geht es beim Auskunftsrecht auch nicht bloss darum, die Richtigkeit der Datenbearbeitung überprüfen zu können.

Die Versicherung wandte weiter ein, dass das Observationsmaterial zeige, dass der Geschädigte hinsichtlich seiner körperlichen Beschwerden übertreibe. Eine Offenlegung habe zur Folge, dass er über den Wissensstand der Versicherung in Kenntnis gesetzt würde, mit der Konsequenz, dass er den in der Klage zu schildernden Sachverhalt entsprechend anpassen könnte. Er könnte somit bereits in der Klage allfällige aus den Observationen ersichtliche und für die behaupteten Beschwerden aussergewöhnliche körperliche Betätigungen so beschreiben, dass jegliche Argumente in der Klageantwort ins Leere führten. Bei nicht objektivierbaren Beschwerden wie dem Schleudertrauma werde die Glaubwürdigkeit des Geschädigten aber an dem von diesem in der Klage fixierten Sachverhalt beziehungsweise an dem in der Klage behaupteten Gesundheitszustand gemessen. Würden nun bereits mit der Klage allfällige Argumente der Versicherung pariert, könne die Glaubwürdigkeit des Geschädigten nicht mehr überprüft werden. Das Aufzeigen von unglaubwürdigen Aussagen werde der Versicherung verunmöglicht. Dabei sei es für sie zentral, Zweifel an der Glaubwürdigkeit des Geschädigten zu streuen. Dies gelinge, wenn der Geschädigte erst in einer allfälligen Replik Stellung beziehen könne, müsse er sich doch dann an die in der Klage beschriebenen Beschwerden halten oder sich auf Kosten seiner Glaubwürdigkeit widersprechen. Somit missbrauche der Geschädigte das Auskunftsrecht allein aus prozesstaktischen Gründen. Der Geschädigte entgegnet, dass das ihm vorgeworfene Vorgehen gar nicht mehr möglich sei, weil er sich bereits mehrfach gegenüber Ärzten, Gutachtern, Case-Managern und Versicherungsmitarbeitern zu seinem Gesundheitszustand geäussert habe. Dabei sei er völlig unbefangen vom Ergebnis einer Observation gewesen. Somit seien die Befürchtungen, wonach er in einer allfälligen Klage die bereits mehrfach vorgebrachten Behauptungen neu darlegen könne, unbegründet. Ferner streitet er nicht ab, die Observationsunterlagen auch im Hinblick auf einen Prozess verwenden zu wollen, damit er nicht innert den kurzen zivilprozessualen Fristen eine Überprüfung der Daten auf ihre Richtigkeit und Rechtmässigkeit hin vornehmen und allfällige medizinische oder sachverhaltsmässige Abklärungen in Auftrag geben müsse. Damit wolle der Geschädigte, so das Obergericht, jene Zeit zur Verfügung haben, welche ihm das DSG dafür auch lasse. Darin sei kein (offenbarer) Rechtsmissbrauch zu erkennen.

Das Obergericht hält fest, dass die Versicherung für die Behauptung des Rechtsmissbrauchs die **Beweislast** trägt, wobei ihr das Recht auf entsprechende Beweisabnahme zusteht. Folglich hätte die Vorinstanz für dieses von der Versicherung behauptete Motiv Beweis abnehmen müssen. Hievon kann aber abgesehen werden, wenn von vorneherein feststeht, dass kein (offenbarer) Rechtsmissbrauch vorliegt.

Zwar muss die betroffene Person ihr Auskunftsbegehren nicht begründen, doch ist die **Darlegung des Interesses an der Auskunft** notwendig, um dem Vorwurf der rechtsmissbräuchlichen Ausübung des Auskunftsrechts entgegenzutreten. Ebenso kann die allenfalls gebotene Abwägung der gegenseitigen Interessen erfordern, dass der um Auskunft Ersuchende seine Interessen darlegt. Folglich kommt den (wahren) Interessen des Geschädigten (betroffene Person), die dieser mit der Geltendmachung seines Auskunftsrechts verfolgt, entscheidende Bedeutung zu.

Mit dem Geschädigten geht das Gericht davon aus, dass Observationsmaterialien durchaus überprüfbar sind, basieren sie doch regelmässig auf einer Auswahl von Videosequenzen und dem subjektiv wertenden Bericht des dem Auftraggeber verpflichteten Observierenden, der nach seiner Auffassung Unwesentliches weglässt oder wegschneidet. Somit wäre das Material durchaus einer Überprüfung hinsichtlich Objektivität beziehungsweise Ausgewogenheit in der Auswahl zugänglich. Doch auch unabhängig von einer allfälligen tendenziösen Berichterstattung seitens des Observierenden lassen sich Bildaufnahmen, zugehörige schriftliche Aufzeichnungen sowie auswertende (ärztliche) Stellungnahmen auf die Schutzfunktionen des datenschutzrechtlichen Auskunftsrechts hin überprüfen, das der betroffenen Person ermöglicht, das gesammelte Datenmaterial auf Rechtmässigkeit in der Beschaffung und Weitergabe sowie auf Richtigkeit, aber auch auf Treu und Glauben und Verhältnismässigkeit in der Bearbeitung zu kontrollieren. Somit beruft sich der Ge-

[135] OGer TG, 2. Abteilung, ZBR.2013.10 vom 14. Mai 2013; Siehe dazu auch Kurt Pärli/Jonas Eggmann, Datenschutz in privaten Arbeits- und Versicherungsverhältnissen, in: Ueli Kieser/Kurt Pärli/Ursula Uttinger, Datenschutztagung 2019, Aktuelle Entwicklungen im Datenschutz, 58–59.

schädigte für sein Auskunftsersuchen durchaus auf **datenschutzkonforme Motive** und Interessen. Sollte der Geschädigte daneben (vor)prozessuale Ziele verfolgen, so lassen diese das Auskunftsbegehren (noch) nicht als (offenbar) rechtsmissbräuchlich erscheinen.

Das Obergericht prüft ferner, **ob der Verantwortliche die Auskunft aus überwiegenden eigenen Interessen verweigern, einschränken oder aufschieben könne**. Es verweist diesbezüglich auf BGE 138 III 433 ff., wo als Beispiele die Befürchtung einer Wirtschaftsspionage, Gefährdungen oder Beeinträchtigungen der Persönlichkeitsrechte des Auskunftspflichtigen oder auch überwiegende finanzielle Interessen genannt werden. Nach der Rechtsprechung des Bundesgerichts ist in einem ersten Schritt die Schutzwürdigkeit der angerufenen eigenen Interessen des Verantwortlichen zu prüfen. Nur wenn diese zu bejahen ist, sind in einem zweiten Schritt die Interessen des Verantwortlichen gegen jene der betroffenen Person abzuwägen. Ein allfälliges Interesse des Verantwortlichen an der Anwendbarkeit zivilprozessualer Regeln im Vorfeld eines sich abzeichnenden Prozesses bildet demgegenüber keinen Einschränkungsgrund. Vielmehr gelten für Auskunftsbegehren, die vor Rechtshängigkeit eines Zivilprozesses gestellt werden, selbst dann die Regeln des Datenschutzrechts, wenn sich ein Prozess anbahnt. Eine Einschränkung des Auskunftsrechts im Vorfeld eines Zivilprozesses ist deshalb nur zulässig, wenn das angerufene Interesse im vorgenannten Sinn schutzwürdig ist und das Interesse des Verantwortlichen überwiegt. Dem ist so, wenn die betroffene Person im konkreten Fall datenschutzfremde Interessen verfolgt, etwa, wenn es ihr (primär oder allein) darum geht, ihre Schadenersatzansprüche abzuklären. Zu beachten ist dabei jedoch, dass die Interessenabwägung nicht pauschal, sondern für jedes Personendatum bzw. Aktenstück gesondert vorzunehmen ist. Selbst bei Bejahung überwiegender eigener Interessen des Verantwortlichen muss daher sorgfältig geprüft werden, wie weit dessen Einschränkungsrecht im Einzelfall konkret reicht.

Sowohl bei der Beurteilung der Rechtmässigkeit einer Observation als auch bei der Prüfung der Zulässigkeit der Einschränkung des Auskunftsrechts ist eine **Interessenabwägung** vorzunehmen. Indessen braucht das Ergebnis nicht dasselbe zu sein, zumal sich der Prüfgegenstand unterscheidet. Die Rechtmässigkeit der Observation war vorliegend nicht zu beurteilen. Vielmehr war einzig das Interesse der Versicherung an der Verweigerung der Auskunft bis zur Klagebegründung durch den Geschädigten respektive das Interesse des Geschädigten an der Auskunft Gegenstand des Verfahrens. Die Versicherung erklärte, ihr privates (finanzielles) Interesse wie auch dasjenige (öffentliche) der Versichertengemeinschaft bestehe darin, nur haftpflichtrechtlich erwiesene Leistungen erbringen zu müssen. Hierfür müsse die Glaubwürdigkeit des Geschädigten in einem zukünftigen Haftpflichtprozess überprüft werden können. Das Obergericht hält diesbezüglich fest, dass das Gericht, das den Haftpflichtfall dereinst zu beurteilen habe, sicherlich zu berücksichtigen wissen werde, dass der Geschädigte die Klagebegründung in Kenntnis der Observationsmaterialien verfasste, und dass es sich dabei um blosse Parteibehauptungen handelt. Das Gericht wird dabei auch ohne weiteres die Angaben des Geschädigten in den medizinischen Akten zu den Observationsmaterialien in Bezug setzen können. Damit fehlt es aber seitens der Versicherung mit Blick auf die (einstweilige) Zurückbehaltung der Akten bereits an einem schutzwürdigen Interesse. Somit scheint die Verweigerung der Herausgabe der Observationsmaterialien im Hinblick auf die Verhältnismässigkeitsprüfung weder geeignet noch notwendig, um die Glaubwürdigkeit des Geschädigten zu beurteilen. Die Versicherung musste dem Geschädigten somit Einsicht in die Observationsunterlagen gewähren.

D. Entscheid betr. Beweisausforschung

Das Bundesgericht hat am 18. November 2020 festgehalten,[136] dass das Auskunftsrecht der Durchsetzung des Persönlichkeitsschutzes dient. «Es ermöglicht der betroffenen Person, die über sie […] bearbeiteten Daten zu kontrollieren mit dem Ziel, die Einhaltung der datenschutzrechtlichen Grundsätze, wie Beschaffung der Daten mit rechtmässigen Mitteln und nicht in gegen Treu und Glauben verstossender Weise oder Gewährleistung der Richtigkeit der Daten und der Verhältnismässigkeit ihrer Bearbeitung, in der Rechtswirklichkeit zu überprüfen und durchzusetzen» (E. 5.2).

Zwar sei für die Ausübung des Auskunftsrechts grundsätzlich kein Interessennachweis notwendig, der Verantwortliche könne aber einen solchen verlangen, um eine Interessenabwägung vornehmen zu können oder um Rechtsmissbrauch auszuschliessen. Letzteres «falle in Betracht, wenn das Auskunftsrecht zu datenschutzwidrigen Zwecken eingesetzt werde, etwa um sich die Kosten einer Datenbeschaffung zu sparen, die sonst bezahlt werden müssten. Zu denken sei auch an eine schikanöse Rechtsausübung ohne wirkliches Interesse an der Auskunft, lediglich um den Auskunftspflichtigen zu schädigen. Eine zweckwidrige Verwendung des datenschutzrechtlichen Auskunftsrechts und damit Rechtsmissbrauch – so das Bundesgericht schliesslich – wäre wohl auch anzunehmen, wenn das Auskunftsbegehren einzig zum Zweck gestellt wird, die (spätere) Gegenpartei auszuforschen und Beweise zu beschaffen, an die eine Partei sonst nicht gelangen könnte. Denn das Auskunftsrecht wolle nicht die Be-

[136] BGer 4A_277/2020 vom 18. November 2020.

weismittelbeschaffung erleichtern oder in das Zivilprozessrecht eingreifen».[137] Das Bundesgericht hält fest, dass das Auskunftsrecht ein datenschutzrechtliches Interesse voraussetze und nicht der alleinigen Abklärung von Prozessaussichten dienen könne.[138]

Im zugrundliegenden Fall war nicht bestritten, dass das Auskunftsbegehren einzig zum Ziel hatte, einen späteren Zivilprozess vorzubereiten und die Prozesschancen abzuklären. Entsprechend qualifizierte das Bundesgericht das Auskunftsbegehren als rechtsmissbräuchlich.

Der Entscheid stellt im Hinblick auf den Sinn und Zweck des Datenschutzgesetzes eine Selbstverständlichkeit dar; datenschutzwidrige Zwecke sind im neuen DSG explizit ausgeschlossen.[139] Für die Abklärung von Prozessaussichten steht im Übrigen die zivilprozessrechtliche vorsorgliche Beweisführung zur Verfügung.[140]

E. Entscheid betr. im Gehirn memorisierte Herkunftsangaben

Nachdem das Bundesgericht im vorstehenden Fall das Berner Obergericht korrigieren musste, war nun am 10. Dezember 2020 (4A_125/2020) das Zürcher Obergericht an der Reihe.[141] Im Zusammenhang mit der Auskunft über die Herkunft von Daten vertrat das Obergericht die Auffassung, als Träger dieser Information kämen nicht nur Sachen (Schriftstücke, physische Datenträger) in Frage, sondern auch das menschliche Gehirn. Mithin sei auch über Herkunftsangaben Auskunft zu erteilen, die im menschlichen Gedächtnis gespeichert seien. Ob solche Angaben verfügbar seien, müsse im Rahmen des Beweisverfahrens durch Zeugen- und Parteibefragungen geklärt werden.

Das Bundesgericht hält – völlig zu Recht – fest: «Der datenschutzrechtliche Auskunftsanspruch erfasst kein allgemeines Recht, durch Partei- und Zeugenbefragung zu erfahren, zwischen wem wann worüber ein personenbezogenes Gespräch stattgefunden hat. Vielmehr erhellt aus der gesetzlichen Regelung der Formalitäten der Auskunftserteilung, dass es dem Gesetzgeber darum geht, schriftlich bzw. ‹physisch› vorhandene, und deshalb auf Dauer objektiv einsehbare Datensammlungen zu erfassen, **nicht aber bloss im Gedächtnis abrufbare Daten**.»[142]

Das Bundesgericht hält weiter fest, dass es keine Verpflichtung gebe, die **Herkunftsangaben aufzubewahren**.[143] «Wird vom Inhaber der Datensammlung nicht verlangt, die Herkunftsangaben zu speichern, kann von ihm im Rahmen von Art. 8 DSG auch nicht verlangt werden, dass er Nachforschungen nach Herkunftsangaben anstellt, die er nicht aufbewahrt hat.»[144] Wenn hingegen eine Aufbewahrung erfolgt, ist diese so auszugestalten, dass darüber Auskunft erteilt werden kann.[145]

In prozessualer Hinsicht enthält der Entscheid hilfreiche Ausführungen zur **Abgrenzung zwischen dem materiell-rechtlichen Anspruch auf Auskunft nach DSG und dem prozessualen Anspruch auf Beweisabnahme**. Beweismittel, wie die Zeugenbefragung oder das Institut der prozessualen Edition, können – so das Bundesgericht – nicht als Instrument der Informationsbeschaffung dienen, sondern stellen nach der Zivilprozessordnung Mittel der Beweiserhebung dar. Das Beweisverfahren darf nicht zur Anspruchsdurchsetzung ohne Prüfung der Anspruchsvoraussetzungen für das Auskunftsrecht nach DSG missbraucht werden, so dass mit dem Beweisverfahren faktisch über den eingeklagten Anspruch entschieden wird, bevor geklärt ist, ob eine Pflicht zur Auskunft überhaupt besteht.[146] «Sowohl für den materiellen Anspruch auf Auskunft nach Datenschutzgesetz als auch für den zivilprozessualen Anspruch auf Beweisabnahme gilt sodann, dass diese nicht zu einer verpönten Beweisausforschung missbraucht werden dürfen.»[147]

Ebenso interessant sind die Ausführungen des Bundesgerichts zur **Beweislast** im Zusammenhang mit dem Auskunftsrecht: «Die zu erteilende Auskunft muss wahr und vollständig sein (…), wofür der Inhaber einer Datensammlung im Streitfall beweispflichtig ist (…). Das Auskunftsrecht erstreckt sich nach der Rechtsprechung und dem Gesetzeswortlaut nur auf noch vorhandene Daten (…). Der Umstand, dass wie hier negative Tatsachen, namentlich das Nichtvorhandensein zusätzlicher, nicht bereits ausgehändigter Informationen über den Beschwerdegegner, bewiesen werden müssen, ändert grundsätzlich nichts an der Beweislast (…). Da es aber naturgemäss einfacher ist, das Vorhandensein von Tatsachen zu beweisen als deren Nichtvorhandensein, ist die Schwelle der rechtsgenüglichen Beweiserhebung vernünftig anzusetzen. Wo der beweisbelasteten Partei der regelmässig äusserst schwierige Beweis des Nichtvorhandenseins einer Tatsache obliegt, ist die Gegenpartei nach Treu und Glauben gehalten, ihrerseits verstärkt bei der Beweisführung mitzuwirken, namentlich indem sie einen Gegenbeweis erbringt oder zumindest konkrete Anhaltspunkte für das Vorhandensein weiterer Daten aufzeigt.»[148]

137 BGer 4A_277/2020 vom 18. November 2020 E. 5.3.
138 BGer 4A_277/2020 vom 18. November 2020 E. 5.4.
139 Art. 26 Abs. 1 lit. c DSG.
140 Art. 158 ZPO.
141 BGer 4A_125/2020 vom 10. Dezember 2020.
142 BGer 4A_125/2020 vom 10. Dezember 2020 E. 3.4.3.
143 BGer 4A_125/2020 vom 10. Dezember 2020 E. 3.2.1 und 3.4.5.
144 BGer 4A_125/2020 vom 10. Dezember 2020 E. 3.4.6.
145 BGer 4A_125/2020 vom 10. Dezember 2020 E. 3.4.5.
146 BGer 4A_125/2020 vom 10. Dezember 2020 E. 1.7.1.
147 BGer 4A_125/2020 vom 10. Dezember 2020 E. 1.7.2.
148 BGer 4A_125/2020 vom 10. Dezember 2020 E. 3.1.2.

F. Entscheid betr. Ausweispflicht

Zwei Geschäftsführer mehrerer Gesellschaften forderten ihre Geschäftsbank auf, ihnen alle sie betreffenden persönlichen Daten zu übermitteln, worauf die Bank u.a. antwortete, sie brauche eine Kopie der Identitätskarte, um dem Auskunftsbegehren nachzukommen. Die belgische *Chambre contentieuse* erwägt, dass die Bank nicht an der Identität habe zweifeln müssen, sei das Gesuch doch auf dem Briefpapier eines im Anwaltsregister eingetragenen Anwalts gestellt worden. Ferner habe die Bank selbst direkt einen der beiden Geschäftsführer angeschrieben.[149] Einen vernünftigen Grund, einen Ausweis einzuverlangen, gab es somit nicht.

Die *Chambre contentieuse* erwähnt den Erwägungsgrund 63 der DSGVO, der folgendes vorsieht: «Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt.» Vorliegend musste indes nicht näher darauf eingegangen werden, da die Bank keine diesbezüglichen Rückfragen gestellt hatte.[150]

Ähnlich entschied die niederländische Datenschutzbehörde, die gegen ein Medienunternehmen eine Busse von 525'000 Euro verhängt hat, weil das Unternehmen von Betroffenen bei Auskunftsbegehren einen Identitätsnachweis in Form eines Ausweisdokuments verlangt hat.[151]

Unseres Erachtens hat der Verantwortliche immer dann einen Identitätsnachweis zu verlangen, wenn diesbezüglich Zweifel bestehen. Die Anforderungen dürfen hier nicht zu hoch gestellt werden, denn es gilt eine Auskunftserteilung an falsche Personen – und damit einen *Data Breach* – zu verhindern.

G. Entscheid betr. Recht auf Kopie zur Kontrolle von Prämienerhöhungen

Im vorliegenden Urteil des Oberlandesgerichts Karlsruhe[152] geht es um einen Versicherten, der im Wege einer Stufenklage Rückerstattungsansprüche gegen eine private Krankenversicherung geltend macht. Die private Krankenversicherung hatte die Prämien erhöht, was in den Versicherungsbedingungen vorgesehen war. Der Versicherte ist der Ansicht, die Prämienerhöhung sei materiell unwirksam, weshalb ihm Rückerstattungsansprüche zustünden. Um diese Ansprüche geltend machen zu können, müsse die Versicherung ihm alle notwendigen Unterlagen und Information zustellen.

Die DSGVO gewährt ein Auskunftsrecht über die Verarbeitung der personenbezogenen Daten. Bei den Versicherungsscheinen und Nachträgen zum Versicherungsschein handelt es sich nicht in ihrer Gesamtheit um persönliche Daten des Versicherungsnehmers. Vielmehr enthalten diese Dokumente nur einzelne persönliche Daten des Versicherungsnehmers und der weiteren Versicherten. Der Kläger hat jedoch seinen Anspruch nicht auf diese persönlichen Daten beschränkt.

Das Recht auf Kopie ist in der DSGVO explizit verankert, [153] wobei es sich um kein anders, unabhängiges Recht handelt, als das generelle Auskunftsrecht. Die betroffene Person hat entsprechend das Recht, eine Kopie von sämtlichen verarbeiteten personenbezogenen Daten zu bekommen. Der Begriff «Kopie» bezieht sich also nicht auf ein Dokument als solches, sondern nur auf die personenbezogenen Daten, die es enthält. Ausnahmsweise kann die Reproduktion des ganzen Dokumentes sich als unerlässlich erweisen, «wenn die Kontextualisierung der Daten erforderlich ist, um ihre Verständlichkeit zu gewährleisten». Der Versicherte kann im vorliegenden Fall kein Recht auf Kopie geltend machen, da dieses Recht nur für personenbezogene Daten gilt und er seinen Anspruch nicht auf diese persönlichen Daten beschränkt.

Einen ähnlichen Fall musste der Bundesgerichtshof am 6. Februar 2024 beurteilen.[154] Aufgrund mehrfacher Prämienerhöhungen forderte die Versicherte ihren Versicherer auf, ihr Auskunft über alle diese Erhöhungen zu erteilen und ihr die damit verbunden Unterlagen zur Verfügung zu stellen. Der Bundesgerichtshof verneint einen Auskunftsanspruch, da nur einzelne Teile der Versicherungsscheine und Nachträge personenbezogene Daten enthalten, es sich aber nicht in ihrer Gesamtheit um personenbezogene Daten handelt. Eine Beschränkung des Anspruchs auf personenbezogene Daten wurde jedoch nicht vorgenommen. Bezüglich des expliziten Rechts auf Kopie betont der Bundesgerichtshof, dass dieses nur die praktischen Modalitäten für die Erfüllung des allgemeinen Anspruchs festlegt, aber keinen weitergehenden eigenen Anspruch gewährt. Der Begriff «Kopie» bezieht sich sodann nur auf die personenbezogenen Daten, nicht auf das gesamte Dokument, ausser wenn dies zur Kontextualisierung der personenbezogenen Daten unerlässlich ist,

[149] *Autorité de Protection de Données, Chambre contentieuse*, DOS-2019-05450 vom 28. April 2020 (Belgien), insb. N 50.

[150] *Autorité de Protection de Données, Chambre contentieuse*, DOS-2019-05450 vom 28. April 2020 (Belgien), insb. N 55.

[151] Autoriteit Persoonsgegevens, DPA fines DPG Media for unnecessarily requesting copies of identity documents, 24. Februar 2022, Internet: https://www.autoriteitpersoonsgegevens.nl/en/current/dpa-fines-dpg-media-for-unnecessarily-requesting-copies-of-identity-documents (Abruf 9.10.2025).

[152] Urteil des Oberlandesgerichts Karlsruhe vom 1. Februar 2024, 12 U 27/23.

[153] Art. 15 Abs. 3 DSGVO.

[154] Bundesgerichtshof, VI ZR 62/23, vom 06.02.2024.

was hier nicht der Fall war. Die Argumente des Bundesgerichtshofes sind substanziell dieselben wie im Urteil des Oberlandesgerichts Karlsruhe. Auch in der Schweiz war ein ähnlich gelagerter Fall mehr oder weniger identisch beurteilt worden.[155]

H. Kein Auskunftsrecht bei einem Vergleich per Saldo aller Ansprüche

In einem arbeitsrechtlichen Fall wurde zwischen dem Arbeitnehmer und Arbeitgeber folgender Vergleich geschlossen: «Mit Erfüllung des Vergleichs sind alle Ansprüche aus dem Arbeitsverhältnis und dessen Beendigung, gleich ob bekannt oder unbekannt, gleich aus welchem Rechtsgrund, abgegolten mit Ausnahme der Arbeitspapiere.»[156] Sämtliche drei aufgerufenen Instanzen haben befunden, dass der Arbeitnehmer damit gültig auch auf sein Auskunftsrecht – jedenfalls für die im Rahmen des Arbeitsverhältnisses erfolgten Bearbeitungen – verzichtet habe.

«Der DSGVO ist das Konzept der Disposition über das Niveau des aus der DSGVO folgenden Datenschutzes im Grundsatz durchaus nicht fremd. Es steht dem Betroffenen […] frei, in die Verarbeitung seiner personenbezogenen Daten einzuwilligen. […]. Dies zeigt, dass das Konzept der Einwilligung ein Grundpfeiler des Datenschutzes ist. Wenn das darin zum Ausdruck kommende Prinzip der Selbstbestimmung es ermöglicht, über die Frage der zulässigen Datenverarbeitung selbst zu bestimmen, liegt es nahe, dass auch die Disposition über den Auskunftsanspruch, der nur einen Einblick in das Ergebnis der – selbstbestimmten – Datenverarbeitung ermöglicht, ebenfalls selbstbestimmt durch den Betroffenen möglich sein muss. Zwar spricht einiges dafür, dass der Auskunftsanspruch […] für die Zukunft unabdingbar ist. Ansonsten bestünde die Gefahr, dass dieser nicht effektiv durchgesetzt werden könnte und letztlich leerliefe. Bei einem – wie hier – beendeten Arbeitsverhältnis ist eine Schutzbedürftigkeit des (grundsätzlich unterlegenen) Arbeitsnehmers hingegen nicht mehr in vergleichbarem Maße gegeben. Eine Disposition über den Auskunftsanspruch für ein Arbeitsverhältnis, das in der Vergangenheit bestanden hat, ist daher möglich.»[157]

Ferner führt das Oberverwaltungsgericht des Saarlands aus: «Der beurkundete Vergleichswille wäre wertlos, wenn über den beurkundeten Inhalt hinausgehende Ansprüche Quelle eines neuen Rechtsstreits sein könnten. Ausgehend von der […] bezweckten ‹Gesamtbereinigung› besteht aus der Sicht des Senats kein Zweifel daran, dass auch der Auskunftsanspruch nach Art. 15 DSGVO hiervon umfasst wird. Einer entsprechenden Klarstellung bedurfte es nicht. […] Für eine ausdrückliche Erwähnung und Hervorhebung datenschutzrechtlicher Ansprüche bei der Abgeltungsklausel besteht keine rechtliche Notwendigkeit.»[158]

VI. Datenschutzrechtliche Bussen

A. Bussen nach DSG & DSGVO

Wenn eine natürliche oder juristische Person das DSG, beziehungsweise die DSGVO verletzt, kann sie unter gewissen Bedingungen zu einer Busse verurteilt werden. Während in der EU die Unternehmen für relativ viele Pflichtverletzungen mit Geldbussen von bis zu 20 Mio. Euro oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes (je nachdem, welcher der Beträge höher ist) bestraft werden können,[159] bestraft die Schweiz grundsätzlich die fehlbare natürliche Person mit einer Busse bis zu CHF 250’000 und nur ausnahmsweise das Unternehmen als solches.[160] Bussbewährt sind insbesondere vorsätzliche Verfehlungen in Zusammenhang mit der Informationspflicht, der Auskunftserteilung, die Übergabe der Datenbearbeitung an einen Auftragsbearbeiter, ohne dass die Voraussetzungen nach Art. 9 DSG erfüllt sind, die Nichteinhaltung der Mindestanforderungen an die Datensicherheit und die nicht korrekte Übermittlung von Personendaten ins Ausland.[161]

B. Das kleine Berufsgeheimnis – Versicherungsgeheimnis?

Ferner ist eine Verletzung der im DSG neu eingeführten **beruflichen Schweigepflicht** (sog. kleines Berufsgeheimnis) strafbar. Letzteres gilt im Versicherungsbereich für Personendaten, die ein Versicherer direkt von der betroffenen Person oder einer dieser zurechenbaren Person erhält und nach den Umständen davon ausgegangen werden musste, dass es sich um geheime Daten handelt.[162] Der Wortlaut der beruflichen Schweigepflicht ist indes weit weniger klar: «Wer geheime Personendaten vorsätzlich offenbart, von denen sie oder er bei der Ausübung ihres oder eines Berufes, der die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat, wird auf Antrag mit Busse bis zu 250 000 Franken bestraft. Gleich wird bestraft, wer vorsätzlich geheime Personendaten offenbart, von denen sie oder er bei der Tätigkeit für eine geheimhaltungspflichtige Person

155 Eingehend zum Auskunftsrecht nach aDSG, DSG und DSGVO: Urteil des Bundesverwaltungsgerichts vom 11. April 2024, A-4873/2021, E. 6.

156 Urteil des Oberverwaltungsgerichts des Saarlands, 2. Senat, vom 13. Mai 2025, 2 A 165/24, N 2.

157 Urteil des Oberverwaltungsgerichts des Saarlands, 2. Senat, vom 13. Mai 2025, 2 A 165/24, N 19.

158 Urteil des Oberverwaltungsgerichts des Saarlands, 2. Senat, vom 13. Mai 2025, 2 A 165/24, N 20.

159 Art. 83 DSGVO.

160 Art. 60–64 DSG.

161 Art. 60 und 61 DSG; Art. 53 FMG betr. Information über Cookies.

162 Rosenthal/Gubler, Die Strafbestimmungen des neuen DSG, SZW 2021, 61, sprechen diesbezüglich von einer stillschweigenden Vertraulichkeitsabrede.

oder während der Ausbildung bei dieser Kenntnis erlangt hat.» [163]

Diese Bestimmung erinnert bspw. an die Geheimhaltungspflicht nach österreichischem Versicherungsaufsichtsgesetz: «Wer als Mitglied eines Organs, als Treuhänder, als verantwortlicher Aktuar, als Dienstnehmer eines Versicherungsunternehmens, eines Rückversicherungsunternehmens, […], als selbständiger Versicherungsvertreter, […] ihm ausschließlich auf Grund seiner beruflichen Tätigkeit bekannt gewordene Verhältnisse oder Umstände, deren Geheimhaltung im berechtigten Interesse der davon betroffenen Personen gelegen ist, weitergibt oder verwertet, begeht eine Verwaltungsübertretung und ist von der FMA mit einer Geldstrafe bis zu 60 000 Euro zu bestrafen, es sei denn, dass die Weitergabe oder Verwertung nach Inhalt und Form durch ein öffentliches oder ein berechtigtes privates Interesse gerechtfertigt oder der Betroffene mit der Weitergabe oder Verwertung ausdrücklich einverstanden ist.»[164] Aufgrund der vorgenannten Bestimmung ist auch eine unbegrenzte Weitergabe von geheimen Tatsachen innerhalb eines Versicherers nicht zulässig, sondern auf jenen Personenkreis zu beschränken, der «rechtmässig mit der Abwicklung der Geschäftsbeziehung zum Kunden befasst ist oder befasst sein könnte».[165]

Unseres Erachtens ist die viel zu offen und unklar formulierte Vorschrift zur beruflichen Schweigepflicht im DSG genau so zu verstehen, wie es hier das österreichische VAG tut, nur freilich nicht auf die Versicherungswelt begrenzt.[166] Eine Strafbarkeit entfällt entsprechend auch, wenn die Offenbarung geheimer Personendaten durch ein berechtigtes privates Interesse gerechtfertigt ist bzw. ganz grundsätzlich, wenn die (übrigen) Bestimmungen des DSG eingehalten werden.[167] Angesichts der generell vage formulierten Datenschutzbestimmungen werden sich die Gerichte hier Zurückhaltung auferlegen.[168] Zum gleichen Ergebnis kommen auch Rosenthal/Gubler, wobei sie auch eine datenschutzrechtlich zulässige Bekanntgabe grundsätzlich der Strafbestimmung unterwerfen, dann aber erklären, dass in den allermeisten Fällen die datenschutzrechtlichen Rechtfertigungsgründe das berechtigte Vertrauen der betroffenen Person in die Geheimhaltung einschränken würden.[169] In der Tat darf bspw. ein Geschädigter, der Gesundheitsdaten der Haftpflichtversicherung des haftpflichtigen Unfallverursachers übermittelt, nicht erwarten, dass die Haftpflichtversicherung diese Daten niemandem bekanntgibt. Vielmehr kann die Haftpflichtversicherung solche Gesundheitsdaten bspw. ihrem Anwalt bekanntgeben und auch im Rahmen von Regressen nutzen, indem sie die Gesundheitsdaten regressierenden Sozialversicherern bekanntgibt oder einem Mithaftpflichtigen, auf welchen die Haftpflichtversicherung Regress nehmen möchte. Hier hat der Haftpflichtversicherer ein berechtigtes privates Interesse an der Bekanntgabe der Personendaten und die betroffene Person, welche ja um die Sozialversicherer und die anderen Mithaftpflichtigen weiss, muss davon ausgehen, dass diesen die Personendaten bekanntgeben werden könnten, so dass sie nicht davon ausgehen durfte, die Personendaten würden diesbezüglich geheim gehalten.

Ferner können Verantwortliche generell die Geheimhaltungserwartung steuern, indem sie bspw. vertraglich die Geheimhaltung ausschliessen oder beschränken und in dem sie in der Datenschutzerklärung darauf hinweisen, an welche Kategorien von Empfängern die Daten bekanntgeben werden.[170] Auf letztere Weise ist unseres Erachtens grundsätzlich auch eine Bekanntgabe von Gesundheitsdaten der Geschädigten vom Erst- an den Rückversicherer zulässig.

Ebenfalls zulässig muss es im öffentlichen Interesse sein, dass Mitarbeiter einer Versicherung bei Verdacht auf Versicherungsbetrug Strafanzeige erstatten oder in einem Gerichtsfall als Zeugen aussagen.[171] Unzulässig wäre es hingegen, Personendaten des Geschädigten an die Marketing-Abteilung des Versicherers weiterzugeben.[172]

C. Versicherbarkeit datenschutzrechtlicher Bussen

Für Unternehmen und Führungspersonen stellt sich die Frage, ob sie diese vorgenannten Risiken bzw. Bussen versichern können. Denkbar wäre es, diese im Rahmen einer Cyberversicherung, die sowohl den Eigenschaden des Versicherten wie auch Haftpflichtansprüche Dritter (wie der betroffenen Person) decken kann,[173] zu tun.

163 Art. 62 DSG.

164 § 321 des österreichischen Bundesgesetzes über den Betrieb und die Beaufsichtigung der Vertragsversicherung (Versicherungsaufsichtsgesetz 2016 – VAG 2016).

165 Felix Hörlsberger/Sarah Pichler, Der Geheimnisschutz nach § 321 VAG 2016 im Lichte der DSGVO, ZVers 2020, 244.

166 In der Schweiz spielt es deshalb keine Rolle, dass der externe Dienstleister nicht explizit erwähnt werden (s. dazu Hörlsberger/Pichler [FN 165], 244).

167 S.a. Hörlsberger/Pichler (FN 165), 249.

168 U.a. auch weil die Verletzung der Schweigepflicht nur bei vorsätzlicher Begehung strafbar ist (Art. 62 DSG). Der Eventualvorsatz muss diesbezüglich besonders zurückhaltend angenommen werden, da es teilweise gar möglich ist, 100 % DSG-konform aufgestellt zu sein und man insb. auch gar nicht weiss, was denn genau 100 % korrekt ist, so dass jeder, der geschäftlich tätig ist, letztlich eine DSG-Verletzung bis zu einem gewissen Grad in Kauf nimmt bzw. nehmen muss. Siehe dazu auch Rosenthal/Gubler (FN 162), 57.

169 Rosenthal/Gubler (FN 162), 61.

170 Rosenthal/Gubler (FN 162), 62 f.

171 Hörlsberger/Pichler (FN 165), 248.

172 Hörlsberger/Pichler (FN 165), 248 f.

173 Jacques de Werra/Yaniv Benhamou, Cyberassurance: instrument utile pour la cybersécurité des entreprises?, Jusletter vom 24. August 2020, 20–21.

In der Schweiz sind Bussen grundsätzlich nicht versicherbar, da dies nicht mit dem Zweck einer Busse vereinbar wäre. Bussen sind in der Schweiz höchstpersönlicher Natur und haben zum Zweck, den Verurteilten zu bestrafen, indem sie in dessen Vermögen eingreifen. Es geht darum, dem Gebüssten ein Übel zuzufügen, um sein Vergehen zu sühnen und ihn zu bessern.[174] Daraus ergibt sich, dass die Busse nicht gültig aus dem Vermögen eines Dritten getilgt werden kann und dass ein Dritter die Pflicht, die Busse zu bezahlen, nicht übernehmen kann. Ein Vertrag, in dem ein Dritter sich verpflichtet, die Busse zu bezahlen, ist somit widerrechtlich.[175] In einem Fall vor Bundesgericht ging es um einen Kunden, der eine Klage gegen eine Bank eingereicht hat, weil ein Angestellter dieser Bank die französischen Behörden über Steuerunregelmässigkeiten des Kunden informiert hatte, was eine Verletzung des Bankgeheimnisses darstellt. Der Kunde wollte, dass die Bank ihm Schadenersatz für die ihm verhängte Busse leiste. Das Bundesgericht betont, dass die Art der Geldbusse entscheidend ist. Soweit es sich um eine Busse mit Straffunktion handelt, kann diese nicht ersetzt werden.[176]

Ein Teil der Lehre nimmt eine Ausnahme an, wenn der Steuerpflichtige ohne eigenes Verschulden ein Delikt begeht, weil er von seinem Berater nicht richtig informiert worden ist.[177] In diesem Zusammenhang muss aber daran erinnert werden, dass jedenfalls in der Schweiz eine steuerrechtliche Busse sowieso nur verhängt werden kann, wenn dem Betroffenen eine Schuld zukommt (siehe Art. 175 DBG «vorsätzlich oder fahrlässig»). Deswegen hat das Bundesgericht diese Ausnahme nicht übernommen.[178]

Im Urteil 4A_21/2017 vom 29. Juni 2017 hat das Bundesgericht entschieden, dass eine Steuerbusse ausnahmsweise durch den Steuerberater repariert werden kann, wenn dieser durch seinen Fehler den Mandanten daran gehindert hat, durch eine rechtzeitige Selbstanzeige eine Reduzierung der Strafe zu erreichen. Dies ist jedoch nur denkbar, wenn der Steuerpflichtige ohne eigenes Verschulden bestraft wird.[179]

Auch im Schweizer DSG kommt Bussen eine Straffunktion zu. Deshalb ist es ausgeschlossen, das Risiko, mit einer Busse bestraft zu werden, zu versichern. Aus demselben Grund werden Bussen auch nicht von der Sozialhilfe übernommen[180] und können nicht von der Steuer als geschäftsmässig begründeter Aufwand abgezogen werden.[181] Ausserdem ist es auch nicht zulässig, für die Bezahlung von Bussen zu bürgen.[182] Strafrechtlich kann die Übernahme einer Busse u.U. auch eine Begünstigung im Sinne von Art. 305 StGB darstellen.

In der europäischen Union kann die Antwort auf die Frage, ob DSGVO-Bussen versicherbar sind, je nach Staat variieren.[183] Da es sich bei der DSGVO-Busse nur um eine administrative Busse handelt, es in vielen Fällen schlichtweg nicht möglich ist, die DSGVO vollständig einzuhalten und somit ohne Bussenrisiko tätig zu sein und die DSGVO-Bussen nach Schweizer Verständnis doch teilweise schwer verständliche Höhen annehmen, stellt sich die Frage, ob man die bisherige Praxis auch auf DSGVO-Bussen übertragen kann, oder ob ein Schweizer Unternehmen, welches auf dem EU-Markt tätig ist, sich nicht auch gegen das Risiko einer DSGVO-Busse versichern können sollte. Parallelen zur Exportrisikoversicherung liessen sich hier bspw. ziehen. Wenn man bedenkt, dass DSGVO-Bussen offenbar selbst in einigen EU/EWR-Staaten versicherbar sind,[184] dürfte dies auch politisch jedenfalls nicht komplett inopportun erscheinen. Mit einem höheren Selbstbehalt könnte man ferner dem Strafcharakter Rechnung tragen und nur jenen Teil der Busse versichern, der aus Schweizer Sicht nicht mehr verhältnismässig erschiene. Letztlich müssen wir uns hingegen doch fragen, ob wir unsere Massstäbe hier anwenden wollen oder ausländische Strafen nicht doch nur dann versichern wollen, wenn diese offen gegen Schweizer Wertvorstellungen (im Sinne eines Ordre Public) verstossen. Hier kann man bei der DSGVO doch festhalten, dass diese demokratisch (wenn auch freilich nicht im Sinne unserer Bundesverfassung) zustande gekommen ist, die Bussen soweit möglich nach objektiven Kriterien vergeben werden und in einem rechtstaatlichen Verfahren überprüfen werden können. So gewinnt man denn auch in der EU den Eindruck, dass Gerichte aktivistische Aufsichtsbehörden keineswegs immer schützen und gerade kleinere und mittlere Unternehmen durchaus auch mit der milde des Richters rechnen dürfen. Insoweit scheint die DSGVO den Schweizer Wertvorstellung nicht grundsätzlich zu widersprechen,

174 BGE 86 II 71 E. 4, siehe auch Arnaud Nussbaumer/Jean-René Oettli, Le recouvrement de l'amende pénale en droit civil, RSJ 113/2017, 176.

175 Art. 20 Abs. 1 OR. Siehe dazu auch Faure/Heine, The Insurance of Fines: The Case of Oil Pollution, The Geneva Papers on Risk and Insurance, Vol. 16, Nr. 58 (Januar 1991), 41 f.

176 BGE 115 II 72, E. 3c.

177 Thomas Koller, Schweizerisches Bundesgericht, I. zivilrechtliche Abteilung, 12.11.2007, Y. AG gegen AG (BGE 134 III 59; 4C.3/2007), AJP 2008, 1297.

178 siehe Art. 175 DBG «vorsätzlich oder fahrlässig»; BGE 134 III 59 E. 2.3.5; BGer 4A_491/2013 vom 6. Februar 2014 E. 2.4.2; Nussbaumer/Oettli (FN 174), 177.

179 BGer 4A_21/2017 vom 29. Juni 2017 E. 4.6 und die dort zitierten Referenzen.

180 Handbuch Berner Konferenz für Sozialhilfe, 2011.

181 BGE 143 II 8, E. 5.2.

182 BGE 86 II 71.

183 Aon/DLA Piper, The price of data security, A guide to the insurability of GDPR fines across Europe, 3. Edition, Mai 2020.

184 Aon/DLA Piper (FN 183), 13.

so dass wir eine Versicherung von DSGVO-Busse eher für problematisch erachten würden.

VII. Auftragsbearbeitung

A. Gesetzliche Regelung

Eine Auftragsbearbeitung liegt vor, wenn die Bearbeitung von Personendaten ausgelagert wird.[185] Die Auslagerung erfolgt juristisch gesehen an einen Dritten, d.h. eine Person, verschieden vom verantwortlichen Auslagernden und der betroffenen Person (um deren Personendaten es geht). Datenschutzrechtlich ist das Wort «Dritter» indes anderweitig besetzt, nämlich im Zusammenhang mit der Bekanntgabe von Personendaten an Dritte. Der **Auftragsbearbeiter** gilt – wie bereits dargelegt – aber in diesem Zusammenhang nicht als Dritter,[186] so dass diesem bei Einhaltung der entsprechenden Voraussetzungen auch besonders schützenswerte Personendaten bekannt gegeben werden dürfen, ohne dass eine Persönlichkeitsverletzung vorliegt. Immerhin gilt der Auftragsbearbeiter aber als Empfänger,[187] über welchen die betroffene Person informiert werden muss.[188] Die Arbeitnehmer gelten weder als Empfänger noch als Dritte und auch nicht als Auftragsbearbeiter. Die Arbeitnehmer sind in die Hierarchie des Arbeitgebers eingebunden, so dass es nicht notwendig erscheint, durch einen Auftragsbearbeitungsvertrag (oder in der EU: Auftragsdatenverarbeitungsvertrag, kurz ADV oder AVV) die korrekte Bearbeitung der Personendaten und deren Kontrolle sicherzustellen.[189] Die Idee bei der Auftragsbearbeitung liegt darin, dass der Verantwortliche für die Bearbeitung der Personendaten verantwortlich bleibt und er diese Verantwortung auch wahrnimmt. Zugleich ist auch nicht jeder Auftragnehmer gleich ein Auftragsbearbeiter im Sinne des Datenschutzes. Damit das Merkmal «Bearbeitung von Personendaten» nicht zur Bedeutungslosigkeit verkommt, muss vielmehr der Schwerpunkt oder jedenfalls ein massgeblicher Teil des Auftrags die Bearbeitung von Personendaten umfassen.[190] Keine Bearbeitung durch einen Auftragsbearbeiter liegt insb. bei einer Funktionsübertragung vor.[191] Bei dieser übernimmt der Dritte die Aufgabe in Eigenverantwortung, was beispielsweise der Fall ist, wenn der Hausarzt den Patienten und somit auch die Verarbeitung seiner Daten an einen Spezialisten überweist.[192] Wie oben schon erwähnt ist ein Anwalt, der Personendaten im Rahmen eines Mandats bearbeitet, etwa um eine Prozessstrategie festzulegen, kein Auftragsbearbeiter, sondern ein Verantwortlicher.[193] Um festzulegen, ob ein Dienstleistungserbringer ein Auftragsbearbeiter ist, müssen mehrere Kriterien beigezogen werden, insbesondere wie autonom der Anbieter bei der Ausführung seiner Leistung ist, wie stark der Kunde (Verantwortlicher) die Leistung kontrolliert/beaufsichtigt, und ob der Dienstleister über Fachwissen verfügt.[194]

Ist der Auftragnehmer kein Auftragsbearbeiter, gilt er grundsätzlich als **Verantwortlicher**. Verantwortlicher ist, wer allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.[195] Dazu weiter unten mehr.

Für die sog. **gemeinsame Verantwortlichkeit**, d.h. wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, gibt es in der Schweiz gesetzlich nur die Regelung, dass die betroffene Person ein Auskunftsbegehren bei jedem Verantwortlichen geltend machen kann.[196] Mit der Regelung der gemeinsamen Verantwortlichkeit will man verhindern, dass die betroffene Person durch die Kooperation mehrerer Verantwortlicher Nachteile erleidet. Es geht darum, eine klare Zuteilung von Verantwortlichkeit und Haftung zu schaffen.[197] Sind diese Voraussetzungen erfüllt, ist nicht einzusehen, weshalb man in der Schweiz den Weg der EU einschlagen und seitenlange Verträge über die gemeinsame Verantwortlichkeit aufsetzen sollte. In der Praxis kriegt man bisweilen den Eindruck, dass Juristen die gemeinsame Verantwortlichkeit immer dann annehmen, wenn ihnen neue (manchmal auch alte) Technologien zu komplex sind, während Informatiker kaum je gemeinsame Verantwortung erkennen, lassen sich die Zugriffsrechte und Datenflüsse bis ins Details regeln, trennen und Verantwortlichkeiten zuweisen. Trotzdem gibt es Situationen, in denen mehrere für eine Bearbeitung von Personendaten verantwortlich sind. Als Praktiker sollte man diese Situationen indes als Ausnahme betrachten.

185 In der Schweiz ist die Auftragsbearbeitung in Art. 9 DSG geregelt; in der EU in Art. 28 DSGVO.

186 Rosenthal (FN 44), 24.

187 Rosenthal (FN 44), 24.

188 Art. 19 Abs. 2 lit. c DSG.

189 Art. 29n DSGVO; David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, Jusletter 17. Juni 2019, 43.

190 Zur sog. Schwerpunkttheorie bspw. Vasella, EDÖB (FN 19); Bayerisches Landesamt für Datenschutzaufsicht, FAQ Abgrenzung Auftragsverarbeitung, 20.07.2018.

191 Ursula Uttinger/Thomas Geiser, Das neue Datenschutzrecht, Basel 2023, 39 N 2.70.

192 Uttinger/Geiser (FN 44), 39 N 2.70.

193 Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen (DSG), Orell Füssli Kommentar, Adrian Bieri/Julian Powell, Zürich 2023, Art. 5 Bst. J N 17–18; Commentaire romand LPD (Philippe Meier/Sylvain Métille), Basel 2023, Art. 5 N 118 und Art. 9 N 33; Rosenthal, Controller (FN 189), Anhang.

194 Commission nationale Informatique & Libertés (CNIL), Règlement européen sur la protection des données personnelles, Guide du sous-traitant, September 2017, 3.

195 Art. 5 lit. j DSG.

196 Art. 17 Abs. 1 DSV. In der EU ist die gemeinsame Verantwortlichkeit detaillierter geregelt (Art. 26 DSGVO) und der EUGH legt den Anwendungsbereich der gemeinsamen Verantwortlichkeit weit aus (s. bspw. Datenschutz-Guru, Newsletter vom 17.01.2025).

197 Der Bayerische Landesbeauftragte für den Datenschutz, Gemeinsame Verantwortlichkeit – Orientierungshilfe, 1. Juni 2024, 9.

B. Im Versicherungsbereich

Als 2018 die EU-DSGVO in Kraft trat, wurden unzählige ADVs, Data Processing Agreements oder wie sie auch immer hiessen, verschickt. Der Autor kann sich bspw. an eine längere Telefonkonferenz mit dem Rechtsteam eines *Managing General Agent (MGA)* erinnern, dem erklärt werden musste, dass der Versicherer nicht der Auftragsbearbeiter des *MGA* ist. Vielmehr ist der Versicherer als solcher immer Verantwortlicher.[198] Auch im Rahmen eines *Fronting* oder einer Mitversicherung ist der Versicherer eigenständiger Verantwortlicher. Genau gleich verhält es sich beim Rückversicherer. Auch der *Managing General Agent*, der Vermittler[199] (in der Regel auch der gebundene) und der Assekuradeur[200] sind in aller Regel als eigenständige Verantwortliche zu betrachten. Rosenthal schränkt dies indes ein, indem er den unabhängigen Makler (wohl den ungebundenen) zwar als eigenständigen Verantwortlichen qualifiziert, aber einschränkt, dass der Makler dann zum Auftragsbearbeiter werde, wenn er gewisse Arbeiten im Rahmen der Abwicklung der Versicherverträge für die Versicherung übernehmen und diese ihm auch Weisungen betreffend die Datenbearbeitung erteilt, welche ihm keine Autonomie mehr belässt.[201] Dies mag in gewissen Fällen zutreffen, wobei man unseres Erachtens den Einzelfall betrachten und sich überlegen muss, was für den Persönlichkeitsschutz der betroffenen Person oder die Datenbearbeitung für den Versicherer bzw. Vermittler gewonnen wird, wenn eine Aufteilung zwischen Vermittler als eigenständiger Verantwortlicher einerseits und Auftragsbearbeiter des Versicherers andererseits vorgenommen wird. Im Zweifelsfalle ist der Vermittler nur eigenständiger Verantwortlicher.

Als Beispiel für die Auftragsbearbeitung nennen die Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft bspw. «elektronische Datenverarbeitung, Scannen und Zuordnung von Eingangspost, Adressverwaltung, Antrags- und Vertragsbearbeitung, Schaden- und Leistungsbearbeitung, Sicherstellung der korrekten Verbuchung von Zahlungseingängen, Zahlungsausgang, Entsorgung von Dokumenten».[202] Soweit die vorstehenden Tätigkeiten von Mitarbeitern des Verantwortlichen ausgeführt werden, liegt keine Auftragsbearbeitung vor. Auch ist unseres Erachtens das blosse Verbuchen von Zahlungsvorgängen keine Auftragsbearbeitung, da hier das Bearbeiten von Personendaten i.d.R. nur untergeordneten Charakter hat.

C. In der beruflichen Vorsorge

Im Bereich der beruflichen Vorsorge (zweite Säule) kommt es vor, dass Vorsorgeeinrichtungen einen Teil oder die Gesamtheit des operativen Geschäftsbetriebs an eine externe Gesellschaft übertragen.[203] In diesem Zusammenhang stellt sich die Frage, ob diese externen Dienstleister Auftragsbearbeiter oder Verantwortliche der Datenbearbeitung sind. Diese Frage wird in der Lehre und Praxis kontrovers diskutiert.

Der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte führt aus, dass solche externe Servicegesellschaften je nach Konstellation entweder als Auftragsbearbeiterinnen oder als Verantwortliche auftreten können. Wenn nur bestimmte operative Tätigkeiten übertragen werden und die Vorsorgeeinrichtung massgeblich in den Prozess eingebunden ist, handle es sich eher um Auftragsbearbeitung. Bei Konstellationen, in denen die Übertragung umfassender sei und nicht nur einzelne Operationen ergreife, sondern die autonome Erfüllung von Aufgaben der beruflichen Vorsorge betreffe, könne die Dienstleistungsgesellschaft eine Verantwortliche darstellen. Dies sei insbesondere der Fall, wenn die Dienstleistungsgesellschaft die Geschäftsführung der Vorsorgeeinrichtung übernehme. Auch bei der Übertragung spezifischer Aufgaben der Vorsorgeeinrichtung könne die Dienstleistungsgesellschaft eine Verantwortliche sein, wenn sie sich beispielsweise um die Beziehung zu den Versicherten kümmere und in diesem Rahmen selbstständig Entscheidungen treffe. Somit müssen in diesem Zusammenhang stets die vereinbarten vertraglichen Verhältnisse hinsichtlich der Aufgabenteilung sowie die konkreten Umstände berücksichtigt werden.[204] Dies bedeutet, dass ein gewisser Spielraum bestehen bleibt, da die Rollen von der Vertragsgestaltung abhängen.[205]

198 Rosenthal, Controller (FN 189), Anhang.

199 Fachverband Versicherungsmakler und Berater in Versicherungsangelegenheiten, Verhaltensregeln gem. Artikel 40 EU-Datenschutz-Grundverordnung für Versicherungsmakler und Berater in Versicherungsangelegenheiten, Stand: August 2021, 4. In diesem Sinne wohl auch die Definition des Begriffs «Vermittler» auf S. 4 der Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft, Stand 29.6.2018.

200 Svenja Richartz/Sebastian Hons/Markus Willmann, Datenschutzrechtliche Verantwortung zwischen Assekuradeur und Versicherer im Lichte der aktuellen EuGH-Rechtsprechung, Zeitschrift für Versicherungswesen, Hamburg 2019, 697 ff.

201 Rosenthal, Controller (FN 189), Anhang.

202 Art. 21 Abs. 1 der Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft, Stand 29.6.2018.

203 Fragen zum Datenschutz, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Internet: https://www.edoeb.admin.ch/edoeb/de/home/deredoeb/kontakt/faq_beratung1.html#-273019898 (Abruf 9.10.2025).

204 Fragen zum Datenschutz (FN 203).

205 David Vasella, EDÖB: Geschäftsführerinnen von Vorsorgeeinrichtungen nicht immer Auftragsbearbeiterinnen, 11. Dezember 2024, Internet: https://datenrecht.ch/edoeb-geschaeftsfuehrerinnen-von-vorsorgeeinrichtungen-nicht-immer-auftragsbearbeiterinnen/ (Abruf 9.10.2025).

Rosenthal geht davon aus, dass die Dienstleistungsgesellschaft zur Verantwortlichen wird, da sie in der Regel allein festlegt, wie die Personendaten verarbeitet werden. Die Stiftung demgegenüber würde (und dürfe) in aller Regel keine Personendaten bearbeiten und lege auch nicht fest, welche Datenbearbeitungen stattfänden.[206] Dies trifft unseres Erachtens nicht zu. Der Schweizerische Pensionskassenverband geht davon aus, dass bei der Auslagerung der Verwaltung an einen Dritten, die Verwaltung als Auftragsbearbeiterin zu qualifizieren sei.[207] Implizit scheinen Schilter/Caveng diese Annahme zu teilen, indem sie sämtliche Pflichten der Vorsorgeeinrichtung als Verantwortliche zuschreiben. [208]

Sieht ein Gesetz die Bearbeitung zu einem bestimmten Zweck vor, so ist normalerweise derjenige Verantwortlicher, der nach dem Gesetz die öffentliche Aufgabe wahrzunehmen hat.[209] Das BVG sieht in erster Linie die Vorsorgeeinrichtung in der Verantwortung.[210]

In der Praxis kann ferner davon ausgegangen werden, dass bestimmte Bearbeitungen naturgemäss mit der Rolle einer Person verknüpft sind, so dass daraus auch auf die Verantwortlichkeiten geschlossen werden kann. Vorliegend dürfte naturgemäss die Vorsorgeeinrichtung als Verantwortliche für die Personendaten ihrer Versicherten gelten. Zum selben Resultat müsste eigentlich auch Rosenthal kommen, indem er rät, auf das Bauchgefühl zu hören und fragt, wen die betroffenen Personen am ehesten als für die inhaltlich korrekte Behandlung ihrer Daten verantwortlich ansehen würden.[211] Hier dürfte die Antwort klar sein: die Vorsorgeeinrichtung. Es ist nämlich sie, die entscheidet, überhaupt an der Durchführung der obligatorischen Versicherung teilzunehmen. Darüber hinaus gewährt das Gesetz der Pensionskasse explizit Freiheiten in der Ausgestaltung ihrer Organisation.[212]

Im Bereich der obligatorischen beruflichen Vorsorge gilt die Vorsorgeeinrichtung als Bundesorgan.[213] Sie bedarf für jede Datenbearbeitung einer gesetzlichen Grundlage.[214] Die Datenbearbeitung ist alsdann auch an den vom Gesetz vorgesehenen Zweck gebunden.[215] Im überobligatorischen Bereich wird der Umfang der notwendigen Datenbearbeitung durch die Vorsorgeeinrichtung, insbesondere durch das von ihr erlassene Reglement bestimmt.[216] Selbst bei vollständiger Delegation der Geschäftsführung bestimmt damit die Vorsorgeeinrichtung bzw. das auf die Tätigkeit der Vorsorgeeinrichtung anwendbare Gesetz, welche Personendaten zu bearbeiten sind.

Die Tatsache, dass der Geschäftsführer selbst auch Entscheidungen über die Bearbeitung von Personendaten trifft, schliesst dieses Fazit nicht aus.[217] Entscheidungen über den Zweck der Bearbeitung sind immer Sache des Verantwortlichen,[218] aber der Auftragsbearbeiter kann bei der Festlegung der Mittel über einen Handlungspeilraum verfügen.[219] Der Verantwortliche muss jedoch über die wesentlichen Mittel entscheiden, d.h. über die Art der bearbeiteten Daten («welche Daten werden bearbeitet?»), die Dauer der Bearbeitung, die Kategorien von Empfängern und von betroffenen Personen. Der Auftragsbearbeiter kann demgegenüber über die praktischen Mittel der Umsetzung wie bspw. die Wahl von Soft- oder Hardware oder die detaillierten Sicherheitsmassnahmen entscheiden.[220]

Auch Rosenthal erachtet es als ausreichend, wenn der Verantwortliche den Rahmen vorgibt, den der Auftragsbearbeiter dann mit seinem Fachwissen und der Nähe zur Sache ausfüllen kann. Steckt der Kunde den Rahmen in Bezug auf die wesentlichen Parameter (welche Kategorien von Personendaten, wo sie beschafft werden und wem sie weitergegeben werden etc.) auch nur abstrakt ab oder gibt er dem Dienstleister einen Zweck vor, aus dem sich die Parameter ergeben (bspw. Einhaltung einer bestimmten Gesetzesnorm, die die Datenbearbeitung definiert), so bleibt der Kunde allein verantwortlich.[221]

Da die Vorsorgeeinrichtung bzw. die auf sie anwendbaren gesetzlichen Bestimmungen den Zweck und die zu bearbeitenden Personendaten festlegen, gilt unseres Erachtens die Vorsorgeeinrichtung als Verantwortliche der Datenverarbeitung und der Geschäftsführer bzw. die Servicegesellschaft als deren Auftragsbearbeiter.

Ferner führt Rosenthal jedenfalls etwas zu pauschal aus, dass soweit die Servicegesellschaft Aufgaben an

206 David Rosenthal, Pensionskassen: Diese DSG-Sonderpflichten gelten für sie, Internet: https://www.vischer.com/know-how/blog/pensionskassen-diese-dsg-sonderpflichten-gelten-fuer-sie-40126/ (Abruf 9.10.2025); David Rosenthal/Barbara Epprecht, Banken und ihre datenschutzrechtliche Verantwortlichkeit im Verkehr mit ihren Dienstleistern, in: Susan Emmenegger (Hrsg.), Banken und Datenschutz, Basel 2019, 154; Rosenthal, Controller (FN 189), Anhang.

207 Schweizer Pensionskassenverband, ASIP, Fachmitteilung Nr. 131 vom 20. Oktober 2022, Ziffer 2.1.

208 Evelyn Schilter/Estelle Caveng, Neues Datenschutzgesetz – Auswirkungen auf Vorsorgeeinrichtungen, Schweizer Personalvorsorge, 04–21, 102–103.

209 European Data Protection Board (EDPB), Leitlinien zu den Begriffen «Verantwortlicher» und «Auftragsverarbeiter» in der DSGVO, Version 2.0 vom 7. Juli 2021, N 24.

210 Art. 48 ff. BVG.

211 Rosenthal, Controller (FN 189), 48.

212 Art. 49 Abs. 1 BVG.

213 ASIP Fachmitteilung Nr. 91, 2.

214 Art. 34 DSG.

215 Art. 6 Abs. 3 DSG.

216 S.a. BGE 129 III 305 E. 2.2 f.

217 European Data Protection Board (EDPB), Leitlinien (FN 209), N 37.

218 EDPB, N 39.

219 EDPB, N 37.

220 EDPB, N 40.

221 Rosenthal, Controller (FN 189), 21.

eine Rückversicherung oder einen Broker delegiert, diese Auftragsbearbeiter seien. Richtigerweise ergänzt er, dass die Rückersicherung, soweit sie Rückversicherungsleistung (im Rahmen der beruflichen Vorsorge eigentlich eine Erstversicherungsleistung) anbietet, eine eigenständige Verantwortliche sei.[222] Hier wäre es einfacher und auch praxisnäher, jedenfalls den Rückversicherer, der in der beruflichen Vorsorge durchaus auch weitere Leistungen als nur die Versicherungsdeckung erbringt, grundsätzlich als eigenständigen Verantwortlichen zu qualifizieren und nicht unnötig kompliziert zwischen einer Leistung als Verantwortlicher und einer solchen als Auftragsbearbeiter zu unterscheiden.

VIII. Fazit

Das Datenschutzrecht ist eines von vielen Rechtsgebieten im rasant wachsenden *Compliance & Regulatory*-Bereich. Die schiere Menge derartiger Vorschriften, die überdies in jedem Land anders gelebt werden bzw. ausserhalb Europas auch einmal komplett anders verstanden werden, stellen für weltweit tätige Unternehmen eine grosse Herausforderung dar, für Startups eine schiere Unmöglichkeit. Der Gesetzgeber, der zusammen mit der Verwaltung diese Vorschriften initiiert, hat demgegenüber keinerlei Compliance-Anforderungen zu erfüllen; politische Vorstösse können noch so unsinnig sein und Gesetze handwerklich noch so ungenügend. Im Datenschutzrecht zeigen die wenigen Gerichtsentscheide, dass die Richter mit dieser Ausgangslage sehr wohl umgehen können; so etwa wenn das Bundesgericht das Auskunftsrecht einschränkt und sich das Genfer Gericht letztlich weigert, Bussen gestützt auf vage Vorschriften zu verteilen. Wenn man die gesetzliche Handlungsanweisung und das Verbot gar nicht ausreichend konkret erkennen kann oder man diese Anweisung, weil lebensfremd, gar nicht einhalten kann und man hierfür auch noch gebüsst werden könnte, dann wäre es letztlich reine Willkür, wer gebüsst wird und wer nicht. Man wünschte, dass nicht nur die Gerichte auf dem Boden unseres Rechtsstaates bleiben und ein gesundes Augenmass walten lassen, denn die meisten Rechtsunterworfenen verspüren wenig Lust, für viel Geld über Jahre zu prozessieren, um von einem Gericht dann hoffentlich einen vernünftigen Entscheid zu bekommen. Vielmehr sind bereits die Behörden aufgerufen, die umfangreichen, teils vagen Gesetze so anzuwenden, dass dem eigentlichen Anliegen zum Durchbruch verholfen wird und sich nicht in Formalien zu verlieren und eine weitere Flut von Verordnungen, Rundschreiben, Weisungen oder Merkblättern zu produzieren. Im Datenschutz bedeutet dies, dass die Persönlichkeit der betroffenen Person geschützt werden soll und die Verantwortlichen hierzu risikoangemessene Vorkehrungen zu treffen haben. Zentrale Punkte sind hier, dass sich der Verantwortliche seiner Datenbearbeitungen bewusst wird, bspw. in dem er ein Bearbeitungsverzeichnis führt, er anschliessend die betroffene Person darüber informiert und sich darum kümmert, dass die Daten sicher bearbeitet werden.

[222] Rosenthal, Controller (FN 189), Anhang.