Secur-Data Betriebsberatungs-Ges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at
Offenlegung gem. MedienG: www.secur-data.at/impressum

DSG-Info-Service

März 2020 Ausgabe Nr. 93

Sehr geehrter DSG-Paket-Kunde!
Sehr geehrter Leser!

Es freut uns, Sie wieder über Datenschutz- und IT-Fragen informieren zu dürfen und Ihnen die aktuellen Ereignisse aus der Datenschutz- und Informationssicherheitswelt präsentieren zu können.

Unser Newsletter umfasst eine Zusammenfassung der aktuellen Urteile, Nachrichten und Tipps mit den Schwerpunkten IT-Security und Datensicherheit.

Viel Spaß beim Lesen!

1. Die dritthöchste DSGVO-Strafe Europas kommt aus Österreich – Quo Vadis DSB?

Man könnte meinen, die österreichische Datenschutzbehörde habe ein gesundes Verhältnis zu „Beraten statt Strafen" entwickelt. Aus der Feder der Datenschutzbehörde entstanden mittlerweile 75 veröffentlichte und weitaus mehr unveröffentlichte Entscheidungen, die sich immer mehr zu einem Gesamtbild fügen. Mit der Strafe gegen die Österreichische Post AG in Höhe von EUR 18 Mio hat sie es zudem geschafft, das dritthöchste Bußgeld[1] in ganz Europa zu vergeben. In Frankreich wurde Google Inc. höher bestraft und in Italien die Telecom Italia. Die scheidende britische Behörde hat gegen British Airways und Marriott die dreistelligen Millionenstrafen lediglich in Aussicht gestellt.

Dabei zeigt sich, dass die Datenschutzbehörde insbesondere in der Strafpolitik durchaus mit Augenmaß vorgeht. Der Sachverhalt im Post-Verfahren ist mittlerweile weithin bekannt und betrifft im Wesentlichen die Verarbeitung von besonderen personenbezogenen Daten (die politische Zugehörigkeit bzw. Affinität) ohne ausreichende Rechtsgrundlage. Es ist das erste Millionenbußgeld, das die österreichische DSB verhängt hat. Bereits zuvor wurde aber schon die *„Allergie Tagesklinik*[2]" mit einem Bußgeld von EUR 50.000 belegt und auch ein

[1] https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020

[2] Allergie-Tagesklinik, DSB 16.11.2018, DSB-D213.692/0001-DSB/2018

Fußballtrainer[3], der seine weiblichen Schützlinge unter der Dusche filmte, wurde mit einer Strafe von EUR 10.000 versehen.

Alle diese Bußgeldentscheidungen sind zum gegenwärtigen Zeitpunkt noch nicht rechtskräftig und werden vor dem Bundesverwaltungsgericht bekämpft. Dazu gehört auch die allererste Strafentscheidung, die überhaupt unter Anwendung der DSGVO verhängt wurde. Das Bußgeld, das einem Glücksspielbetreiber für seine unzulässige Videoüberwachungsanlage auferlegt wurde, war die erste Geldstrafe einer DSB nach DSGVO in ganz Europa.

Dieser Bußgeldbescheid wird derzeit sogar schon vor dem Verwaltungsgerichtshof (VwGH) verhandelt, nachdem er vom Bundesverwaltungsgericht wegen eines Formfehlers aufgehoben wurde. Bemängelt wurde, dass das Bußgeld direkt an die juristische Person als Betreiber ausgestellt wurde, ohne ein „menschliches Handeln", also die Person, die für die Videoüberwachung konkret verantwortlich war, zu nennen. Darin sieht das Bundesverwaltungsgericht einen Verstoß gegen das Bestimmtheitsgebot: Eine handelnde Person, die für eine juristische Person tätig wird, muss eine Verletzung begangen haben, da die juristische Person nicht eigenständig Verstöße begehen kann. Die Datenschutzbehörde habe aber verabsäumt, einen „Schädiger" zu benennen und die Strafe direkt gegenüber der juristischen Person ausgesprochen. Zur Klärung dieser wichtigen Rechtsfrage ist die ordentliche Revision an den Verwaltungsgerichtshof zugelassen und wird für alle Organisationen relevant sein, deren Mitarbeiter an Verstößen unmittelbar beteiligt sind.

Zu hoffen ist, dass die DSB in Zukunft wieder verstärkt Entscheidungen veröffentlichen wird. Die Bescheide bringen einerseits wichtige Klarstellungen in Auslegungsfragen und zudem gelegentliche Einblicke in die Behördensicht, die für alle Verantwortlichen von großer Wichtigkeit sein können.

2. OLG Innsbruck: kein immaterieller Schadenersatz im Post-Verfahren

Aus der Welt der ordentlichen Gerichte gibt es das Urteil[4] des Oberlandesgerichts Innsbruck zu berichten. In diesem wurde die Frage nach immateriellem Schadenersatz für Verletzungen des Datenschutzes verneint, da die betroffene Person nicht nachweisen konnte, dass es zu einer „erheblichen" Beeinträchtigung gekommen ist.

Damit ist das ursprüngliche Urteil des LG Feldkirch, das einen Schadenersatz in Höhe von EUR 800,00 zuerkannt hatte, gekippt worden. Eine Revision an den OGH ist nicht zugelassen. So bleibt einmal mehr die Frage offen, wie ein Schaden aus einer unzulässigen Datenverarbeitung, ob materieller oder immaterieller Natur, überhaupt nachgewiesen werden kann.

Das Volltext-Urteil wurde hier[5] zur Verfügung gestellt und ist noch nicht im RIS abrufbar.

[3] Fußballtrainer https://www.derstandard.at/story/2000107377808/fussballerinnen-nackt-gefilmt-mostviertler-trainer-muss-strafe-zahlen

[4] OLG Innsbruck - 13.02.2020, 1 R 182/19b

[5] https://www.dataprotect.at/app/download/13324526536/Berufungsentscheidung+OLG+Innsbruck+Post+anonymisiert.pdf?t=1583665309

3. OGH bestätigt Rechtsprechungslinie zu Koppelungsverbot

Eine Verbandsklage gegen einen Vermittler von Hotelgutscheinen für auslastungsärmere Zeiten führte zur Prüfung verschiedener Klauseln, die unter anderem ebenfalls das datenschutzrechtliche Koppelungsverbot betrafen.

Die beanstandete Klausel 9, eingebettet in die AGB des Gutscheinvermittlers, beinhaltete eine Einwilligung im Voraus für den Newsletterversand etwaiger Partnerunternehmen. Zu diesem Zweck würden Name und E-Mail-Adresse der betroffenen Person, die im Rahmen der Vertragsanbahnung erhoben wurden, weitergeleitet. Die Verbandsklage betraf unter anderem auch die unzulässige Koppelung der Einwilligung zur Datenverarbeitung mit dem Vertragsabschluss. Betroffenen Personen war es nur nachträglich möglich, den Newsletterversand abzubestellen und ihre Einwilligung zu widerrufen.

Der OGH gab dem klagenden Verband Recht und stellte die Unzulässigkeit der Klausel fest. Der Senat bestätigte die in der ausführlichen Auseinandersetzung der SimpliTV-Entscheidung[6] festgehaltenen strengen Voraussetzungen an die Freiwilligkeit einer Einwilligung. Im vorliegenden Fall lag durch die Bündelung von Einwilligung und AGB ohne separate Auswahlmöglichkeit erneut eine Koppelung einer vertragsunabhängigen Datenverarbeitung an den Vertragsabschluss vor. Der OGH manifestiert somit, dass „grundsätzlich davon auszugehen [ist], dass die Erteilung der Einwilligung nicht freiwillig erfolgt, wenn nicht im Einzelfall besondere Umstände für eine Freiwilligkeit der datenschutzrechtlichen Einwilligung sprechen (6 Ob 140/18h = RS0132251)“. Diese besonderen Umstände des Einzelfalls lagen im vorliegenden Fall nicht vor. Der beklagte Gutscheinvermittler bestritt nicht, dass er nicht bereit war, ein Vertragsanbot der betroffenen Person anzunehmen, wenn die Klausel 10 (sic! vermutl. Klausel 9 gemeint) ausgeschlossen würde. Der OGH ließ auch das Argument, die Einwilligung könne nachträglich ohnehin widerrufen werden, nicht zu, da es keine Schlüsse auf die geforderte Freiwilligkeit zulässt.

Der OGH bestätigt damit erneut die strengen Anforderungen an die Freiwilligkeit, die an eine Einwilligung geknüpft sind. Die jederzeitige Widerrufbarkeit der erteilten Einwilligung ohne Angabe von Gründen lässt keine Schlüsse auf die Freiwilligkeit der Erteilung zu.

4. Data Breach-Modell der ENISA

Die Deutsche Datenschutzkonferenz (DSK) hat bereits ein Positionspapier vorgelegt (siehe DSG Info 92), nach dem die Bußgeldberechnung anhand unterschiedlicher Faktoren vorgenommen wird. Die österreichische Datenschutzbehörde könnte sich an einem ähnlichen Modell orientieren. Die European Union Agency for Cybersecurity (ENISA) hat ein öffentlich verfügbares „Data Breach Notification Tool“[7] entwickelt, das als Instrument zur Einstufung von Datenschutzverletzungen herangezogen werden kann. Daraus lässt sich auch ein Modell zur Bewertung des Schweregrads und damit einhergehend der Strafbemessung ableiten.

[6] OGH 31.8.2018, 6 Ob 140/18h

[7] https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches/personal-data-breach-notification-tool

Die Berechnung des „SE“ (*Severity* = Schwere)-Grades besteht aus der Gleichung:

SE = DPC x EI + CB

„DPC“ steht für das Umfeld und den Kontext der Datenschutzverletzung. Es geht dabei um die Einordnung der Datenverarbeitung, die bei besonderen Datenkategorien aus dem medizinischen Bereich anders ausfallen wird als bei Kontaktdaten einer Lieferantenliste.

„EI“ steht für die Möglichkeit der Identifikation betroffener Personen, also ob es sich um verknüpfte Datensätze handelt, die beispielsweise das Risiko des Identitätsdiebstahls nach sich ziehen.

„CB“ objektiviert die Umstände der Datenschutzverletzung, abhängig davon, ob es sich um eine vorsätzliche Tat oder ein Systemversagen ohne Absicht handelt.

Aus diesen Faktoren ergibt sich der SE-Wert, der in der unten angeführten Tabelle zu einer Bewertung der Meldepflicht führt. Anhand dieser Gleichung lässt sich aber nicht nur eine **Meldepflicht** konstruieren, sondern auch ein **Bewertungsmodell** für einen **Bußgeldkatalog**. Dies ist insbesondere im Hinblick auf das deutsche Modell relevant, das für eine objektivierbare und vor allem bezifferbare Schadensberechnung herangezogen werden kann.

Severity of a data breach		
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

Die gesamte Methodik ist frei auf der Website der ENISA verfügbar.

5. EuGH-Generalanwalt: Standardvertragsklauseln noch immer gültig

In der Rechtssache C-311/18 - Data Protection Commissioner /Facebook Ireland und Maximilian Schrems konnten schon viele grundsätzliche Erkenntnisse gewonnen worden. Sie führte unter anderem dazu, dass das ehem. Safe-Harbor Abkommen für die Übermittlung und Verarbeitung von Daten in den USA durch den sog. Privacy-Shield ersetzt wurde. Nun bringt die Rechtssache eine neue Facette in Bezug auf die Übermittlung von Daten hervor, bei der es um die Anwendbarkeit der „Standardvertragsklauseln“ geht. Nach

Meinung des Generalanwalts des Europäischen Gerichtshofes Henrik Saugmandsgaard Øe[8] kann weiterhin von der Gültigkeit der Standardvertragsklauseln[9] für die rechtskonforme Übermittlung von personenbezogenen Daten in ein Drittland ausgegangen werden.

Dies ist unter dem Gesichtspunkt der veränderten Rechtslage, insbesondere den Vorschriften des Art. 28 DSGVO zu sehen, der zum Teil neue oder strengere Anforderungen an Auftragsverarbeiter gestellt hatte, als dies in den Standardvertragsklauseln vorgesehen war. Standardvertragsklauseln wurden als verbindliches Rechtsdokument von der Europäischen Kommission erlassen und regeln die Rechtsbeziehung zwischen dem Verantwortlichen und einem anderen Verantwortlichen oder Auftragsverarbeiter in Bezug auf das Datenschutzniveau und den internationalen Datentransfer.

Obwohl sich der EuGH in seiner Entscheidung nicht an die Meinung des Generalanwalts halten muss, ist die Argumentation der fortlaufenden Gültigkeit der Standardvertragsklauseln nicht von der Hand zu weisen. Andernfalls wäre der internationale Datentransfer in Länder, für die kein sog. „Angemessenheitsbeschluss“[10] vorliegt, nicht mehr auf Grundlage der Standardvertragsklauseln möglich. Es müsste ggf. sogar auf die Einwilligung der Betroffenen zurückgegriffen werden, was keine zweckmäßige Lösung darstellen kann. Den ersten Angemessenheitsbeschluss seit Geltung der DSGVO wurde von der Kommission am 23. Jänner 2019 für Japan angenommen, weitere Länder sind unter anderem Kanada, Israel und die Schweiz.

6. Brexit

Die Frage der datenschutzrechtlichen Angemessenheit stellt sich insbesondere nach dem mit 31. Jänner 2020 vollzogenen **Brexit** für die Zeit nach Ende der Übergangsphase am 31. Dezember 2020. Laut Medienberichten[11] will sich Großbritannien nicht mehr der DSGVO unterwerfen und ein eigenes Datenschutzgesetz erlassen.

Eine abschließende Bewertung der Lage in Großbritannien ist derzeit noch nicht möglich, da noch nicht bekannt ist, welche Regelungen im Datenschutzbereich getroffen werden. Es steht jedoch fest, dass Großbritannien keine fortlaufende Geltung der DSGVO vorsieht, sodass durch das Ausscheiden des UK aus dem EWR eine Verarbeitungssituation in einem Drittland vorliegen wird. Weitere Informationen[12] werden laufend durch die britische Datenschutzbehörde ICO ergänzt.

---

[8] https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-12/cp190165de.pdf

[9] Beschluss 2010/87/EU der Europäischen Kommission vom 5. Februar 2010

[10] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[11] https://t3n.de/news/dsgvo-grossbritannien-nutzt-fuer-1250027/

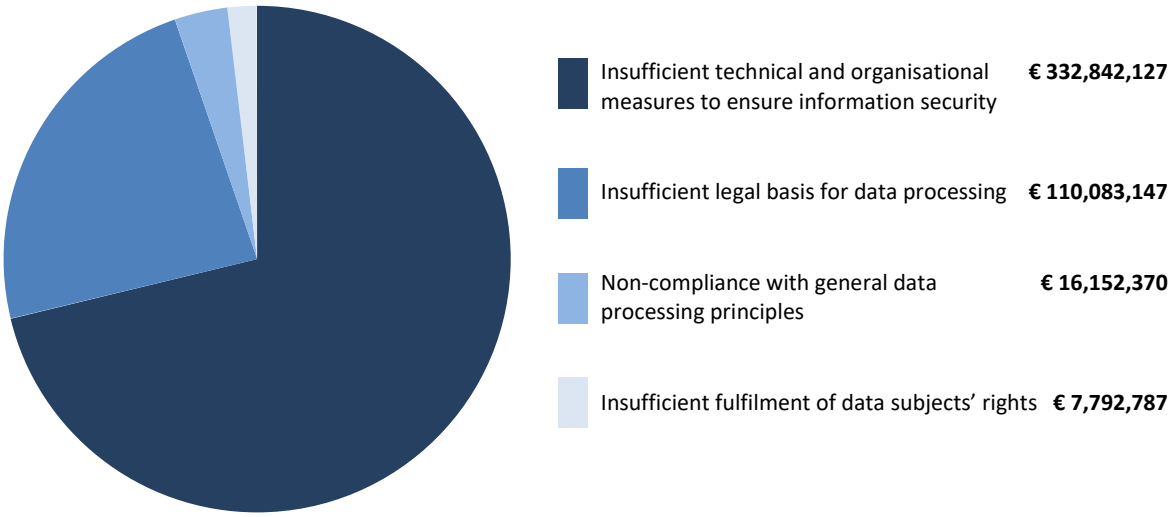
[12] https://ico.org.uk/media/for-organisations/documents/brexit/2617110/information-rights-and-brexit-faqs-v2_3.pdf

7. IT-Security Risiken erkennen und handeln

Das Thema IT-Security ist in aller Munde. Von allen Seiten werden Datensicherheitsvorfälle gemeldet, die nicht nur Unternehmen, sondern zunehmend die öffentliche Verwaltung betreffen.

In den Ausläufern der Weihnachtsfeiertage ist auch das Außenministerium Opfer eines „Cyberangriffes“[13] geworden. Unter dem Begriff „Cyberangriff“ kann eine Vielzahl von widerrechtlichen Eingriffen in ein geschlossenes System verstanden werden. Anhand der Medienberichte war nicht ersichtlich, was genau vorgefallen ist. Oftmals werden Datenschutz- und IT-Risiken unter dem Überbegriff „Cyberangriff“ zusammengefasst, es kommen aber verschiedenste Eingriffe und Verletzungen in Frage.

Die deutsche Stadt Potsdam[14] und das Kammergericht Berlin[15] wurden ebenfalls Opfer von IT-Sicherheitsvorfällen, die dazu geführt haben, dass die komplette Verwaltung offline genommen werden musste und bis dato unklar ist, ob nicht auch die Backups durch Schadsoftware infiziert wurden.



Quelle: https://enforcementtracker.com/?insights

Im Kontext der internationalen Entscheidungen ist auffällig, dass die „teuersten“ Strafen oftmals **Verstöße gegen Art. 32 DSGVO**, also die TOM, betreffen. Datenschutz und IT-Security sind parallel zu verstehen und bedingen sich gegenseitig. Das laufende Jahr sollte

[13] https://orf.at/stories/3149768/

[14] https://www.heise.de/newsticker/meldung/Moegliche-Cyberattacke-Stadt-Potsdam-nimmt-Server-der-Verwaltung-vom-Netz-4644047.html

[15] https://www.heise.de/security/meldung/Emotet-IT-Totalschaden-beim-Kammergericht-Berlin-4646568.html

daher genutzt werden, um das Unternehmen gegen Außen- und Innenangriffe durch angemessene technische und organisatorische Maßnahmen zu schützen.

Dazu genügen bereits einige grundsätzliche Maßnahmen, die große Wirkung zeigen können.

Oftmals sind es Mitarbeiter, die aufgrund fehlender Sensibilisierung unabsichtlich die Tür zur IT-Infrastruktur des Unternehmens öffnen. Zu diesem Bereich gehören insbesondere **Spam- und Phishing-Attacken**, die über E-Mails oder Links in Social-Media-Gruppen in das Unternehmen getragen werden. Um solche Gefahren einzudämmen, muss zusätzlich zu technischen Maßnahmen das Sicherheitsbewusstsein der Mitarbeiter durch regelmäßige Schulungen und aktuelle Informationen zu sicherheitsrelevanten Vorfällen gefördert werden.

Schulungen können auch dabei helfen, das Problem „**Social Engineering**" zu verdeutlichen und die Anfälligkeit von Mitarbeiterinnen, aber auch Führungskräften zu reduzieren. Im Wesentlichen kommt es darauf an, dass man auch abseits von Richtlinien und Dienstanweisungen darüber informiert, dass Informationen, Daten und vor allem Passwörter nicht an Fremde weitergegeben werden dürfen.

Weiters ist ein datenschutzkonformes **„Mobile Device** Management**"** ein gutes und häufig unerlässliches Werkzeug. Die Daten auf mobilen Endgeräten, wie z.B. Notebooks und Mobiltelefonen, die aus dem Verfügungsbereich des Unternehmens gelangt sind, können damit dem Zugriff unberechtigter Personen entzogen und der Datenabfluss unmöglich gemacht werden.

Eine der Kernmaßnahmen zum Schutz gegen Datenabfluss von Firmendaten ist die Verankerung einer **Verschlüsselungsstrategie** für das Speichern von Informationen auf Datenträgern und die Übertragung von Daten über öffentliche Netzwerke. In der deutschen Klinik Vivantes[16] wurden im Zuge eines Diebstahls auch 18.000 Datensätze von Patienten der Urologie gestohlen, wobei nicht klar ist, ob diese Gesundheitsdaten verschlüsselt gespeichert wurden.

Es ist daher darauf zu achten, dass das Thema „TOM" im Unternehmen gemeinsam mit dem Datenschutz behandelt wird und auch den Mitarbeitern zur Kenntnis gelangt, damit vermeidbare Daten- und Informationssicherheitsrisiken entschärft werden.

8. Whistleblowing-RL beschlossen – Umsetzungsfrist bis 2021

Die Richtlinie zum EU-weiten Schutz von Hinweisgebern[17] (auch „Whistleblower" genannt) wurde am 23. Oktober 2019 beschlossen und legt eine Umsetzungsfrist für Mitgliedsstaaten bis zum 17. Dezember 2021 fest. Unternehmen aus dem privaten Bereich sowie öffentliche Stellen müssen sich anschließend um die Einrichtung interner Meldekanäle kümmern, um die Meldewege für das Whistleblowing einheitlich zu regeln und Hinweisgeber vor Vergeltungsmaßnahmen zu schützen.

Die Whistleblowing-RL trifft Unternehmen mit mehr als 50 Mitarbeitern gleichermaßen wie öffentliche Stellen und Bund, Länder und Gemeinden. Die nationalen Gesetzgeber können dazu Ausnahmeregelungen oder Erweiterungen vorsehen, sodass abzuwarten bleibt, wie

[16] https://www.aerzteblatt.de/nachrichten/108969/Tausende-Datensaetze-von-Patienten-in-Berliner-Krankenhaus-gestohlen

[17] https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1582098953782&uri=CELEX:32019L1937

der österreichische Gesetzgeber hier vorgehen wird. Auf international tätige Unternehmen kommen dennoch Umsetzungsmaßnahmen zu, die es in Zukunft zu beachten gilt. Es ist jedoch abzuwarten, wie der österreichische Gesetzgeber vorgehen wird. Eine geplante Sensibilisierung von Führungskräften für das Thema kann die rechtliche Umsetzung jedoch unterstützen.

9. Strengstes Datenschutzgesetz der USA

Als Information am Rande sei angemerkt, dass die DSGVO von anderen Ländern auch als Positiv-Beispiel herangezogen wird. So hat der US-Bundesstaat Kalifornien ein neues Gesetz erlassen, das sich an den Grundsätzen der DSGVO orientiert. Es ist am 1. Jänner 2020 in Kraft getreten.

Was ist zu tun, wenn Sie Daten in die USA, insbesondere nach Kalifornien übermitteln oder von dort erhalten? Der California Consumer Privacy Act (CCPA)[18] ist nun das strengste Datenschutzgesetz der gesamten Vereinigten Staaten, räumlich ist er allerdings auf Kalifornien und sachlich auf Verbraucher und Unternehmen, die dort tätig sind, beschränkt. Unternehmen, die in den Anwendungsbereich des Gesetzes fallen, müssen jedoch einige Schwellenwerte erreichen. KMUs sind explizit ausgenommen, außer ihr Geschäftsfeld liegt zum überwiegenden Teil in der Verarbeitung personenbezogener Daten. Nachdem das Silicon Valley und andere Tech-Giganten in Kalifornien ansässig sind, werden die Normadressaten wohl nicht überraschen. Angesichts der Voraussetzungen würden die meisten europäischen Unternehmen von dem Gesetz nicht betroffen sein, die Vorbildwirkung der DSGVO ist aber eindeutig erkennbar.

[18] https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%280000002%29.pdf