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

DSG-Info-Service

Die Geburtstagsausgabe

Mai 2019 Ausgabe Nr. 91

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

Auch wenn die DSGVO zum Unwort des Jahres 2018 gekürt wurde, möchten wir den ersten Geburtstag zum Anlass nehmen, die aktuelle Entwicklung in Österreich und Europa Revue passieren zu lassen. Die österreichischen und europäischen Datenschutzbehörden haben bereits viele, teils spektakuläre Entscheidungen getroffen, die wir in dieser Ausgabe rekapitulieren wollen.

Unklarheiten über die Auslegung der DSGVO werden durch aufsichtsbehördliche Entscheidungen und Richtliniendokumente beständig weiter zurückgedrängt. Wir stellen die neuen Richtlinien des EPDB zu Online-Diensten sowie eine Entscheidung der österreichischen Datenschutzbehörde zu Werbe-E-Mails vor.

Schließlich berichten wir noch über die Whistleblowing-Richtlinie der EU, deren finaler Text bereits feststeht und die kurz vor der formalen Verabschiedung durch den EU-Rat steht.

1. Ein Jahr DSGVO – ein Grund zum Feiern?

Seit der Geltung der DSGVO ist es in Österreich bereits zu über 1.600[1] Beschwerdeverfahren (Stand 15. Jänner 2019) gekommen, die auch grenzüberschreitende Sachverhalte beinhalten. Zusätzlich hatte die Datenschutzbehörde bereits knapp 600 Meldungen über die Verletzung des Schutzes personenbezogener Daten (Data Breach) zu bearbeiten.

Es sind bereits zwei sog. „Codes of Conduct" genehmigt worden, die als Verhaltensregeln für bestimmte Branchen den Umgang mit personenbezogenen Daten regulieren. Die Datenschutzbehörde forciert die Erlassung von solchen Verhaltensregeln und teilt mit, dass sechs weitere Codes of Conduct bereits eingereicht wurden. Neben Verhaltensregeln liegt der Datenschutzbehörde auch ein Antrag für die Genehmigung sog. „Binding Corporate Rules – BCR" vor, die verbindliche interne Rechts-

[1] Quelle: DSB

vorschriften für ein Unternehmen bzw. einen Konzern darstellen.

Seit dem 25. Mai 2018 wurden 35 Entscheidungen der Datenschutzbehörde im Rechtsinformationssystem des Bundes (RIS) veröffentlicht. Eine Vielzahl von Erkenntnissen ist nicht öffentlich verfügbar. Die meisten Verfahren betrafen Sachverhalte, die sich noch vor der DSGVO zugetragen haben. Allmählich gelangen aber auch Fälle, die allein die DSGVO betreffen, zur Entscheidung. Auch das Bundesverwaltungsgericht als Gerichtshof erster Instanz hat bereits Verfahren entschieden.

Bußgelder wurden bis dato nur bei Sachverhalten in Verbindung mit Videoüberwachungen erteilt. Das schließt an die Spruchpraxis der Vergangenheit an.

Insgesamt ist davon auszugehen, dass die Schonfrist ein Ende findet und die Datenschutzbehörde nun verstärkt eingreifen wird.

2. Internationale Bußgelder

Wie Sie unter anderem der DSG-Info Nr. 90 entnehmen konnten, ist die Österreichische Datenschutzbehörde schon in vielen Fällen tätig geworden und hat sowohl Beschwerdeverfahren als auch Bußgeldverfahren geführt. In diesem Abschnitt möchten wir Ihnen aktuelle internationale Bußgeldverfahren vorstellen.

Hervorzuheben ist dabei das Urteil[2] der französischen Datenschutzbehörde CNIL, die ein Bußgeld in Höhe von EUR 50 Mio gegen Google erlassen hat. Inhaltlich richtet sich das Bußgeld gegen Verstöße der Informationspflichten gem. Art. 13 DSGVO, einer mangelhaften Einwilligung sowie allgemein Verstößen gegen die Grundsätze und Rechtmäßigkeit der Datenverarbeitung.

Weiters hat die Portugiesische Datenschutzbehörde CNPD ein Bußgeld in Höhe von EUR 400.000 gegen ein Krankenhaus verhängt, das weitreichende Berechtigungen an Mitarbeiterinnen und Mitarbeiter zu Patientenakten vergeben hatte, die nur Ärzten hätten zugänglich sein sollen. Durch die Vergabe eines „Technikerprofils“ wurden weitreichende Zugriffsrechte gewährt und damit die Sicherheit der Patientendaten gefährdet. Insgesamt gab es 985 aktive Benutzer, obwohl nur 296 Ärzte im Krankenhaus tätig waren. Dies stellte einen Verstoß gegen die technischen und organisatorischen Sicherheitsmaßnahmen sowie die Grundsätze der Datenverarbeitung in der Ausprägung Integrität und Vertraulichkeit dar.

Bemerkenswert ist auch das Bußgeld, das die polnische Datenschutzbehörde UODO[3] gegen die Wirtschaftsauskunftei Bisnode Polska verhängt hatte, die gegen die Informationspflichten gem. Art. 14 DSGVO verstoßen hatte. Das Bußgeld belief sich auf umgerechnet ca. EUR 222.000 und betraf 6 Mio. Datensätze, die aus öffentlich verfügbaren Quellen erhoben und weiterverarbeitet wurden. Die Aufsichtsbehörde stellte fest, dass Betroffene nicht ausreichend über die Datenverarbeitung und die Herkunft der Daten informiert wurden, da lediglich ein Zehntel der Betroffenen eine elektronische Information erhielt. Der Rest wurde weder elektronisch, telefonisch noch postalisch über die Datenverarbeitung informiert. Als Argument gegen die Benachrichtigung brachte das Unternehmen die Unmöglichkeit bzw. den unverhältnismäßig hohen Aufwand an; die polnische Datenschutzbehörde ließ das allerdings nicht gelten. Das

[2] CNIL, SAN-2019-001 vom 21.01.2019.

[3] PUODO, ZSPR.421.3.2018 vom 15.03.2019.

Ergebnis war die die Feststellung der Verletzung des Art. 14 DSGVO, die Verhängung des Bußgeldes und die Anweisung, die Betroffenen nun auch auf dem Postweg oder telefonisch über die Datenverarbeitung zu informieren.

Die norwegische Aufsichtsbehörde hat wegen unzureichender Datensicherheit gegen die Gemeinde Bergen ein Bußgeld[4] in Höhe von EUR 170.000 verhängt. Im Computersystem der Gemeinde waren 35.000 Datensätze offen zugänglich und ungesichert, mit Benutzernamen und Passwörtern gespeichert, die sowohl Bedienstete der Gemeinde Bergen als auch Schülerinnen und Schüler betrafen. Das hat es Dritten ermöglicht, unberechtigt auf die Daten zuzugreifen und sich mit den jeweiligen Konten anzumelden, um insbesondere Daten von Schülerinnen und Schülern aufzurufen. Zuvor war die Gemeinde Bergen bereits sowohl durch die norwegische Datenschutzbehörde *Datatilsynet* als auch durch Whistleblower über die mangelnde Datensicherheit gewarnt worden, ohne jedoch Maßnahmen zu treffen. Dies und die Tatsache, dass eine große Anzahl der Datensätze vor allem Kinder betraf, führte zur Höhe des Bußgeldes. Die Gemeinde hat angegeben, die Entscheidung nicht zu beanspruchen und hat damit als öffentliche Stelle ein Bußgeld erhalten. Dies ist bemerkenswert, da die DSGVO es im Rahmen einer Öffnungsklausel den Mitgliedstaaten offenlässt, öffentliche Stellen wie Gemeinden vom Bußgeld auszunehmen.

Für den weiteren Überblick über internationale Entscheidungen möchten wir Sie auf die Website www.enforcementtracker.com verweisen, die Bußgelder aus dem europäischen Ausland sammelt und veröffentlicht.

3. Guidelines des Europäischen Datenschutzausschusses zur Vertragserfüllung bei Online-Services

Nachdem die Artikel-29-Datenschutzgruppe durch den Europäischen Datenschutzausschuss (EDPB) ersetzt wurde, veröffentlicht dieser nun in Fortführung der Tätigkeiten der Datenschutzgruppe Leitlinien, Stellungnahmen und Beschlüsse auf europäischer Ebene zum Datenschutz.

Der EDPB veröffentlichte kürzlich eine Guideline[5] zu Art. 6 Abs. 1 lit. b DSGVO, also der Verarbeitung personenbezogener Daten auf Grundlage der (vor)vertraglichen Pflichten bei Online-Services. Hervorzustreichen sind drei wesentliche Aussagen dieser Guideline:

a) In Punkt 45 der Leitlinie (S.12) wird festgestellt, dass Daten, die für die „Verbesserung des Services“ gesammelt werden, nicht der Erfüllung des Vertrages dienen und daher Art. 6 Abs. 1 lit. b DSGVO nicht als Rechtsgrundlage herangezogen werden kann. Es bleibt Verantwortlichen jedoch unbenommen, eine andere Rechtsgrundlage wie die Einwilligung oder das berechtigte Interesse heranzuziehen. Einen ähnlichen Standpunkt vertritt der EDPB bei der Verarbeitung personenbezogener Daten zur Missbrauchsbekämpfung. Es ist zulässig, dass der Verantwortliche Kundenprofile beobachtet, um miss-

[4] https://www.datatilsynet.no/en/about-privacy/reports-on-specific-subjects/administrative-fine-of-170.000--imposed-on-bergen-municipality/

[5] Guidelines 2/2019 (https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b_en)

bräuchliches Verhalten aufzudecken bzw. zu verhindern. Dies hat jedoch keine Grundlage in der Vertragserfüllung, sondern sollte auf die Einwilligung des Betroffenen oder das berechtigte Interesse gestützt werden.

b) Bei verhaltensorientierter Werbung sowie Tracking- und Profiling-Maßnahmen stellt der EDPB in Punkt 47f (S.12) als Grundregel fest, dass verhaltensorientierte Werbung kein notwendiges Element eines Online-Services darstellt.

c) Weiters beantwortet der EDPB die Frage, ob man mit seinen Daten „bezahlen" kann, mit einem klaren Nein. Unter Punkt 51 der Leitlinie (S.13) stellt er fest: „*considering that data protection is a fundamental right guaranteed by Article 8 of the Charter of Fundamental Rights, and taking into account that one of the main purposes of the GDPR is to provide data subjects with control over information relating to them, personal data cannot be considered as a tradeable commodity.*" Damit wäre das Geschäftsmodell von Online-Services, die gratis zur Verfügung gestellt werden und als Gegenleistung die Datenverarbeitung einfordern, nach Meinung des EDPB unzulässig. Betroffene können demnach in die Datenverarbeitung einwilligen, aber ihre personenbezogenen Daten nicht eintauschen: „*Data subjects can agree to processing of their personal data, but cannot trade away their fundamental rights.*"

Fazit: Nach Ansicht des EDPB steht die Bereitstellung von personenbezogenen Daten zur Nutzung eines Gratis-Online-Services nicht in einem entgeltlichen Verhältnis zueinander. Tracking und Profiling bedürfen insbesondere der Einwilligung der Betroffenen. Nachdem die Guidelines des EDPB auch von den Aufsichtsbehörden bei der rechtlichen Beurteilung herangezogen werden, bleibt abzuwarten, wie sich diese Meinung in der Rechtsprechung widerspiegeln wird.

4. Whistleblowing-Richtlinie passiert Europäisches Parlament

Im April 2018 legte die Europäische Kommission (EK) den Vorschlag für eine Richtlinie zum EU-weiten Schutz von Hinweisgebern (auch „Whistleblower" genannt) mit dem Ziel vor, die Meldewege für Whistleblowing einheitlich zu regeln und Hinweisgeber vor Vergeltungsmaßnahmen zu schützen. Ein Jahr später einigten sich die EU-Gesetzgeber auf den finalen Text der Richtlinie, die EU-weite Mindeststandards zum Schutz von Informanten festlegt.

Der Anwendungsbereich umfasst den Schutz von Hinweisgebern, die Verstöße gegen das EU-Recht in einer Vielzahl von Bereichen wie Geldwäsche, Produkt- und Verkehrssicherheit, nukleare Sicherheit, öffentliches Auftragswesen, Finanzdienstleistungen, öffentliche Gesundheit, Verbraucherschutz und Datenschutz aufdecken wollen. Hintergrund der Richtlinie waren die jüngsten Ereignisse rund um den Diesel-Skandal, Luxleaks, die Panama Papers, dem Fipronil-Vorfall oder den Missbrauch personenbezogener Daten bei Cambridge Analytica, wo Hinweisgeber eine entscheidende Rolle gespielt haben.

Die Verpflichtung zur Einrichtung interner Kanäle richtet sich an alle Unternehmen mit 50 oder mehr Beschäftigten bzw. einem Jahresumsatz oder einer Jahresbilanz von mindestens EUR 10 Mio. Unabhängig davon ist die Einrichtung derartiger Meldekanäle in Finanzdienstleistungsbranchen sowie Sektoren, die durch Geldwäsche oder Terrorismusfinanzierung gefährdet sind, verpflichtend.

Um die Sicherheit potenzieller Hinweisgeber und die Vertraulichkeit der offenbarten

Informationen zu gewährleisten, dürfen Hinweisgeber in Zukunft Verstöße über interne und externe Kanäle in Form eines mehrstufigen Meldesystem melden sowie sich unter Umständen auch außerhalb ihrer Organisation direkt an die zuständigen nationalen Behörden bzw. als Ultima Ratio an die Öffentlichkeit wenden.

Der nationale Gesetzgeber hat zwei Jahre Zeit, für die Umsetzung der Richtlinie zu sorgen. Des Weiteren müssen die Mitgliedstaaten umfassende und unabhängige Informationen über Berichtswege, alternative Verfahren sowie kostenlose Beratung und Rechtsbeistand bereitstellen. Als nächstes muss die Richtlinie förmlich vom Rat verabschiedet werden.

Sie finden den angenommenen Text, der noch nicht im Amtsblatt veröffentlicht ist, unter dem Link https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52018PC0218 .

5. DSB-Entscheidung: Zusendung einer Werbe-E-Mail ohne gültige Einwilligung verletzt das Grundrecht auf Datenschutz

In der kürzlich veröffentlichten Entscheidung DSB-D130.033/0003-DSB/2019 vom 7. März 2019 befand die Datenschutzbehörde über die Zusendung einer E-Mail zu Werbezwecken, ohne dass eine Einwilligung des Betroffenen vorlag. Ein Unternehmen hatte den Beschwerdeführer im Mai 2018 (d.h. knapp vor Anwendbarkeit der DSGVO) um Einwilligung zur weiteren Zusendung von E-Mails ersucht. Dieser stellte daraufhin ein Auskunftsbegehren, da er die entsprechende Einwilligung nie erteilt hatte. Anstelle einer Antwort erhielt er im Juli 2018 eine Marketing-E-Mail dieses Unternehmens – woraufhin er sich umgehend an die Datenschutzbehörde wandte.

Das Verfahren zur Verletzung des Auskunftsrechts wurde von der Datenschutzbehörde nach einer verspäteten Beantwortung formlos eingestellt. Offen blieb die Frage der unrechtmäßigen Verarbeitung aufgrund der fehlenden Einwilligung. Es handelt sich dabei um einen Verstoß gegen § 107 Abs. 2 TKG 2003, das als Lex specialis anzusehen ist.

In einem früheren Bescheid[6] hatte die Behörde bereits festgestellt, dass solche Verstöße in ihre Zuständigkeit fallen, sofern sie als Verletzung des Rechts auf Geheimhaltung nach § 1 Abs. 1 DSG zu werten sind. Im Rahmen einer Beschwerde an die Datenschutzbehörde können sich Betroffene grundsätzlich auf jede Bestimmung der DSGVO stützen, sofern sie eine derartige Rechtsverletzung zur Folge hat.

Im aktuellen Fall befand die Datenschutzbehörde die Verarbeitung der Daten ohne gültigen Erlaubnistatbestand als Verletzung des Grundrechts auf Geheimhaltung. Die Daten des Beschwerdeführers waren daher zu löschen (was das verantwortliche Unternehmen nach eigenen Angaben ohnehin bereits getan hatte).

Fazit: Die Rechtmäßigkeit der Zusendung von Werbe-E-Mails richtet sich nach wie vor nach TKG 2003. Die Datenschutzbehörde behält sich aber vor, derartige Rechtsverletzungen gemäß den Bestimmungen der DSGVO zu prüfen. Unrechtmäßige Verarbeitungen nach § 107 Abs. 2 TKG 2003 gehen fast zwangsläufig mit einer Verletzung von Art. 6 DSGVO einher. Eine Verfolgung durch die Datenschutzbehörde ist daher wahrscheinlich.

[6] Werbeanrufe, DSB-D123.076/0003-DSB/2018, vgl. auch DSG-Info 90/2019

Für Verantwortliche bedeutet das, dass die Rechtmäßigkeit der Zusendung elektronischer Werbung eingehend zu prüfen ist; insbesondere sollten dokumentierte Einwilligungen vorliegen. Elektronische Werbezusendungen ohne gültige Einwilligung können als Verstoß gegen sowohl TKG 2003 als auch DSGVO gewertet und mit entsprechenden Bußgeldern geahndet werden.

Neues Produkt: DSGVO Compliance Check

Zur rechtskonformen und angemessenen Umsetzung des Datenschutzes bedarf es regelmäßiger Überprüfungen und Anpassungen: Die rechtlichen Anforderungen ändern sich stetig, daher muss die Umsetzung im Unternehmen laufend angepasst werden. Auch neue Verarbeitungen und allfällige Änderungen sind zu berücksichtigen, um das erreichte Datenschutzniveau zu erhalten und mit den geltenden Bestimmungen in Einklang zu bringen.

Die Pflicht zur regelmäßigen Überprüfung der Datenschutzmaßnahmen ergibt sich insbesondere aus den Artikeln 24 und 32 DSGVO, ist aber bereits in den Datenschutz-Grundsätzen begründet. Eine jährliche Bestandsaufnahme ist in den meisten Fällen das Mindestmaß. Projektbegleitend, zB während der Umsetzung eines breit angelegten Maßnahmenprogramms, kann es aber auch sinnvoll sein, in kürzeren Abständen Überprüfungen durchzuführen.

Secur-Data hat ein Prüfverfahren entwickelt, mit dem die Untersuchung der DSGVO Compliance effizient, in kurzer Zeit und bei minimaler Belastung des geprüften Unternehmens möglich ist. Sowohl die spezielle Situation und Charakteristik des Unternehmens als auch das vorhandene Wissen zu bekannten Problemfeldern werden berücksichtigt, um ein angepasstes und zielführendes Audit durchführen zu können.

Als Ergebnis wird ein Bericht erstellt, der einen raschen Überblick über alle relevanten Bereiche der Datenschutz-Umsetzung gibt und Empfehlungen enthält, die unmittelbar zur Planung der notwendigen Ergänzungen und Verbesserungen herangezogen werden können. Selbstverständlich kann dieser Auditbericht auch als Nachweis im Sinne der Rechenschaftspflicht gegenüber der Datenschutzbehörde eingesetzt werden.

Nähere Details sowie einen Überblick über die geprüften Bereiche finden Sie unter www.secur-data.at

Unser nächstes Seminar

„DSGVO – Rechtsentwicklung und Best Practices“

findet am 22. Oktober 2019 statt.

Es referieren **Prof. KommR Hans-Jürgen Pollirer** sowie **Mag. Judith Leschanz** und **Mag. Katja Wyrobek**.

Außerdem veranstalten wir am 22. und 23. Oktober 2019 das Praxisseminar

„Praxisnahe Updates zu Datenschutz und IT-Sicherheit“

Nähere Informationen finden Sie in Kürze unter www.secur-data.at.