LOSCHELDER

Newsletter Datenschutzrecht

Mai 2020

Sehr geehrte Damen und Herren,

die Diskussion um die Lockerung der Corona-Maßnahmen ist in vollem Gang. Die Politik sucht nach einem angemessenen Weg aus dem *Lockdown* und hin zu einer „neuen Normalität“. Die damit verbundene Selbstverantwortung von Bürgern und Unternehmen wirft auch (wieder) zahlreiche datenschutzrechtliche Fragestellungen auf. Wir haben Ihnen daher die aktuellen Behördenäußerungen zum Thema im ersten Beitrag zusammengefasst. Hieraus dürften sich auch für die Zeit „nach Corona“ interessante Hinweise ergeben.

In den weiteren Beiträgen befassen wir uns mit aktueller Rechtsprechung rund um datenschutzrechtliche Praxisprobleme (Umfang des Auskunftsanspruchs, Datenschutz und Inkasso, Offenlegungsansprüche im Zusammenhang mit Wahlwerbung).

Und zu guter Letzt wollen wir Ihnen auch in diesem Monat die besonders interessanten Bußgeldfälle und einige Kuriositäten nicht vorenthalten.

Inhalt

Datenschutz und Corona – Übersicht

Mit der Corona-Pandemie haben sich auch eine Reihe neuer datenschutzrechtlicher Fragen ergeben, von der Nutzung digitaler Kommunikationstools im Home-Office bis hin zur kontaktlosen Körpertemperaturmessung im Betrieb. Viele Datenschutzaufsichtsbehörden haben sich zu einigen der Themen inzwischen positioniert. Im folgenden Beitrag haben wir die aktuellen Behördenäußerungen zum Thema „Corona" für Sie zusammengefasst. Dies ist aktuell illustrierend und dürfte auch in der Zukunft bei der ein oder anderen Frage hilfreich sein.

Aus der Vielzahl der Äußerungen grundlegend ist die Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 03.04.2020. Bezogen auf die Datenverarbeitung zu Zwecken der Vermeidung der Ausbreitung des Virus hat die DSK festgestellt, dass weiterhin die im Rahmen des Art. 5 DSGVO entwickelten Grundsätze zur Rechtmäßigkeit der Datenverarbeitung gelten: Jegliche Verarbeitung personenbezogener Daten muss auf einer gesetzlichen Erlaubnisgrundlage beruhen, geeignet und erforderlich sein, um tatsächlich der Eindämmung des Virus zu dienen, und die etablierten Konzepte der Datenminimierung und Sicherheit zum Schutz der Vertraulichkeit berücksichtigen. Obwohl dies nichts Neues ist, sah sich die DSK bemüßigt, die Gesetzgeber und Regierungen an diese Grundregeln zu erinnern. Auch für Private und Betriebe bleibt es also grundsätzlich bei den bereits bekannten Regeln.

Um die praktische Umsetzung dieser Prinzipien zu erleichtern, sind die nationalen Aufsichtsbehörden bemüht, möglichst umfangreich darüber zu informieren, welche Datenverarbeitung unter welchen Voraussetzungen zulässig ist. Die DSK hat dahingehend eine Mitteilung über die Verarbeitung personenbezogener Daten durch Arbeitgeber oder Dienstherren herausgegeben. Zusätzlich haben der BfDI sowie einige der Landesdatenschutzbehörden durch Mitteilungen, Presseerklärungen und Informationsblätter Hinweise über die Ausgestaltung der Arbeit im Home-Office, der Nutzung von Videokonferenz-Diensten, der Befragung von Arbeitnehmern und Dritten und, und, und herausgegeben. Natürlich sind sich die verschiedenen Stellen nicht immer einig.

Eine Übersicht über einige, der durch die Aufsichtsbehörden beantworteten Fragen, finden Sie themenbezogen hier. Tendenziell sehen spätere Stellungnahmen eine umfangreichere Datenverarbeitung als zulässig an. Begründet werden kann dies im Querschnitt mit zunehmenden Gesundheitsgefahren, die entsprechend zunehmend gewichtig in die Interessensabwägung einfließen:

Mitarbeiter:

	Zulässig	**Unzulässig**	**Zulässig unter Berücksichtigung der folgenden Einschränkungen**
Befragung der Beschäftigten zu einer positiven Corona-Testung			NRW LDI: bei entsprechenden Verdachtsmomenten Bei positivem Ergebnis besteht Informationspflicht gegenüber Arbeitgeber
Befragung der Beschäftigten zu Krankheitssymptomen	NRW LDI, HH LfDI: Beschränkung der Befragung auf typische Corona-Symptome und Bestehen eines erhöhten Infektionsrisikos		
Befragung der Beschäftigten, ob diese sich in einem Risikogebiet aufgehalten haben oder Kontakt mit erkrankten Personen hatten			NRW LDI, BaWü LfDI, HH LfDI, Sachs LfDI: Begrenzte Befragung ist unter Umständen zulässig, wobei eine diesbezügliche Negativauskunft des befragten Beschäftigten ausreichend ist
Erhebung und Verarbeitung personenbezogener Daten inkl. der Gesundheitsdaten der Beschäftigten	BfDI: zum Zwecke der Eindämmung und Verhinderung der Ausbreitung des Virus (insbesondere wenn Infektionen festgestellt wurden oder nachweislich Kontakt mit Infizierten bestand)		
Erhebung von Handynummern und privaten E-Mailadressen	BfDI: zulässig, wenn die Erhebung zur Sicherstellung einer „durchgehenden Erreichbarkeit“ erfolgt		Sachs LfDI und HH LfDI: Einwilligung der Mitarbeiter erforderlich

Namentliche Offenlegung			Nieds LfDI, Bra LfDI: wenn Kenntnis der Person des Infizierten für Vorsorge-maßnahmen unbedingt erforderlich ist BaWü LfDI, Sachs LfDI: nach Entscheidung der zuständigen Gesundheitsbehörde
Offenlegung einer nachweislichen Infektion oder eines Verdachtsfall	BfDI: zur Information von Kontaktpersonen (wobei Nennung des Namens nur ausnahmsweise zulässig ist)		
Temperaturmessungen vor Zugang zum Arbeitsplatz		RhPf LfDI	NRW LDI: konkrete Verdachtsfälle oder Infektionen im Betrieb; Verwendung der Daten nur zu Einlasszwecken und keine Speicherung HH LfDI: Arbeitsumfeld mit hohem Körperkontrakt und in system-relevanten Berufen
Übermittlung von Daten an die Gesundheitsbehörden			BaWü LfDI, Sachs LfDI: Bei Ersuchen der zuständigen Hoheitsträger besteht eine korrespondierende Übermittlungsbefugnis

Kunden und Besucher:

	Zulässig	**Unzulässig**	**Zulässig unter Berücksichtigung der folgenden Einschränkungen**
Eingangsscreenings bei Kunden und Besuchern vor dem Zugang zu Geschäften und anderen Bereichen		HH LfDI	
Speicherung und Erhebung der Daten von Kunden oder Besuchern von Veranstaltungen und ggfs. Übermittlung der Daten an Gesundheitsbehörden bei Bekanntwerden einer Infektion		Grds. unzulässig	NRW LDI, HH LfDI: bei behördliche Anordnung zur Erhebung, Speicherung und Übermittlung

Home-Office:

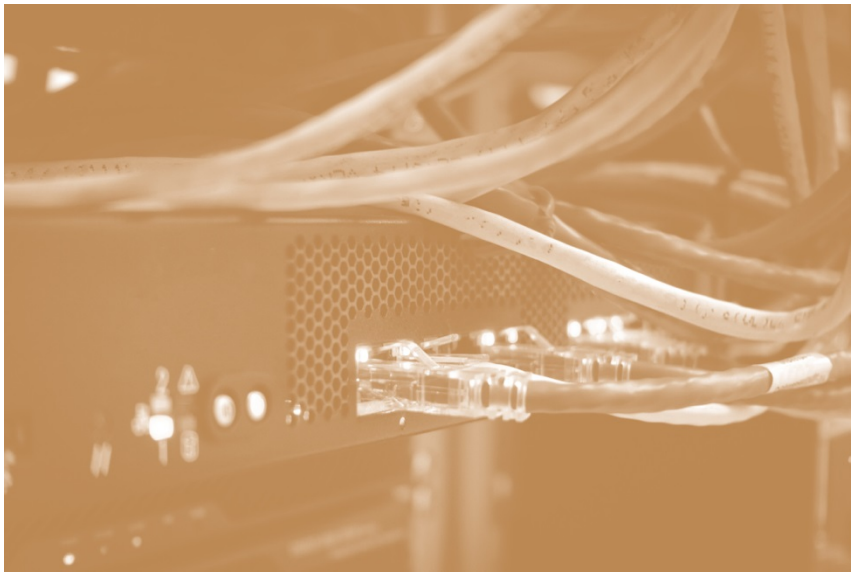
	Zulässig	Unzulässig	Zulässig unter Berücksichtigung der folgenden Einschränkungen
Einwahl in das Unternehmensnetzwerk aus dem Home-Office			RhPf LfDI, Sachs LfDI, SaAn LdFI: wenn Zugriff durch Authentifizierungs-module gesichert ist
Entsorgung von Dokumenten mit personenbezogenen Daten im häuslichen Bereich		RhPf LfDI, Ber LfDI: Im Betrieb ordnungs-gemäß zu entsorgen	
Mitnahme von Personalakten ins Home-Office		BfDI: ausnahmswei se unter Einhaltung der erforderlichen technisch-organisa-torischen Schutzmaß-nahmen zulässig	
Nutzung der Unternehmens-Cloud aus dem Homeoffice			SaAn LfDI: wenn der Zugriff durch Authentifizierungs-modele gesichert ist und Daten nicht auf private Geräte exportiert werden können
Nutzung der vom Arbeitgeber bereitgestellten Endgeräte und Speichermedien			RhPf LfDI, Sachs LfDI, SaAn LdFI, Nied LfDI, ScHo LfDI, Ber LfDI: sofern Geräte verschlüsselt und passwort-geschützt sind und Viren-Programme installiert sind.
Nutzung des privaten WLAN/der privaten Internetverbindung			RhPf LfDI, Sachs LfDI, ScHo LfDI, Ber LfDI: bei verschlüsselter und passwortgeschützter Verbindung; Nutzung von ETHERNET-Kabelverbindungen möglich
Nutzung dienstlicher E-Mailadressen	RhPf LfDI, Sachs LfDI: sofern Verschlüsselung und Datensicherheit gewährleistet ist		

Nutzung privater E-Mailadressen		Sachs LfDI: die generelle Umleitung dienstliche Mails auf das private Postfach	RhPf LfDI, Sachs LfDI: wenn zur Kommunikation unvermeidlich; das europäische Datenschutzniveau muss aber gewahrt bleiben
Nutzung privater (Mobil-)Telefone für betriebliche Dienste		Beim Austausch sensibler Daten	Ber LfDI, ScHo LfDI, RhPf LfDI: wenn personenbezogene Kontaktdaten vom Gerät gelöscht werden können und wenn mögl. mit Rufnummern-unterdrückung
Nutzung privater Endgeräte und Speichermedien		Bei Verarbeitung sensibler Daten	RhPf LfDI, Sachs LfDI, SaAn LdFI, Nied LfDI, ScHo LfDI, Ber LfDI: nach Genehmigung des Arbeitgebers und ausreichenden Schutzmaßnahmen, wie Verschlüsselung, Passwortsicherung und Virenschutz. Zudem muss eine einfache Löschung der Daten möglich sein. Arbeitgeber dürfen keinen Zugriff haben.
Speicherung personenbezogener Daten in privater Cloud		RhPf LfDI: nur ausnahms-weise zulässig, wenn zur Durchführung des Vertrages unvermeidbar und Sicherheitsan-forderungen eingehalten werden	
Telefonie aus dem häuslichen Bereich	RhPf LfDI: unter Sicherstellung, dass personen-bezogene Daten nicht mitgehört werden können und bei nicht personen-bezogenen Daten Hinweis, dass ggfs. Haushalts-mitglieder/Dritte mithören können		

Transport von Dokumenten mit personenbezogenen Daten und von Speichermedien des Arbeitgebers			Sachs LfDI, ScHo LfDI, Ber LfDI: bei ausreichend getroffenen Schutzmaßnahmen (bspw. verschließbare Behältnisse; Passwörter und Verschlüsselungen)
Verarbeitung personenbezogener Daten im Home-Office allgemein	SaAn LfDI, RhPf LfDI, Sachs LfDI, SchlHo LfDI, Br LfDI, BerLfDI: nach Prüfung ob entsprechende Verarbeitung im Home-Office überhaupt erforderlich ist Allgemeine Hinweise zur IT-sicheren Daten-verarbeitung im Home-Office		
Veröffentlichung von Wahlvorschlägen bei Personalratswahlen im Intranet	BfDI: wenn dies zur ordnungs-gemäßen Information der Wahlberechtigten erforderlich ist und keine Bekanntgabe nach außen erfolgt		

Kommunikation (auch aus dem Home-Office):

	Zulässig	**Unzulässig**	**Zulässig unter Berücksichtigung der folgenden Einschränkungen**
Nutzung von Messenger- und Konferenzdiensten	BfDI: bei sorgfältiger Auswahl des Dienstleisters Leitfaden zur Beurteilung von Angeboten des BfDI Informationsblatt des HH LfDI und Checkliste des Ber LfDI	Der Austausch sensibler Daten, sowie die Nutzung privater E-Mail-adressen zur Anmeldung beim Dienst in betrieblichen Kontext sind unzulässig.	



Reichweite des Auskunftsanspruchs gem. Art. 15 DSGVO

Das Auskunftsrecht der Betroffenen gem. Art. 15 DSGVO ist seit Inkrafttreten der DSGVO ein Dauerbrenner in der Praxis. Die immer wiederkehrenden praktischen Schwierigkeiten drehen sich vor allem um den Umfang des Anspruchs und den damit verbundenen Aufwand für Unternehmen. Wir berichten in diesem Artikel über eine neue Gerichtsentscheidung aus diesem Umfeld.

Ein Dauerbrenner ist die Frage, ob die Herkunft der personenbezogenen Daten ebenfalls in der Auskunft enthalten sein muss. Mit dieser Frage hat sich zuletzt das LG Mosbach (Beschluss vom 27.01.2020 - 5 T 4/20) in der folgenden Konstellation auseinandergesetzt: Bestellt ein Kunde online eine Ware oder Dienstleistung, so muss er beim Bezahlvorgang persönliche Daten eingeben. Daher hat der Kunde einen Anspruch auf Auskunft bezüglich dieser Daten. Doch wie stellt sich der Fall dar, wenn er die Daten gar nicht selbst eingegeben hat, sondern eine andere Person diese missbräuchlich für eine Bestellung benutzt hat?

Im vom LG Mosbach entschiedenen Fall hatte ein Unternehmen auf Nachfrage lediglich die Information herausgegeben, dass die personenbezogenen Daten im Rahmen eines einzelnen Bezahlvorgangs erhoben worden seien. Weitere Auskünfte wurden mit dem Hinweis darauf verweigert, dass der Kunde die Daten gar nicht selbst eingegeben habe. Das LG Mosbach entschied jedoch,

dass die Daten trotzdem die Identität des Kunden beträfen, ganz egal, ob er sie selbst eingegeben habe oder nicht. Daher ist das Unternehmen zur Auskunft über alle verfügbaren Informationen über die Herkunft der Daten verpflichtet.

Für Unternehmen ergibt sich aus dieser Rechtsprechung vor allem, dass sie in der Lage sein müssen, die Herkunft personenbezogener Daten nachvollziehen zu können, entweder in abstrakter Weise durch das Verarbeitungsverzeichnis oder durch eine IT-Anwendung im konkreten Fall (E-Mail Postfach, CRM-System etc.). Das bezieht sich sowohl auf die erstmalige Erhebung der personenbezogenen Daten beim Betroffenen als auch den Empfang durch Dritte. Nur dann kann auch dem Betroffenen gegenüber eine solche Auskunft erteilt werden. Dabei muss die Herkunft zumindest abstrakt angegeben werden können, je nach Konstellation können auch detailliertere Angaben erforderlich sein. Wenn hierbei nur für die Ermöglichung der Quellangabe personenbezogene Daten gespeichert werden müssten, ist dies besonders kritisch zu überprüfen, denn auch diese Datenverarbeitung bedarf einer Erlaubnisgrundlage.

Inkasso-Abtretung im berechtigten Interesse

Es ist mittlerweile bekannt, dass das Datenschutzrecht gerne genutzt wird, um sich unliebsamen Ansprüchen des Vertragspartners zu erwehren. Bei der Weitergabe der Schuldnerdaten an eine Inkasso-Gesellschaft gewinnt das Verhältnis von Datenschutzrecht zu Maßnahmen zur Durchsetzung von Zahlungsansprüchen eine besondere Relevanz.

Mit einem Urteil vom 20.02.2020, Az. 1 K 467/19.MZ hat das VG Mainz bei Schuldnern sicherlich für einigen Ungemach gesorgt. Zu entscheiden war über einen Verwarnungsbescheid des LfDI Rheinland-Pfalz nach Art. 58 Abs. 2 lit. b DSGVO gegen einen Tierarzt, der Abrechnungsinformationen seiner Kunden an eine Verrechnungsgesellschaft (VTX) zur Eintreibung offener Forderung weitergegeben hatte. Dabei lag zwar ein Auftragsverarbeitungsvertrag zwischen dem Tierarzt und der VTX vor, eine ausdrückliche Einwilligung der Kunden zur Übermittlung der Daten jedoch nicht. Der Tierarzt wehrte sich gerichtlich gegen die behördliche Aufforderung, in Zukunft solche Übermittlungen nur mit einer ausdrücklichen Einwilligung vorzunehmen.

Im Ergebnis hat das VG Mainz die Weitergabe von Abrechnungsdaten an Verrechnungsgesellschaften oder Inkassounternehmen auch ohne Einwilligung der betroffenen Schuldner abgesegnet. Das Gericht betonte zwar, dass diese Weitergabe keine Auftragsverarbeitung im Sinne des Art. 28 DSGVO darstelle. Nach Ansicht des Gerichts ist die Weitergabe an die VTX aber als erforderliche Verarbeitung zur Erfüllung des Vertrages mit dem Kunden nach Art. 6 Abs. 1 S. 1 lit. b DSGVO auch ohne dessen Einwilligung zulässig: Da die Pflicht zur Zahlung der Vergütung die wesentliche Pflicht des Kunden aus dem Behandlungsvertrag mit dem Tierarzt ist, sei die Datenverarbeitung, die der tatsächlichen Eintreibung dieser Zahlung dient, erforderlich im Sinne der DSGVO. Das gelte auch, wenn die Forderung von einer Inkassogesellschaft und nicht vom Vertragspartner selbst eingefordert wird, und deshalb die abrechnungsbezogenen Daten an die Inkassogesellschaft übermittelt werden. Dabei dürften jedoch nur die Daten übermittelt werden, die für die Eintreibung der Forderung tatsächlich notwendig sind.

Daneben sei es auch das berechtigte Interesse des Tierarztes, zur Eintreibung seiner Forderungen gegen säumige Kunden die Hilfe Dritter, wie Inkassogesellschaften, in Anspruch zu nehmen. Deshalb sei die Weitergabe der abrechnungsbezogenen Daten auch insofern von Art. 6 Abs. 1 S. 1 lit. f DSGVO (Wahrung berechtigter Interessen des Verantwortlichen) gedeckt.

Das Kuriosum des Falls und eigentlich in unsere Rubrik „zu guter Letzt“ gehörig: Dem Vorbringen des Tierarztes, es handle sich bei den übermittelten Daten zudem um Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO auf die die Grundsätze der Einwilligung sowieso nicht anwendbar seien, schenkte das Gericht wenig Beachtung: Die Abrechnungsdaten enthielten eben nur „Gesundheitsdaten“ der behandelten Tiere, über die Gesundheit des zahlenden Besitzers sagt dies in der Regel nichts aus.

Für die Praxis ergibt sich, dass an der bisherigen Praxis der Datenübermittlung an Inkassounternehmen zur Eintreibung von Vertragsleistungen festgehalten werden kann. Es muss allerdings sichergestellt werden, dass tatsächlich nur die Daten übermittelt werden, die für die Durchsetzung der Forderung erforderlich sind.

Kein Anspruch auf Übermittlung persönlicher Daten zur Wahlwerbung

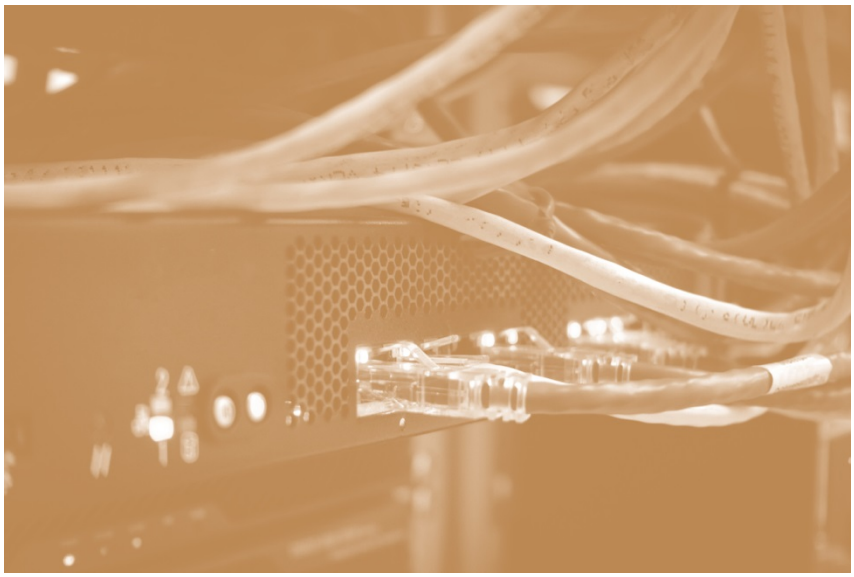
Das Datenschutzrecht vermittelt eine Reihe von Informationsansprüchen für die Betroffenen. Im Umkehrschluss lassen sich aus der DSGVO aber keine Ansprüche auf die Übermittlung personenbezogener Daten an Dritte ableiten.

Mit einem auf das Datenschutzrecht gestützten Anspruchsbegehren hatte sich das OVG Lüneburg auseinanderzusetzen (OVG Lüneburg, Beschluss vom 15.04.2020 - Az. 8 ME 36/20). Es hat entschieden, dass ein Wahlbewerber für die Kammerversammlung der Niedersächsischen Zahnärztekammer keinen Anspruch auf die Übermittlung der Adressdaten der Wähler durch die Kammer hat, um damit Wahlwerbung zu betreiben.

Über die Adressdaten der Kammermitglieder, teils die privaten Anschriften, teils Praxisanschriften, verfügte die Kammer, um mit ihren Mitgliedern in Kontakt treten zu können. Das OVG stellte fest, dass die Kammer keine Pflicht zur Übermittlung dieser Daten an Kammer-Kandidaten zur Wahlwerbung hat. Hierfür fehle es an einem Anspruch des Kandidaten. Weder aus dem kammerspezifischen Wahlrecht noch aus den allgemeinen grundrechtlichen Prinzipien der Freiheit und Gleichheit der Wahl, lasse sich ein solcher Anspruch herleiten. Auch datenschutzrechtliche Erlaubnisgrundlagen können nicht zur Anspruchsnorm für Informationsübermittlung umfunktioniert werden, dient das Datenschutzrecht doch der Beschränkung der Verarbeitung personenbezogener Daten durch öffentliche und private Stellen. Die Normen des Datenschutzrechtes, ob nun im Speziellen § 85a HKG, das Niedersächsische Datenschutzgesetz (NDSG) oder allgemeiner etwa der Art. 6 Abs. 1 lit. b DSGVO können nicht so ausgelegt werden, dass bei einem „wie auch immer gearteten“ berechtigten Interesse ein Übermittlungsanspruch besteht. Vielmehr haben nur die Betroffenen einen Anspruch auf Einhaltung der Vorschriften.

Mit seinem Beschluss hat das OVG einen gegenläufigen Beschluss des VG Stade aufgehoben, der die Kammer zur Übermittlung der Daten verpflichtete. Der klagende Kandidat wird sich nun andere Wege überlegen müssen, um Wahlwerbung zu betreiben.

Für die Praxis wirkt das Urteil als Klarstellung, dass die Zielrichtung der DSGVO der Schutz der Betroffenen ist. Informationsansprüche – auch aus berechtigten Interessen – lassen sich aus dieser für Unbeteiligte nicht herleiten.



Zu guter Letzt: Geldbußen des Monats

Zu guter Letzt haben wir auch diesmal einige interessante Bußgeldfälle für Sie.

- **Polen**

Als durchaus kurios stellt sich dieser in Polen spielende Sachverhalt dar: Dort wurde gegen ein Unternehmen ein Bußgeld in Höhe von rund 4.700 Euro verhängt. Bei dem Unternehmen sollte eine Vor-Ort-Kontrolle durch die polnische Datenschutzaufsichtsbehörde UODO durchgeführt werden. An der Geschäftsadresse war jedoch kein Mitarbeiter anzutreffen. Für die Behörde war dies ein Indiz dafür, dass die Firma eine Kontrolle nach Art. 58 Abs. 1 lit. e und f DSGVO vereiteln wollte. Sie ging davon aus, dass sie daran gehindert werden sollte, Beweise für die rechtswidrige Verarbeitung personenbezogener Daten zu sammeln. Da somit ein Verstoß gegen die Bestimmung der DSGVO vorliegt, der eine Zusammenarbeit von Behörden und Unternehmen vorsieht, verhängte die Aufsichtsbehörde ein Bußgeld in Höhe von rund 4.700 Euro. Den Geschäftsführer

könnte es jedoch noch härter treffen: In Polen sieht Artikel 108 Absatz 1 des Gesetzes über den Schutz personenbezogener Daten bei der Behinderung oder Verhinderung einer Kontrolle eine Haftstrafe von bis zu 2 Jahren vor. Ein entsprechendes Gesetz gibt es in Deutschland nicht.

- **Deutschland**

In Hamburg wendete sich ein Beschäftigter der Universitätsklinik Hamburg wegen der Veröffentlichung seiner Bezüge nach dem Hamburger Transparenzgesetz (§ 3 Abs. 1 Nr. 15 HmbTG) an das Verwaltungsgericht. Bei der Universitätsklinik Hamburg handelt es sich um eine Körperschaft des öffentlichen Rechts. Das Gericht entschied, dass bei der Veröffentlichung der Bezüge kein Verstoß gegen die datenschutzrechtlichen Bestimmungen des BDSG und der DSGVO vorlägen. Vielmehr ergebe sich die Rechtmäßigkeit der Veröffentlichung gerade aus Art. 6 Abs. 1 Buchstabe c bzw. e DSGVO. Auch das Transparenzgesetz an sich sei rechtmäßig, denn es diene der Transparenz und biete der Öffentlichkeit die Möglichkeit, die Verteilung öffentlicher Mittel beurteilen zu können.

- **Schweden**

Die schwedische Datenschutzaufsichtsbehörde (DPA) verhängte gegen das nationale Dienstleistungszentrum der Regierung ein Bußgeld in Höhe von umgerechnet rund 19.000 Euro. Die Untersuchungen der DPA ergaben, dass durch einen Fehler im System Unbefugten der Zugriff auf personenbezogene Daten ermöglicht wurde. Über diesen Fehler habe das Dienstleistungszentrum die Betroffenen jedoch erst nach 5 Monaten und die Aufsichtsbehörde erst nach 3 Monaten unterrichtet. Neben der damit zu langen Zeit bis zur Mitteilung der Sicherheitslücke entsprach diese Mitteilung nach Ansicht der DPA auch nicht vollständig den Anforderungen der DSGVO. Das Dienstleistungszentrum verstieß somit gleich zweimal gegen die Vorgaben der DSGVO, was nach Ansicht der DPA ein Bußgeld in Höhe von rund 19.000 Euro rechtfertigte.

- **Schweden**

Die schwedische DPA hat bereits im März 2020 ein Bußgeld in Höhe von umgerechnet rund 7 Million Euro gegen Google verhängt. Aus der DSGVO ergibt sich das Recht für Einzelpersonen, ihre Suchergebnisse aus den Listen von Google streichen zu lassen. Bei zahlreichen Anträgen sei Google dieser Verpflichtung gar nicht oder nicht ordnungsgemäß nachgekommen. Neben der nur teilweisen Umsetzung der Verpflichtung, teilt Google den Betreibern der entsprechenden Webseiten alle Informationen, die im Zusammenhang mit den Löschungsantrag stehen, mit. Dies ermöglicht es dem Betreiber letztlich, die Webseite auch nach der erfolgten Löschung über eine andere Webadresse erneut zu veröffentlichen. Im Ergebnis führt das zu einer Aushöhlung des Rechts, eine Streichung von den Ergebnislisten bei Google beantragen zu können. Aus diesem Grund hat die DPA Google neben der Verhängung des Bußgeldes in Höhe von rund 7 Million Euro zusätzlich angewiesen, seine Mitteilungs-Praxis in Zukunft zu unterlassen.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Claudia Willmer
+49(0)221 65065-337
claudia.willmer@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de