LOSCHELDER

Newsletter Datenschutzrecht

Juli 2021

Sehr geehrte Damen und Herren,

auch im vermeintlichen Sommerloch gibt es einiges zu berichten in Sachen Datenschutz. Allem voran ein Aufatmen für den Datenaustausch mit dem UK: Die EU-Kommission hat am 28.06.2021 den Angemessenheitsbeschluss fürs UK angenommen. Dieser gilt bis Juni 2025 und führt in der Praxis dazu, dass personenbezogene Daten mit dem UK weiterhin so ausgetauscht werden können, als hätte es den Brexit nicht gegeben.

Zudem möchten wir Sie noch auf eine Neuigkeit in eigener Sache hinweisen: Ab sofort informieren wir Sie praxisnah und aktuell nicht nur über Datennutzung und Datenschutz, sondern auch über weitere Digitalisierungsthemen auf unserem neuen Blog

Digitalisierung & Recht,

erreichbar unter www.digitalisierungsrecht.eu. Unser Ziel: Die für die Praxis relevantesten Entwicklungen kurz und bündig, verständlich und zugänglich auf den Punkt gebracht.

Über Ihr Interesse würden wir uns sehr freuen! Auf unserem Blog werden Sie – neben vielen anderen Themen – auch den ein oder anderen Newsletter-Artikel künftig vorab finden. Gleichwohl werden wir Ihnen die wichtigsten Neuigkeiten auch weiterhin monatlich per E-Mail-Newsletter zukommen lassen.

Inhalt

Neues für Websites: Cookie-Banner und CMP datenschutzkonform gestalten

Digitale Identität: EU-Kommission schlägt Regelungsrahmen für sichere Identitätsnachweise vor

Können Betroffene auf ein „angemessenes Datensicherheitsniveau“ verzichten?

Neues zum Auskunftsanspruch – diesmal in Jugendamtsakten

Zu guter Letzt

Neues für Websites: Cookie-Banner und CMP datenschutzkonform gestalten

Wie Betreiber Websites datenschutzkonform gestalten können, ist nach wie vor ein Dauerbrenner. Von den Aufsichtsbehörden kommen nun weitere Hilfestellungen für die aus ihrer Sicht korrekte Gestaltung der Cookie-Banner und Consent Management Plattformen. Einiges ist dabei nicht neu, zwei Kritikpunkte dürften aber eine Vielzahl von Websites betreffen. Eine kritische Überprüfung der eigenen Websitegestaltung lohnt sich daher.

Vor rund einem Jahr starteten mehrere Datenschutzaufsichtsbehörden in Deutschland eine koordinierte Schwerpunktprüfung von Websites in Bezug auf den Einsatz von Cookies und die Einbindung von Drittanbieterdiensten. 49 Webangebote wurden dabei in 11 Bundesländern unter die Lupe genommen. Ende Juni veröffentlichten einige Aufsichtsbehörden nun eine erste Übersicht über besonders häufige Mängel, die für eine datenschutzkonforme Gestaltung jedenfalls zu vermeiden sind (etwa LDI NRW, HamBfDI, Sachsen).

Die daraus folgenden Vorgaben sind überwiegend nicht überraschend. In zwei Punkten aber adressieren sie Gestaltungsweisen, die weit verbreitet sind: Die farbliche Hervorhebung von „Alle akzeptieren“ und der Verzicht auf einen genauso einfach klickbaren Schalter „Alle ablehnen“ auf der ersten Ebene.

Umso wichtiger ist es, die eigenen Websites auf die Einhaltung dieser Eckpunkte zu überprüfen und sich bewusst für eine Beibehaltung oder Änderung zu entscheiden:

Reihenfolge

Einwilligungsbedürftige Datenverarbeitungsvorgänge dürfen erst starten, nachdem der Websitebesucher auf „OK“ geklickt hat, nicht bereits mit dem Aufrufen der Website selbst. Nach wie vor hätten dies viele Websites ausweislich der Pressemitteilungen der Aufsichtsbehörden nicht technisch korrekt umgesetzt.

Die technisch korrekte Umsetzung ist indes gerade in diesem Punkt zentral: Wenn Daten nur mit Nutzereinwilligung erhoben und verarbeitet werden dürfen, muss der Websitebetreiber die Abgabe dieser Einwilligung auch abwarten. Vor dem Klick auf „Akzeptiert“

darf keine Verarbeitung erfolgen, dürfen die Vorgänge noch nicht gestartet werden.

Informationen

Websitebesucher sind transparent über die Verarbeitungsvorgänge zu informieren. Oft geschieht dies auf erster Ebene durch übersichtliche Zusammenfassungen, die die wesentlichen Abläufe abbilden und für den Nutzer schnell zugänglich sind. Diese Aufteilung der Informationstiefe kritisieren die Aufsichtsbehörden nicht per se, weisen aber darauf hin, dass oftmals „nur unzureichende oder falsche Informationen über das Nutzertracking" gegeben würden.

Es bietet sich an, in regelmäßigen Abständen die Zusammenfassung auf der ersten Ebene des Cookie-Banners daraufhin zu überprüfen, ob die dortigen Ausführungen noch korrekt sind.

Technisch korrekte Erfassung von Einwilligungen und Widerrufen

Nach den Befunden der Aufsichtsbehörden wird der Nutzerklick auf „Alle ablehnen" oft technisch nicht korrekt umgesetzt, sondern es würden dennoch einwilligungsbedürftige Verarbeitungsvorgänge aktiviert. Hier sollte regelmäßig technisch geprüft werden, dass dies nicht geschieht.

Einwilligung ablehnen und Manipulationssorgen

Ein viel beachtetes Thema ist die Frage, ob bereits auf erster Ebene des Cookie-Layers ein „Alle ablehnen" erscheinen muss, oder ob „Alle akzeptieren" und „Einstellungen" ausreicht, wenn hinter „Einstellungen" dann eine Ablehnung auf zweiter Ebene erfolgen kann. Dies ist einer der Punkte, der jüngst auch von NOYB aufgegriffen und zum Gegenstand etlicher Beschwerden gemacht wurde: „Alle ablehnen" müsste genauso einfach mit einem Klick möglich sein, wie „Alle akzeptieren".

Dem schließen sich die Aufsichtsbehörden an: „Während bei allen Einwilligungsbannern auf der ersten Ebene eine Schaltfläche vorhanden ist, mit der eine Zustimmung zu sämtlichen Cookies und Drittdiensten erteilt werden kann, fehlt auf dieser Ebene häufig eine ebenso einfache Möglichkeit, das einwilligungsbedürftige

Nutzertracking in Gänze abzulehnen oder das Banner ohne Entscheidung schließen zu können."

Und sie gehen noch einen Schritt weiter: Oft würde die Ausgestaltung der Einwilligungsbanner die Nutzer unterschwellig zur Abgabe einer Einwilligung drängen, etwa durch farbliche Hervorhebung der Schaltfläche „Alle akzeptieren". Auch dies wird kritisch gesehen und als Manipulation der Nutzer eingeordnet.

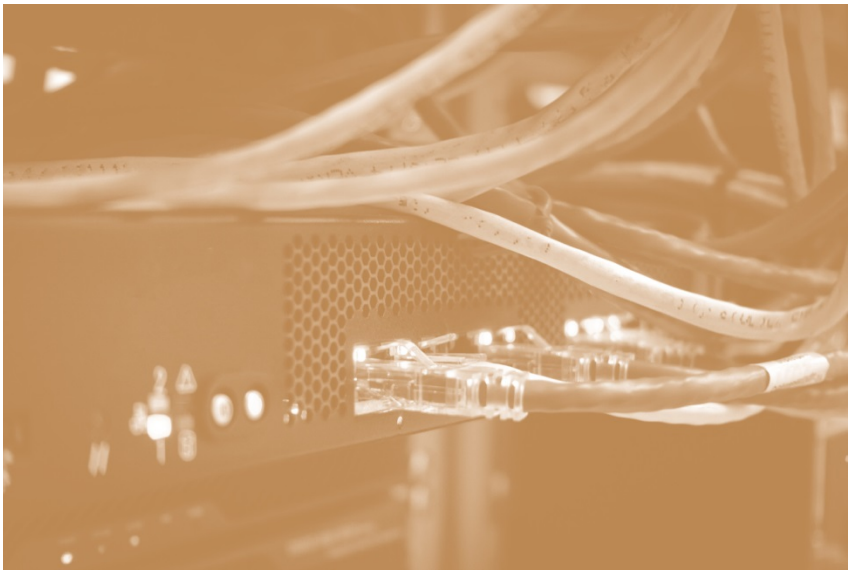
Ob die Position der Aufsichtsbehörden in diesem Punkt durchgreift, bleibt streitbar. Deutlich zeichnet sich damit aber ab, dass bei entsprechender Ausgestaltung ein aufsichtsbehördliches Verfahren droht und abweichende Meinungen sich womöglich allenfalls im Gerichtsverfahren durchsetzen lassen. Wenn daher eine entsprechende Gestaltung weiterhin präferiert wird, sollte dies nur nach umfassender Risikoabwägung erfolgen.

Digitale Identität: EU-Kommission schlägt Regelungsrahmen für sichere Identitätsnachweise vor

In einem weiteren Vorstoß, den europäischen Binnenmarkt für die Digitalisierung zu rüsten, schlägt die EU-Kommission einen Regelungsrahmen über sichere Identitätsnachweise für Unionsbürger und Unternehmen vor. Die wesentlichen Eckpunkte des Vorschlags stellen wir Ihnen vor.

Nach dem Verordnungsvorschlag der EU-Kommission soll es zukünftig allen Unionsbürgern, Einwohnern und Unternehmen möglich sein, ihre Identität digital über eine EU-weit anerkannte EUid-Brieftasche in elektronischer Form nachzuweisen (Informationsseite zur Digitalen Identität in englischer Sprache). Wie die Kommission Anfang Juni in einer Pressemitteilung erläuterte, sollen die Mitgliedstaaten ihren Bürgern digitale Brieftaschen zur Verfügung stellen, in denen diese ihre digitale Identität mit weiteren Nachweisen persönlicher Attribute wie dem Führerschein oder Abschlusszeugnis verknüpfen und EU-weit zum Identitätsnachweis online einsetzen können. Dadurch soll es den Bürgern ermöglicht werden, nicht auf private Dienste zum Identitätsnachweis zurückgreifen zu müssen und unnötige Datenweitergabe zu vermeiden. Für EU-Bürger, -Einwohner und -Unternehmen soll die Nutzung des Dienstes freiwillig sein, bestimmte große Plattformen sollen zur Einbindung der Identifikationsmöglichkeit verpflichtet werden.

Um eine schnelle Umsetzung zu ermöglichen, fordert die Kommission die Mitgliedsstaaten auf, bis September 2022 ein gemeinsames Instrument für die europäische Identität zu erarbeiten und auch im nationalen Recht die Möglichkeiten für einen digitalen Identitätsnachweis zu schaffen. Über den Verordnungsvorschlag der Kommission wird im Weiteren das EU-Parlament im Gesetzgebungsverfahren entscheiden – zeitgleich will die Kommission mit den Mitgliedstaaten an der technischen Ausarbeitung der digitalen Identität arbeiten.



Können Betroffene auf ein „angemessenes Datensicherheitsniveau“ verzichten?

Die Übermittlung sensibler Daten per E-Mail stößt immer wieder auf datenschutzrechtliche Bedenken. In einem Vermerk hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit nun seine Rechtsauffassung zu den Datensicherheitspflichten nach Art. 32 DSGVO und der möglichen Einwilligung in ein niedrigeres Datensicherheitsniveau dargelegt – und zeigt sich dabei sehr praxisfreundlich. In diesem Beitrag stellen wir Ihnen die Einschätzung vor.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HamBfDI) hat in einem Vermerk dazu Stellung bezogen, ob Betroffene auf das nach Art. 32 DSGVO erforderliche Datensicherheitsniveau verzichten können. Anlass war die Frage, ob sensible Daten wie Gesundheitsdaten oder Steuerinformationen von Ärzten, Anwälten oder Steuerberatern per E-Mail ohne eine Ende-zu-Ende-Verschlüsselung verschickt werden können, wenn die betroffene Person damit einverstanden ist, eigentlich aber nach Art. 32 DSGVO die Verschlüsselung erfolgen müsste.

Zur Erinnerung: Art. 32 DSGVO gibt Datenverarbeitern, Verantwortlichen sowie Auftragsverarbeitern vor, ein für die Datenverarbeitungssituation angemessenes Niveau der Datensicherheit zu schaffen. Dies hat der Datenverarbeiter durch Abwägung der Risiken der Verarbeitung, der

Implementierungskosten und der Art, Weise und des Umfangs der Datenverarbeitung zu ermitteln und entsprechende Maßnahmen zu treffen. Das Niveau und die zu treffenden Maßnahmen sind dabei nicht abschließend vorgeschrieben, sondern risiko- und situationsabhängig. Bei der Übermittlung sensibler Daten wie Gesundheitsdaten per E-Mail wird es regelmäßig erforderlich sein, dass die E-Mail-Kommunikation Ende-zu-Ende verschlüsselt ist. Eine reine Transportverschlüsselung ist regelmäßig nicht ausreichend. Zu datenschutzrechtlichen Problemen führt es, wenn eine der beiden Seiten dieses Verschlüsselungsniveau nicht einhalten kann oder will. In diesen Fällen stellt sich die Frage, ob solche Daten trotzdem versendet werden dürfen, wenn der Betroffene darin einwilligt ist.

Selbstbestimmungsrecht der Betroffenen

Nach der Analyse des HamBfDI ist das eine Frage des (informationellen) Selbstbestimmungsrechts über personenbezogene Daten. Zwar sei es das Ziel der DSGVO, ein allgemeines, möglichst hohes und einheitliches Schutzniveau für personenbezogene Daten zu schaffen. Gleichzeitig solle aber auch das individuelle Selbstbestimmungsrecht der Betroffenen über ihre personenbezogenen Daten geschützt werden. Zum Selbstbestimmungsrecht gehöre es auch - so der HamBfDI - Entscheidungen darüber zu treffen, Daten unter einem suboptimalen Schutz verarbeiten zu lassen. Der HamBfDI vergleicht dies mit der Veröffentlichung sensibler Daten: Diese möge zwar in manchen Fällen nicht die objektiv klügste Entscheidung sein, es stehe dem Einzelnen aber zweifelsohne zu. Es sei von der Rechtsordnung gedeckt, auch solche Entscheidungen über seine personenbezogenen Daten ohne Bevormundung zu treffen. So solle es sich auch mit der Entscheidung über ein niedrigeres Schutzniveau bei der Datenübertragung verhalten.

Aber: Verpflichtung der Verarbeiter

Während dem Betroffenen also die freie Entscheidung zusteht, ein niedrigeres Schutzniveau für seine personenbezogenen Daten zu wählen, sind die Datenverarbeiter nach Art. 32 DSGVO verpflichtet, ein geeignetes und angemessenes Niveau sicherzustellen. Dabei merkt der HamBfDI an, dass es für die Bestimmung des Niveaus nicht auf den Einzelfall, sondern auf das typische, für solche Verarbeitungssituationen angemessene Niveau ankommt. Deshalb

müssten Datenverarbeiter grundsätzlich und unabhängig von dem möglichen Willen einzelner Betroffener die Vorkehrungen treffen, die zur Einhaltung des angemessenen Niveaus erforderlich sind. Im konkreten Fall der E-Mail-Kommunikation heißt das, dass die Ende-zu-Ende-Verschlüsselung zumindest auf der eigenen Seite technisch und operationell ermöglicht werden muss.

Dadurch wird dann auch die Freiwilligkeit der Betroffenen gewahrt: Diese können zwischen einem angemessenen und abgesenkten Schutzniveau frei entscheiden, auch, weil der Verpflichtete ein angemessenes Schutzniveau anbietet. Die Einwilligung in ein sub-optimales Schutzniveau ist nicht notwendig, um die Leistung erhalten zu können. Problematisch sind also dann vor allem solche Geschäftsmodelle, im Rahmen derer keine angemessenen Maßnahmen umgesetzt werden. Die Freiwilligkeit könnte sich dann allenfalls in der freiwilligen Teilnahme widerspiegeln. Dieses Problem potenziert sich, wenn es sich um Anwendungen handelt, die für die Betroffenen dringend notwendig sind und/oder keine Alternativen am Markt bestehen.

Einwilligung in niedrigeres Niveau möglich

Ist das gewährleistet, soll es dem einzelnen Betroffenen möglich sein, durch Einwilligung auf die Implementierung des nach Art. 32 DSGVO erforderlichen Datenschutzniveaus zu verzichten. Die Einwilligung muss allerdings die Voraussetzungen der Art. 6 Abs. 1 UAbs. 1 lit. a, Art. 7 DSGVO erfüllen, also insbesondere nach angemessener Aufklärung und üblicherweise schriftlich und nur für den Einzelfall erteilt werden.

Noch einmal zusammengefasst bestehen also die folgenden Voraussetzungen:

1. Der Verantwortliche oder Auftragsverarbeiter hat das erforderliche Datensicherheitsniveau nach Maßgabe des Art. 32 DSGVO geschaffen. Die Möglichkeit der Einwilligung des Betroffenen soll nicht genutzt werden, um Kosten zu sparen und den Betroffenen niedrigere Datensicherheit „aufzudrücken".

2. Die Einwilligung des Betroffenen muss die strengen Anforderungen der Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO und Art. 7 DSGVO erfüllen, bei sensitiven Daten auch des Art. 9 Abs. 2

lit. a DSGVO. Insbesondere muss die Einwilligung freiwillig und informiert erfolgen.

Sind diese Bedingungen erfüllt, hält der HamBfDI die Abweichung vom Niveau des Art. 32 DSGVO für zulässig.

Positive Einschätzung unter Vorbehalt

Bei dem Vermerk des HamBfDI handelt es sich um die Darlegung der Rechtsauffassung einer einzelnen Aufsichtsbehörde. Andere Aufsichtsbehörden und auch Stimmen in der Fachliteratur beurteilen die Abdingbarkeit des Art. 32 DSGVO anders. Neben verschiedenen rechtsdogmatischen Bedenken wird vor allem die Befürchtung geäußert, große Datenverarbeiter könnten Betroffenen ein niedrigeres Datenschutzniveau aufzwingen (s.o.). Aus diesem Grund wird die Frage der Abdingbarkeit des Art. 32 DSGVO teilweise verneint. Dem HamBfDI war daran gelegen, mit seinem Vermerk aufzuzeigen, dass und wie für Berufsgruppen wie Ärzte, Anwälte und Steuerberater, die regelmäßig Umgang mit sensiblen Daten haben, eine Übertragung per (nicht verschlüsselter) E-Mail möglich ist.

Dabei könnte der Ansatz des HamBfDI einen auch für andere Behörden akzeptablen Kompromiss darstellen, da der Verpflichtete in jedem Fall das Angebot mit angemessenem Datensicherheitsniveau bereitstellen muss. Es ist daher nicht möglich – und dies sind oftmals die in der Praxis diskutierten Fälle – generell seitens der Verpflichteten auf ein angemessenes Datensicherheitsniveau zu verzichten und dies durch Einwilligungen der Betroffenen zu erlauben. Abweichend davon betont der HamBfDI, dass es eine echte Wahlmöglichkeit für die Betroffenen zwischen „Angebot mit angemessenem Datensicherheitsniveau“ und „Angebot mit abgesenktem Sicherheitsniveau“ geben muss.

Der Ansatz des HamBfDI wird daher in der Praxis vornehmlich dort helfen, wo grundsätzlich ein angemessenes Sicherheitsniveau gewährleistet ist, Betroffene dafür erforderliche Mitwirkungshandlungen aber meiden möchten. Ganz besonders interessant dürfte sein, ob sich aus dem Ansatz des HamBfDI auch eine Aussage zum Drittstaatentransfer ableiten lässt. Also ob Betroffene beispielsweise in eine Datenübermittlung in die USA

einwilligen können, obwohl keine hinreichenden Sicherungsmaßnahmen für das Datenschutzniveau bestehen.

Neues zum Auskunftsanspruch – diesmal in Jugendamtsakten

Immer wieder stehen Informations- und Auskunftsansprüche datenschutzrechtlichen Bedenken gegenüber (oder wird das Datenschutzrecht zur Abwehr solcher Ansprüche instrumentalisiert). In einem vom OVG Saarlouis entschiedenen Fall scheiterte ein Vater bei der Einsicht in die Jugendamtsakten seiner Kinder an einer Vorschrift über den Schutz von Sozialdaten. In diesem Beitrag stellen wir Ihnen die wesentlichen Aspekte der Entscheidung vor.

Das Oberverwaltungsgericht Saarlouis (OVG) entschied in einem Berufungsverfahren (Beschluss vom 19.04.2021 – 2 A 370/20), dass das Jugendamt einem Vater zurecht die Einsichtnahme in die vom Jugendamt geführte Akte über seine Töchter verwehrte. Vorhergegangen war ein Streit zwischen dem Vater und dem Jugendamt: Der von der Mutter der gemeinsamen Kinder geschiedene Vater hatte zwar das Sorgerecht, aber keinen Kontakt mehr zu den Kindern, die bei der Mutter lebten. Als sich eines der Kinder in psychiatrische Behandlung begab, verlangte der Vater zunächst von der Mutter und anschließend vom Jugendamt Auskunft über den gesundheitlichen Zustand der Tochter und die Hintergründe der psychiatrischen Behandlung. Sowohl die Mutter als auch das Jugendamt verweigerten die Auskunft mit der

Begründung, die Tochter wolle nicht, dass der Vater diese Informationen erhält.

Daraufhin klagte der Vater gegen das Jugendamt auf Akteneinsicht. Begründet wurde das Auskunftsverlangen mit der Ausübung des elterlichen Sorgerechts: Ohne Information über den gesundheitlichen Zustand des Kindes sei dies dem Vater nicht möglich. Das Jugendamt verwehrte die Auskunft und Akteneinsicht unter Bezugnahme auf § 65 SGB VIII. Diese Norm begründet einen besonderen Vertrauensschutz für Sozialdaten, die Mitarbeitern des Jugendamtes zur Wahrnehmung ihrer Aufgaben anvertraut wurden, und erlaubt die Weitergabe oder Übermittlung dieser Daten nur unter engen Voraussetzungen, unter anderem, wenn eine Einwilligung des Betroffenen vorliegt. Diese Voraussetzungen seien für das Auskunftsbegehren des Vaters nicht erfüllt gewesen, entsprechend dürfe keine Akteneinsicht gewährt werden.

Das OVG Saarlouis bestätigte die Ansicht der Behörde. Mit § 65 SGB VIII habe der Gesetzgeber eine Abwägung zwischen der Effektivität der Kinder- und Jugendhilfe und dem aus dem Elternrecht abzuleitenden allgemeinen Informationsrecht getroffen: Kinder und Jugendliche müssten darauf vertrauen können, dass die Angaben, die sie gegenüber dem Jugendamt machen, nur unter den engen Voraussetzungen des § 65 SGB VIII herausgegeben werden. Ohne dieses Vertrauen sei es nicht möglich, die Kinder- und Jugendhilfe effektiv wahrzunehmen. § 65 SGB VIII sei insofern auch mit der DSGVO vereinbar, da die Norm zusätzliche Vorgaben enthalte, die den Schutz der Daten der Betroffenen verstärkten. Außerhalb der Voraussetzungen des § 65 SGB VIII bleibe deshalb auch kein Raum für einen elterlichen Informationsanspruch, weshalb die Klage des Vaters scheiterte.

Zu guter Letzt

In diesem Monat wurden wieder einige spannende, teils auch hohe Bußgelder verhängt. Ein Thema betrifft den Vorwurf der Ausspionage der eigenen Mitarbeiter durch IKEA in Frankreich, welche auch strafrechtliche Konsequenzen nach sich zog. Weiter befassten sich die Datenschutzbehörden etwa mit dem Einsatz von Körperkameras bei Fahrkartenkontrolleuren, dem Versenden unerwünschter Werbung und dem Einsatz biometrischer Technologie zur Durchsetzung eines Hausverbots.

- **Luxemburg: Bußgeld i.H.v. 15.000 Euro und Stärkung des DSB**

Die Rolle des DSB stärkt eine Entscheidung der Datenschutzaufsichtsbehörde in Luxemburg, mit der gegen ein Logistikunternehmen ein Bußgeld i.H.v. 15.000 Euro verhängt wurde, weil dem DSB seine Aufgabenerfüllung nicht gem. Art. 28, 29 DSGVO ermöglicht wurde. Konkret bemängelte die Aufsichtsbehörde, dass der DSB nicht zu allen relevanten Meetings eingeladen und nicht rechtzeitig in die datenschutzrelevanten Themen eingebunden wurde. Hinzu kam, dass er nicht direkt an die Geschäftsführung berichtete und weder ein regelmäßiges Monitoring noch ein Auditplan implementiert waren.

- **Spanien: Kein Einsatz von Gesichtserkennung zur Durchsetzung eines rechtskräftigen Hausverbots**

Ein spanisches Gericht verbot einem Supermarkt die Nutzung von Gesichtserkennungssystemen, um wegen eines gewaltsamen Raubüberfalls in dem Supermarkt verurteilte Personen mit einem Hausverbot am Betreten ihrer Räumlichkeiten zu hindern. Es fehle an einer Erlaubnis für die Verarbeitung von biometrischen und damit besonders sensitiven Daten. Ein öffentliches Interesse könne dies nicht erlauben, vielmehr wäre eine Einwilligung erforderlich gewesen. Darauf könne weder unter Verweis auf eine besonders kurze Verarbeitungsdauer noch auf die Vorfälle verzichtet werden. Die Verurteilung einer Person beraube sie nicht automatisch ihres Rechts auf Privatsphäre. Gerade biometrische Technologien seien besonders invasiv.

- **Italien: Bußgeld i.H.v. rund 2,8 Mio. Euro wegen unerwünschter Werbung und Adresshandel**

Die italienische Datenschutzbehörde verhängte das Bußgeld gegen Iren Mercato S.p.A., ein im Energiesektor tätiges Unternehmen. Anlass waren Beschwerden mehrerer Betroffener wegen unerwünschter Werbung, welche sie ohne vorherige Einwilligung erhalten hatten. Das Unternehmen hatte personenbezogene Daten für Telemarketing-Aktivitäten verarbeitet, die es nicht selbst erhoben, sondern aus anderen Quellen erworben hatte. Dabei war nicht geprüft worden, ob für alle Übermittlungen der Daten gültige Einwilligungen der Werbeadressaten vorlagen. Das Unternehmen, von dem Iren Mercato die Daten erhalten hatte, hatte diese wiederum von zwei anderen Unternehmen erworben. Die diesen erteilte Einwilligung umfasste zwar das von ihnen und von Dritten durchgeführte Telefonmarketing, allerdings nicht die Weitergabe von Kundendaten an Iren Mercato. Die Einwilligung, die ein Kunde einem Unternehmen für Werbemaßnahmen Dritter erteilt, könne nicht auf spätere Übertragungen an andere Werbetreibende erstreckt werden. Erschwerend wurde neben der Dauer des Verstoßes und der Anzahl der Betroffenen in Höhe von mehreren Millionen berücksichtigt, dass die Werbeaktivitäten erst mit Aufnahme behördlicher Ermittlungen eingestellt wurden.

- **Schweden: Bußgeld i.H.v. ca. 1,5 Mio. Euro wegen Einsatzes von Körperkameras durch Fahrkartenkontrolleure**

Gegen die Stockholmer Nahverkehrsgesellschaft wurde ein Bußgeld i.H.v. 1.566.125 Euro erlassen. Die Körperkameras, die ihre Fahrkartenkontrolleure trugen, fertigten kontinuierlich Video- und Tonaufzeichnungen an, welche nach einer Minute gelöscht wurden, sofern der Kontrolleur nicht die Aufnahmetaste der Kamera betätigte. Damit sollten bedrohliche Situationen verhindert, Vorfälle dokumentiert und sichergestellt werden, dass die richtige Person mit einem Bußgeld wegen Schwarzfahrens belegt wird. Die Datenschutzbehörde entschied, dass die Datenverarbeitung für diesen Zweck zu umfangreich und in Teilen überhaupt nicht dienlich gewesen sei. Die Voraufnahmezeit sei für die Zweckerreichung nicht erforderlich gewesen und hätte auf maximal 15 Sekunden reduziert werden müssen. Auch die Audioaufzeichnungen trügen nicht zur Identifizierung von Personen ohne gültigen Fahrschein bei. Dies begründe eine Verletzung der Prinzipien der Rechtmäßigkeit und Transparenz sowie der Datenminimierung. Auch wurde nicht rechtmäßig über die Datenverarbeitung informiert – die Betroffenen wussten nicht einmal um die Tonaufzeichnungen.

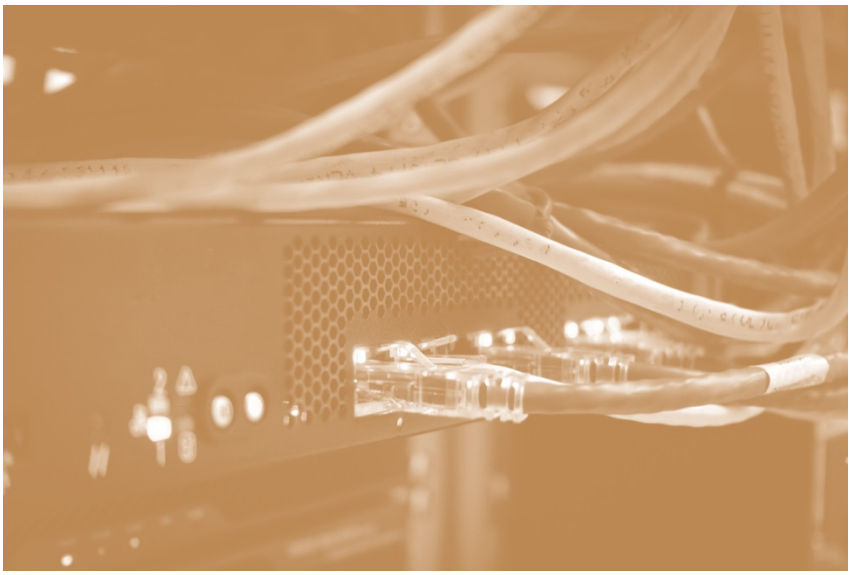
- **Frankreich: Spionage bei Ikea?**

Das Strafgericht Versailles verhängte ein Bußgeld i.H.v. 1 Mio. Euro gegen IKEA. Dieses steht im Zusammenhang mit einem langjährigen Strafverfahren gegen IKEA-Manager. Inhalt war die ausufernde Ausspionierung der französischen Mitarbeiter von IKEA, die weit in das Privatleben der Betroffenen hineinreichte. So waren Kontoauszüge von Beschäftigten ausgewertet und Berichte zu ihren Personen angefertigt worden. Auch ein Zugang zu Polizeiakten soll erkauft worden sein. Diese Vorgehensweise soll dazu gedient haben, gezielt gegen Gewerkschaftsführer vorzugehen und sich in Konfliktfällen Vorteile verschaffen zu können.

- **Frankreich: Bußgeld i.H.v. 500.000 Euro wegen unzureichenden Umgangs mit personenbezogenen Daten ungenutzter Accounts eines Online-Shops**

Die französische Datenschutzbehörde CNIL überprüfte die Verarbeitung von personenbezogenen Daten von Interessenten und Kunden, die über einen Account bei BRICO PRIVÉ – einem Online-Shop zu den Themen Heimwerken und Gartenarbeit – verfügten,

dreimal zwischen 2018 und 2021. Die Überprüfung von 2018 ergab, dass BRICO PRIVÉ keine Aufbewahrungsfrist für gespeicherte Nutzerdaten definiert und somit auch keine regelmäßige Löschung oder Archivierung nicht länger benötigter Daten vorgenommen hatte. So waren in der Datenbank auch Daten von Personen enthalten, welche seit über fünf Jahren keine Bestellung mehr aufgegeben hatten. Das Unternehmen führte danach zwar neue Richtlinien für die Aufbewahrung von Nutzerdaten ein, welche vorsahen, dass diese aus der aktiven Datenbank entfernt werden, wenn das zugehörige Konto gelöscht wird oder für drei Jahre inaktiv bleibt. Nach dieser Zeit sollten die Daten bis zum Ablauf gesetzlicher Fristen archiviert, soweit für vorgerichtliche oder prozessuale Zwecke erforderlich, und danach gelöscht werden. Auch diese seien aber nicht ordnungsgemäß angewandt worden: Daten wurden deutlich länger aufbewahrt, als es die Richtlinien vorsahen. Dies sei eine Verletzung des Prinzips der Speicherbegrenzung. Außerdem habe der Bußgeldempfänger die Betroffenen nicht ordnungsgemäß über die Verarbeitung der Daten informiert. Löschungsanfragen der Betroffenen sei ebenfalls nicht ordnungsgemäß nachgekommen worden, die Accounts wurden lediglich deaktiviert.



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

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@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