2020

TÄTIGKEITSBERICHT

Rückblick auf das Datenschutzjahr 2020 und die ausgeführten Tätigkeiten der Union Betriebs-GmbH im Rahmen des Datenschutzes

UBG

LIEBE LESER*,

das Jahr 2020 verlief wohl in vielerlei Hinsicht nicht wie geplant. Die leider immer noch anhaltende Pandemie stellte uns bereits zu Beginn des letzten Jahres vor große Herausforderungen.

Viele von Ihnen mussten im Eiltempo das Thema Home-Office voranbringen und umsetzen, Veranstaltungen und Sitzungen konnten nicht auf die gewohnte Weise stattfinden, sondern nur unter strengen Bestimmungen oder sie mussten virtuell umgesetzt werden. Und bei allen Änderungen und Problemen durfte der Datenschutz nicht außer Acht gelassen werden.

Welche Videokonferenz-Plattform ist am ehesten datenschutzkonform? Worauf muss im Home-Office geachtet werden? Wie schütze ich mich am besten gegen Hacker und Phisher? Darf sich Mickey Maus auf meine Teilnehmerliste schreiben und wie lange muss ich die Daten aufbewahren?

Und als ob das nicht schon genug wäre, fällten die Gerichte dieses Jahr auch einige weitreichende Urteile, die nach wie vor eine unsichere Rechtslage vorweisen und uns in der Arbeit als Verantwortliche im Datenschutz einschränken.

Als externe Datenschutzbeauftragte für Ihre Geschäftsstelle bin ich der Meinung, dass wir das Jahr 2020 trotz der uns in den Weg gelegten Steine sehr gut gemeistert haben.

Ich freue mich auf die weitere Zusammenarbeit mit Ihnen.
Bleiben Sie gesund!

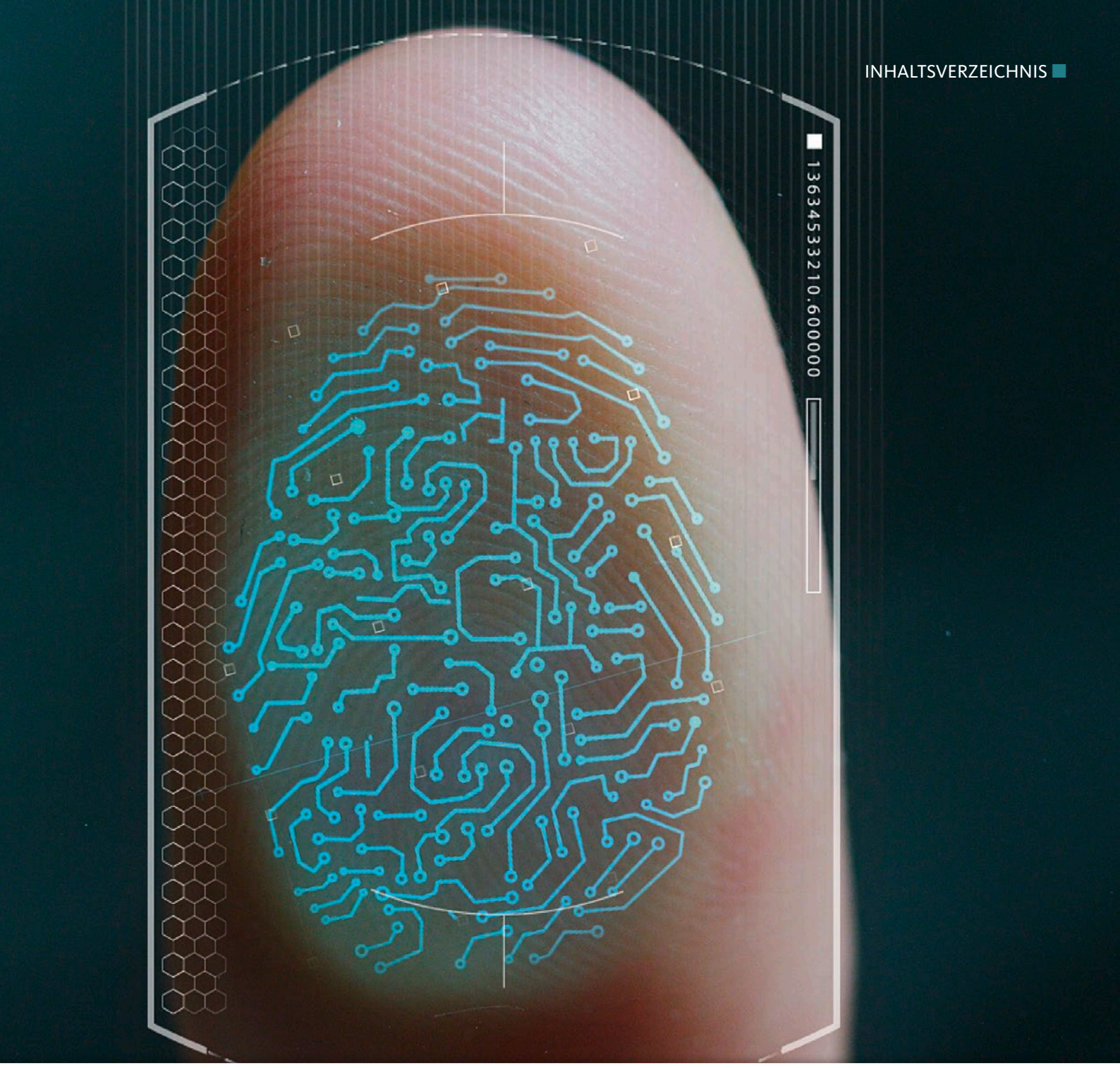
Barbara von Meer
Datenschutzbeauftragte,
Rechtsanwältin (Syndikusrechtsanwältin)

** Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in diesem Bericht die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und stellt keine Wertung dar.*

„UNSERE FREIHEIT BERUHT AUF DEM, WAS ANDERE NICHT ÜBER UNSERE EXISTENZ WISSEN.“

■ Alexander Solschenizyn

INHALT



WICHTIGE GERICHTSURTEILE

NEWSLETTER

AUSBLICK 2021

BEDEUTUNG DES DATENSCHUTZES

Gerade in Zeiten, in denen die Digitalisierung immer mehr Bedeutung für den Staat, die Gesamtgesellschaft aber auch den Einzelnen gewinnt, wird die Frage nach datenschutzrechtlichen Aspekten immer lauter und dringender. Wenn überall persönliche Daten des Individuums gespeichert und verwertet werden, wie sind diese dann am besten zu schützen?

In Deutschland gewährleistet das Grundgesetz jedem Bürger das Recht, selbst über die Preisgabe und Verwendung von Informationen zu seiner Person zu bestimmen. Auf Grundlage dessen hat das Bundesverfassungsgericht 1983 das Grundrecht auf informationelle Selbstbestimmung beziehungsweise das Grundrecht auf Datenschutz entwickelt. Dieses Selbstbestimmungsrecht wurde dann Grundlage für das Bundesdatenschutzgesetz (BDSG) und die Landesdatenschutzgesetze, welche die Datenschutzgrundsätze in Deutschland regeln.

Die EU-Datenschutzverordnung ist eine Verordnung der Europäischen Union, die Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zu deren freien Verkehr enthält. Sie soll die Grundrechte und -freiheiten natürlicher Personen schützen – besonders das Recht auf Schutz der persönlichen Daten. Der Datenschutz soll jedem Bürger Schutz vor missbräuchlicher Datenverarbeitung und den Schutz der Privatsphäre garantieren.

Aus diesem Grund ist die Verarbeitung oder das Verwenden von personenbezogenen Daten (vor allem zum gewerblichen Zweck) grundsätzlich verboten, es sei denn

- die Verarbeitung wird durch eine rechtliche Grundlage gestattet oder
- es liegt eine ausdrückliche, rechtsgültige Einwilligung des Betroffenen vor.

Des Weiteren sollen, im Sinne der Datenschutzgrundsätze, in jedem Fall so wenige Daten wie möglich und nur mit der Kenntnis des Betroffenen erhoben werden. Sie unterliegen einer Zweckbindung und sind zu löschen, sobald der Zweck der Erhebung nicht mehr besteht. Außerdem sind technische und organisatorische Maßnahmen zu treffen, die eine missbräuchliche Datenverarbeitung verhindern.

Die Betroffenen haben das Recht, sich über die Verarbeitung ihrer persönlichen Daten zu informieren (also ein Auskunftsrecht) und gegebenenfalls einen Widerspruch einzulegen beziehungsweise die Berichtigung oder Löschung anzuordnen.

ENTWICKLUNGEN IM JAHR 2020

ZUNAHME DER CYBERKRIMINALITÄT

Besonders während der Corona-Krise haben sich digitale Technologien im privaten und geschäftlichen Alltag etabliert. Technologien wie Cloud Computing, Videokonferenzen, Online-Seminare oder Social Media werden vermehrt eingesetzt. Home-Office ist die Lösung in der Krise.

Leider ist das eine Lage, die Cyberkriminelle für sich ausnutzen. Denn das Klima der Angst und die zunehmende Anzahl an Home-Office-Arbeitsplätzen sind ein idealer Nährboden für erfolgreiche Hackerangriffe. Allein in den ersten 100 Tagen der Corona-Krise haben die Hackerangriffe um 33% zugenommen. So ist Schadsoftware, die per E-Mail verbreitet wird, ein großes Problem in der Praxis. Inzwischen sind E-Mails mit Schädlingen derart „gut" gemacht, sodass es für Empfänger sehr schwer zu erkennen ist, dass es sich dabei um einen Angriff handelt. Die E-Mails werden immer zielgerichteter, mit korrekter Anrede versehen und stammen dabei vermeintlich von Absendern, mit denen die Opfer in der Vergangenheit tatsächlich in Kontakt standen.

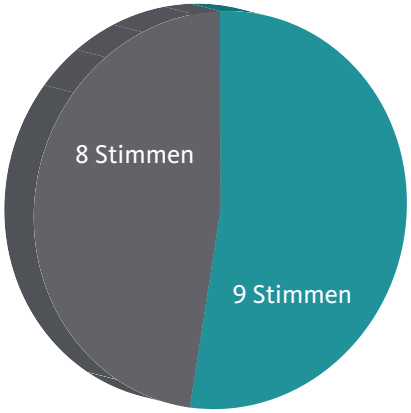
Man spricht in diesem Zusammenhang auch von „Spear Phishing". Einer der bekanntesten Vertreter von Malware, der diese Angriffsart nutzt, ist der extrem gefährliche „Emotet", meist in Kombination mit weiterer Schadsoftware wie „Trickbot" und „Ryuk". Auf einem mit Emotet befallenen Rechner werden nicht nur die Adressbücher des betroffenen E-Mail-Clients, sondern auch die E-Mail-Inhalte ausgelesen und auf einen Server der Angreifer kopiert. Damit können diese weitere gezielte Angriffe durchführen, die mit den echten E-Mail-Inhalten täuschend echt erscheinen.

Quantität ist besser als Qualität – diesen Slogan schreiben sich Cyberkriminelle nach wie vor auf die Fahne. Entsprechend ist eine der größten Gefahren das breite Netz, das Cyberkriminelle mit Phishing per E-Mail oder über soziale Medien auswerfen. Mitarbeiter müssen durch gezielte Security Awareness Trainings auf diese Gefahren und die Tricks der Betrüger aufmerksam gemacht werden und lernen, wie mit diesen Bedrohungen umzugehen ist.

Entsprechende Mitarbeiterschulungen wurden 2020 von uns angeboten. Ebenso wurde durch zahlreiche Newsletter zu Cybersicherheit und Home-Office auf aktuelle Bedrohungen aufmerksam gemacht. Diese Maßnahmen spielen eine enorm wichtige Rolle und können als ein zentraler Baustein des gelebten Datenschutzmanagements auch für Verfahren mit Aufsichtsbehörden essentiell werden.

MICROSOFT 365

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) hat in einer Pressemitteilung vom 02.10.2020 erklärt, dass sie „mehrheitlich zustimmend zur Kenntnis genommen“ hat, „dass [...] kein datenschutzgerechter Einsatz von Microsoft 365 möglich ist“. Die DSK folgt damit einer Bewertung, die der von ihr eingesetzte „Arbeitskreis Verwaltung zur Auftragsverarbeitung bei Microsoft 365“ im Juli 2020 abgegeben hat.



Sie müssen deswegen aber nicht sofort aufhören Microsoft 365 zu nutzen, denn die DSK ist sich hier uneinig. Sie hat die Einschätzung des Arbeitskreises nur „mehrheitlich zustimmend zur Kenntnis genommen“. Und mehrheitlich bedeutet hier die knappe Mehrheit von 9 zu 8 Stimmen. Gegen die uneingeschränkte Zustimmung sprachen sich unter anderem die Landesbeauftragten für den Datenschutz Baden-Württemberg, Bayern, Hessen und im Saarland sowie der Präsident des Bayerischen Landesamts für Datenschutzaufsicht aus, das für die Microsoft Deutschland GmbH zuständig ist. Zwar sehen auch diese Aufsichtsbehörden Verbesserungspotenzial, dennoch halten sie die Bewertung des Arbeitskreises für zu undifferenziert. Außerdem basiere sie auf den Datenschutzbestimmungen vom Januar 2020. Diese sind zwischenzeitlich schon zweimal überarbeitet worden.

Microsoft selbst hat Ende November 2020 verkündet, dass es neue Schutzmaßnahmen umsetzen wird. Dazu gehören vertragliche Verpflichtungen, Herausgabeverlangen von staatlichen Stellen anzufechten sowie eine finanzielle Verpflichtung. Weiterhin wird Microsoft einen Zusatz zur Datenschutzvereinbarung (DPA) mit seinen Kunden aufnehmen. Ob diese Bemühungen ausreichen werden, alle Datenschutzbehörden zu überzeugen, wird sich zeigen.

Es ist aber aktuell nicht damit zu rechnen, dass Microsoft 365 in den nächsten Monaten seitens der Aufsichtsbehörden verboten wird oder mit Bußgeldern oder Untersagungsanordnungen zu rechnen ist.

EINSATZ VON VIDEOKONFERENZSYSTEMEN

Videokonferenzsysteme haben in der Corona-Krise eine zentrale Rolle für die Kommunikation erlangt. Im Rahmen von Videokonferenzen werden personenbezogene Daten der teilnehmenden Personen verarbeitet, Metadaten über die Durchführung der Kommunikation, Daten über die beruflichen Kontakte und viele mehr.

Videokonferenzsysteme sind gemäß Art. 24 und 25 DS-GVO durch Auswahl und Umsetzung geeigneter technischer und organisatorischer Maßnahmen so einzurichten, dass sie den Anforderungen der DS-GVO an die Verarbeitung personenbezogener Daten genügen. So müssen sie eine Verschlüsselung nach dem Stand der Technik implementieren. Nähere Informationen finden sich in der aktuellen Orientierungshilfe Videokonferenzsysteme der Aufsichtsbehörden vom 23. Oktober 2020 *https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSKBeschluessePositionspapiere/Nov20_Checkliste-OH-Videokonferenzsysteme.html?nn=5217228*

VERSCHMELZUNG VON HARDWARE

Im Home-Office wird oftmals auf private Hardware-Geräte zurückgegriffen, um dienstliche Angelegenheiten zu regeln. Das ist aus Datenschutz-Sicht problematisch: Die Vermischung von Privat- und Berufsleben auf einem privaten Endgerät, häufig mit dem Schlagwort Bring-Your-Own-Device (BYOD) zusammengefasst, birgt große Probleme, die schnell zu Datenschutzverstößen führen können.

SANKTIONSMÖGLICHKEITEN UND ABHILFEBEFUGNISSE DER AUFSICHTSBEHÖRDEN

Die DS-GVO sieht erstmals europaweit einheitliche Abhilfebefugnisse vor. Dabei fügt sich die Bußgeldbefugnis in ein Gesamtsystem an differenzierten Abhilfemaßnahmen der Datenschutzbehörden zur Rechtsdurchsetzung ein. Diese reichen von bloßen Warnungen und Verwarnungen über Anordnungen bis hin zur Verhängung von Geldbußen. Die Datenschutzbehörden können im Rahmen ihres Ermessens zwischen verschiedenen Abhilfemaßnahmen wählen oder mehrere kumulativ anwenden.

Nach Art. 58 Abs. 2 lit. i) in Verbindung mit Art. 83 Abs. 4 bis 6 DS-GVO sind für formelle Verstöße Geldbußen von bis zu 10.000.000 Euro oder zwei Prozent des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres und für materielle Verstöße bis zu 20.000.000 Euro oder vier Prozent des weltweiten Jahresgesamtumsatzes des vorangegangenen Geschäftsjahres möglich. Abweichend von der bisherigen deutschen Rechtstradition gilt dabei die darüberhinausgehende, europäische unmittelbare Verbandshaftung innerhalb eines Konzerns. Damit hat die EU den Verstößen gegen das europäische Datenschutzrecht die gleiche Bedeutung und Tragweite zuerkannt, wie für Verstöße gegen das europäische Wettbewerbsrecht.

In der folgenden Tabelle finden Sie eine Übersicht zu den möglichen Geldbußen und Strafen, die mit der Einführung der DS-GVO und der Erneuerung des BDSG möglich sind (inklusive der jeweiligen Rechtsgrundlagen):

VERSTOSS	SANKTION	RECHTLICHE GRUNDLAGE
Bußgeldbewehrte Ordnungswidrigkeit		
unzulässige Verarbeitung der personenbezogenen Daten von Kindern (Einwilligung eines Kindes erst ab 16 Jahren wirksam, bei jüngeren Kindern ist die Einwilligung der Sorgeberechtigten erforderlich)	bis 10 Mio. € oder bei Unternehmen bis 2 % des weltweiten Jahresumsatzes**	Art. 8, 83 Abs. 4a DS-GVO
unnötige Aufbewahrung, Einholung oder Verarbeitung von personenbezogenen Daten zum Zwecke der Identifizierung einer Person, obwohl dies nicht oder nicht mehr erforderlich ist	bis 10 Mio. € oder bei Unternehmen bis 2 % des weltweiten Jahresumsatzes**	Art. 11, 83 Abs. 4a DS-GVO
keine geeigneten technischen und organisatorischen Maßnahmen (TOM) zum Schutz der verarbeiteten personenbezogenen Daten ergriffen	bis 10 Mio. € oder bei Unternehmen bis 2 % des weltweiten Jahresumsatzes**	Art. 25, 83 Abs. 4a DS-GVO
Verstoß gegen die festgeschriebenen Aufgaben des Datenschutzbeauftragten	bis 10 Mio. € oder bei Unternehmen bis 2 % des weltweiten Jahresumsatzes**	Art. 39, 83 Abs. 4a DS-GVO
Verstoß gegen die Vorgaben zur Zertifizierung (Datenschutz-Audit)	bis 10 Mio. € oder bei Unternehmen bis 2 % des weltweiten Jahresumsatzes**	Art. 42, 83 Abs. 4a, b DS-GVO
keine geeigneten Maßnahmen bei einem Verstoß gegen die Verhaltensregeln	bis 10 Mio. € oder bei Unternehmen bis 2 % des weltweiten Jahresumsatzes**	Art. 41, 83 Abs. 4c DS-GVO
Verstoß gegen die Grundsätze der Verarbeitung von personenbezogenen Daten (u. a. Rechtmäßigkeit, Transparenzgebot, Zweckbindung, Datenminimierung, Speicherbegrenzung, Rechenschaftspflicht)	bis 20 Mio. € oder bei Unternehmen bis 4 % des weltweiten Jahresumsatzes**	Art. 5, 83 Abs. 5a DS-GVO

*** je nachdem, welcher Betrag höher ist (angemessene Wahl der Geldbuße unter Berücksichtigung der Umstände des Einzelfalles)*

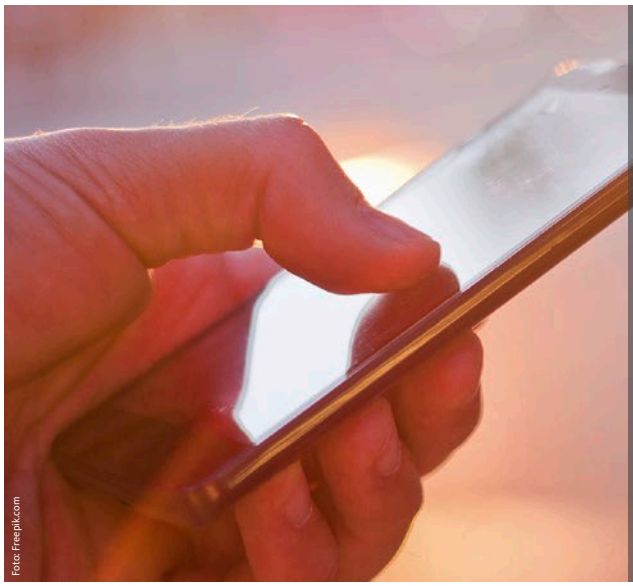
VERSTOSS	SANKTION	RECHTLICHE GRUNDLAGE
Bußgeldbewehrte Ordnungswidrigkeit		
unrechtmäßige Verarbeitung personenbezogener Daten	bis 20 Mio. € oder bei Unternehmen bis 4 % des weltweiten Jahresumsatzes**	Art. 6, 83 Abs. 5a DS-GVO
Verstoß gegen die Bedingungen für eine wirksame Einwilligung des Betroffenen in die Datenverarbeitung, sofern diese erforderlich ist	bis 20 Mio. € oder bei Unternehmen bis 4 % des weltweiten Jahresumsatzes**	Art. 7, 83 Abs. 5a DS-GVO
Verstoß gegen die Beschränkungen bei der Verarbeitung von besonderen Kategorien personenbezogener Daten (u. a. zur ethnischen Herkunft, Weltanschauung, Religion, Gesundheitsdaten, politische Meinung)	bis 20 Mio. € oder bei Unternehmen bis 4 % des weltweiten Jahresumsatzes**	Art. 9, 83 Abs. 5a DS-GVO
Verstoß gegen die Rechte der Betroffenen (u. a. Auskunftsrecht, Recht auf Berichtigung, Recht auf Löschung, Widerspruchsrecht)	bis 20 Mio. € oder bei Unternehmen bis 4 % des weltweiten Jahresumsatzes**	Art. 12 bis 22, 83 Abs. 5b DS-GVO
unzulässige Übermittlung von personenbezogenen Daten an Empfänger in einem Drittland oder internationale Organisation	bis 20 Mio. € oder bei Unternehmen bis 4 % des weltweiten Jahresumsatzes**	Art. 44 bis 49, 83 Abs. 5c DS-GVO
Verweigerung der den Aufsichtsbehörden zustehenden Untersuchungsbefugnisse	bis 20 Mio. € oder bei Unternehmen bis 4 % des weltweiten Jahresumsatzes**	Art. 58 Abs. 1, 83 Abs. 5e, 85 bis 91 DS-GVO
Straftaten (Antragsdelikte, die nur auf Antrag des Betroffenen verfolgt werden)		
unberechtigte, wissentliche Datenübermittlung von personenbezogenen Daten einer großen Anzahl von Personen an Dritte	Geldstrafe oder Freiheitsstrafe bis 3 Jahre	§ 42 Abs. 1 Nr. 1 BDSG
... auf andere Art und Weise zugänglich gemacht	Geldstrafe oder Freiheitsstrafe bis 3 Jahre	§ 42 Abs. 1 Nr. 2 BDSG
unberechtigte Verarbeitung von personenbezogenen Daten, die nicht allgemein zugänglich sind, zum Zwecke der Bereicherung oder Schädigung eines Betroffenen	Geldstrafe oder Freiheitsstrafe bis 2 Jahre	§ 42 Abs. 2 Nr. 2 BDSG
Erschleichen personenbezogener Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben zum Zwecke der Bereicherung oder Schädigung eines Betroffenen	Geldstrafe oder Freiheitsstrafe bis 2 Jahre	§ 42 Abs. 2 Nr. 2 BDSG

*** je nachdem, welcher Betrag höher ist (angemessene Wahl der Geldbuße unter Berücksichtigung der Umstände des Einzelfalles)*

Als Anfang des Jahres 2020 das volle Ausmaß der Corona-Pandemie erstmals sichtbar sei, hatten viele auf einmal ganz andere Sorgen als die Themen DS-GVO und Datenschutz. Auch die Aufsichtsbehörden gingen mit ihrer Nachverfolgung von Datenschutzverstößen und der Verhängung von Bußgeldern deutlich milder vor:

War es im 1. Quartal 2020 noch zu einem vorläufigen Höhepunkt an in Europa verhängten Bußgeldern gekommen (80), so wurden in Q2 lediglich knapp 50 Bußgeldverstöße geahndet. Dies erwies sich aber lediglich als die Ruhe vor dem Sturm. In Q3 schnellten die verhängten Bußgelder auf ein nie dagewesenes Rekordhoch – mit satten Strafen, wie einer 35 Millionen Euro Strafe gegen das Modehaus H&M. Bei der Modekette sei, so die Begründung, in einer Nürnberger Filiale seit Jahren das Privatleben von Mitarbeitern systematisch ausgespäht worden.

Gegen die AOK wurde ein Bußgeld in Höhe von 1,24 Mio. Euro verhängt, weil sie 500 Werbemails an Empfänger ohne deren Einwilligung versandte.



„DATENSCHUTZ IST IM ZEITALTER DER INFORMATIONSGESELLSCHAFT EINE UNVERZICHTBARE BEDINGUNG FÜR DAS FUNKTIONIEREN JEGLICHEN DEMOKRATISCHEN GEMEINWESENS.“

Jörg Tauss, Rede vor dem Deutschen Bundestag, 29. März 2007

Mobilcom-Debitel musste wegen unerlaubter Werbeanrufe ohne wirksame Einwilligung 145.000 Euro Bußgeld zahlen.

Obwohl Vodafone bereits im September ein Bußgeld in Höhe von 60.000 Euro und im Juli in Höhe von 45.000 Euro wegen der Kontaktierung per E-Mail ohne Rechtsgrundlage erhielt, musste das Unternehmen Mitte November erneut ein Bußgeld in Höhe von 12.251.601 Euro wegen unzulässiger Werbeanrufe und -nachrichten begleichen. Auch Sky Deutschland musste ein Bußgeld von 250.000 Euro zahlen, weil Werbeanrufe ohne Einwilligung stattfanden.

Am 11. November 2020 wurde vom Landgericht Bonn ein Bußgeld gegen den Konzern 1&1 bestätigt. Aufgrund eines unzureichenden Authentifizierungsverfahrens bei der telefonischen Kundenbetreuung durch 1&1, konnten Anrufer allein mit Angabe des Namens und Geburtsdatums eines Kunden weitreichende Informationen zu weiteren personenbezogenen Daten dieser Person erhalten. Hierin sah die Aufsichtsbehörde einen Verstoß gegen die Datenschutzgrundverordnung.

Die Marriot Hotel-Gruppe musste ein Bußgeld in Höhe von 20.347.230 Euro zahlen, weil unbekannte Hacker Daten von Hotelgästen erbeuteten. Auch British Airways wurde Opfer eines Cyberangriffs und musste wegen des Diebstahls von Kreditkartennummern und anderen Daten ein Bußgeld von 22.179.588 Euro zahlen. Diesen beiden Unternehmen ist es immerhin aufgrund der massiven wirtschaftlichen Einbrüche durch Corona gelungen, die Bußgelder zu reduzieren, ansonsten wären sie noch höher ausgefallen.

Aber auch Privatpersonen wurden nicht verschont: So versandte eine Privatperson SMS zur Wahlwerbung ohne Einwilligung der Betroffenen und erhielt hierfür ein Bußgeld in Höhe von 2.000 Euro. Gegen den politischen Wahlkandidaten, der ebenfalls diese SMS versendete, wurde eine Geldbuße von 3.000 Euro verhängt. Gegen einen Politiker, der ebenfalls Wahlwerbung per SMS versandte, wurde eine Geldbuße in Höhe von 4.000 Euro ausgesprochen.

Aber auch die Veröffentlichung einer Videoaufnahme aus einer Gerichtsverhandlung auf YouTube wurde gegenüber einer Privatperson mit einer Geldbuße von 3.000 Euro geahndet.

Die Österreichische Post soll ein Bußgeld in Höhe von 18.000.000 Euro zahlen, wegen einer Datensammlung zu politischen Präferenzen von Wählern und Verkauf dieser Daten an Parteien. Neben den bekannten Daten, etwa Name, Adresse, Geschlecht und Alter, hat sie auch die Parteiaffinität abgespeichert. Diese wurde durch ein Rechenmodell erfasst, dass Umfragen, Wahlergebnisse, Hochrechnungen und weitere Statistiken heranzieht und mit den persönlichen Daten abgleicht. Parteien sollen mit dieser Information zielgerichtete Wahlwerbung verschicken können. Gegen dieses Ende Oktober 2020 verhängte Bußgeld, hat die Post angekündigt Rechtsmittel einzulegen. Eine Entscheidung ist noch offen.

DIE ANGST VOR DER VISITENKARTE

In den Medien und sozialen Netzwerken wurde mit einer bestimmten Leidenschaft die Frage der Visitenkartennutzung unter der DS-GVO diskutiert. Ausgehend davon, dass angehende Geschäfts- oder Netzwerkpartner ihre Kontaktdaten per Visitenkarte austauschen, wurde hier diskutiert, ob nicht bereits beim Austausch Verletzungen des Datenschutzrechts stattfinden.

Zwei Fragen standen im Raum:

1. Ist die Verarbeitung von Kontaktdaten auf einer Visitenkarte ohne Einwilligung des Aushändigers überhaupt erlaubt?
2. Wie sind die Informationspflichten nach der DS-GVO zu erfüllen?

Die erste Frage lässt sich mit Blick auf Art. 6 Abs. 1 lit. b) und f) DS-GVO leicht mit einem „Ja“ beantworten. Zudem ist die Übergabe der Visitenkarte sicher als konkludente Einwilligung zu werten.

Die zweite Frage dreht sich um die Informationspflichten nach Art. 13 DS-GVO. Hiernach ist die betroffene Person vor der ersten Verarbeitung mit bestimmten Pflichtangaben zu informieren. Das folgt aus dem Transparenzprinzip der DS-GVO. Nach sehr enger Auslegung ist die Entgegennahme der Visitenkarte bereits eine Datenverarbeitung, da es sich i. d. R. um eine Erhebung – sprich Beschaffung – von Daten handelt, die in einem Dateisystem gespeichert werden sollen (Art. 2 Abs. 1 und Art. 4 Punkt 2 DS-GVO).

Diese Auslegung ist wenig praktikabel. Daher kommt die Berliner Datenschutzbehörde zu dem Ergebnis, dass die reine Entgegennahme einer Visitenkarte keine Datenverarbeitung darstellt, sondern erst die Erfassung im entsprechenden Dateisystem. Damit reicht es, wenn die Informationspflichten, z. B. per E-Mail, zu diesem Zeitpunkt erfüllt werden.

ABMAHNUNG

Bekannt ist, dass es zu ersten Abmahnungen wegen der DS-GVO gekommen ist. Dennoch ist zumindest fraglich, ob Verstöße gegen die DS-GVO einem Mitbewerber genügend Rechtsgrund für eine Unterlassungsklage geben. Hier wird erst die Rechtsprechung der nächsten Jahre Klarheit bringen.

Mit unserem neuen **leistungsfähigen**

Maschinenpark
in der Druckerei,
in unserer Weiterverarbeitung
und unserem Versand

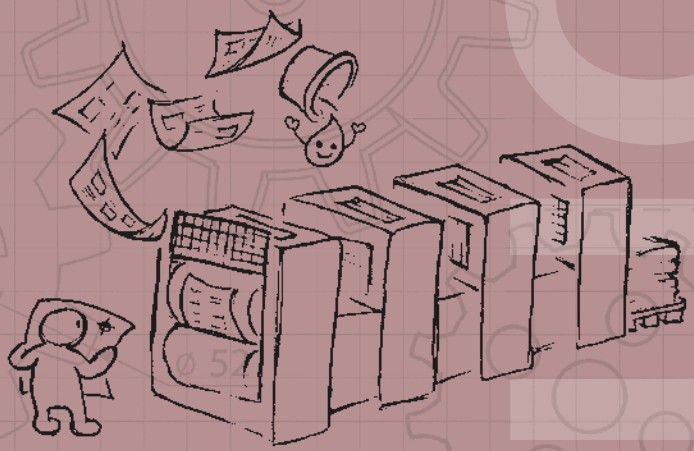
erreichen wir **beste Produktqualität.**

UBG

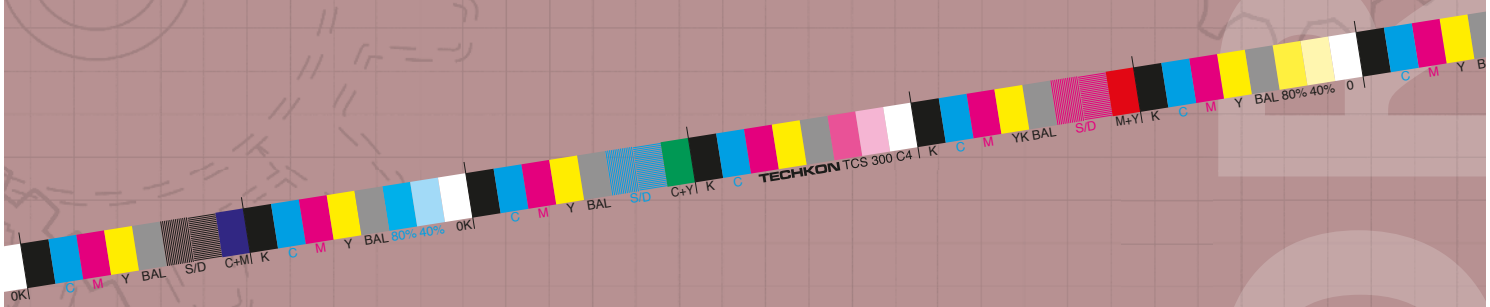
GRAFIKDESIGN

- von der Idee bis zur Realisation
- klassische Reinzeichnung
- Bildbearbeitung/Retusche
- Social-Media-Design
- schnelle und präzise Umsetzung
- Erstellung von Infografiken
- Web-to-Print/Template-Erstellung
- Print und Online

DRUCKEREI und LETTERSHOP



- Offset- & Digitaldruck
- Weiterverarbeitung
- Veredelung
- Adressaufbereitung
- Personalisierung
- Mailings
- Versand
- Druckerei-Fullservice aus einer Hand
- persönliche Betreuung
- höchste Flexibilität
- wir erfüllen auch ausgefallene Wünsche
- transparente Preise
- Adressdaten können direkt von uns aus der ZMD selektiert werden



www.UBG365.de

WICHTIGE GERICHTSURTEILE

FACEBOOK-FANPAGES

Fanpages erfreuen sich bei Unternehmen, Parteien und Behörden großer Beliebtheit. Durch den Betrieb einer Fanpage erhält Facebook jedoch viele Daten der Besucher. Um welche Daten es sich dabei genau handelt und was mit ihnen passiert, ist schwer herauszufinden. Die Deutsche Datenschutzkonferenz (DSK) hat bereits im April 2019 die „Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit“ beschlossen. Darin wird dargelegt, dass die bislang von Facebook zur Verfügung gestellten Informationen nicht ausreichen. Fanpagebetreiber stehen datenschutzrechtlich in einer gemeinsamen Verantwortung mit Facebook und haben daher nach der DS-GVO eine Rechenschaftspflicht gegenüber den Nutzern.

Nach Ansicht der DSK, aber auch nach Ansicht der Gerichte, können die Fanpage-Betreiber dieser Verantwortung ohne nähere Informationen von Facebook nicht nachkommen. Ein datenschutzkonformer Betrieb sei so nach Ansicht der Behörden nicht möglich. Ende Oktober 2019 hat Facebook schließlich neue Informationen zur Datenverarbeitung im Internet veröffentlicht. Diese Informationen werden immernoch in den Gremien der DSK ausgewertet.

In jedem Fall sehen sich die Aufsichtsbehörden durch das Urteil des Bundesverwaltungsgerichts vom 11. September 2019 (Az. 6 C 15.18) gestärkt. Das Gericht hatte bestätigt, dass die deutschen Aufsichtsbehörden unmittelbar gegen Fanpagebetreiber vorgehen und damit auch den Betrieb einer Fanpage untersagen dürfen. Die Behörden müssen insbesondere keine Entscheidung der federführend zuständigen irischen Datenschutzbehörde abwarten.

Festzuhalten ist, dass trotz dieser Ansichten der DSK und der Urteile im Jahr 2019 noch keine Fanpage verboten wurde. Es gibt intensive Gespräche mit Facebook und allen europäischen Aufsichtsbehörden, um eine möglichst einheitliche Aufsichtspraxis in der EU zu gewährleisten. Im gesamten Jahr 2020 gab es hierzu keine nennenswerten Änderungen, abgesehen vom Privacy-Shield (siehe Seite 19).

Vielleicht gibt es 2021 mehr Rechtssicherheit.

Foto: AdobeStock.com / © enzozo

DAS COOKIE-URTEIL

Der Bundesgerichtshof (BGH) hat sich in seiner Entscheidung vom 28.05.2020 (Az. I ZR 7/16) mit der Frage beschäftigt, wie bei der Verwendung von Cookies, die für Werbung und andere Zwecke genutzt werden, vom Webseitenbetreiber zu verfahren ist. Dabei geht es nicht um die technisch notwendigen Cookies, sondern z. B. um Tracking-Cookies. Für die Verwendung dieser Cookies ist eine Einwilligung erforderlich – auch, wenn mit den Tracking-Cookies keine personenbezogenen Daten verarbeitet werden. Eine voreingestellte Zustimmung (z. B. Einwilligungskästchen mit bereits gesetztem Häkchen) ist keine Einwilligung.

Vorausgegangen war eine Entscheidung des Europäischen Gerichtshofs (EuGH), wonach das Setzen von Cookies, die nicht unbedingt erforderlich sind, eine aktive Einwilligung des Internetnutzers erfordert. Dies gelte unabhängig davon, ob es sich bei den abgerufenen Informationen um personenbezogene Daten handelt oder nicht.

Gegenstand der Entscheidung war die Frage, unter welchen Voraussetzungen Internetanbieter Cookies auf den Endgeräten ihrer Nutzer platzieren können. In diesem Zusammenhang stellte der EuGH fest, dass eine wirksame datenschutzrechtliche Einwilligung in diesem Kontext auch im Internet ein aktives Verhalten des Betroffenen voraussetzt. Dieses müsse sich zudem konkret auf die Einwilligung beziehen. Nicht ausreichend sei hingegen die Bestätigung eines vorausgewählten Ankreuzkästchens durch Anklicken einer anderweitigen Schaltfläche, etwa zur Teilnahme an einem Gewinnspiel.

Zudem hat der EuGH klargestellt, dass der Webseitenbetreiber dem Nutzer klare und umfassende Informationen bereitstellen muss, damit die Einwilligung wirksam erteilt werden kann. Hierzu gehören auch die Angaben zur Funktionsdauer der Cookies und dazu, ob Dritte Zugriff auf die Cookies erhalten können.

Der BGH musste nun entscheiden, wie das Ganze im deutschen Recht zu bewerten ist. Deutschland hätte die seit 2009 geltende E-Privacy-Richtlinie, auch bekannt als Cookie-Richtlinie, umsetzen müssen. Die Richtlinie sah prinzipiell ein sog. Opt-In-Verfahren vor, bei dem Nutzer für den Einsatz von Cookies ihre Einwilligung geben müssen. Die Bundesregierung war aber der Auffassung, dass die Cookie-Informationspflichten durch das Telemediengesetz (TMG) bereits EU-rechtskonform umgesetzt seien. Problematisch war allerdings, dass es laut § 15 Abs. 3 TMG im Gegensatz zur Forderung der EU-Cookie-Richtlinie ausreicht, eine Opt-Out-Lösung anzubieten.

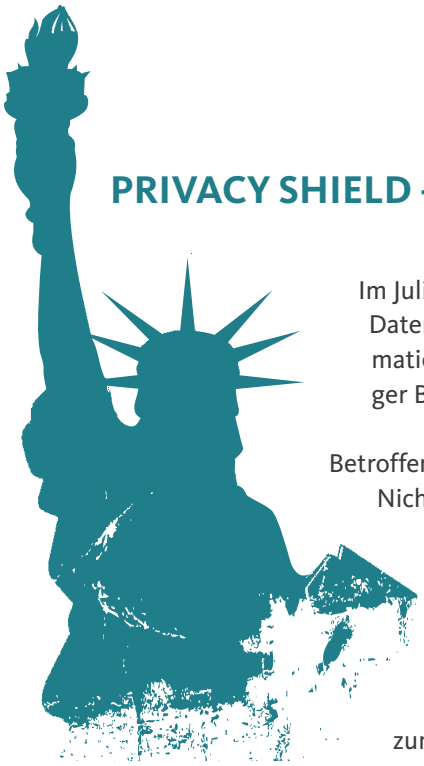
Am 28.05.2020 hat nun der BGH sein Urteil verkündet und letztendlich den EuGH bestätigt.

Werden mehrere Tracking-Cookies verwendet, muss das in einer Liste deutlich gemacht werden und dem Nutzer die Wahlmöglichkeit eröffnet werden.

Danach benötigen Websitebetreiber eine aktive Einwilligung der Besucher, wenn sie Cookies setzen wollen, die technisch nicht unbedingt erforderlich sind. Vorab angekreuzte Auswahlkästchen sind hingegen nicht zulässig. Dies begründet der BGH mit einer richtlinienkonformen Auslegung des § 15 Abs. 3 TMG mit Blick auf § 5 Abs. 3 Satz 1 der E-Privacy-Richtlinie, so dass für den Einsatz von Cookies zur Erstellung von Nutzerprofilen für Zwecke der Werbung oder Marktforschung die Einwilligung des Nutzers erforderlich ist. An dieser Rechtslage hat sich auch mit Inkrafttreten der DS-GVO nichts geändert.

Aus diesem Grunde ist eine Zunahme von umfangreichen Cookie-Bannern im Jahr 2020 zu verzeichnen.

PRIVACY SHIELD – DATENTRANSFER IN DIE USA



Im Juli erklärte der EuGH das sogenannte „Privacy-Shield“ für unwirksam. Damit hat er dem Datentransfer zwischen der EU und den USA größtenteils die Grundlage entzogen. Informationen über europäische Verbraucher seien auf US-Servern nicht vor dem Zugriff dortiger Behörden und Geheimdienste geschützt, so der Richter.

Betroffen von diesem Urteil sind insbesondere Dienste wie Google, Facebook oder Amazon. Die Nicht-Regierungsorganisation „Non-of-your-business“ (kurz: noyb) hatte nach Verkündung des sogenannten Schrems II-Urteils 101 Beschwerden gegen die Nutzung von Google Analytics und Facebook Connect durch europäische Unternehmen eingereicht. Die Beschwerden sind an alle nationalen Aufsichtsbehörden, darunter auch fünf deutsche Landesdatenschutzaufsichtsbehörden, gerichtet. Inhaltlich betreffen die Beschwerden die Frage, ob Google und Facebook über die genannten Produkte weiter personenbezogene Daten in die USA übermitteln dürfen und damit die Nutzung zum Beispiel durch Websites europäischer Anbieter legal ist oder nicht.

Die europäischen Datenschutzbehörden haben mittlerweile eine Taskforce gegründet. Sie soll die schnelle und europaweit einheitliche Bearbeitung der Beschwerden der Organisation zur Nutzung von Google- und Facebook-Services durch europäische Anbieter gewährleisten.

Beide Konzerne stützen sich inzwischen auf die sogenannten Standardvertragsklauseln der Europäischen Union. Ob sie dafür die vom EuGH geforderten „zusätzlichen Maßnahmen“ als Ergänzung der Standardvertragsklauseln ergriffen haben und ob diese Maßnahmen ausreichen, um das vom EuGH geforderte Schutzniveau in den USA zu gewährleisten, ist die inhaltliche Kernfrage der Beschwerdeverfahren. Als Konsequenz haben Deutschland und Frankreich als gemeinsame Initiative eine zweite Taskforce ins Leben gerufen. Diese soll insbesondere Kriterien für die Bewertung einer Datenübermittlung im Einzelfall und Kriterien für zusätzliche Maßnahmen sowie Verfahrensaspekte für deren Umsetzung erarbeiten. Ergebnisse sind noch nicht bekannt. Eins ist aber auf jeden Fall sicher: Mittlerweile müssen zwei Taskforces das Rechtsvakuum, das durch das Urteil entstanden ist, zurechtrücken.

CLOUD ACT

Insbesondere der von der Trump-Regierung 2018 erlassene CLOUD Act stand 2020 im Fokus der Datenschutz-Aufsichtsbehörden.

Der CLOUD Act stellt sicher, dass U.S.-amerikanische Strafverfolgungsbehörden weitreichend auf Daten von Internet-Unternehmen und Providern zugreifen können, unabhängig davon, wo diese gespeichert sind. Das schafft Rechtskonflikte, denn nach einer Einschätzung der europäischen Aufsichtsbehörden sind direkte Übermittlungen an U.S.-Strafverfolgungsbehörden außerhalb des Rechtshilfeweges nur sehr begrenzt mit der DS-GVO vereinbar. Solange keine lebenswichtigen Interessen des Betroffenen berührt werden, setzt eine rechtskonforme Übermittlung bei strafrechtlichen Ermittlungen vielmehr die Einhaltung des bestehenden Rechtshilfeweges voraus.

Neue Abkommen können die Lösung sein, aber die Hürden sind hoch.

Es müssten hinreichende Verfahrenssicherungen und ein hohes Datenschutzniveau vereinbart werden, um einerseits die gewünschte Rechtssicherheit und andererseits für alle Beteiligten einen Vorteil zum Status quo zu schaffen. Auch hier sollen die bereits oben erwähnten Taskforces für mehr Rechtssicherheit sorgen.

ePRIVACY-VERORDNUNG

Ursprünglich sollte die ePrivacy-Verordnung (ePVO) gemeinsam mit der DS-GVO in Kraft treten. Der europäische Gesetzgeber konnte allerdings bislang noch keine Einigung erzielen. Sinn der ePVO ist es, Privatpersonen und Unternehmen zu schützen. Sie löst die E-Privacy-Richtlinie ab, die der deutsche Gesetzgeber größtenteils im Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG) umsetzte.

Viele Unternehmer warnen bereits, dass die ePrivacy-Verordnung das digitale Business schwer schädigen wird. Es stünden sogar ganze Geschäftsmodelle vor dem „Aus“. Viele Unternehmen verfolgen die ePrivacy-Verordnung deshalb mit Argwohn. Als EU-Verordnung gilt die ePVO nach ihrem Inkrafttreten sofort innerhalb der gesamten Europäischen Union. Die nationalen Gesetzgeber können über Öffnungsklauseln in manchen Bereichen aber auch eigene Regelungen erlassen.

Die deutsche EU-Ratspräsidentschaft hatte am 4. November 2020 einen neuen Vorschlag zur ePVO veröffentlicht. Dieser wurde in einer Arbeitsgruppe diskutiert und erneut abgelehnt. Der Vorschlag sah im Grunde nur wenige Änderungen zu dem Vorschlag vor, der bereits ein Jahr zuvor abgelehnt worden war.

Das Thema E-Privacy wird auf den kommenden Sitzungen der Arbeitsgruppe wieder behandelt werden. Die Ratspräsidentschaft wird einen neuen Textvorschlag abfassen. Wann genau es zu einer Einigung kommen wird und die Trilog-Verhandlungen beginnen, ist noch offen.

2021 wird deshalb spannend.

Foto: AdobeStock.com / © Rawf8

Die **UBG** ist eine **Full-Service-Webagentur** der ersten Stunde!

UBG

- Profitieren Sie von einem modernen Design, welches wir nach Ihren Vorgaben mit den neuesten Technologien und der höchsten Sicherheit realisieren.
- Wir bieten Ihnen eine freie und intuitive Gestaltung Ihrer Inhalte sowie eine flexible Einbindung Ihrer sozialen Netzwerke.
- Barrierefreiheit, Volltextsuche, SEO, Responsive Design und sicheres Hosting gehören bei uns zu den Standards.

Unsere Softwarespezialisten entwickeln ständig neue und innovative Anwendungen, die auf Ihre Bedürfnisse optimal zugeschnitten sind. Zusammen mit Ihnen erarbeiten wir individuelle Konzepte und setzen diese erfolgreich um.

- Webdesign
- Newsletter- & SMS-Versand
- Web-Baukasten
- App-Entwicklung
- Software-Entwicklung
- Webhosting
- Cloud-Anwendungen
- Shop-Systeme

Wir sind Designer.
Wir sind Entwickler.
Wir sind Spezialisten.

www.UBG365.de


newsletter
alt

NEWSLETTER

Durch die Pandemie und die vielen Gerichtsurteile haben wir Sie stets mit Informationen durch unseren Newsletter versorgt. Wir haben diese auf den folgenden Seiten noch einmal aufgeführt und thematisch sortiert.

DATENSCHUTZMANAGEMENT

HOME-OFFICE

CYBERCRIME

GERICHTSURTEILE | AUFSICHTSBEHÖRDEN | VERGEHEN

Insgesamt fügten wir folgende Infoblätter bei, die Sie jederzeit in Ihrem Kundenportal abrufen können:

- Liste Aufsichtsbehörden
- Anleitung Datenpanne
- Detailübersicht Aufbewahrungspflichten
- Verantwortung KV – Informationspflichten
- Musterantwort auf Auskunftsverlangen
- Vorlage – Vereinbarung BYOD
- Vorlage – Home-Office-Richtlinie
- FAQ – Arbeitsrecht im Home-Office
- Cookie-Banner-Anleitung
- Bilder
- Veröffentlichung von Personenbildern
- Aufnahmen bei Veranstaltungen
- Veröffentlichung von Zeitungsartikeln
- Urheberrechte
- Aktuelle Bußgelder

Warum muss jeder Mitarbeiter (auch ehrenamtlich Tätige), der mit personenbezogenen Daten in Berührung kommt, auf die Vertraulichkeit verpflichtet werden?

Anders als § 5 BDSG a. F. sieht die DS-GVO keine ausdrückliche Verpflichtung aller bei der Datenverarbeitung beschäftigten Personen auf das Datengeheimnis mehr vor. Allerdings gibt es einige Regelungen in der DS-GVO aus denen sich eine Verpflichtung auf die Vertraulichkeit ergibt: So z. B. aus der allgemeinen Organisations- und Rechenschaftspflicht (vgl. Art. 5, 24 DS-GVO). Hieraus lässt sich schließen, dass weiterhin alle Personen, die mit personenbezogenen Daten in Kontakt kommen, zur Vertraulichkeit zu verpflichten und entsprechend zu schulen sind (vgl. LDA Bayern, Tätigkeitsbericht 2015/2016, Kap. 15.7).

Besonders zu beachten ist, dass Sie auch den Nachweis führen müssen, dass Sie Ihre Pflichten einhalten (Art. 5 Abs. 2, Art. 24 Abs. 1 DS-GVO). Bei diesem Nachweis handelt es sich um einen Entlastungsbeweis, der Sie vor Schadensersatzansprüchen (die unter der DS-GVO auch immaterielle Schäden umfassen) und Geldbußen bis zu 20.000.000 EUR schützen kann. Dies bedeutet letztlich eine umfassende Dokumentationspflicht, der am besten nachzukommen ist, wenn die Mitarbeiter (und ehrenamtlich Tätigen) eine schriftliche Erklärung abgeben. Für den (unwahrscheinlichen) Fall, dass ehrenamtlich Tätige sich weigern, die Verpflichtungserklärung zu unterzeichnen, empfehlen wir, die Verpflichtungserklärung z. B. im Rahmen einer Vorstandssitzung oder Schulung vorzulesen und dies zu protokollieren. So haben Sie dennoch den Nachweis, dass eine (wenigstens mündliche) Verpflichtung stattgefunden hat.

Wer ist zu verpflichten?

Es sind alle Personen zu verpflichten, die Zugang zu personenbezogenen Daten haben (Art. 32 Abs. 4 DS-GVO, Art. 39 Abs. 1 DS-GVO). Es ist also weiterhin erforderlich, alle Personen, die eine tatsächliche Möglichkeit des Zugangs zu personenbezogenen Daten haben, zur Vertraulichkeit zu verpflichten und zu schulen, unabhängig davon, ob sie zu diesem Zugang berechtigt sind oder nicht bzw. ob sie tatsächlich Zugriff nehmen oder nicht. Es sind somit alle Mitarbeiter, Auszubildende, Praktikanten und auch die ehrenamtlich Tätigen zu verpflichten. Aber auch Personen wie Reinigungs- und Wachpersonal gehören dazu, da es in der Praxis nicht möglich ist, einen Arbeitsplatz so „klinisch“ von personenbezogenen Daten zu befreien, dass sie mit diesen nicht in Kontakt kommen.

Auch wenn es lästig erscheint und für Sie mehr Bürokratie bedeutet: Wenn durch Unterrichtung und Schulung der Datenschutz nähergebracht und dessen Bedeutung durch die Vertraulichkeitsverpflichtung unterstrichen wird, werden die Personen sensibilisiert und es verringert sich damit auch rein praktisch die Wahrscheinlichkeit von Verstößen.

DATENPANNE UND DATENKLAU – DAS RICHTIGE VORGEHEN

Newsletter vom 07.05.2020

Unfälle beim Umgang mit sensiblen Daten sollten nicht passieren, aber gerade in Zeiten von Home-Office, Home-Schooling & Kinderbetreuung ist man vielleicht abgelenkt oder nicht so konzentriert: Aus Versehen werden E-Mails mit dubiosen Anhängen geöffnet oder Daten an den falschen Empfänger weitergeleitet.

Kommt es hierbei zu einer Datenschutzverletzung, bei der ein Risiko für die betroffenen Personen besteht, müssen Sie, als verantwortliche Stelle, die zuständige Datenschutzaufsichtsbehörde innerhalb von 72 Stunden darüber informieren. Eine Meldung hat nicht zu erfolgen, wenn diese Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dies bedeutet, dass im Falle einer Datenpanne stets zu prüfen ist, welche Risiken für die betroffenen Personen bestehen.

Die Einschätzung kann äußerst schwierig sein. Deshalb haben wir nachfolgend ein paar praktische Beispiele aufgeführt.

Was ist eine „Datenschutzverletzung“?

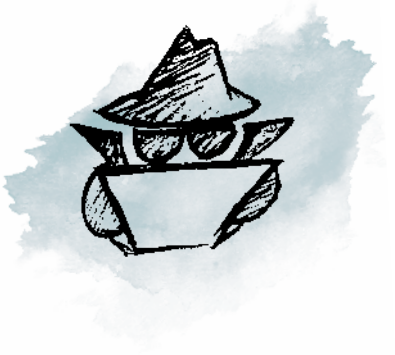
Datenschutzverletzung im Sinne der DS-GVO bedeutet: eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung von personenbezogenen Daten oder einem unbefugten Zugang zu diesen führt.

Wie erfolgt eine Meldung?

In der Regel können Sie die Meldung einer Datenschutzverletzung online bei der zuständigen Aufsichtsbehörde Ihres Bundeslandes durchführen.

Was sind hierfür typische Kategorien?

- Cyberattacken
- Ransomware
- Malware
- Verlust oder Diebstahl
- Fehlversand



CYBERATTACKEN

Was versteht man unter einer „Cyberattacke“?

Cyberattacken umfassen gezielte Angriffe, die über das Internet stattfinden. Dabei kann das Abgreifen von personenbezogenen Daten im Fokus stehen (z. B. Passwörter, E-Mail-Adressen), aber auch reine Beeinträchtigungen bei einem Dienst an sich werden als Cyberattacke bezeichnet (z. B. DDoS-Attacke auf Server).

Ist eine Cyberattacke meldepflichtig?

Ja, sofern personenbezogene Daten betroffen sind. Cyberkriminelle haben in diesen Fällen ein Interesse, die gestohlenen Daten nach einem Angriff zu Geld zu machen z. B. durch Erpressung, Betrug durch gestohlene digitale Identitäten oder Ausnutzen vertraulicher Informationen. Neu ist auch, dass eine Meldepflicht auch bei vorübergehender Unerreichbarkeit der Daten oder dauerhafter Löschung infolge eines Sicherheitsbruchs besteht. Dies setzt eine längere Dauer voraus kann z. B. hervorgerufen werden durch einen Stromausfall (der länger dauert) oder eine DDoS-Attacke.

Tipps zur Reaktion:

- Befallene Systeme identifizieren und isolieren
- Strafanzeige stellen
- Manipulationen finden
- Schadensausmaß feststellen
- Schwachstelle/Lücke finden und Angriff stoppen
- Security Updates einspielen
- Veränderte Datensätze berichtigen (z. B. Backup)

RANSOMWARE

Was versteht man unter „Ransomware“?

Das sind Programme, die Dateien verschlüsseln und somit unbrauchbar machen. Von ihren Opfern verlangen sie dann Lösegeld, um die verschlüsselten Dateien wieder freizugeben. Daher wird oft auch der Begriff Erpressungs- und Verschlüsselungstrojaner verwendet.

Ist ein Ransomware-Befall meldepflichtig?

Meistens. Durch die Folgen eines Ransomware-Angriffs wird die Verfügbarkeit von Daten eingeschränkt. Der Ausfall des Systems bzw. von Dateien kann dann ein Risiko für betroffene Personen bedeuten.

Tipps zur Reaktion:

- Ausbreitung stoppen: Alle befallenen Systeme isolieren bzw. vom Netz nehmen
- Strafanzeige stellen
- Kein Lösegeld zahlen
- Nach Entschlüsselungswerkzeug suchen: **nomoreransom.org**
- Einfallstor finden, um eine erneute Infektion zu vermeiden

MALWARE

Was versteht man unter „Malware“?

Malware bezeichnet schädliche Programme, die sich weiterverbreiten wollen und dabei Daten im System ausspähen, manipulieren oder löschen. Der Trojaner „Emotet“ z. B. liest nach Infektion u. a. die vergangene E-Mail-Korrespondenz aus, welche später genutzt wird, um personalisierte Phishing-Angriffe zu starten.

Ist ein Malware-Befall meldepflichtig?

Teilweise – es kommt auf den konkreten Schädling an. Nicht jeder Virenbefall muss gemeldet werden. Sobald jedoch eine Malware personenbezogene Daten abgreift oder in einer Art und Weise beeinflusst, die ein Risiko für die betroffenen Personen darstellt, muss der Vorfall gemeldet werden.

Tipps zur Reaktion:

- Befallene Systeme identifizieren und isolieren
- Mit nachgeladenen Schadcode rechnen
- Strafanzeige stellen
- Schadensausmaß feststellen (Risiko bestimmen)
- Prüfen, welche (Zugangs-)Daten betroffen sind
- Bei Emotet: Kommunikation mit betroffenen Personen nach Art. 34 DS-GVO führen
- Vollständige Security-Scans durchlaufen lassen

VERLUST ODER DIEBSTAHL

Ist ein Verlust oder Diebstahl von USB-Sticks oder externen Festplatten meldepflichtig?

Wenn der USB-Stick wirksam verschlüsselt war, dann ist der Verlust nicht meldepflichtig. Eine Meldepflicht besteht nur, wenn die Daten nicht anderweitig gesichert sind.

Tipps zur Reaktion:

- Schadensausmaß feststellen (Risiko bestimmen)
- Prüfen, welche Daten betroffen sind

FEHLVERSAND

Ist ein offener E-Mail-Verteiler meldepflichtig?

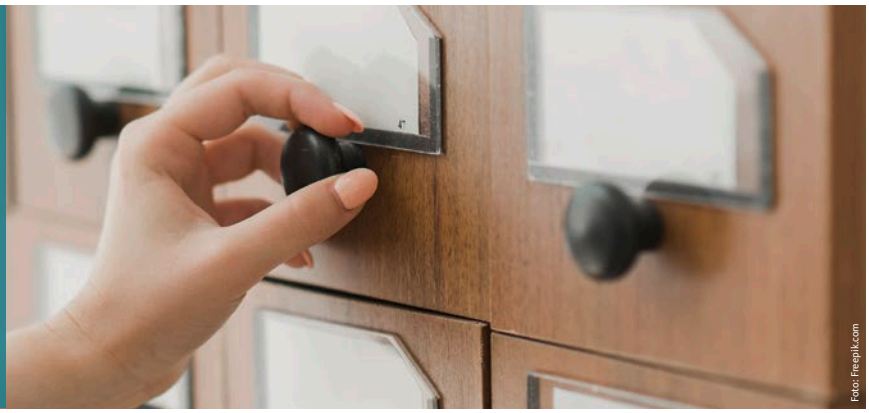
Ja, bei einer großen Empfängeranzahl oder, wenn der Inhalt besonders sensibel ist und die Offenlegung die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen verletzt.

Tipps zur Reaktion:

- Schadensausmaß feststellen (Risiko bestimmen)
- Prüfen, welche Daten betroffen sind

AUFRÄUMEN UND AUSMISTEN – WIE LANGE MUSS ICH WAS AUFBEWAHREN?

Newsletter vom 09.07.2020



Seit Beginn der Pandemie und während der Zeit im Home-Office, haben sich viele entschieden, ihre Ordner aufzuräumen und dabei auch ältere Papiere und elektronische Akten zu entsorgen. Trotz aller gesetzlichen Regelungen treten immer wieder Fragen zu den Aufbewahrungspflichten für Unterlagen auf.

Von daher möchten wir Ihnen helfen, Ihre Unterlagen sicher aufzubewahren bzw. zu vernichten. Hier finden Sie einen kurzen Überblick von einigen gesetzlichen Aufbewahrungsfristen:

Was mache ich mit...

BANKBELEGEN

Belege aus der Zeit von 2009 und davor können nun weg. Gleiches gilt für Barbelege usw. (Aufbewahrungspflicht von 10 Jahre).

BEWERBUNGSUNTERLAGEN

Bei Einstellung: zur Personalakte nehmen
Bei Absage: spätestens 6 Monate nach Beendigung des Bewerbungsverfahrens, sind Bewerbungsunterlagen zu löschen. Diese Frist folgt aus der Möglichkeit des Bewerbers, nach dem Allgemeinen Gleichbehandlungsgesetzes (AGG) zu klagen. Solange der Arbeitgeber mit einer solchen Klage rechnen muss, kann er die Bewerberdaten speichern. Die Löschfrist gilt jedoch dann nicht, wenn der Bewerber dazu eingewilligt hat, dass seine Daten länger gespeichert werden dürfen, etwa für den Fall, dass der Arbeitgeber die Bewerberdaten für eine mögliche zukünftige vakante Stelle im Auge behalten möchte.

EINNAHMEN-ÜBERSCHUSS-RECHNUNG

Unterlagen aus 2009 und früher können entsorgt werden (Aufbewahrungspflicht von 10 Jahre).

E-MAILS/BRIEFE

Es kommt auf den Inhalt an: Sie bewahren sie so lange auf, wie ein entsprechendes Dokument in Papierform, also z. B.:

- unverbindliche Anfragen per E-Mail = keine Aufbewahrung nötig → mit Erledigung der Anfrage zeitnah löschen
- Auftragsbestätigungen per E-Mail = 6 Jahre
- Rechnungen per E-Mail = 10 Jahre
- E-Mails mit steuerlichem Inhalt müssen auch elektronisch archiviert werden

AUFTRAGSBESTÄTIGUNGEN

Für Handels- bzw. Geschäftsbriefe gilt eine Aufbewahrungspflicht von 6 Jahren → d. h. alle solche Briefe aus 2011 und vorher können vernichtet werden! Anfragen, denen keine Aufträge folgten, können jederzeit entsorgt werden, da keine Aufbewahrungspflicht existiert.

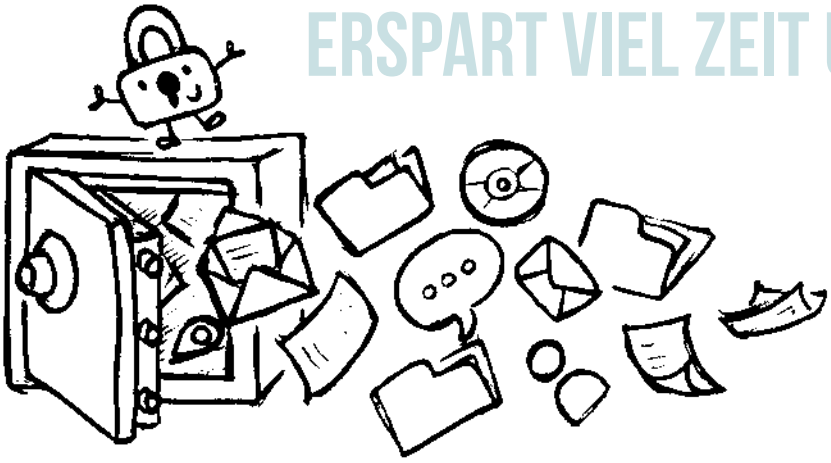
Wichtig!

Die Aufbewahrungsfrist beginnt immer am **Ende des Kalenderjahres**, in dem sich der dokumentierte Geschäftsvorfall zugetragen hat. Entscheidend ist der Ablauf des Jahres, in dem Sie beispielsweise die letzte Eintragung in den Büchern vorgenommen, die Bilanz aufgestellt, den Handels- oder Geschäftsbrief empfangen haben oder in dem die sonstigen Unterlagen entstanden sind.

Unterlagen dürfen Sie nicht vernichten, wenn sie für folgende Fälle von Bedeutung sind:

- eine begonnene Außenprüfung;
- anhängige Steuerstraf- oder bußgeldrechtliche Ermittlungen;
- ein schwebendes oder aufgrund einer Außenprüfung zu erwartendes Rechtsbehelfsverfahren oder
- zur Begründung der Anträge an das Finanzamt und bei vorläufigen Steuerfestsetzungen.

EIN JEDES DING AN SEINEM ORT,
ERSPART VIEL ZEIT UND BÖSE WORT.



Die Corona-Pandemie versetzt unsere Welt in einen Ausnahmezustand. Möglichst viele Menschen sollen in den eigenen vier Wänden bleiben und Sozialkontakte meiden. So soll die exponentiell ansteigende Ansteckungskurve gestreckt werden. Immer mehr Arbeitnehmer arbeiten von zu Hause aus. Was viele nicht bedenken, die Vorschriften der DS-GVO gelten auch bei der Arbeit im Home-Office. Die gleichen Schutzmaßnahmen, die in Ihrer Geschäftsstelle getroffen werden, sollten auch auf Ihre von zu Hause aus arbeitenden Mitarbeiter angewendet werden.

Wenn Sie mobiles Arbeiten bereits schon länger ermöglicht haben, haben Sie wahrscheinlich alles bereits vertraglich geregelt, dienstliche Laptops stehen bereit und auch für die technische Sicherheit bei der Arbeit im Home-Office ist gesorgt.

Falls Sie jetzt aber Neuland betreten, möchten wir Ihnen gerne folgende Hinweise geben, die Sie bitte bei der praktischen Umsetzung von Home-Office für Ihre Mitarbeiter berücksichtigen sollten:

1. Welches Gerät wird genutzt?

Bevorzugen Sie betriebliche Geräte gegenüber persönlichen Geräten der Mitarbeiter. Auf diese Weise können Sie sicherstellen, dass die technischen Sicherheitsvorkehrungen wie Firewall, Anti-Virus usw. in dem Computer, den der Mitarbeiter benutzt, korrekt angebracht sind. Wenn im Notfall private Geräte eingesetzt werden müssen, schließen Sie bitte eine Vereinbarung (BYOD) ab.

2. Haben Sie Ihre Mitarbeiter hinsichtlich der technischen Sicherheit bei der Arbeit im Home-Office belehrt?

Technische Sicherheit am Arbeitsplatz ist das A & O. Fürs Home-Office sind ein paar Besonderheiten zu beachten. Hierzu zählen auch die Sicherung der häuslichen Arbeitsräume, keine Notizen mit Passwörtern herumliegen zu lassen oder den Bildschirm beim Verlassen des Raumes (z. B. zum Kaffeekochen) zu blockieren, etc.

3. Nehmen die Mitarbeiter auch physischen Akten mit nach Hause?

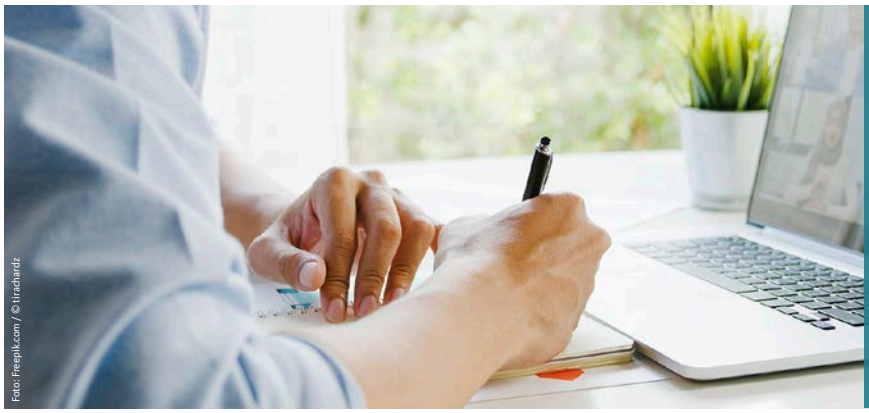
Falls der Mitarbeiter auch mit physischen Akten arbeitet, stellen Sie sicher, dass diese an einem sicheren Ort, z. B. in einem verschlossenen Schrank, aufbewahrt werden.

4. Setzen Sie ein VPN ein?

Wenn möglich, nutzen Sie einen VPN-Dienst, damit Sie sicherstellen können, dass die Internetverbindung verschlüsselt ist.

5. Sind die Mitarbeiter zur Datengeheimhaltung bzw. Datensicherheit verpflichtet?

Verpflichten Sie Ihre Mitarbeiter zu Sicherheitsmaßnahmen. Hierfür können Sie eine Richtlinie erstellen, die die Mitarbeiter über alle ihre Verpflichtungen bei der Arbeit von zu Hause aus informiert.



DIE SICHERHEITSLÜCKEN VON ZOOM UND WIE SIE SICHER VIDEO-CHATS DURCHFÜHREN

Newsletter vom 19.05.2020

Die Corona-bedingten Einschränkungen des öffentlichen Lebens in Deutschland bedeuten nicht nur im Privatleben, sondern auch für Arbeitgeber und Arbeitnehmer eine große Herausforderung für die internen Abläufe. Persönliche Besprechungen, Konferenzen oder Meetings werden durch Video-Chats ersetzt. Einige waren hierauf gut vorbereitet, der Großteil musste allerdings schnell improvisieren.

Sei es aus Unkenntnis anderer Alternativen, sei es durch Marketing und breite Berichterstattung: Mitarbeiter, Unternehmen und Büros griffen zur Zoom-App.

Wer Zoom als cloudbasierte Konferenzsoftware nutzen will, braucht lediglich ein aktuelles Tablet oder einen Browser. Inzwischen ist aber deutlich, dass es bei Zoom datenschutzrechtliche Probleme gibt:

Datenübertragung an Facebook

Bereits Ende März merkte das Online-Magazin Motherboard in einem Artikel an, dass die App Daten über die Nutzung an das Netzwerk Facebook sendet.

Die Übertragung erfolgte unabhängig von einer Anmeldung über Facebook. Für Apps, die das Development-Kit von Facebook einsetzen, ist das kein ungewöhnlicher Vorgang. Allerdings fehlte in der Datenschutzerklärung von Zoom jeglicher Hinweis auf die Übertragung.

Aber auch die ungefragte Datenweitergabe der Nutzer von Zoom an Werbekunden, ist datenschutzrechtlich zu beanstanden.

Windows-Passwort kann ausgelesen werden

Doch damit nicht genug. Hacker hatten leichtes Spiel mit der App. So war der Zutritt zu einer Konferenz nicht durch ein Passwort gesichert. Es genügt der Versand eines präparierten Links, um darüber das Anmeldepasswort für Windows von Nutzern auszulesen. Somit bestand die Gefahr, dass über diesen Weg Schadsoftware oder Spyware eingeschleust werden konnten.

Des Weiteren wurden bereits Zugangsdaten von Zoom-Accounts zum Kauf im Darknet angeboten.

Aber auch Mac-Nutzer blieben nicht verschont. Auch hier gab es massive Sicherheitsprobleme.

Zoom ergreift Konsequenzen

Die Sicherheitslücken sind nach Aussage von Zoom inzwischen geschlossen. Außerdem hat das Unternehmen eingeräumt, dass die verwendete Verschlüsselung nicht den heutigen Standards entspricht.

DIE SICHERHEITSLÜCKEN VON ZOOM UND WIE SIE SICHER VIDEO-CHATS DURCHFÜHREN

Newsletter vom 19.05.2020

Foto: Freepik.com / © tirachardz

Die Entwickler ergreifen nun Maßnahmen, um die Sicherheit ihrer Systeme zu erhöhen. Dennoch will die Staatsanwaltschaft von New York den Dienst genauer unter die Lupe nehmen.

So schaffen Sie IT-Sicherheit im Video-Chat

Die verschiedenen Vorfälle und Pannen lassen Zoom nicht als vertrauenserweckend erscheinen. Auf dem Markt gibt es zahlreiche Alternativen. Viele Anbieter bieten als Reaktion auf die Corona-Krise ihre Lösungen für einen begrenzten Zeitraum kostenlos an.

So auch die Firma Microsoft Deutschland GmbH. Microsoft hat uns zu Beginn der Pandemie zur Unterstützung Ihrer Arbeit in diesen bewegenden Zeiten, kostenlose Office 365 Lizenzen für einen begrenzten Zeitrahmen zur Verfügung gestellt. Mit diesen Lizenzen können Sie die Funktionalitäten ausgiebig testen, nutzen und bewerten. Ferner ist das Produkt Microsoft Teams mit inbegriffen, mit welchem Sie Video- und Telefonkonferenzen durchführen sowie Online-Abstimmungen tätigen können.

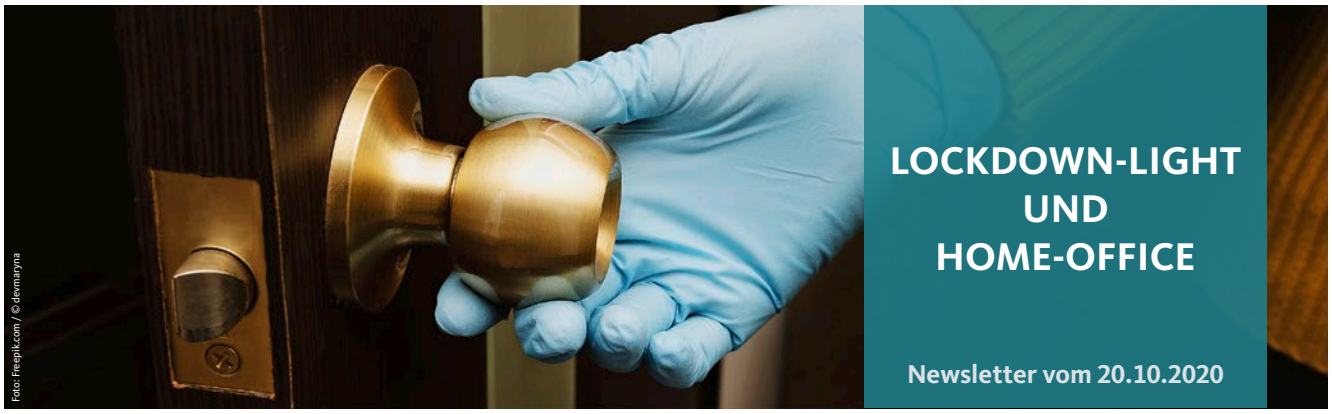
Sollten Sie dennoch unbedingt Zoom verwenden wollen, helfen entsprechende Einstellungen.

Mitarbeiter sensibilisieren!

Egal welches System Sie einsetzen:
Bitte sensibilisieren Sie Ihre Mitarbeiter und geben ihnen Handlungsempfehlungen!

NACHTRAG:

Zoom hat auf die Kritik reagiert und sowohl die Datenweitergabe an Facebook beendet als auch die Sicherheitslücken entschärft, etwa durch die Einführung einer Passwortfunktion und einer besseren Verschlüsselung für die Meetings.



Die zweite Corona-Welle hat Deutschland erreicht und angesichts der hohen Infektionszahlen, fordern Bund und Länder mit dem aktuellen Beschluss vom 28.10.2020 die Unternehmen eindringlich auf, wo immer es umsetzbar ist, ab dem 02.11.2020 Heimarbeit oder das mobile Arbeiten zu Hause zu ermöglichen.

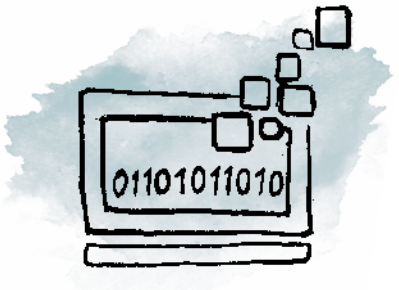
Wenn Sie Ihren Mitarbeitern erneut (oder immer noch) Home-Office oder mobiles Arbeiten ermöglichen, bedenken Sie bitte die datenschutzrechtliche Komponente. Denn im Home-Office sind Daten und IT Ihrer unmittelbaren Kontrolle entzogen. Gleichzeitig steigt die Gefahr unberechtigter Zugriffe durch Dritte. Diesen Risiken müssen Sie begegnen, indem Sie entsprechende technische und organisatorische Sicherheitsmaßnahmen ergreifen.

Jeden Tag entstehen im Internet 350.000 NEUE Schadprogramme. Pro Woche macht das fast 2,5 Millionen neue Bedrohungen für jeden einzelnen Rechner, der ans Internet angebunden ist oder beispielsweise über einen USB-Anschluss verfügt. Jedes dieser Schadprogramme kann sich durch einen PC den Weg zu Ihnen bahnen.

Einen 100%igen Schutz gibt es leider nicht. Oft sind die Cyberkriminellen den Sicherheitsprogrammen und -vorkehrungen einen Schritt voraus – denn die größte Schwachstelle sind wir Menschen. Irgendwann werden doch die unsicheren E-Mail-Anhänge geöffnet oder der Link angeklickt und schon ist die Misere da. Auch USB-Sticks sind gerne Quellen solcher Schadprogramme, die sich dann schnell im ganzen Unternehmensnetzwerk verbreiten können, wenn sie erstmal auf einem PC angekommen sind. Deshalb ist es gerade in diesen Zeiten umso wichtiger, dass Sie Ihre Mitarbeiter (noch einmal) für den Datenschutz sensibilisieren und für die Arbeit im Home-Office eine Datenschutzvereinbarung schließen.

Im Idealfall sollte Ihr Mitarbeiter nicht mit einem privaten PC oder Laptop arbeiten. Stellen Sie Ihren Mitarbeitern für das Home-Office einen eigenen PC oder Laptop zur Verfügung. Privates und berufliches gehört eben nicht zusammen. Sollte es in absoluten Ausnahmefällen nicht möglich sein, dass Sie dienstliche Geräte zur Verfügung stellen, sollten Sie mit dem Mitarbeiter den Einsatz privater Endgeräte unbedingt regeln. Eine Musterregelung haben wir ebenfalls beigefügt.

Neben dieser datenschutzrechtlichen Komponente werden wir auch oft zu der arbeitsrechtlichen Komponente befragt. Aus diesem Grunde haben wir FAQ zusammengestellt, die hier die wichtigsten Fragen beantworten.



Internet-Kriminelle nutzen die aktuelle Corona-Krise aus, um per E-Mail-Phishing an persönliche Daten der Empfänger zu kommen.

So werden im Moment gefälschte E-Mails der Sparkasse, worin Kunden zur Eingabe ihrer persönlichen Daten aufgefordert werden, versendet. Der Vorwand für die Kontaktaufnahme ist die angebliche Schließung von Filialen, zu denen es regional kommt. Um eine reibungslose Kommunikation per Telefon oder Chat zu gewährleisten, werden Betroffene über einen Link auf eine authentisch aussehende Eingabemaske geleitet, die die Daten nach der Eingabe direkt an die Betrüger sendet.

Die E-Mail sieht so aus:

Umgang mit dem COVID-19-Erreger

18. März 2020 um 07:27

Sparkasse

Sehr geehrte Kundinnen und Kunden,

Ihre Sicherheit und Gesundheit und auch die unserer Mitarbeiter liegt uns sehr am Herzen.

Vor diesem Hintergrund haben wir uns dafür entschieden, unsere kleineren Filialen bis auf weiteres zu schließen.

Sehr gerne stehen wir Ihnen telefonisch, per E-Mail und in unserem Online-Banking auch im Chat persönlich zur Verfügung. Die SB-Bereiche sind uneingeschränkt nutzbar.

Bitte nehmen Sie sich deshalb die 2 Minuten Zeit, um

– Ihre Adresse(n)
– Ihre Telefonnummer(n)
– und Ihre E-Mail-Adresse(n)

zu überprüfen und gegebenenfalls zu aktualisieren, um weiterhin eine reibungslose Kommunikation bei anliegenden Fragen zu gewährleisten.

In diesen Tagen müssen wir es als Gemeinschaft dem Erreger so schwer wie möglich machen, sich schnell zu verbreiten.

Prävention ist keine Hysterie, und Ignoranz ist auch kein Mut! Wir hoffen sehr auf Ihre Solidarität und Ihr Verständnis.

Vielen Dank!

Mit freundlichen Grüßen

Ihr Sparkassenverband.

Andere E-Mails kommen angeblich von der Weltgesundheitsorganisation WHO. Im Anhang der E-Mail befindet sich ein E-Book der WHO, dass die neuesten Informationen zum Corona-Virus enthalten soll. Öffnet man das E-Book, das sich in einem ZIP-Archiv befindet, dann wird unbemerkt ein Trojaner namens FormBook auf den PC nachgeladen. FormBook überwacht dann Ihre Tastatureingaben, stiehlt Daten aus dem Windows-Clipboard und aus Browsern und schickt diese dann an einen bestimmten Server. Die WHO selbst macht auf ihrer Website darauf aufmerksam, dass sie niemals unaufgefordert E-Mail-Anhänge verschickt und Empfänger niemals auf Links klicken sollen, die nicht auf die Domain who.int verweisen.

Auch die Sorge vieler Unternehmer und Selbständiger beuten Betrüger aus. Mit dem verlockenden Versprechen: „Sie erhalten bis zu 30 000 Euro Soforthilfe vom Staat ohne Rückzahlung!“ versuchen Betrüger aktuell, personenbezogene Daten von Bürgern abzugreifen. Wer sich für das Soforthilfeprogramm der Bundesregierung aufgrund der Corona-Pandemie interessiert, gelangt möglicherweise auf diese Fake-Seite. Bitte geben Sie auf keinen Fall Daten auf der Seite **soforthilfe-fur-corona** ein oder laden dort etwas hoch.

Diese Seite ist keine offizielle Seite der Bundesregierung oder eines Bundeslandes. Es werden dort keine Gelder vergeben. Stattdessen werden die eingegebenen Daten für andere Betrugsmaschen genutzt.

Auch die Anzahl der professionell aussehenden Fake-Shops hat zugenommen: Schutzmasken und Desinfektionsmittel stehen hoch im Kurs. Das Geld dafür ist natürlich per Vorabkasse fällig, die erworbenen Schutzmasken gibt es aber gar nicht und werden nie geliefert. Das Geld ist verloren.

Zusätzlich zu den oben genannten Angriffsversuchen verbreiten sich aktuell viele Gerüchte und Falschmeldungen über Messenger-Dienste und soziale Netzwerke. Auch sogenannten Kettenbriefen, die über Messenger-Dienste oder soziale Netzwerke verbreitet werden, sollte kein Glauben geschenkt werden. Leiten Sie diese Nachrichten nicht weiter und helfen Sie mit, die Verbreitung von Falschmeldungen zu unterbinden. Wir können hier nicht alle Maschen der Betrüger aufzeigen. Aber wir bitten Sie um Vorsicht. Ein gesundes Misstrauen ist keine Unhöflichkeit.

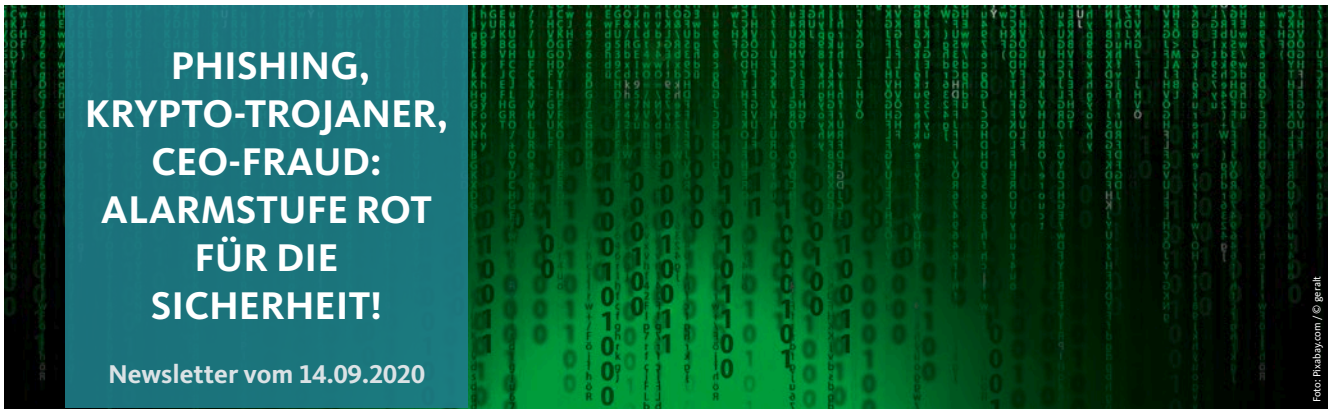
Bitte nehmen Sie sich folgende Sicherheitshinweise zu Herzen:

- Öffnen Sie keine unbekannten Dateien.
- Überprüfen Sie den Ursprung und die Absender von E-Mails.
- Hinterfragen Sie gründlich enthaltene Verlinkungen.
- Nennen Sie nie Passwörter, Zahlungsinformationen oder sensiblere Informationen per E-Mail oder Telefon.
- Übersenden Sie nie eine Kopie Ihres Personalausweises per E-Mail.
- Klicken Sie keine Popup-Fenster an, die Ihnen z. B. Heilmittel, Impfungen oder sonstige Behandlungen gegen Corona anbieten. Solche Banner oder Popups können Schadsoftware enthalten, unabhängig von den Produkten, für die sie werben.

Ist es trotz allem dazu gekommen, dass Sie sensible Informationen eventuell an Betrüger versendet haben, ändern Sie bitte sofort Ihr Passwort. Haben Sie zudem Passwörter übermittelt, die Sie für mehrere Accounts verwenden, ist es unbedingt notwendig, bei all diesen Zugängen die Passwörter zu ändern. In solchen Fällen ist es empfehlenswert, auch das Passwort bei Ihrem E-Mail-Anbieter zu verändern.

Wenn es um dienstliche Angelegenheiten ging, informieren Sie bitte sofort Ihren Arbeitgeber.

Bleiben Sie auch in Zeiten der Corona-Krise besonnen und halten Sie sich an die üblichen Vorsichtsmaßnahmen, damit Sie nicht zum Opfer von (Internet-)Kriminellen werden.



Die digitale Kriminalität durch Cyberkriminelle nimmt leider in Zeiten von Home-Office immer mehr zu. Wichtig ist daher, dass Sie das Vorgehen der Kriminellen kennen und sich richtig verhalten.

PHISHING

Was ist das?

Mit falschen und täuschend echt aussehenden E-Mails von Behörden, Banken, Onlineshops, sozialen Netzwerken oder Zahlungsdienstleistern wird Handlungsdruck beim Empfänger aufgebaut. Um Schaden oder Ärger zu vermeiden, soll das potenzielle Opfer eine Datei öffnen oder sich auf einer gefälschten Webseite mit seinen Benutzerdaten anmelden.

Wie erkenne ich Phishing?

Typischerweise weisen Phishing-Mails meist mehrere der folgenden Merkmale auf:

- Handlungsdruck wird erzeugt: Wird nicht sofort gehandelt, passiert angeblich etwas Schlimmes, oder es kommt zu einem finanziellen Schaden.
- Anmeldeinformationen oder Passwörter sollen geändert, aktualisiert oder bestätigt werden. Dazu sollen Sie sie auf einer echt aussehenden Webseite eingeben.
- Unpersönliche Ansprache und unpersönliche Grußformel am Schluss der E-Mail: Sie werden als Kunde angesprochen, oder die E-Mail ist nur vom „Kundenmanagement“ unterschrieben.
- Fehlerhafte Sprache: Achten Sie auf Schreibfehler oder Fehler im Satzbau.
- Ungewöhnliches Verhalten des angeblichen Absenders: Passt die Mail nicht zum bisherigen Verhalten des Absenders, sollte Sie das stutzig machen.

Was muss ich im Fall der Fälle tun?

Auf keinen Fall das machen, was in der E-Mail gefordert wird. Auch sollte die E-Mail nicht an Kollegen weitergeleitet werden. Schlussendlich entscheidend ist: Es dürfen keine Anmeldeinformationen oder Passwörter auf der gefälschten Webseite eingegeben werden. Im Zweifel unbedingt die Kollegen oder den Vorgesetzten fragen, was diese von der E-Mail halten.

Auch die IT-Abteilung oder die Datenschutzbeauftragte kann bei der Bewertung helfen. Ist es dann doch passiert, sollten Sie unverzüglich den Vorgesetzten und die Datenschutzbeauftragte informieren.

KRYPTO-TROJANER

Was ist das?

Ausgangspunkt ist auch hier in der Regel eine E-Mail, mit der Druck aufgebaut wird. Will das potenzielle Opfer etwa einen finanziellen Schaden vermeiden, soll es den Anhang öffnen. Dabei passiert meist Folgendes: Mit dem Öffnen installiert das Opfer ein Programm, das Schadsoftware (Malware) aus dem Internet nachlädt. Meist ist das nicht mehr einfach nur ein Trojaner, der etwa Anmeldeinformationen und Passwörter ausspäht. Vielmehr kommt ein Krypto-Trojaner zum Einsatz, der alle erreichbaren Daten verschlüsselt. Nur gegen Zahlung eines „Lösegelds“ soll der Erpresste die Informationen zur Entschlüsselung seiner Daten erhalten. Egal, ob man seine Daten wiederbekommt oder nicht, der Schaden ist meist immens.

Wie erkenne ich Krypto-Trojaner?

Anhänge in Phishing-Mails dürfen Sie auf keinen Fall öffnen. Aktivieren Sie keine in Dateien enthaltenen Makros bzw. installieren Sie keine Programme. Ist das dennoch passiert, merken Sie, dass ein Krypto-Trojaner aktiv ist, etwa an einer Verlangsamung Ihres Computers. Eventuell stellen Sie auch fest, dass Dateien auf Ihrem Computer eine andere Endung erhalten haben.

Was muss ich im Fall der Fälle tun?

Versuchen Sie schnellstmöglich, alle Netzwerkverbindungen zu trennen. Krypto-Trojaner verschlüsseln nämlich alle Dateien, die sie irgendwie erreichen können. Fahren Sie den Rechner herunter. Geht das nicht, ziehen Sie den Stecker oder entfernen Sie den Akku. Ggf. können Sie den Rechner auch durch langes Drücken des Ein-/Aus-Knopfs ausschalten. Informieren Sie dann unverzüglich die IT-Abteilung und den Datenschutzbeauftragten. Warten Sie nicht, jede Minute zählt.

CEO-FRAUD

Was ist das?

Was der Vorgesetzte sagt, wird gemacht – auf dieses Prinzip setzen Kriminelle beim sogenannten CEO-Fraud (Chef-Trick). Mit angeblichen Anweisungen des Vorgesetzten werden Mitarbeiter mit Zuständigkeit für Finanzen, Zahlungen und Konten dazu verleitet, oftmals sehr hohe Geldbeträge an „Geschäftspartner“ etwa für einen Unternehmenszukauf zu zahlen. Oder Mitarbeiter werden dazu verleitet, vertrauliche Informationen und Geheimnisse preis zu geben. Genauso wenig wie die Anweisung des echten Vorgesetzen, gibt es auch die Geschäftspartner nicht. Dahinter stecken die Kriminellen.

Wie erkenne ich das?

Dem Vorgesetzten geht es um eine eilige und streng vertrauliche Transaktion. Nur Sie dürfen davon wissen. Und Sie müssen machen, was er sagt.

Was muss ich im Fall der Fälle tun?

Haben Sie keine Scheu und kontaktieren Sie die betreffende Person (Vorgesetzten). Fragen Sie ausdrücklich nach einer Bestätigung auf einem anderen Weg, etwa per Fax. Sprechen Sie mit dem Vorgesetzten oder der Datenschutzbeauftragten, bevor Sie irgendeine Transaktion veranlassen.

Aktuell erhalten viele Verbände, Selbständige und Unternehmen eine E-Mail des gelben Branchenbuchs. Darin geht es um Ihre gespeicherten Daten, die aufgrund des Datenschutzes zu überprüfen sind. Vorsicht! Hierbei handelt es sich um reine Abzocke!

Wenn Sie eine E-Mail mit dem Betreff „Datenverifikation und Premiumeintrag“ und / oder dem folgenden Inhalt erhalten, antworten Sie nicht!

> ***z. Hd. Geschäftsleitung***
>
> ***Sehr geehrte Firma ...,***
> ***nach den geltenden gesetzlichen Bestimmungen zum europäischen Datenschutz unter Beachtung der Direktive 2002/58 werden Ihnen hiermit die Daten, die zu Ihrer Unternehmung elektronisch gespeichert wurden, mitgeteilt.***
>
> ***Bitte verifizieren Sie die Daten und nehmen Sie den Anhang zur Kenntnis. Diesen können Sie uns ggf. per Fax oder gescannt als Mailnachricht zurücksenden. Die Daten sind öffentlich auf der Web Site des Gelben Branchenbuchs einzusehen.***
>
> ***Freundliche Grüsse***

Als Absender sind zurzeit folgende Adressen bekannt:

- Vanna Adams – info@gbbuchmailing.com
- Amber Sommar – info@gbbuchmailing.com
- Mahala Hernander – info@gbbmailing.directory
- Cheslie Mosteller – info@branchenkontrolle.online
- Moria Rohrbaugh – info@branchenbuch-data.site

In der Anlage der E-Mail befindet sich ein Formular, das bereits mit Adressdaten des Empfängers ausgefüllt ist. Wenn Sie diese Daten tatsächlich abgleichen, ergänzen und das Formular unterzeichnet zurücksenden, bekommen Sie wenig später eine Rechnung. Denn tatsächlich geht es hier nicht um einen Datenabgleich, sondern um ein Angebot für einen Eintrag in ein unbekanntes Internetverzeichnis. In den AGB des Unternehmens ist zu lesen, dass das Angebot durch Unterzeichnung angenommen wird. Es wird daraus ein kostenpflichtiger Auftrag für einen Interneteintrag, der pro Monat 65 Euro kostet – zahlbar jeweils jährlich im Voraus (780 EUR). Die Vertragslaufzeit beträgt drei Jahre und verlängert sich jeweils um ein weiteres Jahr, wenn nicht spätestens drei Monate vor Ablauf des jeweiligen Vertragszeitraums gekündigt wird.

Sie lösen mit der Unterschrift also einen Auftragswert von **2.340 Euro** aus.

Bei dem Versender handelt es sich um kein deutsches Unternehmen. Vielmehr sitzt die Firma im Ausland. Dieser Vertragspartner ist auf dem Formular angegeben: GBB Ltd. , Trust Company Complex, Ajeltake Rd., Ajeltake Island, Majuro, Marshall Islands, MH 96960, Company Number: 37214.

Auf der Webseite gelbesbranchenbuch.info, welche auf gelbesbranchenbuch.com umleitet, ist aktuell gar kein Impressum angegeben. Damit entspricht die Webseite nicht den deutschen Rechtsnormen. Deshalb noch einmal: **Es handelt sich nicht um ein seriöses Angebot. Ignorieren Sie diese Mails, auch wenn noch so viele Erinnerungsmails kommen.**

WERBUNG PER E-MAIL ODER SMS – EIN FALL FÜR DIE DATENSCHUTZ-BEHÖRDE!

Newsletter vom 23.01.2020

Was war passiert?

Ein Verband versandte per SMS einen Wahlaufruf. Ein Empfänger der SMS beschwerte sich und wandte sich an die Aufsichtsbehörde, die sofort ein Bußgeldverfahren eröffnete. Der Empfänger hatte nämlich nie die Einwilligung dazu gegeben, dass der Verband seine Mobilfunknummer nutzen durfte.

Was viele nicht wissen, Mobilfunknummern, Telefonnummern oder E-Mail-Adressen, die Sie z. B. auf Webseiten finden, dürfen nicht ohne Einwilligung der Betroffenen für Werbung oder Einladungen zu Veranstaltungen genutzt werden.

Warum ist das so?

Elektronische Kommunikation wird von der Rechtsprechung und dem Gesetzgeber als unzumutbare Belästigung angesehen. Bürger und Unternehmen sollen hiervor geschützt werden. Deshalb ist diese nur erlaubt, wenn der Bürger bzw. das Unternehmen vorher aktiv seine Einwilligung hierzu gegeben hat.

Der Verband zum Beispiel wandte jedoch ein, dass Wahlwerbung oder Einladungen zu politischen Veranstaltungen Ausdruck des verfassungsmäßigen Auftrags der politischen Willensbildung seien. Leider folgen weder die Aufsichtsbehörden noch das Bundesverfassungsgericht dieser Argumentation! Bei Einladungen zu Veranstaltungen heißt es z. B.: „Mit diesen Einladungen wird das Interesse verfolgt, Öffentlichkeit zu erzeugen. Derartige Einladungen können eine Nähe zu werblichen Zusendungen haben und aus der Perspektive des allgemeinen Persönlichkeitsrechts betrachtet, als potenzielle lästige Beeinträchtigung zu werten sein. Hier ist regelmäßig eine Einwilligung erforderlich.“ Das Bundesverfassungsgericht bewertet dementsprechend das Interesse der Empfänger, solche Informationen auf elektronischem Wege nicht zu erhalten höher ein, als das Interesse der politischen Partei auf ihre Arbeit aufmerksam zu machen.

DIE GUTE ALTE BRIEFPOST – TEUER ABER RECHTSKONFORM!

Bei Werbung per Briefpost oder Einladungen zu Veranstaltungen per Briefpost gibt es hingegen keine Einwilligungserfordernis. Somit hätte der Verband an öffentlich zugängliche Daten z. B. eine Einladung an Gewerbetreibende in Ihrem Ort zu einer wirtschaftspolitischen Veranstaltung per Briefpost versenden können. Wichtig ist hierbei nur, dass nicht wahllos alle möglichen Adressen gesammelt und eingeladen werden, sondern immer eine Interessenabwägung nach Art. 6 Abs. 1 lit. f) DS-GVO durchgeführt wird. Hierbei muss das Interesse, den Adressaten zu einer Veranstaltung einzuladen, höher zu bewerten sein, als das Interesse des Adressaten in Ruhe gelassen zu werden. Eine Interessenabwägung sollte immer dokumentiert werden.

Auch bei der Briefpost müssen Sie unbedingt 2 Dinge beachten:

1. Weisen Sie unbedingt den angeschriebenen Personenkreis darauf hin, dass er zukünftig, wenn er solche Einladungen nicht mehr möchte, der Verwendung seiner Daten widersprechen kann. Bei einem Widerspruch stellen Sie sicher, dass die Adressen nicht mehr von Ihnen genutzt werden können. Am einfachsten geschieht dies mit einer Sperrliste.

2. Und denken Sie bitte immer daran: Sobald Sie die Adressen verarbeiten, fallen die Informationspflichten nach Art. 13 DS-GVO an! Das heißt, Sie müssen die Betroffenen unter anderem darüber informieren, welche Daten Sie zu welchem Zweck von ihm verarbeiten und wer die verantwortliche Stelle ist.

VORSICHT BEI DER VERÖFFENTLICHUNG VON PERSONENBILDERN AUF FACEBOOK

Newsletter vom 13.03.2020

Foto: Pixabay.com / © geralt

Ohne sich groß dabei etwas zu denken, passiert es ganz oft: Schnell werden Fotos von Veranstaltung geschossen auf denen auch einzelne Personen erkennbar sind und im Internet oder auf der Fanpage veröffentlicht.

Das Verwaltungsgericht Hannover (Az. 10 A 820/19) hat jetzt geurteilt: Der Post eines Fotos mit einer Menschenmenge auf einer Facebook-Fanpage ist datenschutzwidrig, wenn einzelne Personen zu erkennen sind und diese der Veröffentlichung nicht zugestimmt haben!

In dem Streitfall hatte ein SPD Ortsverein auf seiner Fanpage bei Facebook über die Errichtung einer Fußgänger-Ampel in seinem Stadtteil berichtet. In diesem Zusammenhang postete der Verband zwei Fotos von den örtlichen Gegebenheiten. Auf einem der Bilder, war auch eine Menschenansammlung zu erkennen. Diese hatte sich vor Ort versammelt. Die Presse veröffentlichte ebenfalls einen Pressebericht und ein Foto.

Ein Ehepaar, das auf dem Bild zu erkennen war, machte geltend, dass das vom SPD Ortsverein gepostete Bild ohne deren Zustimmung veröffentlicht wurde und verlangte die Löschung des Fotos. Das Bild wurde vom Ortsverein umgehend gelöscht. Darüber hinaus wendete sich das Ehepaar an die Niedersächsische Landesdatenschutzbeauftragte. Die Behörde wertete das Verhalten des Ortsvereins als Datenschutzverletzung. Da das Bild aber zwischenzeitlich entfernt wurde, sprach sie lediglich eine Verwarnung aus. Die Kosten für das Verfahren in Höhe von 362,25 Euro sollte der Ortsverein der Behörde erstatten. Gegen die Verwarnung und die Kostenerstattung klagte der Ortsverein vor dem Verwaltungsgericht (VG) Hannover.

Die Klage hatte keinen Erfolg. Das Verwaltungsgericht entschied, dass der Post des Bildes auf der Fanseite von Facebook rechtswidrig ist.

Es gilt nicht das Presseprivileg!

Eine Veröffentlichung von Bildern auf einer Fanpage einer Partei bei Facebook hat, nach Ansicht des Gerichts, eine ganz andere Qualität als die Veröffentlichung in der Presse. Eine politische Partei kann nicht die gleichen Rechte wie Journalisten für sich in Anspruch nehmen. Sie kann sich nicht auf das Presseprivileg berufen. Einer Veröffentlichung widerspreche den berechtigten Interessen der abgebildeten Personen, da die Veröffentlichung von Daten auf einer Fanpage bei Facebook unkalkulierbare Risiken für die betroffenen Personen hat. Diese haben insbesondere keine effektive Kontrolle mehr über die Weiterverwendung ihrer Daten. Vor allem etwaige Löschungsansprüche können gegen Facebook kaum wirksam durchgesetzt werden. Zudem, so der Senat weiter, wird der Öffentlichkeit durch das Foto auf der Fanpage eine etwaige Zustimmung des Ehepaares zu der politischen Tätigkeit der politischen Partei suggeriert, auch wenn diese tatsächlich nicht besteht. Dasselbe gilt für Unternehmen, die Bilder von Privatpersonen in ihren Kampagnen verwenden.

Vollständige Ablichtung der Gesichter der Personen nicht erforderlich

Zwar besteht ein berechtigtes Interesse daran, auch durch die öffentliche Verwendung von Fotos für die politische Tätigkeit zu werben und damit gemäß Art. 21 Abs. 1 Satz 1 Grundgesetz an der politischen Willensbildes des Volkes mitzuwirken. Auch für Unternehmen kann ein berechtigtes Interesse vorliegen, mit solchen Fotos zu werben. Aber hierzu ist eine vollständige Ablichtung der Gesichter der Personen nicht erforderlich, weil es in diesem Fall nicht darauf ankommt, dass gerade die abgebildete Person als solche in einen spezifischen Kontext zur politischen Tätigkeit der Partei gesetzt wird. In diesem Fall hätte es ausgereicht, die abgebildete Person unkenntlich zu machen, etwa durch Verpixelung der Gesichter. Dies ist, so das Gericht mit einfacher Bildbearbeitungssoftware möglich und zumutbar.

Deshalb bitten wir Sie, veröffentlichen Sie Fotos von Personen nur, wenn Sie von den betroffenen Personen die Einwilligung hierzu haben. Liegt Ihnen diese nicht vor, machen Sie bitte die Gesichter der abgebildeten Personen unkenntlich.

Wichtig ist auch: Eine Einwilligung kann jederzeit widerrufen werden. Bei einem Widerruf sind Sie verpflichtet, die Bilder zu löschen.

VORSICHT BEI ANWALTS-POST DER KSP RECHTSANWÄLTE IM AUFTRAG DER DPA PICTURE ALLIANCE GMBH

Newsletter vom 19.03.2020

In den letzten Wochen haben einige unserer Kunden Post von den Rechtsanwälten ksp aus Hamburg erhalten. Die Kanzlei vertritt die dpa picture alliance GmbH, eine 100%ige Tochter der dpa (Deutsche Presseagentur).

In diesen Schreiben geht es um die Verletzung von Urheberrechten. In der Regel wird moniert, dass auf der Homepage ein Bild der dpa picture alliance GmbH verwendet wird, ohne hierzu die erforderlichen Rechte erworben zu haben (Lizenzierung).

Obwohl es sich hierbei nicht um eine klassische Abmahnung handelt und nicht zur Abgabe einer Unterlassungserklärung aufgefordert wird, empfehlen wir, die Schreiben ernst zu nehmen.

Mit den Anwälten und der dpa picture alliance GmbH ist nicht zu spaßen. Wird auf das Schreiben der Anwälte nicht reagiert, wird sehr zügig ein gerichtliches Mahnverfahren eingeleitet. Die Anwälte scheuen sich auch nicht, Klage einzureichen. Der dpa picture alliance GmbH geht es schlicht weg um Schadensersatz, also um Geld!

Sind die Schreiben und die Schadensersatzforderungen gerechtfertigt?

Das hängt sehr vom Einzelfall ab und vom Vorwurf, der Ihnen gemacht wird.

Unserer Erfahrung nach werden oftmals aus Unwissenheit auf Webseiten Urheberrechtsverstöße begangen: So reicht es z. B. aus, wenn einfach Zeitungsartikel mit Bildern veröffentlicht werden, ohne hierzu die Erlaubnis zu haben. Was viele nicht bedenken: Sowohl der Urheber des Zeitungsartikels als auch der Fotograf des Bildes genießen Urheberschutz. Ohne deren Einwilligung dürfen die Zeitungsartikel oder Bilder nicht veröffentlicht werden. Erfolgt dennoch eine Veröffentlichung entstehen Schadensersatzansprüche.

Bei einigen Anbietern von Web-Baukastensystemen kann es passieren, dass Artikel, die auf Webseiten veröffentlicht werden, als öffentliche Artikel gekennzeichnet sind. Diese werden dann allen Kunden zur Verfügung gestellt. Deshalb achten Sie bitte darauf, dass Sie diese Funktion deaktivieren. Sollten Sie die Funktion nicht deaktivieren, kann es sein, dass dieser Artikel über Ihre Webseite veröffentlicht wird. Somit verstoßen Sie gegen das Urheberrecht und machen sich Schadensersatzpflichtig, obwohl Sie nichts aktiv eingestellt haben.

Wir bitten Sie deshalb, Ihre Webseiten zu kontrollieren. Bitte klären Sie die Rechte an den veröffentlichten Texten und Bildern. Deaktivieren Sie die Funktion des öffentlichen Hochladens von Texten und Bildern von Dritten auf Ihren Seiten.

Sofern wir Änderungen und Neuigkeiten bezüglich des Vorgehens von ksp oder dpa picture alliance GmbH haben, werden wir Sie gerne hierüber erneut informieren.

Bitte beachten Sie auch die weiteren Informationen zum Urheberrecht und zu Bildrechten.

COOKIE-BANNER WIRD PFLICHT

Newsletter vom 09.06.2020

Der Bundesgerichtshof (BGH, 28.05.2020 – Az. I ZR 7/16) urteilte Ende Mai, dass für den Einsatz von nicht notwendigen Cookies die Einwilligung des Nutzers erforderlich ist.

Wie kam es zu dem Urteil?

Nachdem die Verbraucherzentrale einen Webseiten-Betreiber wegen eines Cookie-Banner abgemahnt hatte, begann der Rechtsstreit durch die Instanzen bis zum BGH. Und der BGH verwies den Fall zur Klärung einiger spezieller Fragen zum EuGH. Nach dem EuGH Urteil im Jahr 2019 urteilte jetzt der BGH als abschließende Instanz.

Was bedeutet das Urteil?

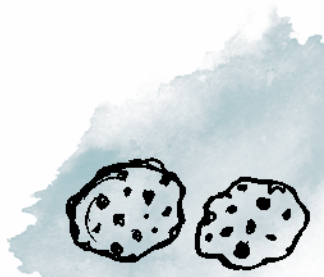
Der EuGH und aktuell auch der BGH haben entschieden, dass Webseiten, die bestimmte Cookies setzen, hierfür eine aktive Einwilligung der Besucher benötigen. Das oft genutzte Banner „Mit der Nutzung der Webseite stimmen Sie Cookies zu“ reicht nicht aus, denn hierdurch wird keine aktive Einwilligung erteilt.

Auch eine schon ausgewählte Checkbox ist nicht erlaubt. Auch das stellt nach dem Urteil des BGH keine echte aktive Einwilligung dar.

Denn eine Einwilligung kann nur „in Kenntnis der Sachlage“ erfolgen, wenn man weiß, dass die Erklärung ein Einverständnis darstellt und worauf sie sich im konkreten Fall bezieht, so der BGH. Das sei bei diesen einfachen Cookie-Bannern nicht der Fall, denn hier könne der Besucher der Webseite erst in einem aufwendigen Verfahren eine Auswahl treffen, welche Cookies automatisch gesetzt werden und diesen widersprechen.

Welche Folgen hat das BGH-Urteil für Sie bzw. den Einsatz von Cookies auf Ihrer Website?

- Sie benötigen für alle nicht notwendigen Cookies – vor allem für Tracking Cookies wie etwa von Google Analytics, aber auch für alle anderen Tools und PlugIns, die technisch nicht notwendig sind – eine echte Einwilligung der Nutzer auf Ihrer Webseite. Dies gilt auch, wenn die IP-Adresse pseudonymisiert wird.
- Die Einwilligung muss nachweisbar protokolliert werden.
- Ein „Durch Weitersurfen akzeptieren Sie alle Cookies“-Banner oder ein Cookie-Banner mit schon vorangekreuzter Checkbox, reichen für die Einwilligung nicht aus.
- Das Cookie- bzw. Einwilligungs-Banner muss die Cookies auch wirklich blockieren, bis der Nutzer eingewilligt hat.



Ausnahme von Einwilligungserfordernis: Unbedingt notwendige Cookies

Einzig nicht davon betroffen sind Cookies, die für eine Website unbedingt notwendig sind.

Hierzu gehören beispielsweise die Folgenden:

- das Cookie, das den Einwilligungsstatus für andere Cookies festhält
- Session-Cookies, die den Warenkorb-Status eines Online-Shops oder eines Input-Formulars kurzfristig festhalten
- kurzfristige Login-Cookies
- Einstellungs-Cookies, die zum Beispiel die Spracheinstellungen oder andere Einstellungen auf einer Website festhalten (jedenfalls, wenn sie nur kurz gespeichert werden)
- Multimedia-Cookies, etwa für Flash-Player
- Session-Cookies zur Lastverteilung auf dem Server

Diese Cookies werden als unbedingt notwendig angesehen, weshalb es keiner vorherigen Einwilligung bedarf. Wichtig ist aber, dass in diesen Cookies auch tatsächlich nur die notwendigen Angaben gespeichert werden, und dies zeitlich auch nicht über Gebühr.

EUROPÄISCHER GERICHTSHOF ERKLÄRT DATENTRANSFER IN DIE USA GRÖSSTENTEILS FÜR UNGÜLTIG!

Newsletter vom 27.07.2020

Erneut hat uns der Europäische Gerichtshof mit einer Aufsehen erregenden aktuellen Entscheidung (EuGH, 16.07.2020 – Az. C-311/18) vor neue Herausforderungen gestellt.

Der EuGH hat nämlich das sogenannte „Privacy-Shield“ für unwirksam erklärt. Damit hat er dem Datentransfer zwischen der EU und den USA größtenteils die Grundlage entzogen. Informationen über europäische Verbraucher seien auf US-Servern nicht vor dem Zugriff dortiger Behörden und Geheimdienste geschützt, so der Richter.

Die US-Behörden hätten zu weitgehende Prüfungsrechte, die Datenzugriffe bei Nicht-US-Bürgern auch ohne richterlichen Beschluss und ohne Rechtsschutz erlaubten. Aus diesem Grunde sei ein Schutzniveau, das dem der Datenschutz-Grundverordnung entspreche, nicht gewährleistet. Der Datenverkehr zwischen den USA und der EU ist deshalb in den meisten Fällen rechtswidrig.

Das betrifft insbesondere die großen Anbieter wie z. B. Google, Facebook, Amazon, Amazon-Cloud, Dropbox, aber auch Tracking- und Newsletter-Anbieter, wenn Daten von EU-Bürgern auf Servern mit dem Standort USA gespeichert werden. Nur wenn die sogenannten Standardvertragsklauseln bei vergleichbarem Schutzniveau eingehalten werden, dürfen noch Daten von EU-Bürgern in Staaten außerhalb von Europa verarbeitet werden. Ob das aufgrund der US-Gesetze möglich ist, ist nach dem Urteil des EuGHs fraglich.

Was bedeutet das Urteil für die Praxis?

Wie so oft im Bereich Datenschutz herrscht nach dem Urteil des EuGHs zum Privacy-Shield eine große Rechtsunsicherheit.

Darüber hinaus können wir im Moment folgende Empfehlungen geben:

- Überprüfen Sie, welche Softwareanbieter und Dienstleister aus den USA Sie einsetzen.
- Kontrollieren Sie, ob personenbezogene Daten an diese Unternehmen übermittelt werden.
- Prüfen Sie, ob die Datenübermittlung in die USA auf der Grundlage des Privacy-Shields-Abkommens gestützt war. Einen solchen Hinweis finden Sie meist in den entsprechenden Verträgen mit den Unternehmen.
- Wenn Sie weiter US-Anbieter nutzen möchten, dann fragen Sie nach, ob eine Verarbeitung auf Servern mit Standort in Europa möglich ist. Hier besteht zwar eine Rechtsunsicherheit, aber es ist eine sicherere Variante, als die Daten in den USA zu speichern.
- Achten Sie auch darauf, dass Ihr Dienstleister keine US-Subunternehmen einsetzt, die Daten in den USA verarbeiten. Lassen Sie sich das am besten schriftlich bestätigen.
- Passen Sie Ihre Datenschutzerklärungen und Verträge an und entfernen Sie dabei beispielsweise Hinweise auf das Privacy-Shield.

TROTZ CORONA – AUFSICHTS-BEHÖRDEN VERHÄNGEN HOHE BUSSGELDER

Newsletter vom 07.08.2020

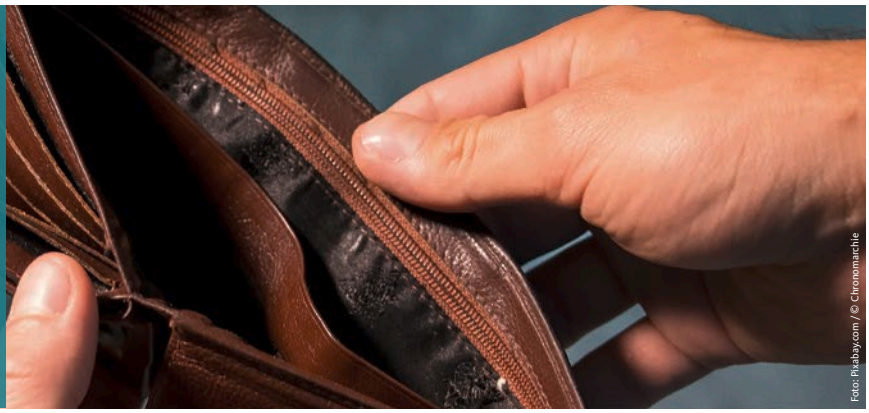


Foto: Pixabay.com / © Chronomarchie

Aus den zahlreichen E-Mails und Beratungsgesprächen mit Ihnen wissen wir, viele arbeiten Corona-bedingt noch im Home-Office. Was Sie aber trotz der veränderten Arbeitsbedingungen nicht vergessen sollten: Die Aufsichtsbehörden nehmen auf die Pandemie keine Rücksicht.

War 2019 noch das Jahr, wo sich alle auf die neuen Regelungen einstellen konnten und das Datenschutzmanagement organisieren konnten, machen die Aufsichtsbehörden, was die Bußgelder angeht dieses Jahr ernst.

Besonders oft werden die Aufsichtsbehörden aktiv, wenn Personen per (Werbe-)E-Mail angeschrieben oder angerufen werden, obwohl sie hierzu keine Einwilligung gegeben haben.

Ganz aktuell wurde in Baden-Württemberg ein Bußgeld in Höhe von 1,24 Mio. Euro gegen eine Krankenkasse verhängt, weil 500 Teilnehmer eines Gewinnspiels, anschließend eine (Werbe-)E-Mail erhielten, obwohl sie hierzu keine Einwilligung erteilt haben.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit, Maja Smoltczyk, hat im März 2020 die Deutsche Gesellschaft für Politikberatung (degepol) wegen eines Verstoßes gegen die Datenschutz-Grundverordnung (DS-GVO) verwarnt. Die degepol hatte wiederholt per E-Mail Verbände und deren Vertreter, die ins öffentliche Lobbyregister des Bundestags eingetragen sind, anschreiben lassen und zur Teilnahme etwa an Umfragen aufgefordert. Somit ist seit diesem Fall klargestellt, dass der Datenschutz nicht danach differenziert, ob die Tätigkeit des Dateninhabers gesellschaftlich hohes Ansehen genießt oder nicht. Es werden im Datenschutzrecht alle gleich behandelt.

Deshalb unsere dringende Bitte: Kontrollieren Sie Ihre Verteiler. Prüfen Sie auf welcher Rechtsgrundlage Sie die Daten verarbeiten. Wählen Sie sodann den geeigneten Kommunikationsweg aus. Wenn Sie Zweifel an der Herkunft der Daten haben (gerade, wenn es sich um elektronische Kommunikationsdaten handelt) und keine Einwilligung vorliegt, überlegen Sie bitte dreimal, ob Sie dieses Risiko eingehen möchten. Am sichersten ist es, Ihre Verteiler endgültig aufzuräumen und „unsichere“ Datensätze zu löschen.

DAS sind WIR...

Verpackungstechniker Fahrer Digitaldrucker Dankbar Plakatroller An-die-Hand-Nehmer Falzer Dauerläufer Feinschmecker Brötchengeber Roll-Upper Sekretäre Blickwinkel-Veränderer Gärtner Handwerker Helden der Arbeit Informatiker Mediengestalter flexibel Dynamisch Möbelpacker Festungsbauer SQL-Abfragegestalter Crossmedia Spezialisten Ratgeber Leimer Report-Designer Skript-Programmierer Süßigkeiten-aus-dem-Automatenzieher Techniker um-die-Ecke-Gucker Verhandlungspartner Verpackungskünstler Web-Designer Bereichsleiter Über-den-Tellerrand-Gucker Fernsteuerer Datenbankadministratoren Controller Offsetdrucker Begleiter Lettershop Nerds Veredler Berliner Mütter Riller IT-Profis Wagenschieber Brillenträger belastbar Helfer Kreative Köpfe Kaffeeauffüller Töchter Künstler

Netzwerker Kartengeber viele Designer App-Entwickler Familie Klimaneutral Datenumformatierer UBGler International Datenmanager Praktiker Schrauber Wegbereiter Organisatoren spitze Kundenversteher Buchbinder Briefboten Briefmarkenschlecker Controller Ideengeber einzigartig Scharfseher Dienstleister Viren- und Trojanerbekämpfer Netzwerker schnell herzlich Zuhörer Ausbilder zuverlässig Roadrunner flauschig Alleswisser Aushilfen Passwortbodyguards Sachbearbeiter Möglichmacher Ideengeber Vernetzer Auftragsverarbeiter Dialogpostmanager Juristen Söhne Politiker Teamplayer Problemlöser bunt Hotliner Charakterköpfe Farbmischer Kaffeetrinker Messestand-Aufbauer Bürohopser Verleger Chancengeber Berater Kreative Mädchen für alles Kaufleute Internet-Experten Gabelstaplerfahrer Postler Auslieferer Frühaufsteher Weltverbesserer Auszubildende Blöckchenmacher Umweltschützer IT-Supporter Datenverarbeiter Formulargestalter Assistenten Palettenbauer Lagerist Kundenbetreuer Buchhalter Stapler Administratoren Programmierer Frankierer Versender Rheinbacher Väter Postleitzahlenjongleure Papierpresser Supporter Exporteure Dauerbrenner Betriebsräte Chefs Strippenzieher Pixelschubser Rentner Rüttler Farbgeber Datenschützer

... Wir sind Kollegen, ein Team und Menschen!

UBG

AUSBLICK 2021

Mit Spannung werden die Ergebnisse der Taskforces und der europäischen Datenschutzaufsichtsbehörden hinsichtlich des **Datentransfers in die USA** erwartet. Ebenso soll es in Kürze eine Richtlinie der europäischen Aufsichtsbehörden bezüglich der **Zielgruppenansprache von Social Media-Nutzern** geben.

Das Thema **Cookie-Banner** und deren Gestaltung wird uns auch 2021 weiterbeschäftigen. Durch den Aufbau und das Design vieler Banner werden Benutzer oft dazu gebracht, bestimmten Tracking-Cookies zuzustimmen, obwohl sie das gar nicht möchten, insoweit ihren Interessen oder ihrem Willen entgegenlaufen. Dies wird auch **„Dark Pattern“** genannt und wird bewusst eingesetzt. Es bleibt die Entwicklung abzuwarten, wie sich die Aufsichtsbehörden hier positionieren werden.

Cybersicherheit wird uns auch 2021 begleiten und einen Großteil unseres Augenmerks einnehmen. Gerade jetzt sind wir einem höheren Risiko ausgesetzt, da viele Mitarbeiter von zu Hause aus arbeiten. Cyber-Bedrohungen gibt es in vielen Formen, und die häufigste unter ihnen ist E-Mail-Phishing.

Die Nutzung von Clouddiensten bietet eine Vielzahl von Vorteilen: Flexibilität, Globale Vernetzung, Zugang von überall, einfacher Wissensaustausch auch mit verschiedenen Arbeitszeitmodellen. Darin auch umfassende Funktionalitäten wie zum Beispiel konstante Zuverlässigkeit, verbesserte Notfallwiederherstellung, Kostenreduzierung und Zusammenarbeit etc.. Aber auch hier kommt es 2021 auf die Auswahl der Anbieter an und insbesondere auf die Cloud Security.

Künstliche Intelligenz ist auch die Grundlage für unzählige technologische Innovationen wie Gesichtserkennung, Datenverarbeitung, Spracherkennung usw. geworden. Die Möglichkeiten sind noch lange nicht erschöpft. Dieses Thema wird uns 2021 noch stärker begegnen.

Eins wird jedoch weiterhin bleiben: **Unklare, schwammige Formulierungen.** Die DS-GVO ist gespickt mit weichen Formulierungen und Begriffen. Alleine der Begriff „angemessen“ kommt fast 50 Mal vor. Der Wunsch nach Klarstellung muss daher unerfüllt bleiben. Die Ursache liegt vor allem im risikobasierten Ansatz der DS-GVO.

Datenschutz und Datensicherheit wird auch 2021 ein ständiger Prozess sein

Der Verantwortliche soll die Risiken seiner individuellen Datenverarbeitung unter dem aktuellen Stand der Technik erkennen, ständig bewerten und die daraus erforderlichen Maßnahmen in eigener Verantwortung bestimmen und umsetzen.

Bei der Beurteilung dieser Maßnahmen stehen wir Ihnen gerne zur Verfügung und begleiten Sie in diesem Prozess.

TÄTIGKEITSBERICHT FÜR IHRE GESCHÄFTSSTELLE

Zwar sind wir laut den geltenden Datenschutzgesetzen nicht dazu verpflichtet einen Tätigkeitsbericht zu führen, dennoch haben wir das bewusst in unsere Verträge aufgenommen. Zu Dokumentations- und Nachweiszwecken Ihnen gegenüber und auch im Notfall gegenüber den Aufsichtsbehörden, dokumentieren wir alle unsere für Sie getätigten Aktivitäten. Dies umfasst unsere komplette Korrespondenz (E-Mail, Post und Telefon), eventuell abgehaltene Schulungen oder Unterweisungen sowie die Auswertung Ihrer Online-Prüfung und die damit verbundenen Technischen organisatorischen Maßnahmen (TOM).

Wir verwahren Ihre Tätigkeitsberichte und stellen Ihnen diese auf Wunsch gerne zur Ansicht zur Verfügung. Bei Interesse fordern Sie den Tätigkeitsbericht einfach an.

DATEN-POD – DA LAUFEN DIE DATEN ÜBER!

Im August 2020 starteten wir zusätzlich mit einem Podcast, in dem wir über datenschutzrelevante aber auch andere rechtlich interessante Themen sprechen. Wir wollen uns stetig verbessern und auch persönlicher für Sie werden, daher arbeiten wir auch daran den Podcast für ein besseres Verständnis zu visualisieren.

Aktuell umfasst unser Podcast die folgenden Episoden:

1. Videokonferenzen und Passwörter
2. Cookies
3. Bildrechte, Fotos und Lizenzen – Teil 1
4. Bildrechte, Fotos und Lizenzen – Teil 2
5. „Der gläserne Mensch“ – Sonderfolge

Hören können Sie den Podcast aktuell auf Spotify, iTunes, Deezer oder Podimo.

Ihre Plattform ist nicht dabei? Sie haben einen Themenvorschlag oder wollen uns einfach Feedback geben?

Schreiben Sie uns eine Nachricht an: **podcast@ubgnet.de**
Alternativ können Sie auch vollkommen anonym unser Kontaktformular nutzen, das wir auf unserer Podcast-Seite für Sie erstellt haben.

Ihre Ansprechpartner

Union Betriebs-GmbH
Leitung Datenschutz & Recht
Barbara von Meer
Betriebsstätte Berlin
Klingelhöferstraße 8
10785 Berlin
Tel. + 49 (0) 30 / 22070-570
datenschutz@ubgnet.de

Herausgeber

Union Betriebs-GmbH
Geschäftsführer: Jürgen von Meer
Egermannstraße 2
53359 Rheinbach
Tel. + 49 (0) 2226 / 802-0

Illustrationen:
Isa Schulz · #schulz_malt

Als Medienhaus mit dem Standort Rheinbach und der Betriebsstätte Berlin sind wir stolz darauf, dass unsere Qualität in ganz Deutschland geschätzt wird.

UBG

Wie können wir Ihnen helfen?

Union Betriebs-GmbH
Rheinbach: Egermannstraße 2 | 53359 Rheinbach
Telefon 02226 802-0 | Telefax 02226 802-111
info@ubgnet.de

Berlin: Klingelhöferstraße 8 | 10785 Berlin
Telefon 030 220 70-271 | Telefax 030 220 70-279
www.UBG365.de

Wir schützen Ihre Daten.
Wir schützen Ihre Privatsphäre.
Sicher, zuverlässig und blickdicht.