DOSB FÜHRUNGS AKADEMIE

FA Datenschutzportal

DSP Info-Brief

Nr. 44 / März 2017

INHALT

DATENSCHUTZPORTAL INTERN

IN DER DISKUSSION – NEUIGKEITEN RUND UM DEN DATENSCHUTZ

MEDIEN –TECHNIK – SICHERHEIT

GESETZGEBUNG

AKTUELLE URTEILE

Herausgeber
Führungs-Akademie des DOSB

Kontakt FA
Führungs-Akademie des DOSB
Willy-Brandt-Platz 2 / 50679 Köln
Tel. 0221 – 221 275 94 /// Fax: 0221 – 221 220 13
www.fuehrungs-akademie.de
niewerth@fuehrungs-akademie.de

Technische Umsetzung
Führungs-Akademie des DOSB

Redaktion
Toni Niewerth / Robert Graf

Kontakt SVBG
Sachverständigenbürogemeinschaft Mülot:Graf
Westfalenweg 2
33449 Langenberg
www.muelot.de/
r.graf@muelot-graf.de

DATENSCHUTZPORTAL INTERN

1 Info-Briefe
Aktualisierte Übersicht über alle behandelten-Themen 2013 – 2016

Der seit Anfang 2013 angebotene Service des monatlichen Info-Briefes bietet monatlich aktuelle Berichte zu relevanten Themen des Datenschutzes im Verein und Verband. Mit Berichten sowohl zu Neuerungen im Portal selbst wie zu aktuell im Datenschutz diskutierten Themen sind die Info-Briefe neben den Live-Chats und dem Dokumentenpool die inhaltlich dritte Säule unseres Info-Angebots zum Datenschutz.

Um Ihnen die Möglichkeit zu geben, sich schnell und vor allem auch umfassend über die behandelten Themen zu informieren, haben wir die Titel aller in den Info-Briefen diskutierten bzw. vorgestellten Themen in eine Excel Datei übertragen. Mit Angaben zum Titel des Beitrags, zu Ausgabe, Rubrik und Seitenangabe erhalten Sie damit einen schnellen und sicheren Zugriff auf Themen, die für Sie relevant sind.

Insgesamt stehen damit vier Übersichten zur schnellen Suche nach Themen zur Verfügung:

1. Datei mit allen im Portal bereitgestellten Dokumenten
2. Datei mit den Inhalten aller Info-Briefe
3. Datei mit allen Themen der Live-Chats
4. Datei mit allen im Portal vorgestellten Gerichtsurteilen zum Datenschutz.[1] [TN]

FÜHRUNGS AKEDEMIE — **DSP Info-Briefe** — Seite 1 (19)
Übersicht - Alle Themen alle Ausgaben (Jan. 2013 - Dez. 2016)

INFO Brief Nr.	AUSGABE DATUM [JJJJ-MM]	RUBRIK	THEMA	Seite [Beginn]
01	2013-01	GESETZGEBUNG	Zum Unterschied zwischen förmlichen Gesetzen und Rechtsverordnungen	1
02	2013-02	IN DER DISKUSSION: NEUES RUND UM DEN DATENSCHUTZ	Verunsicherung beim Newsletter-Versand nach Urteil zu ‚Double-Opt-In-Verfahren	1
03	2013-03	IN DER DISKUSSION: NEUES RUND UM DEN DATENSCHUTZ	Darf man selbst aufgenommene Fotos von anderen ins Internet hochladen und damit veröffentlichen?	1
04	2013-04	AKTUELLE URTEILE	Arbeitsgericht Frankfurt: Umgang mit Fotos ausgeschiedener Mitarbeiter(innen)	1
04	2013-04	AKTUELLE URTEILE	Landesarbeitsgericht Schleswig-Holstein: Arbeitnehmerfoto auf der Webseite des Arbeitgebers	2
05	2013-05	IN DER DISKUSSION: NEUES RUND UM DEN DATENSCHUTZ	Löschfristen für Daten von Bewerber(inne)n	1
06	2013-06	AKTUELLE URTEILE	Arbeitsgericht Cottbus: Automatischer Wegfall der Bestellung als DSB bei Betriebsübergang – ein Widerruf dazu ist unnötig	1
06	2013-06	IN DER DISKUSSION: NEUES RUND UM DEN DATENSCHUTZ	Betriebswirtschaftliches Know-how – Ein Risikomanagement für den Datenschutzbeauftragten	5
07	2013-07	AKTUELLE URTEILE	Unbedachter Umgang bei der Versendung von Serien-E-Mails mit sichtbarem E-Mail Verteiler führt zu Bußgeld	2
07	2013-07	DATENSCHUTZPORTAL INTERN	Redaktionelle Überarbeitung von Dateien	3
07	2013-07	DATENSCHUTZPORTAL INTERN	Gut informiert in den Tag: der Datenschutz-Tages-Ticker der Plattform	4
08	2013-08	IN DER DISKUSSION: NEUES RUND UM DEN DATENSCHUTZ	Datenschutz in den Wahlprogrammen von Parteien	1
08	2013-08	AKTUELLE URTEILE	Beschluss des Bundesgerichtshofes zur Übermittlung unternehmensinterner Daten per ungesicherter E-Mail-Übertragung	2
08	2013-08	IN DER DISKUSSION: NEUES RUND UM DEN DATENSCHUTZ	Aufsichtsbehörden: Bußgeldverfahren gegen einzelne Mitarbeiter	2

DATEI: _INFO-BRIEFE_Übersicht_alle-behandelten-Themen_160508.xlsx — BLATT: DSP Info-Briefe Alle Themen — DATUM: 31.03.2017

[1] Eine aktualisierte Übersicht erhalten Sie mit der nächsten Ausgabe des Info-Briefes (Nr. 45, 2017-04)

2 Themen und Inhalte des Live-Chats vom 31.3.2017

Ist das Auslegen von Trainingsplänen mit den Angaben *Name*, *Vorname*, *Übungen* zur Selbstentnahme datenschutzrechtlich unproblematisch?

Unsere Fitnesstudios haben an der Theke die Trainingspläne der einzelnen Fitnessstudionutzer hinterlegt. Die Mitglieder nehmen sich hier ihre Pläne selbst aus dem Ordner mit zu ihren Trainingsgeräten. Auf diesen Plänen sind nur der *Name* und *Vorname* und die einzelnen *Übungen* eingetragen. Es sind keine sonstigen persönlichen Daten, wie Geburtsdatum, Anschrift, Gesundheitsdaten etc. aufgeführt. Die Gesundheitsdaten der einzelnen Mitglieder werden separat in Ordner aufbewahrt und nur bei Bedarf von den Mitarbeitern an das Mitglied ausgegeben bzw. für Einträge genutzt.

Meine Fragen:
1. Dürfen wir dies so weiter handhaben oder müssten die Trainingspläne immer persönlich ausgeben werden?

2. Welche Möglichkeiten hätten wir, sollte diese Lösung datenschutzrechtlich nicht zulässig oder bedenklich sein, wir aber an der Selbstentnahme festhalten möchten? Wäre es datenschutzrechtlich zulässig, wenn auf den Trainingsplänen nicht der Name, sondern nur die Mitgliedsnummer oder nur der Nachname und der erste Buchstabe des Vornamens steht?

AW:
Sie sollten die Trainingspläne persönlich ausgeben. Mit den von Ihnen genannten Daten auf dem Trainingsplan haben die Sportler die Möglichkeit, auf personenbezogene Daten anderer Sportler zuzugreifen, damit können Sie das Ziel der Vertraulichkeit nicht mehr gewährleisten. Ggf. sind die Trainingspläne auch als personenbezogene Daten mit medizinischem Hintergrund zu werten, da sie ggf. Rückschlüsse auf die Fitness oder Gesundheit des jeweiligen Sportlers zu lassen. Diese Daten erfordern einen besonderen Schutz vor Zugriff und Zugang von Unbefugten.

In diesem Fall würde ich auch eine Pseudonymisierung, also eine Steuerung über die Mitgliedsnummer für nicht ausreichend erachten, da diese verschiedenen Personen bekannt sei kann. [R. Graf]

Umgang mit Trainingsplänen der Teilnehmer/innen im Fitnessstudio?

In unserem Verein werden die Trainingspläne persönlich an die Teilnehmer/innen ausgegeben. Eigentlich vorgesehen ist, dass die Teilnehmer/innen die Pläne mit nach Hause nehmen und beim nächsten Besuch des Studios wieder mitbringen. Nachdem Teilnehmer/innen, denen das zu umständlich war, bei uns nachgefragt haben, ob sie die Trainingspläne nicht im Studio lassen könnten, haben wir in einem Schrank Karteikästen zur Verfügung gestellt, in dem diejenigen, die den Trainingsplan nicht mit nach Hause nehmen möchten, ihren Plan deponieren können. Dieses Angebot wird von ca. der Hälfte der Teilnehmer/innen genutzt. Da das Einstellen von den Teilnehmern selbst erfolgt, sind wir davon ausgegangen, dass diese Praxis datenschutzrechtlich unproblematisch ist. Ist das richtig?

AW:
Sie haben recht, datenschutzrechtlich ist das eine Einwilligung der Teilnehmer. Ich würde jedoch aus Beweisgründen empfehlen, sich die Einwilligung für diesen Vorgang schriftlich geben zu lassen. [R. Graf]

Nutzung von WhatsApp auf den Diensthandys des Vereins

Der Verein hat einigen Mitarbeitern, vor allem auch den Sportlehrern ohne Bürozeiten, ein Diensthandy ausschließlich zur dienstlichen Nutzung (private Nutzung ist in einer Handyvereinbarung, die jeder einzelne unterzeichnen musste, verboten) ausgegeben.

Da in vielen Bereichen schnell Vertretungen gesucht, oder aber auch Teilnehmer von Kursen kurzfristig informiert werden müssen, wurde deshalb die Nutzung von WhatsApp erlaubt. Ist dies aus datenschutzrechtlicher Sicht ein Problem, bzw. welche Alternative gäbe es. Uns stellt sich hier das Problem, dass, sollten wir uns für einen anderen Anbieter entscheiden, unsere Mitglieder/Sportler oder Sonstige dann nicht mehr für uns erreichbar sind, da die Mehrheit im Allgemeinen WhatsApp-Nutzer sind.

AW:
Ich bitte Sie die entsprechenden Beiträge im Live Chat Bereich zu prüfen.***** Dort haben wir zum Thema Whatsapp schon einiges geschrieben. Zusammenfassend: Es gibt einige Bedenken bezüglich der Datenübertragung in Drittländer, hier die USA. Eine Übertragung personenbezogener Daten in Drittländer unterliegt erheblichen datenschutzrechtlichen Einschränkungen. Es handelt sich hierbei um die Daten der Kontakte im Kontakteordner des Smartphones und um die „Metadaten", wer hat mit wem kommuniziert. Es gibt diesbezüglich auch schon eine Anordnung des Hamburgischen Datenschutzbeauftragten und auch die Verbraucherschutzzentralen klagen gegen WhatsApp.

Die hohe Verbreitung des Programmes bringt natürlich entsprechende Probleme, wenn man es nicht mehr benutzt. Dies ist aber aus datenschutzrechtlicher Sicht unerheblich.

Eine Alternative kann der Messenger „Signal" sein, der komplett verschlüsselt ist und keine solche Datenweitergabe durchführt.

Weitere weniger problematische Messenger sind Telegram, Threema und Hoccer.

Die Problematik stellt sich vielen Organisationen und ggf. muss die Kommunikation auf andere Medien umgestellt werden, z. B. E-Mail. [R.Graf]

* Als Anlage erhalten Sie mit diesem Schreiben die Datei „Live-Chat Archiv" mit allen in den Live-Chats seit 2013 behandelten Themen. Wenn Sie hier mit den Stichpunkten „app" oder „messenger" suchen, werden alle entsprechenden Stellen angezeigt.

Nutzung der Adressdaten von Kursteilnehmern zur Information über neue Kursangebote und Aktivitäten des Kreissportbundes

Im Rahmen unseres Gesamtangebots bietet der Kreissportbund seit vielen Jahren auch eine Reihe von Kursen durch. Die zur Anmeldung notwendigen personenbezogenen Daten werden nicht in eine eigene Datenbank des KSB eingepflegt, sondern in eine zentra-

le Datenbank des LSB. Die Eingaben in die Datenbank werden von uns selbst vorgenommen. Die Zuordnung der eingegebenen der Daten zum Kreissportbund erfolgt über eine Kennziffer.

Die von uns in der beim LSB liegenden Datenbank eingegebenen Kontaktdaten möchten wir jetzt gerne nutzen, um die (ehenmaligen) Kursteilnehmer/innen auf neue Kurse, Aktivtäten und Veranstaltungen des KSB hinzuweisen. Auf Anfrage, ob wir die Kontaktdaten dazu nutzen dürfen, haben wir vom LSB die Nachricht erhalten, dass wir Daten aus der Datenbank des LSBs nur für postalische Werbung (Kursangebote, Reisen etc.) nutzen dürfen, nicht aber für E-Mail-Werbung. Ist das richtig? Besteht datenschutzrechtlich ein Unterschied, ob ich die Daten per Post oder per E-Mail versende?

AW:
Zunächst eine Vorbemerkung. Sie pflegen ihre Teilnehmerdaten in eine Datenbank des Landesportbundes ein. Damit verarbeitet der Landessportbund diese Daten für sie im Auftrag, also liegt hier eine Auftragsdatenverarbeitung vor. Bitte berücksichtigen Sie dies und schließen Sie – sollte kein Vertrag vorliegen– gemäß §11 BDSG einen entsprechenden Vertrag zur Auftragsverarbeitung mit dem Landesportbund ab.

Nun zur Zulässigkeit der Bewerbung von Kunden per E-Mail: Hier ist der §7 Abs. 3 UWG relevant.

Da es sich bei den Daten um Ihre eigenen Daten handelt, können Sie sie auch im Rahmen Ihrer Zweckbestimmung nutzen. Insofern teile ich die Ansicht des LSB, dass Sie die Daten auch nutzen können, um die ehemaligen Kursbesucher auf postalischem Wege auf neue Aktivitäten hinzuweisen

Die unterschiedliche Bewertung der Zulässigkeit auf Grund der Versendungsart liegt daran, dass die gesetzlichen Vorlagen beim Versand von Werbung per E-Mail nicht vom BDSG, sondern vom Gesetz gegen den unlauteren Wettbewerb (UWG) geregelt wird. Um die Verbraucher vor ungewollten Werbungen zu schützen, hat der Gesetzgeber hier höhere Maßstäbe gesetzt und strengere Vorschriften erlassen, die es zu beachten gilt.

Eine schriftliche Einwilligung ist hier der sichere Weg. In den Anmeldeformularen können Sie ja – zumindest für zukünftige Teilnehmer/innen – eine entsprechende Einwilligungserklärung aufnehmen. Bitte denken Sie auch daran, dass sowohl in der Einwilligungserklärung als auch beim Mailing selbst immer auch ein Widerrufungshinweis vorhanden sein muss.

Eine ausführliche Beschreibung der Bedingungen und entsprechende Vorgehensweisen finden Sie im nachfolgenden Link. Möglicherweise ergibt sich aus der Lektüre auch noch einmal ein Ansatzpunkt zu einem Gespräch mit dem LSB [LINK: E-Mailwerbung im UWG].

IN DER DISKUSSION – NEUIGKEITEN RUND UM DEN DATENSCHUTZ

3 Persönliche Daten im freien Internet schützen

Quelle: Bundesministerium für Wirtschaft und Energie, anlässlich des G20 Digitalministertreffens

Daten sind im digitalen Zeitalter so wertvoll wie noch nie. Laufend entstehen neue Geschäftsmodelle, die persönliche Daten nutzen, um uns maßgeschneiderte Dienste anzubieten und unser Leben zu vereinfachen.

Doch die Sicherheit der Daten und die informationelle Selbstbestimmung dürfen dabei nicht zu kurz kommen. Deshalb brauchen wir Regeln, auf die sich die Nutzer auch im Internet verlassen können.

Viele Online-Plattformen und Apps machen unser Leben leichter. Beispiel WhatsApp: Statt sich mit jedem Freund einzeln abzustimmen, kommuniziert man gleichzeitig mit dem gesamten Freundeskreis. Und verabredet sich mal schnell für abends zum Glas Wein beim Italiener. Eine solche Kommunikation erzeugt jede Menge Daten, die vom Messenger-Dienst erhoben und weiterverarbeitet werden. Was mit den Daten passiert, kann der Nutzer nicht immer nachvollziehen. Er hat dann nur die Wahl, das hinzunehmen oder ganz auf den Dienst zu verzichten.

Deshalb sollte das Leitbild der Datensouveränität mehr in den Mittelpunkt rücken. Das bedeutet: Jeder Nutzer soll eine stärkere Kontrolle haben, wann und wo er welche Daten preisgibt. Dadurch kann er selbst entscheiden, wie stark er seine persönlichen Daten schützen möchte. Und bekommt ein besseres Verständnis dafür, dass Online-Plattformen und Apps seine persönlichen Daten zu Werbezwecken nutzen - sozusagen als Bezahlung für die meist kostenlosen Dienste.

Wie lässt sich mehr Datensouveränität erreichen?

Um mehr Datensouveränität zu ermöglichen, sind beide Seiten gefragt. Einerseits müssen die Nutzer lernen, mit ihren Daten kompetent und selbstbestimmt umzugehen. Dafür ist digitale Bildung eine wichtige Voraussetzung. Andererseits könnten Unternehmen neue Formen der Einwilligung anbieten, damit der Nutzer überhaupt entscheiden kann, wie viele Daten er preisgibt. Online-Plattformen und Apps lassen sich auch so gestalten, dass sie auf technischem Wege („by design") oder durch datenschutzfreundliche Grundeinstellungen („by default") den bestmöglichen Datenschutz gewährleisten.

Auch der Gesetzgeber ist beim Thema Datensouveränität aktiv. Im Mai 2018 greift die neue Datenschutz-Grundverordnung der EU. Sie sieht verschiedene Neuerungen vor, die die Datensouveränität des Einzelnen stärken. Hierzu gehört etwa das „Recht auf Vergessenwerden", das nunmehr erstmals ausdrücklich festgeschrieben wird: Nutzer können persönliche Informationen, die über sie von einem Unternehmen gespeichert werden, leichter löschen lassen. Wenn ein Nutzer von einer Plattform auf eine andere „umziehen" möchte, kann er zudem sein „Recht auf Datenübertragbarkeit" geltend machen - Stichwort Datenportabilität. Damit können Nutzer zum Beispiel leichter zwischen Musik-Streamingdiensten wechseln.

Was können die G20 tun?

Auch außerhalb der EU wollen wir bessere Datenschutzstandards erreichen. Die Menschen sollen sich darauf verlassen können, dass ihre persönlichen Daten bei Unternehmen sicher sind. Deshalb setzt sich die deutsche G20-Präsidentschaft dafür ein, Vereinbarungen zum Schutz der Privatsphäre und zum Datenschutz, zur Datensicherheit und zum Verbraucherschutz weltweit zu treffen.

Bei alldem muss das Prinzip des freien Internets gelten: Das Internet darf von keinem Staat zensiert, abgeschaltet oder für eigene Zwecke missbraucht werden. Es bildet die Grundlage für ungehinderten Wissensfluss, für Meinungsvielfalt und eine erfolgreiche digitale Wirtschaft: Jeder Nutzer kann sich jederzeit frei äußern und informieren, jedes Unternehmen seine Dienste weltweit ungehindert anbieten. [RG]

MEDIEN –TECHNIK – SICHERHEIT

4 Passwort-Manager LastPass: Passwortklau möglich

Fundort: SICHER • INFORMIERT- Der Newsletter des Bürger-CERT vom 30.03.2017

Wie unter anderem heise.de berichtet, besteht im Passwort-Manager LastPass aktuell eine Sicherheitslücke, über die es möglich ist, Passwörter abzugreifen oder auch zu ändern. Zudem kann über das Plug-in in der Binärcode-Version ein Schadcode auf dem jeweiligen Rechner ausgeführt werden. LastPass hat nun reagiert und kündigt im Unternehmens-Blog einen baldigen Patch an, der die Lücke schließen soll. Außerdem rät das Unternehmen Nutzerinnen und Nutzern bis dahin folgendes: Erstens sollten Webseiten, deren Zugangsdaten mit LastPass verwaltet werden, nur direkt über den Tresor (Vault) des Programmes geöffnet werden. Zweitens sollte soweit möglich die Zwei-Faktor-Authentifizierung aktiviert werden. Und drittens wird darauf verwiesen, dass sich die Anwenderinnen und Anwender vor Phishing-Angriffen in Acht nehmen sollten. [TN]
[LINK zum Artikel auf heise.de /// LINK zum Blog von LastPass]
Ergänzende INFOs zum Thema Pishing und zum Schutz vor Pishing.

5 Malware: Word-Makro als mögliches Einstiegstor für Hacker

Fundort: SICHER • INFORMIERT- Der Newsletter des Bürger-CERT vom 30.03.2017

Derzeit ist laut ZDNet eine neue Form von sogenannten Makro-Viren in Umlauf. Das Besondere: Sie greifen sowohl Windows-PCs als auch Apple-Systeme mit Mac OS X an. Eine manipulierte Word-Datei führt je nach Betriebssystem, auf dem sie geöffnet wird, unterschiedlichen Code aus. Vorher muss das Opfer allerdings dazu verleitet werden, die Word-Sicherheitswarnung vor der Ausführung von Makros aus unbekannten Quellen zu deaktivieren. Spätestens bei einer solchen Aufforderung sollten Nutzerinnen und Nutzer skeptisch werden, das Dokument schließen und löschen. [LINK zum Artikel auf ZDNet] [TN]

6 WIRE – Eine sichere Alternative zu WhatsApp?

Neben den auf S. 5 genannten Alternativen zu WhatsApp, wie *Telegram*, *Threema* und *Hoccer* wird aktuell der Messenger-Dienst WIRE in verschiedenen Foren und Webseiten erneut vorgestellt, so u.a. in der Süddeutschen Zeitung, der Computerzeitschrift Chip, unter www.Datenschutzbeauftragter-info.de im DatenschutzTicker.

Kurzbeschreibung

Das hinter Wire stehende Unternehmen, die Wire Swiss GmbH, hat ihren Sitz in der Schweiz und betreibt die technische Entwicklung ihres Instant Messengers in Berlin. Die Server sollen nach Angaben des Unternehmens in Europa stehen. Eine erste Version von

Wire wurde am 3. Dezember 2014 für iOS, Android und OS X veröffentlicht. Mit den im August 2015 und März 2016 durchgeführten Updates sind mit jetzt auch Gruppentelefonate mit bis zu fünf Personen in Stereo-Qualität und Video-Telefonie möglich. Alle Kommunikationsinhalte auf Wire sind Ende-zu-Ende verschlüsselt. So wird bei Textnachrichten und Bildern Off-the-Record (OTR) verwendet. Der Messenger verwendet Axolotl-Ratchet und Pre-Keys, die für mobiles Messaging optimiert sind. Anrufe verwenden für den Schlüsselaustausch und die Authentifizierung DTLS sowie SRTP für die Transportverschlüsselung der Mediendaten. [Auszug aus Wikipedia: Wire (Messenger)].

Für die Computerzeitschrift „Chip" ist Wire „ein verschlüsselter Messenger, der plattformübergreifend arbeitet und mit einem modernen Design punktet." In seinem Fazit weist der Autor, Michael Humpa, zwar auch darauf hin, dass Wire „sicherlich keine Revolution auf dem Messenger-Markt" sei, hebt aber gleichzeitig auch hervor, dass „durch das ansprechende Design, den Standort der Server und die fast grenzenlose Kompatibilität zwischen diversen Geräten … Wire aber durchaus eine interessante Alternative zu Skype, WhatsApp und Co" seien. [LINK zum Beitrag in Chip]

In einem der nächsten Info-Briefe werden wir das Thema Messenger-Dienste noch einmal aufgreifen und die Alternativen zu WhatsApp vorstellen. [TN]

7 Betrüger kapern immer wieder Verkäufer-Konten auf Amazon

Fundort: https://www.sicher-im-netz.de/node/1823 (16.2.17)

Online Bestellungen gehen (zumeist jedenfalls) schnell, bieten eine breite Vielfalt unterschiedlichster Angebote, erfordern keine zusätzlichen Fahrzeiten und bieten sich damit nicht nur im privaten Bereich immer häufiger als Alternative zum Einkauf vor Ort an, sondern werden auch immer selbstverständlicher in Vereinen und Verbänden genutzt. Allerdings sind sie auch immer wieder Opfer von Pishing Attacken.

Wie www.sicher-im-netz.de berichtet, scheint nicht zuletzt AMAZON davon betroffen zu sein.

„Bereits seit einigen Jahren gibt es eine Betrugsmasche auf Amazon, bei der Betrüger gekaperte Verkäufer-Konten nutzen, um Käufer um ihr Geld zu bringen. Mit gut gemachten Phishing-Mails gelangen Betrüger dabei an die Zugangsdaten etablierter Amazon-Händler und stellen anschließend unzählige Lock-Angebote zu sehr guten Preisen ein.

Um von den sehr günstigen Preisen profitieren zu können, werden Kunden dazu aufgerufen, eine Zahlung abseits der Amazon-Plattform vorzunehmen. Kommt man dieser Forderung nach, landet das Geld direkt bei den Betrügern - die versprochene Ware gibt es nicht. Amazon übernimmt in solchen Fällen den Schaden nicht - der Käuferschutz gilt nur bei einer Zahlung über die Webseite.

SiBa rät bei verdächtig günstigen Angeboten zur Vorsicht, insbesondere wenn zu einer Zahlung außerhalb von Amazon aufgerufen wird: Melden Sie das Verkäufer-Konto in solch einem Fall zur Überprüfung bei Amazon. Stellen Sie Strafanzeige, wenn Sie bereits eine Zahlung abseits von Amazon geleistet haben." [LINK zum vollständigen Text mit weiteren Infos u.a. zu: Wie schütze ich mich? und Wer kann mir helfen?] [TN]

8 Telefonbetrugsmasche arbeitet mit Tonmitschnitten

Fundort: https://www.sicher-im-netz.de/node/1822 vom 16.2.17

„Bei unklaren Rechnungen für angeblich telefonisch getätigte Bestellungen sollte man noch einmal zu klären versuchen, ob es sich um eine tatsächlich erfolgte Bestellung handelt oder um einen Betrugsversuch.

Eine neue Art des Telefonbetrugs beginnt mit der harmlosen Frage "Können Sie mich hören?". Antwortet der Angerufene mit "Ja", wird diese Antwort aufgezeichnet und anschließend mit anderen Aufnahmen so zusammengeschnitten, dass der Eindruck erweckt wird, der Betroffene habe eine Bestellung aufgegeben.

Anschließend werden die Betroffenen unter Druck gesetzt: Die Betrüger fordern die Zahlung der in Rechnung gestellten Summe und drohen alternativ mit der Beauftragung eines Inkassobüros: Letzteres kann, trotz ungerechtfertigter Forderung, zu einer schlechteren Bonitätsbewertung des Opfers führen - die Korrektur ist oftmals langwierig und mühselig.

Neben "Hören Sie mich?" werden auch andere Fragen genutzt, um dem Betroffenen ein "Ja" zu entlocken - Betroffene sollten bei verdächtigen Anrufen sofort auflegen. Sollten Sie bereits Opfer des Betrugs sein, zahlen Sie keinesfalls die geforderte Summe - die Forderung hat keinerlei Rechtsgrundlage. Erstatten Sie stattdessen Anzeige mit Uhrzeit, Datum und Telefonnummer des Anrufs.“ [Link zum vollständigen Beitrag mit weiteren Infos zu: Wie schütze ich mich? und Wer kann mir helfen?] [TN]

GESETZGEBUNG

9 Entwurf zum Bundesdatenschutzgesetz verspielt Chance auf besseren Datenschutz! Pressemitteilung der unabhängigen Datenschutzbehörden der Länder vom 1.2.2017

Fundort: www.datenschutz.rlp.de

Am … Mittwoch [1.2.2017] hat das Bundeskabinett den Entwurf zu einem neuen Bundesdaten-schutzgesetz (BDSG) beschlossen, der jetzt in den Bundestag eingebracht werden soll. Anlass der Gesetzesnovelle ist das neue EU-Datenschutzrecht, bestehend aus der Datenschutz-Grundverordnung (DS-GVO) und der Datenschutz-Richtlinie im Bereich Justiz und Inneres. Die Mit-gliedstaaten haben bis Mai 2018 ihr nationales Datenschutzrecht an die Verordnung anzupassen und die Richtlinie in nationales Recht umzusetzen.

Nach Auffassung der unabhängigen Datenschutzbehörden der Länder wird der im Bundeskabinett beschlossene Gesetzentwurf den europarechtlichen Vorgaben nicht gerecht und stellt bereits be-stehende datenschutzrechtliche Standards in Frage. So schränkt der Entwurf die Informations-, Auskunfts- und Löschrechte der betroffenen Personen erheblich ein. Diese Einschnitte in die Be-troffenenrechte stellen lediglich eine Arbeitserleichterung für die Daten verarbeitenden Stellen dar und stehen dem Schutzcharakter der Vorschriften zur Auskunft, Information und Löschung von Da-ten diametral entgegen. Die DS-GVO gestattet dem nationalen Gesetzgeber nur in sehr engem Rahmen weitere Einschränkungen der Betroffenenrechte vorzusehen. Entsprechend der Intention der DS-GVO haben die Verantwortlichen vielmehr primär durch geeignete technische und organisa-torische Maßnahmen dafür Sorge zu tragen, ihren Informations-, Auskunfts- und Löschpflichten zu genügen. Der nationale Gesetzgeber sollte auf eine weiter gehende Beschneidung der Betroffenen-rechte verzichten.

Der Entwurf beschränkt zudem die Aufsichtsbefugnisse der Datenschutzbehörden gegenüber Be-rufsgeheimnisträgern dahingehend, dass sie ihnen und ihren Auftragsverarbeitern gegenüber nur ausgeübt werden dürfen, soweit hierdurch keine Berufsgeheimnisse verletzt werden. Gerade im Bereich der Tätigkeit von Berufsgeheimnisträgern werden häufig besonders schützenswerte Daten, wie z.B. Gesundheitsdaten, verarbeitet. Eine gesonderte Regelung für Beschränkungen der Aufsicht bei Berufsgeheimnisträgern ist weder notwendig noch verhältnismäßig, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen. Der Ge-setzgeber sollte hier keine derart undifferenzierte Regelung treffen.

Darüber hinaus sieht der Gesetzentwurf zur Verarbeitung von Gesundheitsdaten sehr weitgehende Regelungen ohne Interessenabwägung vor. Er schafft damit zu allgemeine gesetzliche Verarbei-tungsbefugnisse sowohl für nicht-öffentliche als auch öffentliche Stellen. Es werden zudem keine verbindlichen technisch-organisatorischen Schutzmaßnahmen geregelt. Dies kann zu Lücken im gebotenen Grundrechtsschutz führen.

Daten dürfen nur zu einem oder mehreren vorab festgelegten Zwecken verarbeitet werden. Die auch hier bestehende Möglichkeit für den nationalen Gesetzgeber, in engem Rahmen konkrete Normen zur Zweckänderung zu schaffen, ist als Ausnahmetatbestand restriktiv auszulegen. Die detaillierten nationalen Regelungen des Gesetzentwurfs überdehnen ihn aber über alle Maßen, höhlen damit die Zweckbindung weiter aus und konter-

karieren überdies das Ziel der Vereinheitlichung des europäischen Rechts. Diese Aushöhlung des Grundsatzes der Zweckbindung darf nicht Geset-zeskraft erlangen.

Wiederholt haben die Datenschutzbeauftragten des Bundes und der Länder ein umfassendes Gesetz zum Beschäftigtendatenschutz gefordert. Der Gesetzentwurf sieht demgegenüber lediglich einige klarstellende Regelungen für den Beschäftigtendatenschutz vor. Stattdessen bedarf es aber detaillierter bereichsspezifischer Regelungen auf Grundlage der DSGVO.

Auch im Entwurf zum neuen BDSG findet sich die ausgeweitete Regelung zur Videoüberwachung durch Private, wie sie bereits mit dem „Videoüberwachungsverbesserungsgesetz" eingefügt werden soll. Diesbezüglich wird auf die Entschließung der DSK vom 09.11.2016 verwiesen.

Schließlich kritisieren die Datenschutzbehörden der Länder, dass die Bundesbeauftragte für den Datenschutz als alleinige Vertreterin für alle deutschen Datenschutzbehörden im Europäischen Da-tenschutzausschuss (EDSA) vorgesehen ist. Stattdessen fordern die Landesdatenschutzbehörden eine Vertretungsregelung, die nicht nur der Unabhängigkeit aller Aufsichtsbehörden, sondern auch den tatsächlichen Vollzugszuständigkeiten Rechnung trägt, die vorwiegend bei den Ländern liegen. Dem EDSA kommt zukünftig eine zentrale Bedeutung zu, kann dieser doch Beschlüsse treffen, die für alle Aufsichtsbehörden verbindlich sind.

Der vom Kabinett verabschiedete Entwurf ist nach alledem trotz einiger Verbesserungen im Ver-gleich zu Vorentwürfen an einigen Stellen europarechtlich zweifelhaft und enthält eine Reihe von datenschutzrechtlichen Rückschritten.

AKTUELLE URTEILE

10 BVwefG erhöht den Persönlichkeitsschutz bei Darstellung von Personen in räumlich privat geprägten Situationen

Persönlichkeitsschutz bei Darstellung von Personen in räumlich privat geprägten Situationen erhöht

Quelle: *Bundesverfassungsgericht, Beschluss vom 09.02.2017; AZ: 1 BvR 2897/14, 1 BvR 790/15 und 1 BvR 967/15*
Fundort: www. kostenlose-urteile.de (ra-online GmbH), Berlin *15.03.2017*; Dok.--Nr.: *23984*

Das Bundesverfassungsgericht hat entschieden, dass die Zivilgerichte im Rahmen der vorzunehmenden Abwägung das Gewicht der Pressefreiheit bei der Berichterstattung über Ereignisse, die von großem öffentlichen Interesse sind, ausreichend berücksichtigen müssen. Von Bedeutung ist dabei unter anderem, ob sich die abgebildete Person im öffentlichen Raum bewegt. Betrifft die visuelle Darstellung die Privatsphäre oder eine durch räumliche Privatheit geprägte Situation, ist das Gewicht der Belange des Persönlichkeitsschutzes erhöht.

Dem Fall lag folgender Sachverhalt zugrunde: Gegen den Kläger der Ausgangsverfahren wurde ein Strafverfahren wegen des Verdachts der Vergewaltigung geführt, in dessen Vorfeld er auch in Untersuchungshaft saß. Das Verfahren endete mit einem Freispruch.

Sachverhalt im Verfahren 1 BvR 967/15

Die Beschwerdeführerin und Beklagte des Ausgangsverfahrens im Verfahren 1 BvR 967/15 begleitete den Strafprozess mit einer umfangreichen Berichterstattung. Sie illustrierte die Wortberichterstattung unter anderem mit einem Lichtbild des Klägers, das ihn wenige Meter vom Eingang der Kanzlei seiner Verteidigerin entfernt auf dem Gehweg zeigt. Der Kläger machte letztinstanzlich erfolgreich die Unterlassung der Bildberichterstattung geltend. Hiergegen wandte sich die Beschwerdeführerin mit ihrer Verfassungsbeschwerde. Sie rügte im Wesentlichen die Verletzung ihrer Pressefreiheit. …

Pressefreiheit ermöglicht freie Bestimmung der Art und Ausrichtung sowie Inhalt und Form des Publikationsorgans

Das Bundesverfassungsgericht erklärte die Verfassungsbeschwerde im Verfahren 1 BvR 967/15 für begründet. Im Zentrum der grundrechtlichen Gewährleistung der Pressefreiheit steht das Recht, Art und Ausrichtung sowie Inhalt und Form des Publikationsorgans frei zu bestimmen. Die Vorschriften über die Veröffentlichung fotografischer Abbildungen von Personen enthalten ein abgestuftes Schutzkonzept, das sowohl dem Schutzbedürfnis der abgebildeten Person wie den von den Medien wahrgenommenen Informationsinteressen der Allgemeinheit Rechnung trägt. Für die Gewichtung der Belange des Persönlichkeitsschutzes wird neben den Umständen der Gewinnung der Abbildung auch bedeutsam, in welcher Situation der Betroffene erfasst und wie er dargestellt wird. …

Diesen verfassungsrechtlichen Anforderungen genügen die angegriffenen Entscheidungen nicht; sie verletzen die Beschwerdeführerin in ihrer Pressefreiheit. Die Gerichte berücksichtigen nicht ausreichend das Gewicht der Pressefreiheit aufgrund des großen öffentlichen Informationsinteresses. Der Kläger durfte nicht die berechtigte Erwartung haben, nicht in den Medien abgebildet zu werden, etwa weil er in Begleitung seiner Verteidigerin

abgebildet wurde. Auch hat er sich nicht in einer durch räumliche Privatheit geprägten Situation befunden, sondern in einem öffentlichen Bereich, in dem er aufgrund der Gesamtumstände damit rechnen musste, dass er dort wahrgenommen wird.

Persönlichkeitsrecht in räumlich privat geprägten Situationen erhöht

In den Verfahren 1 BvR 2897/14 und 1 BvR 790/15 erklärte das Bundesverfassungsgericht die Verfassungsbeschwerden für unbegründet. Die den Entscheidungen zugrundeliegende Abwägung ist mit den verfassungsrechtlichen Anforderungen vereinbar. Das Gewicht der mit der Abbildung verbundenen Beeinträchtigungen des Persönlichkeitsrechts ist erhöht, weil sich der Abgebildete in einer durch räumliche Privatheit geprägten Situation in einem vom öffentlichen Raum nur eingeschränkt einsehbaren Innenhof befand. In dieser Situation, in der sich der Abgebildete im Vorfeld des Prozesses auf privates Gelände zurückgezogen hatte, durfte er die berechtigte Erwartung haben, nicht in den Medien abgebildet zu werden. [LINK zum kompletten Beitrag]

11 Transportunternehmen sind zur Datenübermittlung von Lenk- und Ruhezeiten von LKWs verpflichtet

Aufsichtsbehörden dürfen Übermittlung von Unterlagen zur Gewährleistung der Verkehrssicherheit verlangen

Quelle: *Verwaltungsgericht Mainz, Urteil vom 08.03.2017 ; AZ: 3 K 621/16.MZ*
Fundort: www. kostenlose-urteile.de (ra-online GmbH), Berlin *24.03.2017*; Dok.--Nr.: *24029*

Das Verwaltungsgericht Mainz hat entschieden, dass Transport-unternehmen grundsätzlich verpflichtet sind, zur Überprüfung der Einhaltung von straßenverkehrsrechtlichen Vorschriften auf Aufforderung der zuständigen Aufsichtsbehörde Daten aus dem Massenspeicher des Kontrollgeräts eines LKWs vorzulegen.

Dem Fall lag folgender Sachverhalt zugrunde: Anlässlich einer polizeilichen Kontrolle wurden bei einem Fahrzeug des klagenden Transportunternehmens mehrere Verstöße gegen die gesetzlichen Lenk- und Ruhezeiten festgestellt. Gegen den Unternehmensinhaber erging ein Bußgeldbescheid in Höhe von 300 Euro. Die zuständige Behörde forderte daraufhin von dem Unternehmen die Vorlage der Daten aus dem Massenspeicher des digitalen EG-Kontrollgeräts im betreffenden Fahrzeug für einen zurückliegenden Zeitraum von vier Monaten und verwies darauf, dass mit Blick auf die der Allgemeinheit drohenden Gefährdungen und Schäden durch übermüdetes und überarbeitetes Fahrpersonal die Beachtung der im Straßenverkehr geltenden Rechtsvorschriften zu überprüfen sei. Der Kläger wandte sich nach erfolglosem Widerspruchsverfahren gerichtlich gegen die behördliche Anordnung und machte geltend, dass das seinerzeitige Fehlverhalten in einem Zusammenhang mit einer besonderen betrieblichen Situation zu sehen sei. [LINK zum kompletten Beitrag]

Führungs-Akademie
des Deutschen Olympischen Sportbundes
Willy-Brandt-Platz 2
50679 Köln

Tel. 0221/221 220 13
Fax: 0221/221 220 14
info@fuehrungs-akademie.de
www.fuehrungs-akademie.de