DOSB FÜHRUNGS AKADEMIE

FA Datenschutzportal

DSP Info-Brief

Nr. 43 / Februar 2017

INHALT

DATENSCHUTZPORTAL INTERN

IN DER DISKUSSION – AKTUELLES 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 / Dirk-Michael Mülot

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

DATENSCHUTZPORTAL INTERN

1 Die Themen und Inhalte des Live-Chats vom 24. Februar

1 Die Verankerung des Datenschutzes in der Satzung
Frage nach Tipps zur optimalen Gestaltung- Was muss / sollte in die Satzung, was kann ‚anderweitig' geregelt werden?

Die Datenschutzerklärung im Rahmen unserer Vereinssatzung wird im Verhältnis zu den anderen Paragraphen recht umfangreich, auch deshalb, da wir mit ca. 20 Sparten viele Stellen auflisten müssen, an die Daten weitergegeben werden: "Als Mitglied des ... (Landessportverband und sonstige Verbände mit Adresse einsetzen) ist der Verein verpflichtet, seine Mitglieder an den Verband zu melden ...". Bei jeder Änderung wäre dann auch eine Satzungsänderung notwendig.

Neben der Satzung haben wir auch eine Geschäfts- und Finanzordnung, die von der Delegiertenversammlung genehmigt wird. Besteht die Möglichkeit in der Satzung eine kürzere Datenschutzerklärung aufzunehmen, die für Details auf die Geschäfts- und Finanzordnung verweist?

AW 1:
Sie könnten die Datenschutzerklärung in einer gesonderten Datenschutzpolicy aufnehmen und in der Satzung dann auf die jeweils gültige Datenschutzerklärung verweisen. In der Satzung machen Sie dann nur allgemeine Ausführungen. Alle Details auch zu den Sparten können Sie dann in einer "Datenschutzpolicy" festhalten, die dann mitgeltend ist. Im Vorfeld der Mitgliederversammlung sollten Sie den Vorschlag noch einmal juristsch prüfen lassen. Im Portal finden Sie im Bereich Dokumente im Ordner „Datenschutz im Verein" eine – allerdings eher ausführliche – Mustervorlage [MV_Datenschutz in der Vereinssatzung]. [RG]

AW 2:
Zur weiteren Information und Anpassung der eigenen Satzung an allgemeine Vorlagen bieten auch die Landessportbünde Mustersatzungen mit entsprechenden Ausführungen zum Thema Datenschutz an, die man zur Orientierung zu Rate ziehen kann. Als Beispiele sei an dieser Stelle auf die Vorlagen von zwei Landessportbünden verwiesen:

Der Bayerische Landes-Sportverband bietet Mustervorlagen sowohl für kleinere Vereine als auch für größere Mehrspartenvereine an [LINK zu den Mustervorlagen). Ein zweites Beispiel ist die Mustervorlage, die auf der VIBSS-Seite des LSB Nordrhein-Westfalen veröffentlicht ist [LINK zur Mustervorlage des VIBSS. [TN]

> *PS: Die Frage wurde mit der Bitte um Tipps zur Vorgehensweise dem User-Forum entnommen, wurde dort aber bisher nicht von anderen Mitgliedern des Portals aufgenommen.*
>
> *Tipps zur Verankerung des Datenschutzes in der Satzung können Sie gerne weiterhin dort einstellen. [TN]*

2 Umgang mit besonders schützenswerten Daten, hier Daten im Rahmen von Reha-Maßnahmen

Reicht eine unterschriebene Erklärung zum Datenschutz im Rahmen des Aufnahmeantrags auch noch aus wenn das Mitglied im Zuge der Mitgliedschaft an einem Reha Kurs im Verein teilnimmt? Die Reha Daten werden nur in Papierform gespeichert bzw.. verarbeitet. Die Abrechnungsdaten werden über die vereinseigene EDV bearbeitet.

AW:
Je nach Sportart und Disziplin sind in den Vereinen und Verbänden häufig medizinische Daten vorhanden, die u.a.. in Form von Leistungs- oder Gesundheitsdaten z.B. als Zugangsvoraussetzung zur Teilnahme an bestimmten Wettkämpfen etc. verarbeitet werden. Sollten auf diese Datenarten keine expliziten Verweise vorhanden sein, müssen die mit Hinweis auf die Konsequenzen einer Nichteinwilligung und Widerspruchsmöglichkeiten sowie Freiwilligkeit ergänzt werden.

Mit Sicht auf die kommende EU Datenschutzgrundverordnung ist es zu empfehlen alle vorhandenen Einwilligungen zu überprüfen, inwieweit die Erklärungen noch detailliert genug sind und alle Datenarten erfasst werden.

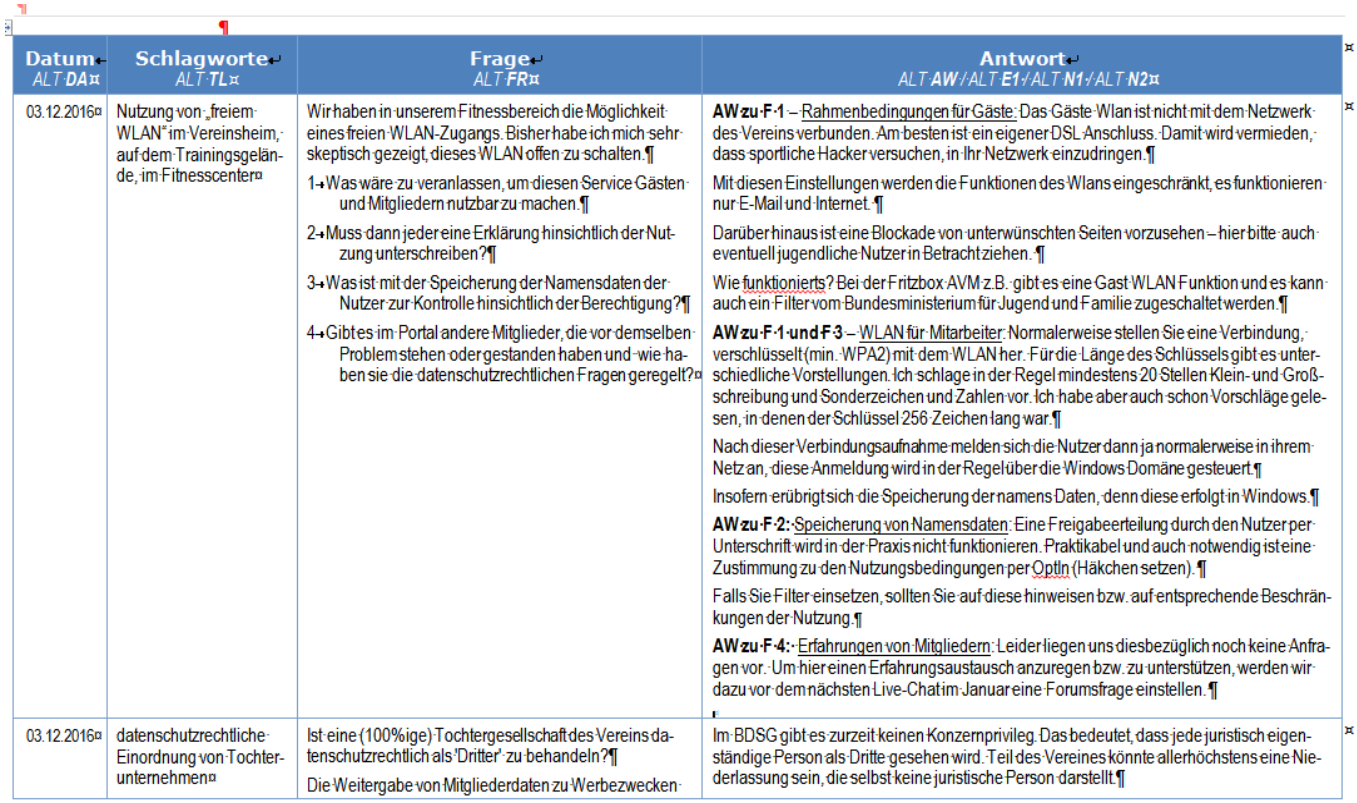
2 Live-Chat Archiv: März 2013 – Dezember 2016
Aktualisierte Übersicht mit allen Fragen und Antworten in einer Datei zusammengefasst

Der seit Anfang 2013 angebotene Service des monatlichen Live Chats ermöglicht eine individuelle und direkte Unterstützung bei konkreten Fragen, Aufgaben und Problemen aus dem eigenen Verein bzw. Verband.

Er ist gleichzeitig für alle Abonnent(inn)en eine zusätzlich nutzbare Quelle zur Lösung von Problemen. Darüber hinaus bieten die Live-Chats die Möglichkeit, Kontakt zu anderen Nutzer(inne)n aufzunehmen, die sich bereits mit einem vergleichbaren Problem auseinandergesetzt haben.

Da die Suche in einer einzigen Excelliste gegenüber der Suche im Portal (noch) weniger aufwendig ist und sich Mehrfachtreffer schnell in einer neuen Datei zusammenfassen lassen, haben wir 2016 damit begonnen, eine regelmäßig aktualisierte Übersicht mit allen Fragen und Antwortender Live-Chats in einer Datei zusammenzufassen.

Die Datei haben wir jetzt wieder auf den neuesten Stand gebracht und ins Portal gestellt. Gleichzeitig übermitteln wir Ihnen die Datei als Anlage, sodass Sie auch offline jederzeit Zugriff auf die Datei haben.



Datum ALT DA	Schlagworte ALT TL	Frage ALT FR	Antwort ALT AW / ALT E1 / ALT N1 / ALT N2
03.12.2016	Nutzung von „freiem WLAN" im Vereinsheim, auf dem Trainingsgelände, im Fitnesscenter	Wir haben in unserem Fitnessbereich die Möglichkeit eines freien WLAN-Zugangs. Bisher habe ich mich sehr skeptisch gezeigt, dieses WLAN offen zu schalten. 1→Was wäre zu veranlassen, um diesen Service Gästen und Mitgliedern nutzbar zu machen. 2→Muss dann jeder eine Erklärung hinsichtlich der Nutzung unterschreiben? 3→Was ist mit der Speicherung der Namensdaten der Nutzer zur Kontrolle hinsichtlich der Berechtigung? 4→Gibt es im Portal andere Mitglieder, die vor demselben Problem stehen oder gestanden haben und wie haben sie die datenschutzrechtlichen Fragen geregelt?	**AW zu F 1** – Rahmenbedingungen für Gäste: Das Gäste Wlan ist nicht mit dem Netzwerk des Vereins verbunden. Am besten ist ein eigener DSL Anschluss. Damit wird vermieden, dass sportliche Hacker versuchen, in Ihr Netzwerk einzudringen. Mit diesen Einstellungen werden die Funktionen des Wlans eingeschränkt, es funktionieren nur E-Mail und Internet. Darüber hinaus ist eine Blockade von unterwünschten Seiten vorzusehen – hier bitte auch eventuell jugendliche Nutzer in Betracht ziehen. Wie funktionierts? Bei der Fritzbox AVM z.B. gibt es eine Gast WLAN Funktion und es kann auch ein Filter vom Bundesministerium für Jugend und Familie zugeschaltet werden. **AW zu F 1 und F 3** – WLAN für Mitarbeiter: Normalerweise stellen Sie eine Verbindung, verschlüsselt (min. WPA2) mit dem WLAN her. Für die Länge des Schlüssels gibt es unterschiedliche Vorstellungen. Ich schlage in der Regel mindestens 20 Stellen Klein- und Großschreibung und Sonderzeichen und Zahlen vor. Ich habe aber auch schon Vorschläge gelesen, in denen der Schlüssel 256 Zeichen lang war. Nach dieser Verbindungsaufnahme melden sich die Nutzer dann ja normalerweise in ihrem Netz an, diese Anmeldung wird in der Regel über die Windows Domäne gesteuert. Insofern erübrigt sich die Speicherung der namens Daten, denn diese erfolgt in Windows. **AW zu F 2:** Speicherung von Namensdaten: Eine Freigabeerteilung durch den Nutzer per Unterschrift wird in der Praxis nicht funktionieren. Praktikabel und auch notwendig ist eine Zustimmung zu den Nutzungsbedingungen per OptIn (Häkchen setzen). Falls Sie Filter einsetzen, sollten Sie auf diese hinweisen bzw. auf entsprechende Beschränkungen der Nutzung. **AW zu F 4:** Erfahrungen von Mitgliedern: Leider liegen uns diesbezüglich noch keine Anfragen vor. Um hier einen Erfahrungsaustausch anzuregen bzw. zu unterstützen, werden wir dazu vor dem nächsten Live-Chat im Januar eine Forumsfrage einstellen.
03.12.2016	datenschutzrechtliche Einordnung von Tochterunternehmen	Ist eine (100%ige) Tochtergesellschaft des Vereins datenschutzrechtlich als 'Dritter' zu behandeln? Die Weitergabe von Mitgliederdaten zu Werbezwecken	Im BDSG gibt es zurzeit keinen Konzernprivileg. Das bedeutet, dass jede juristisch eigenständige Person als Dritte gesehen wird. Teil des Vereines könnte allerhöchstens eine Niederlassung sein, die selbst keine juristische Person darstellt.

IN DER DISKUSSION – NEUIGKEITEN RUND UM DEN DATENSCHUTZ

3 Die EU-Anti-Terror-Verordnungen

Ein Blick ins Netz zu den Anforderungen und Konsequenzen

Problemaufriss

Mit der zunehmenden Terrorgefahr, den Forderungen nach strikter Umsetzung bestehender gesetzlicher Regelungen und den Diskussionen um eine weitere Verschärfung von Gesetzen zum Schutz vor terroristischen Gewalttaten ist auch ein Thema wieder in den Blick geraten, das zwar nicht neu ist, bisher aber möglicherweise wenig beachtet wurde – die Umsetzung der EU-Anti-Terror Verordnungen aus den Jahren 2001 und 2002. Ziel der Verordnungen war und ist es, jegliche finanzielle und wirtschaftliche Unterstützung von Terroristen oder Terrorgruppen sowohl direkt als auch indirekt auszuschließen.

Auch 15 Jahre nach Verkündung der Verordnungen gibt es nach wie vor zahlreiche Unsicherheiten darüber,

- **wer** die Verordnungen anzuwenden hat [nur (Rüstungs-)Firmen, nur international agierende Firmen oder generell alle Firmen (und damit auch alle Vereine u. Verbände)
- **welche Bereiche** bzw. Aktivitäten davon betroffen sind
  - nur Warenlieferungen (nur bestimmte / internationale Warenlieferungen) oder auch alle Mitarbeiter / oder zusätzlich alle Vereinsmitglieder
- wie die Überprüfung zu erfolgen hat (mit welcher Methode, in welchem Umfang, in welcher Häufigkeit)

Da die Frage nach der Bedeutung und Umsetzung im Sport im Live-Chat des Datenschutzportals angesprochen wurde, greifen wir das Thema auch im Info-Brief des Portals auf.

Der Text versteht sich ausdrücklich nicht als fertige Handlungsanleitung oder gar als Form einer Rechtsberatung, sondern als Diskussions- und Arbeitspapier, das die zentralen Punkte der Verordnungen unter Berücksichtigung von im Netz veröffentlichter Positionen zur Anwendung vorstellt.

Explizit erwünscht sind ergänzende Kommentare und Stellungnahmen, gerne auch zur Praxis im eigenen Verein / Verband oder – so Sie diese eingeholt haben – von Rechtsanwälten oder Landesdatenschutzbehörden. Für Ihre Kommentare und Diskussionsbeiträge wird im Portal ein eigenes Diskussionsforum eingerichtet werden; sie können Ihren Beitrag aber auch an die E-Mail Adresse ds-communicator@fuehrungs-akademie senden. Dass alle Rückmeldungen vertraulich behandelt werden und im geschützten Bereich des Portals bleiben, ist natürlich selbstverständlich!

Hintergrund

Im Zentrum der Verordnungen zur Terror-Abwehr stehen zwei, 2001 und 2002 verabschiedeten Verordnungen, die VO (EG) Nr. 2580/2001 und die VO (EG) Nr. 881/2002. Letztere ordnet an, „dass diejenigen Personen, Gruppen und Organisationen, die im Anhang der Verordnung aufgeführt sind, … mit bestimmten spezifischen restriktiven Maßnahmen belegt werden." Zu diesen Maßnahmen gehört vor allem ein umfassendes Verfü-

gungsverbot. Das bedeutet, dass Vermögen, Eigentum und wirtschaftliche Ressourcen dieser Personen, Gruppen und Organisationen eingefroren werden, ihnen Gelder weder direkt noch indirekt zur Verfügung gestellt werden oder zugute kommen dürfen und ihnen keine wirtschaftlichen Ressourcen zur Verfügung gestellt werden dürfen, wodurch sie Gelder, Waren oder Dienstleistungen erwerben könnten. Es ist also z.B. verboten, an sie Geld für Waren, Dienstleistungen, Gehälter, etc. zu zahlen, an sie Immobilien zu verkaufen oder gewerblich zu vermieten oder von ihnen Immobilien zu erwerben." [1]

Mit den Verordnungen soll das „Zurverfügungstellen" von Geld, Finanzmitteln und Finanzderivaten an Terroristen und deren Organisationen unterbunden werden. Martin M. Thorwesten (IHK Hannover) hat bereits 2005 auch unter Hinweis auf ergänzende Erläuterungen des Bundeswirtschaftsministerium und des Auswärtigen Amtes argumentiert, dass die Verordnungen nicht nur einige Warengruppen oder ausgewählte Länder beträfen, sondern „für alle Geschäfte" gelte. Ergänzend weist er darauf hin, dass sich die Verordnungen nicht auf die Beziehungen mit Drittländern beschränken ließen, sondern auch den Binnenmarkt und damit auch alle Inlandsgeschäfte beträfen.

> *„Das Bundeswirtschaftsministerium und das Auswärtige Amt sehen jede Warenlieferung als potenziell von der EG-Verordnung erfasst an. In diesem Sinne stellt das Merkblatt über Embargomaßnahmen zur Bekämpfung des Terrorismus des Bundesamtes für Wirtschaft und Ausfuhrkontrolle (BAFA) fest: Weder direkt noch indirekt dürfen Terroristen und Terrorgruppen Geld und wirtschaftliche Ressourcen zur Verfügung gestellt werden. Wirtschaftliche Ressourcen sind Vermögenswerte jeder Art, so dass die Verordnung auch die direkte oder indirekte Lieferung von Gütern verbietet."* [2]

Umsetzung der EU Anti-Terror Verordnungen

In Folge der Anti-Terror Verordnungen werden in Unternehmen[3] regelmäßige Screenings zum Abgleich sowohl von Kunden als auch von Mitarbeitern durchgeführt, wobei Umfang, Methode und Häufigkeit differieren.[4]

Von Datenschützern als besonders problematisch wird dabei das Screening von Mitarbeitern eingeschätzt. So haben sich die im Düsseldorfer Kreis[5] zusammengeschlossen Landesdatenschutzbeauftragten mehrfach gegen anlasslose Screenings von Mitarbeitern ausgesprochen, weil es dazu einer „speziellen Rechtsgrundlage" bedürfe, die nach wie

---

1 Justizportal des Bundes und der Länder: Ermittlung von Personen, Gruppen und Organisationen, für die aufgrund einer Sanktion ein umfassendes Verfügungsverbot besteht; Stand 27.01.2017)

2 IHK Hannover: M. Thorwesten: Terrorismusbekämpfung betrifft Unternehmen, 15.07.2005 [LINK]

3 Informationen oder Schätzungen, wie hoch der Anteil an Unternehmen ist, die die Vorschriften der Verordnungen anwenden, konnten nicht ermittelt werden, ein Blick in die Referenzlisten von Softwareanbietern, die automatisierte Screenings anbieten, macht aber zumindest deutlich, dass sich die Anwendung nur auf global agierende Großunternehmen handelt.

4 Vgl. z.B. „Deutschland verstößt gegen Anti-Terror-Verordnung" ARD Tagesschau v. 15.9.2016; ebenso: Focus v. 15.09.2016; F. Wisdorff: Diese Unternehmen durchleuchten ihre Mitarbeiter. In: Die Welt v. 28.01.2015

5 Der Düsseldorfer Kreis wurde 2013 als Gremium in der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder gebildet und dient der Kommunikation, Kooperation und Koordinierung der Aufsichtsbehörden im nicht-öffentlichen Bereich. [LINK]

vor fehle.[6] Bestätigt sehen sich die Landesdatenschutzbeauftragten in ihrer Ablehnung des anlasslosen Mitarbeiterscreenings durch eine Erklärung der Bundesregierung aus dem Jahre 2010:

> *„Auch die Bundesregierung ist der Auffassung, dass die Terrorismusverordnungen keinen systematischen, anlassunabhängigen Abgleich von Mitarbeiterdateien mit den Sanktionslisten verlangen. Allenfalls nach Maßgabe von Sorgfaltspflichten und differenzierend nach verschiedenen Verkehrskreisen und Risikolagen seien solche Abgleiche zulässig. Es bleibe den Unternehmen überlassen, wie sie die Einhaltung der Terrorismusverordnungen sicherstellen." (Bundestags-Drucksache 17/4136 vom 03.12.2010)*

Inwieweit diese Stellungnahme im Ernstfall vor einem Gericht Bestand hat und vor einer Verurteilung schützen kann, ist unklar. Im Telefonat weist Peter Meier, Ansprechpartner beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) ausdrücklich darauf hin, das aus Sicht des BayLDA entsprechende Kontrollen nach dem BDSG möglich sind und dass die Verantwortung für die Umsetzung der rechtlichen Vorgaben immer beim Unternehmen selbst liegen. Wer in dieser Frage das Risiko minimieren will, wird nicht umhin können, sich durch professionelle Rechtsberatung abzusichern. Immerhin drohen bei vorsätzlichen Verstößen „Freiheitsstrafen nicht unter zwei Jahren" und „Geldstrafen von bis zu 500.000 Euro, Umsatzabschöpfung, Verfall und Einziehung".[7]

Aufgaben und Rolle des Datenschutzbeauftragten

Zunächst sein noch einmal darauf hingewiesen, dass für die Einhaltung der gesetzlichen Regelungen und für die Entscheidung, ob, in welchem Umfang und auf welche Weise Überprüfungen im Rahmen der Terrorabwehr durchgeführt werden nicht der / die Datenschutzbeauftragte verantwortlich ist, sondern die verantwortliche Stelle.

Die Rolle des / der Datenschutzbeauftragen besteht allerdings nicht alleine in der Sicherstellung eines datenschutzrechtlich sauberen Verfahrens (Aufnahme ins Verfahrensverzeichnis / Umgang mit den gewonnenen Daten etc., sondern er habe, so eine Mitarbeiterin des LDI NRW, auch die Aufgabe, die Geschäftsführung proaktiv auf diese Verordnungen hinzuweisen.

Werden Kontrollen eingerichtet, hat der Datenschutzbeauftrage vor allem in zwei Bereichen eine Funktion: bei der Erfassung entsprechender Überprüfungen im Verfahrensverzeichnis und beim datenschutzkonformen Umgang mit den personenbezogenen Daten, die aufgrund von Überprüfungen erfasst und verarbeitet werden.

Wie kann eine Prüfung erfolgen?

Für die Überprüfung von verdächtigen Personen und Personengruppen bietet das Justizportal der Länder eine ständig aktualisierte Online-Suche an, die eine „Ermittlung von Personen, Gruppen und Organisationen" ermöglicht, „für die aufgrund einer Sanktion ein umfassendes

---

6 Vgl. hier auch die Argumentation einiger großer deutscher Konzerne, die ein eigenes Mitarbeiterscreening mit der Begründung unterlassen, dass Lohn- und Gehaltszahlungen über Banken abgewickelt werden, die ihrerseits verpflichtet seien, ihre Kunden mit den Anti-terror-Lisen abzugleichen.

7 EG-Anti-Terrorismus-Verordnungen und die Auswirkungen, in: Boorberg: www.Sicherheitsmelder.de

Verfügungsverbot besteht." Das Tool durchsucht dabei die umfassende von der EU erstellte Liste sanktionierter Personen und Organisationen, welche sämtliche Sanktions-Verordnungen der EU berücksichtigt." Ob diese ‚einfache' Recherche im Zweifelsfall von Untersuchungsbehörden als ausreichend zur Erfüllung der Vorgaben angesehen werden, ist unklar. Angemerkt wird jedenfalls, dass diese Liste nicht alle Sanktions-Verordnungen abdecke, „durch die entsprechende Verfügungsverbote … ausgesprochen werden". Auch hier ist somit in jedem Falle anzuraten, dies juristisch klären und ggf. absichern zu lassen.

Ausblick

Wir werden zu diesem Thema in den kommenden Wochen weiter recherchieren, um offene Fragen zu klären, divergierende Standpunkte zu dokumentieren, hoffen aber zugleich auch Ihre Kommentare und Anregungen. *[TN]*

4 Datentransfer zwischen der EU und den USA

Quelle: IITR, S. Kraska, Datenschutz-Newsletter v. 31.1.17

US-Präsident Trump hat eine "Executive Order" von Präsident Obama dahingehend verändert, dass US-Geheimdienste wieder in größerem Umfang auf Daten von Nicht-US-Bürgern zugreifen dürfen. Die "Executive Order" in ihrer ursprünglichen Fassung hatte eine zentrale Rolle in den Verhandlungen zwischen den USA und der EU bei der Verabschiedung des EU-US-Privacy-Shields gespielt. Die zuständige EU-Kommissarin Jourova hat Präsident Trump inzwischen um eine Bestätigung der seinerzeit mit Präsident Obama getroffenen Vereinbarungen gebeten. [Mehr auf techcrunch.com] [TN]

5 Was sind Daten? Was bedeutet „Information" – Video zur datenschutzrechtlichen Begriffsbestimmung

Quelle: IITR, S. Kraska, Datenschutz-Newsletter v. 30.12.2016

Die zentralen Begriffe im Datenschutz – „Daten" und „Information" – sind vielfach be- und umschrieben, trotzdem, so E. Kraska in seinem Datenschutz-Blog fehle immer noch eine einheitliche Definition. Um hier einen Schritt weiterzukommen hat Kraska ein erläuterndes Video mit einem Definitionsvorschlag veröffentlicht. [LINK zum Video]

MEDIEN –TECHNIK – SICHERHEIT

6 Datenschutzvorfälle – Infoseite mit Beispielen zu Datenschutzverstößen

Wir möchten Ihnen an dieser Stelle eine interessante Webseite empfehlen, die es sich zur Aufgabe gemacht hat, Fälle von Datenpannen und Datenmissbrauch zu dokumentieren: www.projekt-datenschutz.de

Auf dieser Webseite werden seit 2007 Datenschutzvorfälle gesammelt. Diese Datenschutz Vorfälle können sehr gut als Beispiel in der eigenen Organisation benutzt werden, um deutlich zu machen, wie sensibel das Thema Datenschutz ist.

Auf dieser Webseite finden Sie aus den verschiedenen Bundesländern, aus verschiedenen Branchen und Organisationen Information über bekannt gewordene Vorfälle bezüglich personenbezogener Daten. Sie finden dort eine Beschreibung des Vorfalles, gegebenenfalls den Umfang, eine Beschreibung und jeweilige Quelle.

Die Liste ist chronologisch sortiert, man kann aber über die Suche das ganze zum Beispiel auf Vereine eingrenzen.

Falls Sie also noch Argumentationshilfe für die Umsetzung des Datenschutzes in ihrer Organisation brauchen, ist diese Seite eine sehr nützliche Quelle. [RG]

7 Datenleck Windows 10

Auf immer mehr Rechnern findet sich inzwischen das aktuelle Betriebssystem von Microsoft „Windows 10". Microsoft hat zwei Jahre lang, etwas für dieses Unternehmen ungewöhnliches getan: es verschenkte das neue Betriebssystem an alle willigen Benutzer.

Dieses Vorgehen war verbunden, mit einem teilweise penetranten Hinweis, man solle das neue Betriebssystem jetzt bitte installieren. Das ging so weit, dass der Benutzer alleine durch die Nutzung der Windows Update Funktion, wenn er nicht aufpasste, ein Upgrade auf Windows 10 auslöste. Manche Benutzer luden sich Programme, die diese versteckte Upgrade-Funktion ausschalteten.

Natürlich stellte sich die Frage, warum Microsoft, den bisherigen Umsatzbringer Betriebssystem Windows, freiwillig verschenkte. Hierüber können nur Vermutungen angestellt werden, eine klare Aussage des Unternehmens hierzu fehlt.

Es ist nicht zu übersehen, dass Microsoft in den letzten Jahren auf dem Gebiet „Big Data", erheblich ins Hintertreffen gegenüber Google, Facebook, Apple und anderen gekommen ist. All diese Firmen sind auf dem Gebiet des Sammelns von Daten erheblich erfolgreicher als Microsoft. Schon die Suchmaschine Bing von Microsoft hat nur einen geringen Anteil an Suchanfragen gegenüber Google.

Eine Interpretation des Vorgehens von Microsoft beim Verschenken von Windows 10 ist, Microsoft will auf den Zukunftsmarkt „Big Data" auch eine gewichtige Rolle spielen. Mit

Windows 10 könnte dies Microsoft gelingen, denn Microsoft erhält über die verschiedenen Funktionen von Windows 10 erhebliche Mengen von Informationen und Daten der Benutzer. Im Bereich der PC Betriebssysteme war das in diesem Umfang bisher nicht bekannt.

Das Sammeln von Daten war bisher eine Kernstrategie von Firmen wie Google, Apple und Facebook etc., die über ihre Smartphones und Apps in verschiedenster Weise die Daten der Benutzer aufzeichnen, speichern und auswerten. Wie verschiedentlich schon zu lesen ist, ist das „Gold der 2000er Jahre", die Daten der Benutzer von Smartphones und Applikation.

Im Internet finden sich mehrere Artikel zu diesem Thema Windows 10 und dort wird teilweise schon von Windows 10, als dem „Spion in meinem PC" gesprochen.

Das beginnt schon damit, dass Microsoft den Benutzern vermittelt, dass Windows 10 nur sinnvoll mit einem Microsoft Account zu nutzen wäre. Ein Hinweis dass man Windows auch ohne einen solchen Account nutzen kann ist versteckt. Trotzdem bleibt die Bedingung, dass der Benutzer bei der Erstinstallation sich bei Microsoft anmelden muss, ein späteres Umstellen auf lokale Einstellung sollte dann durchgeführt werden. Hat man sich über einen Windows Account mit Microsoft verbunden, fällt es leicht, verschiedenste Informationen, die der Nutzer in Windows 10 erzeugt, an Microsoft zu übertragen.

Auch bei einer Umstellung auf lokale Nutzung, wird deutlich, dass Microsoft viele Dienste darauf ausgelegt hat, dass mit einem Microsoft Konto kommuniziert wird und im lokalen Modus dann einige Funktionen nicht nutzbar sind.

Wer die Übertragung von Daten an Microsoft so gering wie möglich halten will, sollte den lokalen Weg gehen. Bei Bedarf lässt sich jedoch auch ein Microsoft-Konto über die Einstellungen wieder in ein lokales Konto "umwandeln", indem man die Verbindung zum Microsoft-Konto trennt.

Wichtig: Übernehmen Sie bei der Installation von Windows 10 nicht die Standardeinstellungen für die Privatsphäre, sondern achten Sie darauf, sämtliche Schieberegler auf Aus zu stellen. So wird ein Großteil der Schnüffelfeatures gar nicht erst aktiviert.

Weitere Betriebssystem Funktionen wie Cortana speichern Vorlieben und hören mit. Hier unterscheidet sich übrigens Windows 10 nicht von Smartphones, bei denen die Spracheingabe genutzt wird. Neu ist jedoch, dass diese Funktion in dem verbreitetsten Betriebssystem der Welt Eingang gefunden hat.

Edge, der Nachfolger des Internet Explorers, sammelt Browser-Vorlieben. Microsoft Edge setzt stark auf Microsofts Suchmaschine Bing und Microsofts News-Plattform MSN. Diese Dienste tracken das Internet-Verhalten des Nutzers, darunter Standorte, den Suchverlauf und die Browser-Historie. Eingaben von URLs werden live an Microsoft übertragen, um pro-aktiv Websites vorzuschlagen. Der schon von Windows 8 bekannte SmartScreen-Phishing-Filter analysiert besuchte Websites und scannt heruntergeladene Dateien auf Schad-Software – die Daten werden dafür an Microsoft übermittelt. Und auch Cortana liefert Antworten, bevor eine Frage ausformuliert wurde.

Windows 10 sammelt Standort-Daten, scannt Webinhalte, auf die Apps zugreifen, per SmartScreen-Filter, erlaubt Apps die Identifikation durch eine Werbe-ID und sendet Informationen über das Schreibverhalten an Microsoft.

Wer sich mit einem Microsoft-Konto an sein Windows-10-System anmeldet, erhält automatisch Speicherplatz bei OneDrive - Microsofts Online-Festplatte. Das ist zwar bequem, doch unterliegen diese Microsofts Nutzungsbestimmungen. Das bedeutet, dass Microsoft sich unter anderem das Recht nimmt, ihre Foto-Dateien auf illegale Inhalte zu scannen.

In Windows 10 speichert der Explorer, welche Dateien zuletzt geöffnet wurden und welche Ordner der Nutzer häufig verwendet und blendet diese gut sichtbar auf jeder Explorer-Seite ein. Diese Daten werden nach derzeitigem Kenntnisstand zwar nicht an Microsoft übertragen, das Windows sie erhebt und so prominent anzeigt, dürfte trotzdem vielen Nutzern sauer aufstoßen.

Auch die Verbraucherzentrale Rheinland-Pfalz warnt in einer Pressemitteilung von einer „Überwachung bis zum letzten Klick" und nennt das Betriebssystem eine Art private Abhöranlage.

In Windows 10 speichert der Explorer, welche Dateien zuletzt geöffnet wurden und welche Ordner der Nutzer häufig verwendet und blendet diese gut sichtbar auf jeder Explorer-Seite ein. Diese Daten werden nach derzeitigem Kenntnisstand zwar nicht an Microsoft übertragen, das Windows sie erhebt und so prominent anzeigt, dürfte trotzdem vielen Nutzern sauer aufstoßen.

Es gibt zwar die Möglichkeit über die Einstellungen verschiedene Datenschutz Regeln zu modifizieren, nur dann stellt sich die Frage, welches die großen Vorteile von Windows 10 dann noch sind.

Auf eigene Gewähr: Es gibt inzwischen auch zu diesem Thema kleine Hilfsprogramme, die die verschiedenen Einstellungen beschreiben und gegebenenfalls abschalten möglich machen. Eines dieser Programme heißt „shutup10" der Firma O&O, Programm kann man ohne Installation aufrufen und sich wenigstens einen Eindruck darüber gewinnen über die vielfältigen Möglichkeiten Daten an Microsoft zu übertragen. Bitte beachten Sie, dass diese Empfehlung unter Ausschluss jeglicher Gewährleistung gegeben wurde.

Was bedeutet dies für den Datenschutzbeauftragten?

Da über PCs im Verein oder in den Verbänden in der Regel auch personenbezogene Daten verarbeitet werden, muss der Datenschutzbeauftragte prüfen, inwiefern es hier zu Übermittlung personenbezogener Daten in Drittländer (USA) kommt.

Es stellt sich hier sicherlich die Frage, auch mit Blick auf die Datenschutz Grundverordnung, inwiefern der Einsatz von Windows 10 in der nicht modifizierten Version möglich ist.

Natürlich sollte man sich auch in seinem privaten Umfeld Gedanken über eine solche Datenausspähung machen. [RG]

GESETZGEBUNG

8 Aktueller Fahrplan für das DSAnpUG-EU (Datenschutzanpassungs und Umsetzungsgesetz EU, inkl. BDSG-neu)

Quelle: **https://dsgvo.expert/aktueller-fahrplan-fuer-dsanpug-eu-inkl-bdsg-neu/**

Fundort: *Werner Hülsmann, vom 21.2.2017*

Der aktuelle Fahrplan des Gesetzgebungsverfahrens zur Verabschiedung des DSAnpUG-EU (inkl. des darin in Artikel 1 enthaltenen BDSG-neu) sieht nach dem Kabinettsbeschluss des Regierungsentwurfs vom 01.02.2017 wie folgt aus:

- Bundesrat – Ausschuss für Innere Angelegenheiten: 23.02.2017
- Bundesrat Plenum 1. Beratung: vsl. 10.03.2017
- Bundestag:
  - vsl. 09.03.2017: 1. Lesung (parallel zur Behandlung im Bundesrat wegen der Eilbedürftigkeit)
  - vsl. 26.04.2017: abschließende Behandlung im federführenden Innenausschuss
  - vsl. 27.04.2017: 2. und 3. Lesung (und damit Gesetzesbeschluss im Bundestag)
  - Bundesrat Plenum: vsl. 12.05.2017: 2. Beratung (als zustimmungspflichtig eingestuft)
  - Anschließend: Unterschrift durch den Bundespräsidenten und Verkündung im Bundesgesetzblatt

Wenn dieser Fahrplan eingehalten wird, wird das deutsche Umsetzungsgesetz zur DSGVO etwas mehr als ein Jahr vor dem Gültig-Werden verabschiedet. Die Übergangsfrist von der Veröffentlichung des Gesetzes im Bundesgesetzblatt bis zu dessen Inkrafttreten wird dann etwa ein Jahr sein.

9 Bundeskabinett beschließt Regierungsentwurf des BDSG-neu

Quelle: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2017/02/datenschutz-grundverordnung.html

Die Bundesregierung hat heute den vom Bundesminister des Innern vorgelegten Gesetzentwurf zur Anpassung des Bundesdatenschutzgesetzes an die EU-Datenschutz-Grundverordnung beschlossen. Mit dem Gesetzentwurf werden zugleich wichtige Teile der EU-Datenschutz-Richtlinie Polizei und Justiz umgesetzt.

Kernstück des Gesetzentwurfs ist die Neukonzeption des Bundesdatenschutzgesetzes. Es ergänzt künftig die unmittelbar geltende Datenschutz-Grundverordnung um die Bereiche, in denen den Mitgliedstaaten Gestaltungsspielräume verbleiben.

„Mit der Anpassung des Bundesdatenschutzgesetzes an die Datenschutz-Grundverordnung machen wir einen großen Schritt zur Angleichung der Datenschutzregelungen in Europa und damit zu einem harmonisierten digitalen Binnenmarkt. Frühzeitig und als erstes Land in Europa schaffen wir damit Rechtsklarheit. Das gibt allen Beteiligten genug Zeit, sich

auf die neue Rechtslage vorzubereiten. Durch die gleichzeitige Umsetzung wesentlicher Teile der Datenschutzrichtlinie im Bereich Polizei und Justiz schaffen wir ein stimmiges Regelungskonzept innerhalb des EU-Rechtsrahmens. Im Interesse der Betroffenen und im Interesse der Wirtschaft nutzen wir dabei die Spielräume der Datenschutz-Grundverordnung und schaffen damit zugleich Rechtssicherheit und einen angemessenen Ausgleich der Interessen.", so Bundesinnenminister Dr. Thomas de Maizière.

Darüber hinaus sieht der Gesetzentwurf Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes, des Sicherheitsüberprüfungsgesetzes und des Artikel-10-Gesetzes vor, die aus der Ablösung des bisherigen Bundesdatenschutzgesetzes resultieren.

Die am 27. April 2016 verabschiedete EU-Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) und EU-Datenschutz-Richtlinie im Bereich Polizei und Justiz (Richtlinie (EU) 2016/680) erfordern bis Mai 2018 eine Anpassung des deutschen Datenschutzrechts auf Bundes- und Länderebene.

Download des Gesetzentwurfes

Der Gesetzentwurf umfasst 83 Seiten und kann ab sofort von der Website des Bundesministeriums des Innern heruntergeladen werden. [LINK zum Download]

Hinweise / Kommentare

Die Diskussion um den Gesetzentwurf werden wir auch in den nachfolgenden Info-Briefen verfolgen und Sie darüber informieren. Nachfolgend ein erster Kommentar von Werner Hülsmann vom 21.2.2017 [https://datenschutzwissen.de/].

> *Leider erfüllt der Gesetzentwurf noch immer nicht in allen Teilen die Anforderungen der EU-Datenschutz-Grundverordnung (DSGVO) obwohl es Änderungen gegenüber der Fassung des Referentenentwurfs für die Länder- und Verbändeanhörung gab.*
>
> *Meine kurze Einschätzung zum Regierungsentwurf des neuen BDSG finden Sie als PDF-Datei hier bzw. unter diesem Kurzlink: https://dsgvo.expert/KEBDSGRegE .*
>
> *Dieser Entwurf wird – wie auch schon der Referentenentwurf, der in die Länder- und Verbändeanhörung ging – von DatenschützerInnen scharf kritisiert (vgl. u.a. die Pressemitteilung und die Stellungnahme der Deutschen Vereinigung für Datenschutz e.V.).*
>
> *Nun muss der Gesetzentwurf noch von Bundestag und Bundesrat behandelt werden. Ich gehe davon aus, dass es im weiteren Gesetzgebungsverfahren noch zu Änderungen am Text des Entwurfs kommen wird. Die Beschlussfassung im Bundesrat soll bereits für den 08. März 2017 – also in fünf Wochen – vorgesehen sein.*

10 EU-DSGVO: Artikel-29-Datenschutzgruppe legt Leitlinien zu den Begriffen *Datenübertragbarkeit*, *Datenschutzbeauftragter* und Zuständigkeit der federführenden Aufsichtsbehörde vor

Fundort: *IITR, S. Kraska, Datenschutz-Newsletter v. 16.12.16*

Die Artikel-29-Datenschutzgruppe (ein Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes) hat Leitlinien veröffentlicht, mit denen Details zur Auslegung der europäischen Datenschutz-Grundverordnung (gilt ab 25. Mai 2018) vorbereitend geklärt werden sollen. Aktuell werden die Themen Datenübertragbarkeit, Datenschutzbeauftragter und Zuständigkeit der federführenden Aufsichtsbehörde behandelt.

Die Leitlinien selbst sind rechtlich nicht verbindlich, bilden in der Praxis aber de facto eine gute Orientierung für Unternehmen und Aufsichtsbehörden.

Links zu den Dokumenten:

- Datenübertragbarkeit (Artikel 20 DSGVO): Leitlinien – FAQ
- Datenschutzbeauftragter (Artikel 37 DSGVO): Leitlinien – FAQ
- Zuständigkeit der federführenden Aufsichtsbehörde (Artikel 56 DSGVO): Leitlinien – FAQ

AKTUELLE URTEILE

11 Gefahr der Prangerwirkung: Bewertungsportal für Autofahrer muss aus Datenschutzgründen angepasst werden

Datenschutz bewerteter Fahrer überwiegt Informationsinteresse der Nutzer

Quelle: *Verwaltungsgericht Köln, Urteil vom 16.02.2017 [AZ: 13 K 6093/15]*
Fundort: www. kostenlose-urteile.de (ra-online GmbH), Berlin *27.02.17*; Dok.–Nr.: *23883*

Das Verwaltungsgericht Köln hat entschieden, dass die gegenüber der Betreiberin eines Fahrer-Bewertungsportals ergangene datenschutzrechtliche Anordnung – zur Verhinderung einer Prangerwirkung der bewerteten Fahrer – rechtmäßig ist.

Worum geht es?

Dem Verfahren lag folgender Sachverhalt zugrunde: Derzeit können Nutzer eines Fahrer-Bewertungsportals das Fahrverhalten anderer Personen unter Angabe eines Kfz-Kennzeichens nach einem Ampelschema (rot = negativ, gelb = neutral, grün = positiv) bewerten. Eine Detail-Bewertung erfolgt durch Auswahl aus vorgegebenen Bewertungen. Die Bewertungsergebnisse zu einzelnen Kfz-Kennzeichen sind in Form einer durchschnittlichen Schulnote für jeden Nutzer einsehbar. Die Klägerin beabsichtigt, mithilfe des Portals Autofahrer dazu anzuhalten, die eigene Fahrweise zu überdenken. Auf diese Weise möchte sie einen Beitrag zu mehr Sicherheit im Straßenverkehr leisten.

Datenschutzbeauftragter will durch neue Vorgaben Prangerwirkung des Portals verhindern

Der beklagte Datenschutzbeauftragte für das Land Nordrhein-Westfalen hat der Klägerin aufgegeben, das Portal so zu verändern, dass nur noch nach bestimmten Vorgaben registrierte Kfz-Halter die Bewertungsergebnisse zu ihrem eigenen Kfz-Kennzeichen abrufen können. Damit soll eine Prangerwirkung des Portals verhindert werden.

Derzeit steht bei Fahrerbewertungsportal Prangerwirkung einzelner Fahrer im Vordergrund

Das Verwaltungsgericht Köln wies die hiergegen erhobene Klage ab und führte zur Begründung aus, dass die auf dem Fahrerbewertungsportal zu einzelnen Kfz-Kennzeichen erhobenen und gespeicherten Daten personenbezogen seien. Die jeweiligen Fahrer bzw. Fahrzeughalter könnten von der Klägerin und auch Portalnutzern mit verhältnismäßigem Aufwand bestimmt werden. [LINK zum vollständigen Artikel]

12 Social-Media-Nutzung durch Arbeitgeber: Facebook-Auftritt nur mit Zustimmung des Betriebsrats vom Prof. Dr. Michael Fuhlrott

Quelle: Bundesarbeitsgericht (BAG), Urteil v. 13.12.2016, Az. 1 ABR 7/15

Fundort: LTU Legal Tribune Online [LINK zum Beitrag]

In der Dezemberausgabe des Info-Briefes (Info-Brief 41, S. 21) haben wir bereits über das Urteil berichtet. Wir möchten hier noch einmal das Thema aufgreifen und auf ein Interview mit Peter Wedde, Leiter des Instituts für Datenschutz, Arbeitsrecht und Technologieberatung (d+a consulting GbR) hinweisen. [LINK zum Interview]

13 Ausblick: Klarmachen zum Ändern? – Speicherung von IP-Adressen vor dem BGH

Quelle: DatenschutzbeauftragterInfo: Informationen zum Datenschutz v. 14.02.2017

Seit Jahren streitet der schleswig-holsteinische Abgeordnete der Piratenpartei Patrick Breyer dafür, dass seine IP-Adresse bei der Nutzung von Webseiten der Bundesministerien nicht gespeichert wird. Getreu seinem Motto „Klarmachen zum Ändern" möchte er Internetgeschichte schreiben und endlich anonym surfen. Heute begann die mit Spannung erwartete Fortsetzung des Rechtsstreits vor dem BGH. …

Bereits im Jahre 2007 erreichte Patrick Breyer einen ersten aufsehenerregenden Erfolg. Das Landgericht Berlin untersagte dem Bundesjustizministerium, die IP-Adresse des Abgeordneten bei der Nutzung des Internetportals des Justizministeriums zu speichern.

Der Abgeordnete Breyer setzte danach die Segel, um die Speicherung seiner IP-Adresse bei Nutzung aller Internetportale des Bundes zu unterbinden. Für Breyer geht es vor allem darum, dass das Surfverhalten von Internetnutzer Privatsache bleibt … [Link zum vollständigen 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