DOSB FÜHRUNGS AKADEMIE

FA Datenschutzportal

DSP Info-Brief

Nr. 49 / August 2017

INHALT

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 im Live-Chat vom 28.08.2017

1.1 Weitergabe von Spielberichtsdaten an einen ehrenamtlich im Verband engagierten Funktionsträger

Zur statistischen Auswertung von Spielberichtsdaten hat ein ehrenamtlicher Funktionsträger des Verbandes darum gebeten, ihm die Spielpläne ausgewählter Saisons zu überlassen.

Auf den Spielbericht sind neben den Informationen zum Spiel (beteiligte Mannschaften; Ort, Zeit etc.) auch personenbezogene Daten der Spieler festgehalten (Vorname, Name, Geburtsdatum, Passnummer sowie weitere Hinweise wie gelbe / rote Karten)

F1:Unter welchen Bedingungen darf der Verein dem interessierten Funktionsträger die gewünschten Spielberichte überlassen?

F2: Gibt es überhaupt Einschränkungen, da die dort festgehaltenen Daten (wer gespielt hat, wer eine gelbe oder rote Karte bekommen hat) sowieso in der Öffentlichkeit stattgefunden haben oder müssen datenschutzrechtliche Vorkehrungen getroffen werden?

F3: Müssen z.B. die personenbezogenen Daten, wie Name, Vorname, Geb.-Datum, Pass-Nr., vor der Weitergabe geschwärzt werden.

AW R. Graf
Ich gehe davon aus, dass der ehrenamtliche Funktionsträger wie ein Mitarbeiter zu behandeln ist. Das gilt im Übrigen ganz allgemein für ehrenamtliche Mitarbeiter.

Damit würde es zu einer Verarbeitung personenbezogener Daten durch einen Mitarbeiter kommen, der aufgrund der Daten eine Statistik erstellt. Auch andere Mitarbeiter innerhalb des Verbandes arbeiten mit personenbezogenen Daten zur Erfüllung der Geschäftszwecke.

Eine Notwendigkeit der Anonymisierung oder Pseudonymisierung ergibt sich aus heutiger Sicht nicht zwingend.

ACHTUNG: Mit der EU Datenschutz-Grundverordnung, die ab Mai 2018 zur Anwendung kommt, ändert sich die Regelung: Mit der EU-DSGVO gibt es die Verpflichtung für Organisationen, wenn möglich frühzeitig eine Pseudonymisierung vorzunehmen. Daher wäre es aus meiner Sicht ratsam, die personenbezogenen Daten durch den Archivar schon jetzt zu schwärzen.

1.2 Weitergabe von Mitarbeiterdaten an einen Ombudsmann

Handelt es sich bei der Weitergabe von Mitarbeiterdaten an einen externen Ombudsmann um Auftragsdatenverarbeitung? Oder können die Daten so zur Verfügung gestellt werden?

Als Ombudsmann wird ein Rechtsanwalt eingesetzt der dementsprechend der anwaltlichen Verschwiegenheitspflicht unterliegt.

AW R. Graf
Hier ist zunächst zu klären, für welchen Zweck die Mitarbeiterdaten an den Ombudsmann weitergegeben werden.

Wenn es zum Beispiel um das Thema Anti-Korruption geht, werden diese Fragen zur Klärung häufig an den Ombudsmann gegeben. Zu beachten ist aber, dass die anwaltliche Verschwiegenheitspflicht nur gegenüber dem Mandanten gilt und nicht zwingend gegenüber den Mitarbeitern.

Falls der Rechtsanwalt die Daten im Rahmen einer Auftragsdatenverarbeitung verarbeitet, ist dies auch entsprechend zu berücksichtigen.

1.3 Auskunftsersuchen - Betroffenenrecht

Wer zeichnet das Schreiben an den Betroffenen zum Auskunftsersuchen mit den bereitgestellten Informationen ab?

- Datenschutzbeauftragter oder
- Geschäftsleitung

AW R. Graf
Hier gibt es keine festgelegte Empfehlung, hier kann entweder Datenschutzbeauftragte oder die Geschäftsleitung unterschreiben. Oder eben beide, dies würde die Wichtigkeit des Datenschutzthemas betonen.

1.4 Dürfen die Namen von diensthabenden Bademeistern am Eingang des Schwimmbades ausgehängt werden?

Die Bademeister unseres Vereinsschwimmbads haben sich bei mir als DSB beschwert, dass neuerdings die Namen der aktuell diensthabenden Bademeister am Eingang ausgeschildert sind. Ich konnte datenschutzmäßig darin kein Problem erkennen, da wir ja ein Verein sind und es doch zu einer guten Vereinskultur gehören sollte, wenn man den Namen der Funktionsträger kennt. Außerdem wird außer dem Vor- und Zunamen kein weiteres personenbezogenes Datum angegeben.

Einzig, dass die Betroffenen nicht vorab davon informiert wurden, habe ich als etwas schlechten Stil gerügt. Frage: Liege ich mit meiner Einschätzung richtig?

AW R. Graf
Als erstes müsste die Frage des Zwecks geklärt werden und darauf basierend die Rechtsgrundlage.

Ich gehe davon aus, dass den Besuchern des Schwimmbades hier die Möglichkeit gegeben werden soll, den Bademeister mit Namen anzusprechen. Der Betroffene sollte natürlich vorher darüber informiert werden.

Ähnliches kennt man ja auch aus anderen Unternehmensbereichen mit Publikumsverkehr, in denen, wie z.B. zuweilen in Kaufhäusern, die Mitarbeiter auch Namensschilder zwecks besseren Kontaktes zum Kunden tragen.

Möglicherweise gib es in Schwimmbädern aus Sicherheitsgründen sogar eine besondere Vorschrift, die die Nennung des verantwortlichen Bademeisters vorschreibt. Das wäre in jedem Falle vorab zu klären, da sich die Rechtsgrundlage dann aus dem Arbeitsvertrag ableiten ließe.

1.5 Nutzung von Daten, die bei der Zugangskontrolle zu Sportstätten erhoben werden

Für unsere Schwimmhalle und unsere Fitnessstudios wurden die alten Zugangskontrollsysteme - übrigens ohne mich als DSB vorher davon zu informieren (-> Vorabkontrolle) - erneuert.

Jetzt haben sich Mitglieder beschwert, dass nicht nur der Zutritt erfasst, sondern jetzt über das Ausbuchen beim Verlassen der Sportanlagen auch die Verweildauer des jeweiligen Sportlers dokumentiert wird. Die Vereinsführung sah kein Problem darin, da damit ihrem berechtigten Interesse nachgekommen würde für die Belegungsplanung wichtige Statistiken zu erhalten. Ich habe dagegen dem Vorstand mitgeteilt, dass ich die Beschwerde der Mitglieder nachvollziehen kann und gefordert, dass nach dem Verlassen der Sportler von den Sportanlagen die Daten für die Statistiken im System vorher anonymisiert werden müssen. Für den Fall, dass dies systemtechnisch nicht möglich sein sollte, habe ich gefordert, dass alternative TOMs entwickelt werden müssen, um eine Nachvollziehbarkeit, wer, wann und wie lange die Sportanlagen genutzt hat, nicht möglich ist. Frage: Liege ich mit meiner Einschätzung richtig?

AW R. Graf
Da hier personenbezogene Daten verarbeitet werden, muss als erstes der Zweck der Verarbeitung und darauf basierend die Rechtsgrundlage geklärt werden [PS: dafür ist der Fachverantwortliche verantwortlich – nicht der DSB selbst (!)].

Des Weiteren ist zu klären, ob die Daten nicht pseudonymisiert werden können. Spätestens mit Anwendung der EU-DSGVO ab Mai 2018 (DSGVO) muss immer geprüft werden, ob Daten für die weitere Verarbeitung nicht pseudonymisiert werden können.

Soweit ich Ihrer Beschreibung entnehme, ist die Verarbeitung der personenbezogenen Daten für eine Belegungsstatistik nicht erforderlich. Daher besteht auch die Möglichkeit zur Anonymisierung, sodass ein Rückschluss auf die Besucher nicht mehr möglich wäre. Ist also eine Rückverfolgbarkeit der Belegungsstatistik nicht notwendig, dann sind die Daten zu anonymisieren.

D. h.: Sollte weder eine Pseudonymisierung noch eine Anonymisierung der Daten möglich sein, weil die Personendaten noch gebraucht werden, dann bitte den Zweck und die Rechtsgrundlage in einem Verfahren beschreiben lassen (z. B. Vertragserfüllung). Ich sehe das hier aber nicht.

1.6 Datenschutzkonformer Einsatz von Google Analytics

Google bietet die Möglichkeit, die IP-Adresse der Nutzer mit der Tracking-Code-Erweiterung „anonymizeIp" zu anonymisieren. Ist der Einsatz von Google-Analytics damit datenschutzkonform möglich (auch hinsichtlich der neuen EU-DSGVO), sofern die weiteren Rahmenbedingungen (Vertrag zur Auftragsdatenverarbeitung, Widerspruchsrecht der Nutzer, angepasste Datenschutzerklärung auf der Homepage) gegeben sind?

Oder sollten zum Website-Tracking besser andere Dienstanbieter wie Piwik genutzt werden?

AW R. Graf
Die von Ihnen erwähnten Maßnahmen sind nach den Angaben der Landesdatenschutzbehörden ausreichend.

Sicherlich gibt es hier noch einige Kritikpunkte, wie z. B. der, dass es mit einem Dritten in einem Drittland keine Privilegierung gem. §11 BDSG geben kann. Da die Aufsichtsbehörden die Maßnahmen aber als ausreichend klassifiziert haben, kann man das nun auch so umsetzen.

Man muss auch zugeben, dass Google Analytics vermutlich eines der besten Tools ist, aber die Daten müssen eben an Google (mehr oder weniger gut) anonymisiert übertragen werden.

PS: Piwik – richtig konfiguriert – ist aber auch gut.

IN DER DISKUSSION – NEUIGKEITEN RUND UM DEN DATENSCHUTZ

2 Haftungsrisiken in der neuen EU-DSGVO

Die EU-DSGVO bringt zahlreiche Neuerungen und Herausforderungen sowohl für die Datenschutzbeauftragten als auch für die jeweils Verantwortliche Stelle. Ein Thema, das schon jetzt für eine gewisse Unsicherheit unter Datenschützern sorgt ist die Frage, inwieweit sich das Haftungsrisiko für die Datenschutzbeauftragten erhöhen wird.

Da diese Frage gerade auch ein Thema im „Datenschutz-Ticker" war, dokumentieren wir an dieser Stelle zunächst die dortige Einschätzung. Auch im Datenschutzportal werden wir die Frage natürlich weiter begleiten und dokumentieren.

Worum geht es?

Die Frage des höheren Haftungsrisikos in der DS-GVO soll sich auch aus der Formulierung des Art. 39 Datenschutz-Grundverordnung (DS-GVO) ergeben, wonach der Datenschutzbeauftragte die Einhaltung der Verordnung und anderer Datenschutzvorschriften überwachen soll. Hintergrund dafür ist die Beobachtung, dass der Gesetzgeber diese Formulierung auch für andere Beauftragte zu speziellen Themen gewählt habe. Ähnlich wie der Compliance-Beauftragte müsse der Datenschutzbeauftragte nun damit rechnen, dass er selbst Bußgelder tragen müsse oder sich gar strafrechtlich dafür verantworten müsse.

Hier die Stellungnahme des Herausgebers des Datenschutz-Tickers, Wolfram von Gagern

Nicht Ihr Job: Die Verantwortung für die Datenschutzumsetzung

Generell ist es so, dass die Umsetzung der datenschutzrechtlichen Anforderungen Sache des Verantwortlichen ist. Da gibt es vom Grundsatz her auch keinen Unterschied zur heutigen Situation, in der das Unternehmen die Verantwortung für die Einhaltung der Regelungen zum Datenschutz trägt. Als Datenschutzbeauftragter haben Sie heute einen Hinwirkungsauftrag. Das Hinwirken besteht in erster Linie im Beraten in Datenschutzfragen, in der Sensibilisierung von Beschäftigten und in der Kontrolle von Verfahren zur Verarbeitung personenbezogener Daten. In Zeiten der DS-GVO wird sich hier nichts Wesentliches ändern, auch wenn die DSGVO in Art. 39 eher von einem Überwachungsauftrag spricht.

Den Begriff der Überwachung in Art. 39 Abs. 1 Buchst. b DS-GVO interpretieren manche Juristen – wahrscheinlich auch diese Kanzlei – so, dass den Datenschutzbeauftragten eine Verantwortung trifft. Wahrscheinlich sieht man hier Parallelen zum Compliance-Officer, den unter Umständen eine gewisse Verantwortung und Haftung treffen können. Vor allem unter strafrechtlichen Gesichtspunkten kann den Compliance-Officer eine Garantenpflicht treffen, sprich: er muss gewissermaßen dafür sorgen, dass es nicht zu Gesetzesverstößen kommt. Inwieweit beide Funktionen vergleichbar sind, kann derzeit wohl niemand sagen. Einschlägige Rechtsprechung zur Verantwortung des Datenschutzbeauftragten für das Fehlverhalten anderer Personen gibt es bislang nicht. *[Quelle: Datenschutz-Ticker: Newsletter@news.bwr-media.de vom 21.8.2017]*

3 Biometrische Gesichtserkennung in der polizeilichen Erprobung in der Kritik

Die Bundespolizei hat mitgeteilt, dass es sich bei den an die Testteilnehmer ausgegeben Token, mit denen über ein Referenzsystem Fehler bei der Gesichtserkennung festgestellt werden sollen, nicht um passive RFID-Chips, sondern um aktive Bluetooth-Transponder mit iBeacon-Funktion handelt. Letztere senden dauerhaft und überall Informationen, die nicht nur von den Lesegeräten der Bundespolizei am Bahnhof, sondern von jedermann mit einem Smartphone, auf dem eine entsprechende App installiert ist, empfangen werden können. Über diesen Umstand wurden die Teilnehmer im Vorfeld der Abgabe ihrer Einwilligung nicht informiert.

Andrea Voßhoff: Gerade bei Verfahren, die mangels anderweitiger Rechtsgrundlagen auf Einwilligungen zurückgreifen, ist es essentiell, dass den Betroffenen sämtliche Informationen zur Verfügung gestellt werden, die sie benötigen um eine wohlüberlegte Entscheidung zu treffen. Auch wenn die Informationen, die der Transponder aussendet, datenschutzrechtlich nicht besonders sensibel sind, ist das Versäumnis der Bundespolizei, die Testteilnehmer hinreichend zu informieren, keine Lappalie. Zum einen kann es für jemanden durchaus relevant sein zu wissen, dass er mit einem dauerhaft sendenden Chip durch die Stadt läuft. Zum anderen ist es unabhängig vom Einzelfall essentiell, die Einhaltung der datenschutzrechtlichen Vorgaben an eine wirksame Einwilligung konsequent einzufordern, um diese dem Schutz der Einwilligenden dienenden Elemente nicht sukzessive verwässert und unterlaufen werden.

Bei dem Pilotprojekt am Berliner Südkreuz testet die Bundespolizei Verfahren zur biometrischen Gesichtserkennung mit freiwilligen Teilnehmern, die in die hierfür erforderliche Datenverarbeitung eingewilligt haben. Die BfDI hatte das Projekt unter der Voraussetzung einer informierten Einwilligung für datenschutzrechtskonform erklärt. Gleichzeitig hat sie jedoch auch darauf hingewiesen, dass der flächendeckende Einsatz einer automatisierte Gesichtserkennung ohne Einwilligung der Betroffenen einen erheblichen Grundrechtseingriff darstellen würde, der zwingend einer verfassungskonformen Rechtsgrundlage bedürfe. [*Quelle:* Pressemitteilung der BfDI vom 24.08.17]

MEDIEN –TECHNIK – SICHERHEIT

4 Kurz notiert: Aktuelle Warnmeldungen

eine Auswahl der vom BSI veröffentlichter Warnmeldungen

Trojaner: Vorsicht vor Videolink im Facebook-Messenger

Derzeit verbreitet sich ein Trojaner über den Facebook-Messenger. Dabei erhält der Empfänger über den Messenger eine Nachricht, die augenscheinlich von einem "Freund" kommt. Wie unter anderem der Spiegel berichtet, ist in der Meldung ein Link zu einem angeblichen Video enthalten. Sobald der Empfänger diesen anklickt, lädt er sich eine Schadsoftware auf sein Endgerät. Diese greift sowohl auf E-Mail-Accounts als auch auf Passwörter und den Browser-Verlauf zu. Parallel dazu verschickt der Trojaner die schadhafte Nachricht von dem Facebook-Account der betroffenen Person an dessen Freundeskreis.

Betroffene sollten sich deswegen umgehend mit allen Geräten von ihrem Facebook-Profil abmelden. Zudem wird empfohlen, alle Passwörter zu ändern, einen Viren-Scan durchzuführen und den Verlauf des Browsers zu löschen. Auf der Webseite BSI für Bürger sind einige Tipps aufgeführt, was Sie bei der Kommunikation mit einem Instant Messenger beachten sollten. [LINK zur Website]. *[Quelle: Buerger-Cert-Newsletter] SICHER • INFORMIERT vom 31.08.17]*

Spyware: Apps mit unerwünschten Erweiterungen

Sicherheitsforscher haben bei einer Routineüberprüfung ein Software Development Kit für Werbeeinblendungen entdeckt, das Schnüffelfunktionen besitzt. Dieses war in mehr als 500 Apps enthalten, darunter Spiele- und Wetter-Apps, die im offiziellen Google Play Store angeboten wurden, so ein Artikel auf heise.de. Die Spionagefunktion ist in der Lage, Werbung einzublenden und Befehle von einem Server zu empfangen und auszuführen. dies geschieht allerdings nur, wenn der Nutzer oder die Nutzerin bei der Installation der Apps entsprechende Berechtigungen erteilt hat. Mittlerweile hat Google die Apps gelöscht beziehungsweise die Funktion entfernt.

Worauf Sie bei der Installation einer App auf Ihrem Android-Gerät und der angeforderten Berechtigungsvergabe achten sollten, erfahren Sie auf der Webseite BSI für Bürger. [LINK zur Website]. *[Quelle: Buerger-Cert-Newsletter] SICHER • INFORMIERT vom 31.08.17]*

Schwachstelle: Automatische Link-Updates in Word bergen Risiken

Sicherheitsexperten haben eine Funktion entdeckt, mit der Cyber-Kriminelle mittels Microsoft Word Systeme mit Malware infizieren. Dazu nutzen sie eine eingebettete Verlinkung, die sich immer wieder automatisch aktualisiert, sobald der Nutzer oder die Nutzerin das Word-Dokument öffnet, so ein Blogbeitrag auf botfrei.de. Ziel ist es, eine bösartige "PE-Netwire RAT"-Datei über einen PowerShell-Befehl-Programmbefehl herunterzuladen und auf dem betroffenen System zu starten.

Sie können Ihre Geräte schützen, indem Sie dafür sorgen, dass Ihr Betriebssystem und alle verwendeten Applikationen stets mit Updates auf dem aktuellen Stand gehalten wer-

den. Zudem sollten Sie niemals Office-Dateien öffnen, die von nicht vertrauenswürdigen Quellen stammen. Wie wichtig Patch-Management in diesem Zusammenhang ist, erfahren Sie auf der BSI für Bürger Webseite [LINK zur Website]. *[Quelle: Buerger-Cert-Newsletter] SICHER • INFORMIERT vom 31.08.17]*

Spam-Welle: Falsche Rechnungen und Mahnungen häufen sich

Aktuell beobachtet das BSI eine Spam-Welle, die zur E-Mail-Adresse passende persönliche Daten verwendet. Die E-Mail enthält beispielsweise eine Mahnung und fordert dazu auf, offene Rechnungen zu begleichen. Der als Kostenaufstellung getarnte Anhang erhält jedoch eine Schadsoftware. Die gleiche Vorgehensweise nutzen Cyber-Kriminelle aktuell in Form einer Paketankündigung von DHL. In der E-Mail mit dem Betreff "Informationen über die Sendung Nr. 13469035607715" ist ein Link enthalten, der zu einem Virus-Anhang führt, wie auf Spam-Info zu lesen ist.

Um sich zu schützen, sollten Sie bei E-Mails von unbekannten Absendern keine Anhänge öffnen oder Links anklicken. Weitere Hinweise zum Umgang mit E-Mails gibt unser 3-Sekunden-Sicherheitscheck als Video auf der BSI für Bürger Webseite. [LINK zur Website]. *[Quelle: Buerger-Cert-Newsletter] SICHER • INFORMIERT vom 31.08.17]*

Phishing: Falsche Warnhinweise zu Amazon-Konto

Kaum ein Tag vergeht, an dem keine neue Phishing-Mail bekannt wird. Mit diesen E-Mails, die etwa vorgaukeln von einem bestimmten Unternehmen zu stammen, versuchen Cyber-Kriminelle an persönliche Nutzerinformationen zu gelangen, beispielsweise Zahlungs-, Nutzer- oder Bankdaten. Wie die Verbraucherzentrale in ihrem Phishing-Radar schreibt, haben es Betrüger derzeit auf die persönlichen Informationen von Amazon-Kunden abgesehen.

Um nicht in die Phishing-Falle zu tappen, sollten Nutzer eine solche E-Mail sofort löschen. Wozu trügerische Webseiten in der Lage sind und wie Sie Phishing-E-Mails und -Webseiten erkennen können, erklären wir in der Rubrik Risiken auf der Webseite BSI für Bürger: [LINK zur Website]. *[Quelle: Buerger-Cert-Newsletter] SICHER • INFORMIERT vom 31.08.17]*

5 Sicheres Cloud Computing: BSI zertifizierte Cloud-Dienste

Der Einsatz von Cloud-Computing spielt – wie auch die Fragen dazu im Live-Chat unseres Datenschutzportals zeigen – auch bei Vereinen und Verbänden eine immer größere Rolle. Aufgrund der damit erhofften Kostenvorteile ebenso wie aus Gründen der (bei Netzzugang) sowohl räumlich als auch zeitlich unbeschränkten Verfügbarkeit hat sich dabei die Frage nach dem „Ob" mehr und mehr in Richtung der Frage nach dem „Bei Wem" verändert.

Um den Kunden eine unabhängige Orientierung zu bieten hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) 2016 einen umfangreichen „Anforderungskatalog Cloud Computing (C5) entwickelt, in dem auf insgesamt 94 Seiten „Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten" vorgestellt werden. Ziel des Anforderungskata-

loges, der kostenfrei als PDF-Datei heruntergeladen werden kann [LINK zum Anforderungskatalog des BSI] war und ist es, „den Kunden eine Hilfestellung für einen besseren Überblick zu mehr Sicherheit" zu geben und damit zugleich Mehrfachprüfungen der diversen auf dem Markt angebotenen Standards und Zertifizierungen zu vermeiden.

Nach der Zertifizierung von *Amazon Web Services*, *Box* und *Fabasoft* hat das BSI jetzt auch an Microsoft Azure Deutschland ein Testat nach den Anforderungen des Anforderungskatalogs Cloud Computing (Cloud Computing Controls Catalogue, C5) vergeben.

Als nationale Cyber-Sicherheitsbehörde gestalte das BSI Informationssicherheit in der Digitalisierung auch durch die Schaffung von IT-Sicherheitsstandards wie dem C5-Katalog, erklärte BSI-Präsident Arne Schönbohm. Der Katalog ist in Basis-Anforderungen und höherwertige Anforderungen unterteilt, um verschiedene Sicherheitsbedürfnisse zu adressieren. Er richtet sich an professionelle Cloud-Anbieter, deren Prüfer sowie Kunden. Weitere Informationen finden Sie in der zugehörigen Pressemitteilung auf der BSI-Website [Link zur Website].

PS: Die Zertifizierung bedeutet nicht, dass der Standort der Server in Deutschland oder in der EU ist. Die Zertifizierung beinhaltet allerdings das Kriterium, dass der Standort der Server angegeben ist. Die Server des jetzt zertifizierten Anbieters *Microsoft Azure Deutschland* stehen in Deutschland [LINK]. *Amazon Web Services* bietet seit neuestem ebenfalls einen Standort in Deutschland an (Frankfurt) [Link] Bei *Fabasoft* kann der Kunde eine Datenspeicherung in Deutschland auswählen. *Box*, Marktführer in den USA hat zwar 2016 angekündigt, Server in Europa bereitzustellen, hat das aber offensichtlich noch nicht umgesetzt [vgl. trusted Test]

Einen Vergleichstest zu 32 aktuellen Cloud-Anbietern (u.a. auch mit Angaben zum Serverstandort] finden Sie auf der Website von trusted. [LINK zum Vergleichstest].

Vgl. auch die Hinweise im Juli Live-Chat (auch abgedruckt im Info-Brief 2017-07).

AKTUELLE URTEILE

6 Urteil des Bundesarbeitsgerichts zur Verwendung von Keyloggern zur Überwachung von Arbeitnehmern

Durch Keylogger gewonnene Erkenntnisse nicht verwertbar

Quelle: *Bundesarbeitsgericht, Urteil vom 27.07.2017; AZ: 2 AZR 681/16*
Fundort: www. kostenlose-urteile.de (ra-online GmbH), Berlin *31.07.17;* Dok.-Nr.: 24627

Worum geht es?

Besteht kein auf den Arbeitnehmer bezogener, durch konkrete Tatsachen begründeter Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung, dann ist der Einsatz eines Software-Keyloggers, mit dem alle Tastatureingaben an einen dienstlichen Computer für eine verdeckte Überwachung und Kontrolle des Arbeitnehmers aufgezeichnet werden, nach § 32 Abs. 1 BDSG* unzulässig. Dies hat das Bundesarbeitsgericht nunmehr in seiner Entscheidung bekanntgegeben.

Im hier zu entscheidenden Fall war der Kläger bei der Beklagten seit 2011 als „Web-Entwickler" beschäftigt. Im Zusammenhang mit der Freigabe eines Netzwerks teilte die Beklagte ihren Arbeitnehmern im April 2015 mit, dass der gesamte „Internet-Traffic" und die Benutzung ihrer Systeme „mitgeloggt" werde. Sie installierte auf dem Dienst-PC des Klägers eine Software, die sämtliche Tastatureingaben protokollierte und regelmäßig Bildschirmfotos (Screenshots) fertigte.

Privattätigkeiten im erheblichen Umfang durch Keylogger erfasst

Nach Auswertung der mit Hilfe dieses Keyloggers erstellten Dateien fand ein Gespräch mit dem Kläger statt. In diesem räumte er ein, seinen Dienst-PC während der Arbeitszeit privat genutzt zu haben. Auf schriftliche Nachfrage gab er an, nur in geringem Umfang und in der Regel in seinen Pausen ein Computerspiel programmiert und E-Mail-Verkehr für die Firma seines Vaters abgewickelt zu haben. Die Beklagte, die nach dem vom Keylogger erfassten Datenmaterial davon ausgehen konnte, der Kläger habe in erheblichem Umfang Privattätigkeiten am Arbeitsplatz erledigt, kündigte das Arbeitsverhältnis außerordentlich fristlos, hilfsweise ordentlich.

Verletzung des allgemeinen Persönlichkeitsrechts durch Keylogger-Einsatz

Die Vorinstanzen haben der dagegen gerichteten Kündigungsschutzklage stattgegeben. Die Revision der Beklagten hatte vor dem Bundesarbeitsgericht keinen Erfolg. Die durch den Keylogger gewonnenen Erkenntnisse über die Privattätigkeiten des Klägers dürfen im gerichtlichen Verfahren nicht verwertet werden. Die Beklagte hat durch dessen Einsatz das als Teil des allgemeinen Persönlichkeitsrechts gewährleistete Recht des Klägers auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG) verletzt. [LINK zum vollständigen Artikel]

7 Rechtmäßige Untersagung der permanenten Überwachung des Verkehrsgeschehens mittels einer Dashcam

Verstoß gegen § 6 b des Bundes-datenschutzgesetzes

Quelle: *Verwaltungsgericht Göttingen, Urteil vom 31.05.2017; AZ: 1 A 170/16*
Fundort: www. kostenlose-urteile.de (ra-online GmbH), Berlin *28.07.2017;* Dok.--Nr.: 24619

Worum geht es?

Überwacht ein Verkehrsteilnehmer mittels einer Dashcam permanent das Verkehrsgeschehen, um die so gewonnenen Daten zur Einleitung von Ordnungswidrigkeitenverfahren zu verwenden, verstößt er gegen § 6 b des Bundes-datenschutzgesetzes (BDSG). Ihm kann daher die permanente Überwachung des öffentlichen Verkehrsraums untersagt werden. Dies hat das Verwaltungsgericht Göttingen entschieden.

Dem Fall lag folgender Sachverhalt zugrunde: Ein als "Knöllchen-Horst" bekannt gewordener privater Ermittler von Ordnungswidrigkeiten hatte in seinem Fahrzeug zwei Dashcams installiert, um den vorausfahrenden und nachfolgenden Straßenverkehr aufzeichnen zu können. Er nutzte die Aufzeichnungen seit November 2014 zur Anzeige von Verkehrsordnungswidrigkeiten. Da auf den Aufnahmen Aufschriften auf Pkws, Gesichter sowie Kfz-Kennzeichen zu erkennen waren und die Aufnahmen zudem Angaben zu den Längen- und Breitengraden sowie den Zeitpunkt ihrer Entstehung enthielten, erließ die zuständige Datenschutzbehörde im Juni 2016 eine Anordnung, wonach "Knöllchen-Horst" untersagt wurde, permanent den öffentlichen Verkehr mittels von Dashcams zu überwachen. Dieser war damit nicht einverstanden. Er führte an, die Aufzeichnungen zu eigenen Zwecken zu nutzen und erhob daher Klage gegen die datenschutzaufsichtliche Anordnung.

Verbot der permanenten Überwachung des Verkehrsgeschehens mittels einer Dashcam rechtmäßig

Das Verwaltungsgericht Göttingen entschied gegen den Kläger. Die beklagte Behörde habe die permanente Überwachung des Verkehrsgeschehens mittels einer Dashcam gemäß § 38 Abs. 5 BDSG untersagen dürfen, da der Kläger gegen § 6 b BDSG verstoßen habe. Ein Verstoß liege schon deshalb vor, weil der Kläger den Umstand der Beobachtung gemäß § 6 b Abs. 2 BDSG nicht durch geeignete Maßnahmen erkennbar gemacht habe.

Wahrnehmung berechtigter Interessen rechtfertigt keine anlasslose und regelmäßige Überwachung

Die permanente Videoüberwachung sei darüber hinaus nicht gemäß § 6 b Abs. 1 Nr. 3 BDSG gerechtfertigt gewesen, so das Verwaltungsgericht. Zwar könne eine Videoüberwachung zum Zwecke des Selbst- und Eigentumsschutzes und einer diesbezüglichen Beweissicherung der Wahrnehmung berechtigter Interessen dienen. Dies rechtfertige aber allenfalls den Einsatz der Kameras im Einzelfall und nicht die anlasslose und regelmäßige Videoüberwachung des Straßenverkehrs. [LINK zum vollständigen Artikel]

8 Werbeblocker verstoßen nicht gegen Kartell-, Wettbewerbs- und Urheberrecht

Geschäftsmodell mit Open Source-Software ist nicht als verbotene aggressive zu Werbung qualifizieren

Quelle: *Oberlandesgericht München, Urteil vom 17.08.2017; AZ:*
Fundort: www. kostenlose-urteile.de (ra-online GmbH), Berlin *18.08.17*; Dok.--Nr.: 24717

Worum geht es?

Das Oberlandesgericht München hatte darüber zu entscheiden, ob eine Open Source-Software, die Werbung auf Websites unterdrückt, wettbewerbs-, kartell- und urheberrechtliche zulässig ist.

Dem Verfahren lag folgender Sachverhalt zugrunde: Die Klageparteien betreiben für die Nutzer kostenlose Internetseiten mit journalistischen Inhalten. Diesen Onlineauftritt finanzieren sie durch Werbung.

Software der Beklagten unterdrückt Werbeeinblendungen beim Aufruf einer Internetseite

Die Beklagte vertreibt seit dem Jahr 2011 eine für den Nutzer unentgeltliche Open Source-Software, die der Unterdrückung von Werbeeinblendungen beim Aufruf einer Internetseite dient. Dabei besitzt das Programm der Beklagten selbst keine eigene Filter-Funktionalität, sondern muss mit Vorgaben ergänzt werden, welche Inhalte blockiert werden sollen. Diese sind in sogenannten Filterlisten ("Blacklists") enthalten, die dem Nutzer standardmäßig vorgeschlagen werden. Die Software der Beklagten ist nach dem Download so voreingestellt, dass nach ihren Kriterien ("Whitelist") als nicht störend eingestufte Werbung angezeigt werden kann. Jeder Webseitenbetreiber hat die Möglichkeit, am "Whitelisting" der Beklagten teilzunehmen und seine Seiten von ihr freischalten zu lassen. Von Betreibern größerer Webseiten verlangt die Beklagte dafür eine Lizenzzahlung.

Kläger beanstanden massive Umsatzeinbußen durch Einsatz der Software der Beklagten

Die Kläger haben in den Verfahren die Ansicht vertreten, dass der Einsatz der Software zu massiven Umsatzeinbußen führt, sie gezielt behindert und unlauter Druck auf sie ausübt, mit der Beklagten eine kostenpflichtige Vereinbarung über eine "Freischaltung" von Werbeinhalten abzuschließen.

LG weist Klage ab

Das Landgericht wies die Klagen, mit denen die Klageparteien wettbewerbs- und kartellrechtliche sowie urheberrechtliche Unterlassungs-, Auskunfts- und Schadensersatzfeststellungsansprüche geltend gemacht haben, ab. [LINK zum vollständigen Artikel]

9 Phishing: Weitergabe einer TAN am Telefon stellt grobe Fahrlässigkeit dar

Bank muss über Phishing ergaunertes Geld nicht erstatten

Quelle: Amtsgericht München, Urteil vom 05.01.2017; AZ: Amtsgericht München, Urteil vom 05.01.2017
Fundort:: www. kostenlose-urteile.de (ra-online GmbH), Berlin 18.08.17; Dok.--Nr.: 24716

Worum geht es?

Die Weitergabe einer TAN in einem Telefongespräch begründet den Vorwurf der groben Fahrlässigkeit, so dass eine Bank nicht verpflichtet ist, das über Phishing ergaunerte Geld zu erstatten. Dies entschied das Amtsgericht München.

Dem Fall lag folgender Sachverhalt zugrunde: Ein Ehepaar aus Aying unterhält bei der beklagten Bank ein Girokonto. Beide nutzten das Direct B@nking-Angebot der Bank im Internet für ihr Girokonto. Am 12. Mai 2014 erhielt die Ehefrau eine Phishing-E-Mail, die als Absender "HypoVereinsbank [mailto:direct-b@hypovereinsbank]" auswies und mitteilte, dass der Zugang zum "Direct B@nking" bald ablaufe, sofern die Synchronität der SEPA-Umstellung im Zugang nicht aktualisiert werde. Es wurde aufgefordert, auf einen Link zur manuellen Aktualisierung des Zugangs zu klicken.

Kontoinhaberin gibt TAN für Überweisung per Telefon weiter

Die Ehefrau klickte auf diesen Link und gab dort ihren Namen, ihre Kontonummer sowie ihre Festnetznummer an. Am 13. Mai 2014 rief eine weibliche Person die Ehefrau des Klägers an und gab sich als Mitarbeiterin der Bank aus. Von dieser wurde die Ehefrau gebeten, sich Nummern zu notieren, und diese mit den Nummern zu vergleichen, die ihr sogleich in einer SMS mitgeteilt werden würden. Falls die Buchstaben/Ziffern übereinstimmen würden, sollte sie die letzte Ziffernfolge in der SMS der Anruferin mitteilen. Nach Erhalt der SMS mit dem Inhalt "Die mobile TAN für Ihre Überweisung von 4.444,44 EUR auf das Konto ES (...) mit BIC (...) lautet: 253844" teilte die Ehefrau die Ziffernfolge 253844 der Anruferin mit. In der Folge wurde ein Betrag von 4.444,44 Euro auf das Konto ES (...) mit BIC (...)überwiesen.

Bank verweigert Schadensersatzzahlung

Die Ehefrau ließ das Konto am 18. Mai 2014 sperren und stellte am 19. Mai 2014 Strafanzeige gegen Unbekannt. Versuche, den Betrag von diesem Konto zurückzuerlangen, blieben ohne Erfolg. Die Bank weigerte sich, den Schaden zu ersetzen. Daraufhin erhob das Ehepaar Klage auf Zahlung von 4444,44 Euro.

Weitergabe der TAN im Telefongespräch begründet Vorwurf der groben Fahrlässigkeit

Das Amtsgericht München wies die Klage ab. Das Geld des Ehepaars ist weg. Die Weitergabe der TAN im Telefongespräch begründe den Vorwurf der groben Fahrlässigkeit, so das Gericht. Beim mobilen TAN-Verfahren würde eine TAN stets für eine konkrete Aktion, vor allem für eine konkrete Überweisung erzeugt und per SMS auf das Mobiltelefon des Kunden verschickt. Die SMS enthalte aber gerade nicht nur die TAN, sondern lautet wie hier: "Die mobile TAN für Ihre Überweisung von 4.444,44 EUR auf das Konto ...". [LINK zum vollständigen Artikel]

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