DOSB FÜHRUNGS AKADEMIE

FA Datenschutzportal

DSP Info-Brief

Nr. 41 / Dezember 2016

INHALT

DATENSCHUTZPORTAL INTERN

1 Themen des Live-Chats 2016-11 3

IN DER DISKUSSION – NEUIGKEITEN RUND UM DEN DATENSCHUTZ

2 Neue Vorgaben zur E-Mail-Archivierung – Übergangsregel endet 8

3 Tipps zur Vereinsarbeit auf privaten Computern 10

MEDIEN –TECHNIK – SICHERHEIT

4 Zugangsdaten von gesperrtem PC geklaut 13

5 Neue Schadsoftware befällt Android-Geräte …..... 13

GESETZGEBUNG

6 Änderungen zum AGB-Recht 15

7 Aktueller Status EU-DSGVO …..... 16

8 Videoüberwachung zwischen BDSG und EU DSGVO 18

AKTUELLE URTEILE

9 Social-Media-Nutzung durch Arbeitgeber: Facebook-Auftritt nur mit Zustimmung ..... des Betriebsrats. Von Michael Fuhlrott 21

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 Themen des Live-Chats 2016-11

Weitergabe von Adressdaten an eine Druckerei

Unsere Sportjugend möchte gerne eine Broschüre der dsj versenden. Die dsj bietet an, dies direkt über eine Druckerei zu machen.

Dürfen die Adressdaten an die Druckerei weitergegeben werden (Auftragsdatenverarbeitungsvereinbarung vorausgesetzt) oder ist dies nicht zulässig, da wir keine Einwilligung der Jugendleiter haben, dass sie von anderen Personen angeschrieben werden?

Wir könnten die Broschüre auch selber verschicken, was aber deutlich mehr Kosten verursachen würde.

AW R. Graf
Im Falle der Auftragsdatenverarbeitung wird die Druckerei, bildlich gesprochen, Teil der Sportjugend bzw. des Vereins oder Verbandes. Insofern ist die Datenverarbeitung dem Verein oder Verband zuzuordnen und in diesem Falle wäre keine gesonderte Einwilligung erforderlich, sondern würde über den Paragraph 28 Abs. 1 BDSG abgedeckt.

Ich würde aber sicherlich deutlich machen, dass der der Verband der Absender ist und nicht die Druckerei.

Mitgliedskontrolle durch ehrenamtliche Abteilungs- und Übungsleiter auf dem eigenen Smartphone

Mein Verein überlegt, seine Abteilungsleiter und evtl. auch die Übungsleiter, die überwiegend nicht beim Verein angestellt, sondern nur ehrenamtlich tätig sind, auch mit der Mitgliederkontrolle zu beauftragen. Aufgrund unseres vorhandenen Systems könnte die Möglichkeit durch einen persönlichen Zugang geschaffen werden, die Mitgliedskontrolle per Smartphone oder Laptop durchzuführen.

Zur Prüfung der Mitgliedschaft muss dem Abteilungs- bzw. Übungsleiter zumindest Name, Vorname, Geburtsdatum, Eintritt oder auch Austritt angezeigt werden.

1. Mir ist klar, dass diese Personen eine Datenschutzerklärung unterzeichnen müssten.
2. Wie sieht es aus, wenn diese Ehrenamtlichen unsere Daten mit dem eigenen Telefon/Laptop abfragen (eine Bearbeitung wäre nicht möglich)?

Kann ich davon ausgehen, dass diese Nutzung auf privaten Geräten datenschutzrechtlich nicht korrekt ist?

AW R. Graf
die Verarbeitung personenbezogener Daten auf privaten Geräten von Mitarbeitern bzw. ehrenamtlich tätigen Personen (werden wie Mitarbeiter behandelt), ist datenschutzrechtlich kaum unbedenklich umsetzbar.

Es gibt viele Fragen, die zuvor geklärt werden müssen. An dieser Stelle kann nur auf einige wenige hingewiesen werden.

- Auch wenn ein Verarbeiten nicht möglich ist, werden diese Daten im System des Benutzers, z.B. im Kontakteordner des Benutzers, gespeichert werden.
- Auch die Einhaltung von Datensicherheitsmaßnahmen auf den privaten Smartphones und Laptops der ehrenamtlich arbeitenden Personen kann der Verein nicht gewährleisten. Als verantwortliche Stelle ist der Verein aber gemäß BDSG für die Umsetzung der technischen und organisatorischen Maßnahmen verantwortlich.
- Die Erfahrung zeigt, dass die Einhaltung notwendiger und vorgeschriebener Sicherheitsmaßnahmen (z.B. die Verschlüsselung von Daten (Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle) auf privat genutzten Geräten kaum zu realisieren ist.
- Auch kann nicht mit Sicherheit festgelegt werden, wer diese Daten einsehen kann.
- Bei der Nutzung der Daten auf Smartphones kommt hinzu, dass in den meisten Fällen Android Smartphones zum Einsatz kommen, die datensicherheitstechnisch auf der untersten Ebene anzusiedeln sind. Installiert der Nutzer zum Beispiel eine neue App, kann der Verein nicht gewährleisten, dass diese App keinen Zugriff auf die auf dem Smartphone befindlichen Daten des Vereins hat. Genau diese unbefugte Nutzung von Daten muss der Verein jedoch verhindern.

Gleichzeitig muss noch einmal darauf hingewiesen werden, dass die oben genannten Daten nur in verschlüsselter Form per E-Mail an die Übungsleiter gesendet werden dürfen. Schon dies stellt in vielen Fällen eine oft unüberwindliche Hürde dar.

Fazit: So unglaublich es sich im Jahre 2016 anhören mag, in diesem Fall ist ein die gesetzlichen Regeln einhaltender Datenaustausch über Brief und Papier noch am einfachsten zu realisieren.

Datenschutzrechtliche Bedingungen zur Auswertung und Weitergabe von Anmeldedaten zu Veranstaltungen

Ein Verband betreibt per Lizenz (Nutzungsvertrag) ein Portal für die Organisation von Sportveranstaltungen, eine ADV mit dem technischen Betreiber ist vorhanden. Der Verband vergibt Unter-Lizenzen an Vereine, die Ihre Sportveranstaltungen über dieses Portal abwickeln können (ebenfalls ADV zwischen Vereinen und Verband). Ferner können sich (auch international) Einzelsportler über dieses Portal für die entsprechenden Sportveranstaltungen anmelden – sowohl die Vereine als auch die Einzelsportler müssen sich dazu registrieren. (Dass dieses Konstrukt per Rahmenvertrag mit dem technischen Betreiber des Portals und damit ggf. datenschutzrechtlich einfacher zu lösen wäre, steht hier nicht zur Debatte.)

Bei der Registrierung wird eine Checkbox angeklickt, durch die bestätigt wird, dass man die Nutzungs- und Datenschutzbedingungen, die an dieser Stelle entsprechend verlinkt sind, gelesen hat und in diese einwilligt. Andernfalls ist eine Registrierung nicht möglich.

Dazu folgende Fragen:

1. Als verantwortliche Stelle wird in der Datenschutzerklärung (nur) die Organisation angegeben. Ist das korrekt?

2. Ferner sollen die Daten zu Marketingzwecken verwendet werden - sprich für statistische Auswertungen, aber auch ggf. für Anschreiben der registrierten Personen bei ähnlichen Veranstaltungen etc. Das macht der technische Betreiber des Portals.

   Reicht es, innerhalb der Datenschutzerklärung anzugeben, dass die Daten auf Grundlage der ADV an den technischen Betreiber des Portals weitergegeben werden und dieser die Daten zu Marketingzwecken auswerten bzw. nutzen kann oder muss das explizit bei der Registrierung per eigener Checkbox geschehen? „Ich bin damit einverstanden, dass meine Daten an XY weitergegeben werden und zu Marketingzwecken von XY genutzt werden …"?

AW R. Graf
Zu 1: ich gehe davon aus, dass mit der Organisation der Verband gemeint ist. Des Weiteren gehe ich davon aus, dass auch im Falle von Unterlizenzen erkenntlich ist, dass der Verband der Betreiber des Portals ist. Dass der Verband ein Auftragnehmer zur Verarbeitung seiner Daten nutzt, kann, muss aber nicht explizit erwähnt werden. Über den Auftragsdatenverarbeitungsvertrag wird der Auftragnehmer in den Verband eingebunden, und ist somit nicht mehr Dritter.

In der Datenschutzerklärung des Verbandes wird die Nutzung der Daten bezüglich der Funktionalität des Portals erläutert, dieser Datenschutz Erklärung ist zuzustimmen über ein Option Häkchen.

Zu 2: Datenverarbeitung die über den eigentlichen Zweck der Nutzung des Portals hinausgehen, in Ihrem Fall die Marketingzwecke, bedürfen auf jeden Fall einer ergänzenden Zustimmung. Ich gehe hier davon aus, dass die Marketingzwecke den Verband zuzuordnen sind. Der technische Betreiber des Portals also nach wie vor Auftragsdatenverarbeiter ist.

Die Datenschutzerklärung sollten auf jeden Fall ausführlich die Nutzung der Daten darstellen. Bitte beachten Sie auch entsprechende Prozesse, falls der Betroffene, also der Nutzer, sofern es sich um eine natürliche Person handelt, der Verarbeitung auch widersprechen können muss.

Ist eine (100%ige) Tochtergesellschaft des Vereins datenschutzrechtlich als 'Dritter' zu behandeln?

Die Weitergabe von Mitgliederdaten zu Werbezwecken an Dritte gehört nicht zu den von § 28 Abs.1 S.1 Nr.1 BDSG datenschutzrechtlich gebilligten vereinsinternen Zwecken und ist daher ohne Einwilligung untersagt.

1. Gilt eine Tochtergesellschaft als 'Dritter' oder ist sie bei einer Mehrheitsbeteiligung des Vereins als Teil des Vereins?

2. Wie ist eine 100-prozentige Tochtergesellschaft des Vereins datenschutzrechtlich einzuordnen - als Teil des Vereins oder als 'Dritter'?

AW R. Graf
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.

Bezüglich der Anpassung an die Datenschutzgrundverordnung im Mai 2018 wird es das sogenannte Konzernprivileg geben, ohne mich festlegen zu wollen, dazu die gesamte Umsetzung noch zu unklar, ist zu erwarten dass dann solche Mutter Tochterkonstruktionen denkbar sind. im BDSG gibt es zurzeit kein 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.

Bezüglich der Anpassung an die Datenschutz Grundverordnung im Mai 2018 wird es das sogenannte Konzernprivileg geben, ohne mich festlegen zu wollen, dazu die gesamte Umsetzung noch zu unklar, ist zu erwarten dass dann solche Mutter Tochterkonstruktionen denkbar sind.

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 R. Graf

- Frage 1 – <u>Rahmenbedingungen für Gäste:</u> 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.

- Frage 1 und 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.

- Frage 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.
  Frage 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.

IN DER DISKUSSION – TIPPS & NEUIGKEITEN ZUM DATENSCHUTZ

2 Neue Vorgaben zur E-Mail-Archivierung – Übergangsregel endet

E-Mail-Archivierung betrifft heute nahezu jedes Unternehmen. Bereits seit dem 1. Januar 2015 haben die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" (GoBD) die bis dahin gültigen GoBS und GDPdU abgelöst. Zum 31. Dezember 2016 endet nun endgültig die Übergangsfrist.

Anforderungen aus den GoBD

Die GoBD verlangen von Unternehmen einen professionellen Umgang bei der elektronisch gestütztem Erzeugung, Empfang, Übermittlung und Verarbeitung von buchungsrelevanten Daten, wie Angeboten, Rechnungen etc.

Geschäftsvorfälle müssen belegbar sein, weshalb ein bloßes „Liegenlassen" der E-Mails im Eingangsordner den gesetzlichen Anforderungen nicht genügt. Stattdessen dürfen E-Mail weder gelöscht noch verändert werden. Haben stets abrufbar und auffindbar zu sein.

Diese 10 Grundregeln müssen beachtet werden!

Die Bitkom hat die wichtigsten Anforderungen an die E-Mail Archivierung in einem gut aufbereiteten Positionspapier abgehandelt. Folgende 10 Merksätze sind demnach zu beachten:

- E-Mails sind aufbewahrungspflichtig
- E-Mails sind elektronisch aufzubewahren
- Dateianhänge sind im Original aufzubewahren
- E-Mail lediglich als Transportmittel
- E-Mails sind zu indexieren
- E-Mails sind unverändert zu archivieren
- Die Konvertierung von E-Mails unterliegt spezifischen Vorgaben
- Der Umgang mit E-Mails ist zu dokumentieren
- E-Mails unterliegen dem Recht auf Datenzugriff
- Rechnungen als E-Mails sind zulässig

Was wird zur Umsetzung benötigt?

Um dies umzusetzen gibt es Software-Lösungen. Diese sind bereits seit Jahren ausgereift und meist auch unabhängig zertifiziert. Viele dieser Lösungen haben heute schon einfach zu bedienenden Oberflächen, leistungsfähige Datenbanken und ermöglichen die einfache Integration mit diversen E-Mail-Servern. So kann jede eingehende und ausgehende E-Mail vor der Zustellung an den Empfänger in unveränderlicher Weise archiviert werden. Auffindbar sind die E-Mails dann wieder über eine leistungsfähige webbasierte Suche oder eine Outlook-Integration.

Datenschutz im Fuhrparkmanagement

Viele Unternehmen, Vereine und Verbände ab einer gewissen Größe halten einen eigenen Fuhrpark für ihre Mitarbeiter bereit. Oft sind die Wagen einzelnen Mitarbeitern als Firmenwagen zugeordnet, oft stehen sie aber auch in einem Pool demjenigen zur Verfügung der gerade ein Fahrzeug benötigt. Die folgenden 5 Empfehlungen sollen Ihnen helfen, Datenschutz in Ihrem Fuhrpark besser umzusetzen.

Verträge und Richtlinien

Im Rahmen der Dienstwagenüberlassung sollte darauf geachtet werden, dass sowohl Überlassungsverträge als auch Car-Policies erstellt und verwaltet werden. Dienstwagenregelungen können entweder innerhalb der Arbeitsverträge oder als separate Dienstwagenüberlassungsverträge realisiert werden. Diese werden vom Fuhrparkmanagement für Unbefugte unzugänglich aufbewahrt (Abgeschlossene Schränke, passwortgeschützte elektronische Zugänge).

Nachweisbarkeit der Fahrzeugnutzung

Man muss geeignete organisatorische Maßnahmen ergreifen, um die konkrete Fahrzeugnutzung nachvollziehen zu können. Es ist unabdingbar, dass ein Fahrer bei gutem Willen und sachgerechter Organisation und Dokumentation der innerbetrieblichen Abläufe identifiziert werden kann. (Wer hat welches Fahrzeug zu welchem Zeitpunkt genutzt?)

Kontrollen der Führerscheine

Einsicht in die Führerscheine ist erlaubt. Auch Fotokopien der Führerscheine, zur Durchführung der Führerscheinkontrolle zu erstellen, ist durchaus rechtens. Der Personalausweis darf nicht kopiert oder eingescannt werden. Relevante Ausweisdaten dürfen abgeschrieben und notiert werden. Achtung: Die Berechtigungsnummer der neuen Ausweise zählt niemals dazu! Es dürfen nur solche Mitarbeiter des Fuhrparkmanagements auf die Führerscheindaten zugreifen, die diese zur Ausübung ihrer betriebsinternen Aufgaben benötigen.

Rechtsgültige Einwilligungen

Der Dienstwagenberechtigte sollte ferner vor Übergabe des Fahrzeugs schriftlich darauf hingewiesen werden, welche Daten bei der Fahrzeugnutzung automatisiert anfallen. Dazu zählen Telematik, Navigationsgerät, Tankkartenbenutzung, etc. Diese lassen theoretisch Rückschlüsse auf Bewegung, Fahrweise (Verbrauch) usw. zu.

Der Nutzer sollte hierzu freiwillig einwilligen und per Unterschrift bestätigen. Dies kann auch über eine Betriebs- oder Dienstvereinbarung geregelt sein. Die Einwilligungen sind ebenfalls zusammen mit den Dienstwagenunterlagen unter Verschluss zu halten.

Betriebsvereinbarungen

Die Einführungen von technischen Einrichtungen im Dienstwagen, die Aufschluss über Verhalten und /oder Leistung des Fahrers geben können (Autotelefon, Navigationssyste-

me, freiwillige Fahrtenschreiber, Unfalldatenschreiber, etc.) unterliegen der Mitbestimmungspflicht. Diese müssen mit dem Betriebsrat in Betriebsvereinbarungen geregelt werden. Im öffentlichen Recht kommen hier alternativ Dienstvereinbarungen in Betracht.

3 Tipps zur Vereinsarbeit auf privaten Computern

Da viele Vereine die „Vereinsarbeit" auch auf privaten Computern durch Mitglieder/Vorstandsmitglieder durchführen lassen, sollten Sie sich den folgenden Beitrag zu Herzen nehmen.

Hackerangriffe, Datenlecks, Ransomware– Wie kann man sich als privater Nutzer vor den zahlreichen Risiken aus dem Internet schützen? Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierzu eine Handreichung herausgegeben, die es Nutzern ermöglichen soll, die Risiken weitgehend einzuschränken. Wir stellen diese Handreichung vor.

Handreichung des BSI

Gibt es einen hundertprozentigen Schutz gegen die Gefährdungen aus der Online-Welt? Nein. Allerdings können Nutzer vieles tun, um die Risiken für sich und ihre Daten weitgehend einzuschränken. Ziel ist es, es einem potentiellen Angreifer so schwer wie möglich zu machen.

Die Handreichung des BSI stellt einen guten Anfang hierfür dar – so zu sagen das Einmal eins im Umgang mit dem Computer. Die Handreichung ist eingeteilt in

- sog. „Kernmaßnahmen", die sich jeder Nutzer dringend zu Herzen nehmen soll, und in
- sog. „ergänzende Maßnahmen", die eher ein nice-to-have sind.

Kernmaßnahmen

Updates

Hersteller von Betriebssystemen und Software (z.B. Internet-Browser, Office, Adobe Reader, Quick Time) bieten, die Möglichkeit, automatisch Sicherheitsupdates zu installieren. Ob sie diese Updates automatisch oder manuell installieren soll ihnen überlassen sein. Es empfiehlt sich jedoch diese Updates regelmäßig zeitnah zu installieren, da diese Sicherheitslücken im Betriebssystem oder in der Software beheben und das System auf aktuellen Stand halten.

Virenschutz

Gleiches gilt für den Virenschutz auf Ihrem Computer. Sie sollten ihr Virenschutzprogramm stets auf dem aktuellen Stand halten, um so der Schnelllebigkeit von Viren entgegentreten und ihre System bestmöglich schützen zu können.

Bei der Wahl eines Virenscanner sollte auch auf eine gute Heuristik-Funktion geachtet werden, wodurch Gefahren erkannt und bekämpft werden, bevor es eine entsprechende Virensignatur gibt. Dies ermöglicht es noch unbekannte Schadprogramme proaktiv zu identifizieren und zu bekämpfen.

Firewall

Jeder Nutzer sollte außerdem die Firewall seines Systems nutzen. Diese sind heutzutage bei Betriebssystemen teilweise vorinstalliert und schützen den einzelnen Computer oder ein Rechnernetz vor unerwünschten Angriffen von außen.

Die Firewall dient insofern als der Wächter zu Ihren Daten, indem sie alle Verbindungen des Computers in andere Netzwerke kontrolliert. Dabei wird auch der Datenfluss in und aus dem Internet auf Ihren Rechner überprüft. Sofern die systemseitige Firewall den Verkehr nach außen nicht überwacht, sollte man darüber nachdenken, eine alternative Firewall zu installieren, die auch den abgehenden Verkehr kontrolliert.

Durch eine individuelle Konfiguration der Firewall, bei der Ihnen sicherlich der IT-ler ihres Vertrauens zu Seite stehen kann, kann das Sicherheitsniveau ihres Rechners angepasst werden.

Separate Benutzerkontos

Das BSI empfiehlt außerdem, dass ein Nutzer selbst für seinen privaten Computer ein separates Benutzer-Konto einrichten sollte. Dieses Vorgehen ist für Unternehmen stets zu empfehlen und auch für Privatrechner lässt sich das heutzutage sehr leicht einstellen. Ein IT-ler im Unternehmen hat in der Folge sowohl ein reguläres Mitarbeiterkonto als auch ein Administrationskonto. Dies bietet sich insbesondere an, wenn sie viel im Internet surfen, da hier das Risiko für ihre Systeme erhöht ist. So können Sie beispielsweise mittels des Administrationskontos im Falle eines Virenbefalls oder Hackerangriffs noch reagieren, da nur ihr normales Benutzerkonto befallen ist.

Mitdenken ist gefragt

Der wohl wichtigste Tipp des BSI für Nutzer ist gleichzeitig auch der trivialste. Nutzer sollten Vorsicht im Hinblick auf ihr Surfverhalten walten lassen und darüber nachdenken und hinterfragen welchen personenbezogenen Daten Sie herausgeben.

Öffnen Sie also keine Anhänge von Ihnen unbekannten E-Mail-Anschriften oder suspekt vorkommenden Sendern. Klicken Sie nicht jeden Link im Internet an. Achten sie auf vorangekreuzte Auswahlfelder und nutzen Sie vor allen Dingen unterschiedliche und komplexe Passwörter.

Ergänzende Maßnahmen unter dem Stichwort „Prävention"

Zusätzlich zum Einmaleins des Umgangs mit dem Computer, zählt das BSI noch zahlreiche Maßnahmen auf, mit deren Hilfe es potentiellen Angreifern noch schwieriger gemacht werden soll an ihre Daten zu kommen. Prävention ist das Stichwort!

Sichere Passwörter

Das „perfekte" Passwort gibt es nicht – darüber sind wir uns alle einig. Dennoch können Sie Ihr Passwort so sicher wie möglich gestalten. Die Sicherheit eines Passwortes hängt prinzipiell von zwei Faktoren ab: von seiner Komplexität und von seiner Länge.

Das BSI hat auch hier einen Mindeststandard definiert, an dem sich jeder Nutzer orientieren kann:

- mindestens 8 Zeichen, wobei sich die Länge nach dem Schutzbedarf der Daten richten sollte;
- Kombination aus Groß-, Kleinbuchstaben, Sonderzeichen und Ziffern (3 von 4 Kriterien sollten erfüllt sein; technische Umsetzung am Idealsten);
- keine Verwendung von Trivialpasswörtern, die leicht zu erraten sind; bspw. fortlaufende Ziffern, Name des Haustieres, Geburtsdatum, oder einer Kombination dieser;
- keine fortlaufenden Passwörter, bspw. Kennwort-1, Kennwort-2.

Verschlüsselte Verbindung

Wenn Sie sich im Internet befinden, sollten Sie immer sichergehen, dass eine verschlüsselte Verbindung vorhanden ist, wenn Sie persönliche Daten übertragen (bspw. beim Onlineshoppen oder -banking). Jeder Nutzer kann eine sichere Verbindung an Hand des Schlosssymbols im Adressfeld des Browsers einfach identifizieren.

Backups

Außerdem sollte jeder Nutzer regelmäßige Backups seiner Daten durchführen. Hierbei ist jedoch zu beachten, dass dies idealer Weise nicht bloß ein Backup auf der Festplatte des eigenen Rechners sein sollte (bspw. in einer sog. Partition), sondern tatsächlich auf einer externen Festplatte liegen sollte.

Dies hat sich insbesondere im Rahmen diverser sog. Erpressertrojaner („Ransomware") als probates Mittel herausgestellt, da Sie im Fall der Fälle immer noch Zugriff auf Ihre Daten auf dem Backup haben. Das Backup mag vielleicht von gestern sein, aber wenigstens haben Sie Ihre Daten noch.

WLAN – privat und öffentlich

Sollten Sie ein WLAN nutzen, also ein drahtloses Netzwerk, dann sollten Sie sicherstellen, dass dies mittels einer sog. WPA2-Verschlüsselung erfolgt. Handelt es sich außerdem um ein öffentliches Netzwerk bspw. im Café neben an, sollten Sie sich außerdem überlegen, was Sie im Netz machen und welche Daten Sie preisgeben, da Ihre Daten mit relativ einfachen Mitteln von Dritten im WLAN abgefangen werden können.

Eigenverantwortliches Handeln

Jeder Nutzer sollte eigenverantwortlich mit seinen Daten umgehen und versuchen, die Angriffsfläche seines Systems so klein als möglich zu halten. Hundertprozentige Sicherheit wird es allerdings nicht geben.

MEDIEN –TECHNIK – SICHERHEIT

4 Zugangsdaten von gesperrtem PC geklaut

Was soll schon in der Pause passieren, wenn der Bildschirm gesperrt ist? Wie kann ein Angreifer mit einem USB-Stick quasi im Vorbeigehen die Zugangsdaten abziehen?

Wer physischen Zugang zu einem PC hat, kann ihm in aller Regel auch seine Geheimnisse entreißen. Dass dazu jedoch selbst bei einem gesperrten PC bereits 20 Sekunden gegen, ist schon erschreckend. Der unter dem Handle mubix bekannte Sicherheitsforscher Rob Fuller demonstrierte, dass er nur ein Stick-förmiges Device an den USB-Port eines gesperrten Windows-PCs anschließen muss, um die Zugangsdaten eines angemeldeten Benutzers abzuziehen.

Das Prinzip ist einfach: Das USB-Device ist eigentlich ein kleiner Computer, der sich als neues Netzwerk-Interface beim PC anmeldet. Das erkennt Windows auch im gesperrten Zustand und richtet es via DHCP ein. Auf dem Computer am USB-Port läuft ein Linux mit einem speziellen Responder, der auf alle Anfragen antwortet. Unter anderem setzt er sich als Default-Gateway und DNS-Server und preist eine Proxy-Konfigurations-Datei wpad.dat an. In der Folge läuft der Netzwerkverkehr über den angestöpselten USB-Computer. Dort antwortet der Responder auf alle Anfragen und erzwingt eine Authentifizierung. Beim Versuch, sich gegenüber dem Responder auszuweisen, liefert Windows dem Angreifer dann die Login Credentials frei Haus.

USB-Mini-PCs als Einfallstor

In vielen Fällen bekommt der Angreifer damit dann zwar nicht direkt das Passwort, sondern nur dessen Hash. Zumindest die einfachen NTLM-Hashes lassen sich schnell knacken. Doch in vielen Fällen braucht es das gar nicht. Mit der Angriffstechnik Pass-the-Hash kann sich ein Angreifer bei vielen Diensten in Windows-Netzen direkt mit dem abgefangenen Hash ausweisen. Als Basis für diesen Angriff verwendete Mubix einen Hak5 LAN Turtle für etwa 50 Dollar und einen etwas teureren USB Armory. Der Diebstahl gelang mit einer Vielzahl von Systemen von Windows XP bis hin zu Windows 10 Home und Enterprise. Interessanterweise berichtet er, dass er auf diesem Weg sogar einem Mac mit El Capitan Login Credentials entlocken konnte; zu näheren Details dazu lässt er sich jedoch nicht aus.

5 Neue Schadsoftware befällt Android-Geräte

Drei Viertel aller Android-Geräte sind gefährdet: Die schadhafte Software Gooligan hat mehr als eine Million Google-Konten attackiert. Und sie installiert ungefragt Apps.

Die israelische Sicherheitsfirma Check Point warnt vor einer Schadsoftware, die Android-Geräte befällt und Google-Konten angreift. Die Malware mit Namen Gooligan hat demnach weltweit bereits mehr als eine Million Google-Nutzerkonten gehackt.

Das Programm zielt auf Android-Smartphones und -Tablets, auf denen die Betriebssystemversionen Android 4 (Jelly Bean, KitKat) oder 5 (Lollipop) installiert sind. Die Systeme laufen nach aktuellem Stand auf ungefähr drei von vier Android-Geräten. Check Point hat eigenen Angaben zufolge Google nach Entdeckung des Schadcodes umgehend informiert.

Check Point zufolge werden seit Ende August jeden Tag weltweit mehr als 13.000 neue Android-Geräte von der Malware befallen. Das Programm verstecke sich in Dutzenden legitim anmutenden Apps, die auf alternativen Downloadplattformen angeboten werden. Damit werde der Schadcode vom Nutzer selbst auf den Geräten installiert. Außerdem versuchten die Täter, ihre Schadsoftware über falsche Links in SMS oder Messaging-Nachrichten zu verbreiten.

Betroffene Dienste sind Gmail, Docs und G Suite

Gooligan versucht dann, sich über mehrere bekannte Schwachstellen weitreichende Zugriffsrechte einzuräumen, schreibt Check Point weiter. So könnten Angreifer Apps, Daten und die Hardware des Geräts aus der Ferne kontrollieren.

Der Schadcode erfasst zu Google-Diensten passende E-Mail-Adressen und entsprechende Authentifizierungs-Token. Die Token, die lokal auf einem Gerät gespeichert werden, identifizieren den Nutzer und loggen ihn automatisch in einen Dienst ein. Haben Kriminelle Zugang zu den Token, kommen sie auch ohne Passwort in ein Benutzerkonto. Betroffen sind Google-Services wie Gmail, Google-Drive, Google Docs, Google Play, Google Photos und G-Suite.

Einige der kompromittierten E-Mail-Adressen gehörten laut Check Point zu Finanzdienstleistern und Unternehmen. Aber auch Bildungseinrichtungen und Regierungsbehörden sollen in einigen Ländern betroffen sein. Google selbst habe bisher allerdings keine Hinweise darauf, dass persönliche Daten von Nutzern kompromittiert wurden, heißt es in einem Blogeintrag.

Fast zehn Prozent der infizierten Geräte befinden sich dem Unternehmen zufolge in Europa, mehr als 55 Prozent in Asien. "Dieser Diebstahl von über einer Million Google-Kontodaten ist beispiellos und stellt die nächste Stufe der Cyberangriffe dar", sagt Michael Shaulov, der bei Check Point für Cloud- und Mobilsicherheit verantwortlich ist.

Der Schadcode lädt Check Point zufolge außerdem weitere Apps aus Googles Play-Store. Diese werde dann vom Nutzer unbemerkt im Hintergrund ausgeführt. Sicherheitsexperten gehen davon aus, dass täglich 30.000 Apps installiert werden.

Ähnlich wie andere Schadprogramme soll Gooligan auch Daten zur Geräteidentifizierung fälschen, um eine App mehrmals herunterzuladen. Die Malware soll außerdem in Googles App-Store eine positive Bewertung der heruntergeladenen App hinterlassen. Bei Google sind bereits neue Schutzmechanismen in die Verify-Apps-Technologie eingebaut worden.

Check Point bietet unter dem Link https://gooligan.checkpoint.com/ ein kostenloses Online-Tool an, mit dem Android-Nutzer prüfen können, ob sie betroffen sind. Sollte ein Konto gehackt worden sein, sei eine einwandfreie Neuinstallation des Betriebssystems nötig. Das Sicherheitsunternehmen empfiehlt, diesen Flashing genannten Vorgang von einem zertifizierten Techniker oder dem Mobilfunkprovider vornehmen zu lassen. Danach sollten sämtliche Google-Passwörter geändert werden. Zudem sollten Nutzer Googles offiziellen Play-Store nutzen und einen Virenscanner installieren.

GESETZGEBUNG

6 Änderungen zum AGB-Recht

Wir berichteten bereits darüber, dass seit dem 24.02.2016 Datenschutzverstöße von Verbänden und sog. Abmahnvereinen geahndet werden können. Die Grundlage dafür war ein neues Gesetz, welches nun in einer zweiten Stufe für Änderungen im AGB-Recht sorgt. Diese Änderungen müssen bereits zum 01.10.2016 umgesetzt sein, denn dann tritt dieses Gesetz in Kraft. Reagieren Sie nicht rechtzeitig, so können Sie abgemahnt werden.

Rechtliche Grundlage

§ 309 Nr. 13 BGB in der alten Fassung gültig bis 30.09.2016

> eine Bestimmung, durch die Anzeigen oder Erklärungen, die dem Verwender oder einem Dritten gegenüber abzugeben sind, an eine strengere Form als die Schriftform oder an besondere Zugangserfordernisse gebunden werden;

§ 309 Nr. 13 BGB in der neues Fassung gültig ab 01.10.2016

> Auch soweit eine Abweichung von den gesetzlichen Vorschriften zulässig ist, ist in Allgemeinen Geschäftsbedingungen unwirksam
>
> eine Bestimmung, durch die Anzeigen oder Erklärungen, die dem Verwender oder einem Dritten gegenüber abzugeben sind, gebunden werden
>
> a) an eine strengere Form als die schriftliche Form in einem Vertrag, für den durch Gesetz notarielle Beurkundung vorgeschrieben ist oder
> b) an eine strengere Form als die Textform in anderen als den in Buchstabe a genannten Verträgen oder
> c) an besondere Zugangserfordernisse.

Nach der alten Fassung waren Klauseln unwirksam, die für eine Anzeige oder Erklärung des Verbrauchers eine strengere Form als die Schriftform (§ 126 BGB) vorsahen. Nunmehr darf keine strengere Form als die Textform i.S.v. § 126b BGB vereinbart werden. Der Textform genügt u.a. eine E-Mail oder ein Fax.

Was heißt das für Sie in der Praxis?

In der Praxis bedeutet das, dass Klauseln wie

- Die Kündigung des Vertrages bedarf der Schriftform

oder in einer AGB-Klausel zum Eigentumsvornehalt

- Der Kunde hat den Verkäufer unverzüglich in Schriftform zu benachrichtigen, wenn und soweit Zugriffe Dritter auf die Waren des Verkäufers erfolgen

sowie ähnliche AGB-Klauseln ab 01.10.2016 abgemahnt werden können. Sie sollten Ihre AGB also auf derartige Klauseln überprüfen.

Übergangsregelung für Altverträge

Altverträge sind übrigens nicht betroffen. Hier hat der Gesetzgeber eine Übergangsregelung geschaffen. Diese wurde in Art. 229 § 37 EGBGB normiert. Unabhängig davon, wäre es einem Abmahner ohnehin kaum möglich gewesen Altverträge abzumahnen. Schließlich werden Verträge in der Regel nicht öffentlich.

Fazit

Prüfen Sie – sofern Sie dies noch nicht getan haben – Ihre AGB und lassen Sie im Zweifelsfall einen Rechtsanwalt die Lage beurteilen.

7 Aktueller Status EU-DSGVO

Mit der Datenschutz-Grundverordnung sollte der Datenschutz EU-weit auf das deutsche Niveau angehoben werden. Doch das Innenministerium nimmt die Anpassung des Bundesdatenschutzgesetzes zum Anlass, den deutschen Datenschutz in vielen Bereichen abzuschwächen. Das geht aus einem neuen Leak des Gesetzesentwurfs hervor.

Nach jahrelanger Debatte trat im Mai die europäische Datenschutz-Grundverordnung (DSGVO) in Kraft, mit der laut Wikipedia „die Regeln für die Verarbeitung von personenbezogenen Daten […] EU-weit vereinheitlicht werden". Als Verordnung gilt sie unmittelbar in allen EU-Mitgliedstaaten, dennoch enthält sie „verschiedene Öffnungsklauseln, die es den einzelnen Mitgliedstaaten ermöglichen, bestimmte Aspekte des Datenschutzes auch im nationalen Alleingang zu regeln". Diese Anpassung des deutschen Bundesdatenschutzgesetzes (BDSG) an die EU-Verordnung wird derzeit vom Innenministerium erarbeitet, im September wurde ein erster Entwurf veröffentlicht. Jetzt hat das Innenministerium seinen Referentenentwurf fertig gestellt und an Verbände geschickt.

Auch dieser Entwurf ist ein „Datenschutzverhinderungsgesetz". Zwar gibt es minimale Verbesserungen gegenüber dem breit kritisierten ersten Entwurf. Dem stehen aber weiterhin Einschränkungen der Kontrollbefugnisse der Datenschutzbeauftragten, fehlende Sanktionsmöglichkeiten und eine Beschränkung der Auskunftsansprüche von Bürgern entgegen. Hinzu kommt, dass die Ausweitung der Videoüberwachung, die noch in das alte Bundesdatenschutzgesetz einfließen soll, auch Teil dieser Gesetzesnovelle werden wird.

Auskunftsansprüche von Betroffenen eingeschränkt

Die Deutsche Vereinigung für Datenschutz (DVD) kritisiert, dass der Entwurf „alte und teilweise auch neue europarechts- und verfassungswidrige inakzeptable Regelungen" enthalte. Beispiel ist eine Beschränkung der Kontrollbefugnis der Datenschutzaufsichtsbehörden auf technische Aspekte bei Berufsgeheimnisträgern wie z. B. Ärzten, Psychologen und Anwälten. Dringend nötige Regelungen zum Schutz der Berufsgeheimnisse unterblieben dagegen. Die Einschränkungen des Auskunftsanspruchs der Betroffenen mit

Argumenten der Sicherheit sowie des Schutzes von Betriebs- und Geschäftsgeheimnissen verletze das verfassungsmäßige Grundrecht auf Datenschutz.

Kritik am Entwurf

Der Entwurf ist eher ein Datenschutzverhinderungsgesetz. Das Bundesjustiz- und Verbraucherministerium, das Bundeswirtschafts- sowie das Bundesforschungsministerium müssen unbedingt umgehend intervenieren, da die Zeit für eine rationale Gesetzgebung in dieser Legislaturperiode ausläuft und grundlegende verfassungsrechtliche Notwendigkeiten sowie die Belange von Wirtschaftsunternehmen, Verbrauchern und Forschung ignoriert werden.

Kritisiert werden auch die weiterhin enthaltenen Beschränkungen der Prüf- und Berichtsbefugnis der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) im Geheimdienstbereich und die Beschränkung der Sanktionsmöglichkeiten der BfDI in den Bereichen Polizei und Justiz.

Gesetz schwächt den Datenschutz

Auf der diesjährigen „Das ist Netzpolitik!"-Konferenz kritisierte der ehemalige Bundesdatenschutzbeauftragte Peter Schaar schon den ersten Referentenentwurf heftig. Insgesamt sei von dem viel zitierten hohen deutschen Datenschutzstandards in dem Entwurf nichts zu spüren. In der aktuellen Form würde das Gesetz den Datenschutz schwächen, wo es nur gehe, so Schaar. Die Öffnungsklauseln der Datenschutzgrundverordnung würden genutzt, um die Befugnisse von datenverarbeitenden Stellen auszuweiten und die Rechte von Betroffenen einzuschränken. „Mit der Verpflichtung zu einem möglichst hohen Datenschutzniveau hat das nichts zu tun." Schaars Befürchtung: Wenn gerade Deutschland, dessen datenschutzrechtliches Niveau bislang als vergleichsweise hoch galt, jetzt ein solches Gesetz beschließt, das nicht nur unter das Schutzniveau der DSGVO, sondern auch unter das bisherige deutsche Niveau falle, wird dies Signalwirkungen für andere Länder haben.

Ausweitung der Videoüberwachung

Im Entwurf enthalten ist nun auch die Ausweitung der Videoüberwachung. Innenminister Thomas de Maizière will Stadien, Einkaufszentren, Diskotheken und andere Orte des öffentlichen Lebens stärker mit Kameras überwachen. Mit dem so genannten Videoüberwachungsverbesserungsgesetz soll das Aufstellen und Betreiben von optisch-elektrischen Überwachungsanlagen deutlich erleichtert werden, weil die allgemeine Sicherheitslage in die Abwägung mit einfließen soll, ob eine Kamera aufgestellt wird. Das Gesetz wird noch in die alte Fassung des BDSG einfließen und dann in der Novelle übernommen werden.

Kritik am Videoüberwachungsverbesserungsgesetz

Bei den materiellen Regelungen versucht das BMI eine vom Bundesgesetzgeber noch gar nicht verabschiedete Vorschrift zur Videoüberwachung nach Wirksamwerden der DSGVO

fortzuschreiben, mit welcher Sicherheitsbelangen der Vorrang vor dem Datenschutz eingeräumt wird und für die der nationale Gesetzgeber überhaupt keine Regelungsbefugnis hat.

Im Videoüberwachungsverbesserungsgesetz wird auch mit der Prävention von Straftaten und Terrorismus argumentiert. Für eine präventive Wirkung von Überwachungskameras gibt es jedoch keine empirischen Belege.

8 Videoüberwachung zwischen BDSG und EU DSGVO

Die Datenschutz-Grundverordnung (DSGVO) enthält viele Neuerungen, die nicht nur Unternehmen und Behörden, sondern auch den deutschen Gesetzgeber vor große Herausforderungen stellt. Erste Hilfe gibt ein Rechtsgutachten im Auftrag des Bundesministeriums des Innern (BMI), das die Neuregelungen und Veränderungen im Vergleich zum BDSG analysiert. Heute soll der Aspekt der Videoüberwachung näher beleuchtet werden.

Rechtsgutachten zum innerstaatlichen Regelungsbedarf

Die DSGVO verfolgt das Ziel, das europäische Datenschutzrecht auf eine einheitliche Grundlage zu stellen. Durch zahlreiche Öffnungsklauseln belässt sie den Mitgliedsstaaten aber teilweise große Regelungsspielräume. Öffnungsklauseln sind Ausnahmen von den verbindlichen Vorgaben der DSGVO, die es den Mitgliedstaaten ermöglichen, in bestimmten Bereichen eigene Regelungen zu erlassen.

Das stellt die Gesetzgeber vor eine große Aufgabe. Denn zum Stichtag am 25. Mai 2018 müssen die Öffnungsklauseln ausgefüllt und die nationalen Gesetze an die DSGVO angepasst sein. Das betrifft auch das Bundesdatenschutzgesetz (BDSG), sofern es als solches bestehen bleibt.

Im Juni erschien ein umfassendes Rechtsgutachten im Auftrag des BMI, das die verschiedenen Öffnungsklauseln der DSGVO und die notwendigen Anpassungen des BDSG analysiert. Wir widmen uns in diesem Beitrag dem Aspekt der Videoüberwachung.

Videoüberwachung

Gesetzliche Regelung nach dem BDSG

Die Videoüberwachung öffentlich zugänglicher Räume richtet sich bisher nach § 6b BDSG. Für sonstige Überwachungsmaßnahmen, insbesondere in privaten Räumen gilt daneben der Erlaubnistatbestand des § 28 Abs. 1 S. 1 Nr. 2 BDSG. Im Arbeitsverhältnis richten sich Überwachungsmaßnahmen nach der Sondervorschrift des § 32 Abs. 1 BDSG.

§ 6b Abs. 1 BDSG erlaubt die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung), soweit sie

- zur Aufgabenerfüllung öffentlicher Stellen,
- zur Wahrnehmung des Hausrechts oder

- zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

§ 6b Abs. 2 bis 5 BDSG enthält daneben Sonderregelungen zur Hinweispflicht, zur Nutzung der durch die Überwachung gewonnenen Daten, zur notwendigen Benachrichtigung Betroffener und zur Löschung der gewonnenen Daten.

Neuregelung nach der DSGVO

Die Datenschutz-Grundverordnung enthält keine speziellen Regelungen für Maßnahmen der Videoüberwachung. Ihre Zulässigkeit richtet sich daher nach den allgemeinen Zulässigkeitsvorschriften der Art. 5 DSGVO und Art. 6 DSGVO.

Art. 6 Abs. 1 lit. e), Abs. 2 und 3 DSGVO sieht eine Öffnungsklausel für Datenverarbeitungen vor, die für die Wahrnehmung einer Aufgabe erforderlich sind, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. In diesem Bereich dürfen die Mitgliedsstaaten also selbst Regelungen erlassen.

Im Übrigen richtet sich die Zulässigkeit der Videoüberwachung nach Art. 6 Abs. 1 lit. f) DSGVO. Demnach ist eine Datenverarbeitung grundsätzlich dann rechtmäßig, wenn sie zur Wahrung berechtigter Interessen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten des Betroffenen überwiegen.

Vorgaben zur Transparenz, zur Benachrichtigung und zur Löschung enthalten in dem Zusammenhang nur die allgemeinen Normen des Art. 5 Abs. 1 lit. a), Art. 12 ff., 13 und Art. 17 Abs. 1 lit. a) DSGVO.

Schließlich ist als Neuerung bei der systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche gemäß Art. 35 Abs. 3 lit. c) DSGVO nunmehr grundsätzlich eine Datenschutzfolgenabschätzung nötig. Diese löst die nach deutschem Recht unter den Voraussetzungen des § 4d Abs. 5 BDSG erforderliche Vorabkontrolle ab.

Konsequenzen für das BDSG

Nach Ansicht der Verfasser des Gutachtens könnte aufgrund der Öffnungsklausel in Art. 6 Abs. 1 lit. e), Abs. 2 und 3 DSGVO insbesondere die Zulässigkeitsvorschrift des § 6b Abs. 1 Nr. 1 BDSG im Bereich der öffentlichen Aufgabenerfüllung beibehalten werden.

§ 6b Abs. 1 Nr. 2 und Nr. 3 BDSG werden aufgrund der vorrangigen Regelungen der Datenschutz-Grundverordnung aber entfallen. Die Videoüberwachung zur Wahrung des Hausrechts und berechtigter Interessen richtet sich damit zukünftig allein nach Art. 6 Abs. 1 lit. f) DSGVO.

Gleiches gilt für die Sonderregeln hinsichtlich der Transparenz und Benachrichtigungspflicht. In diesen Bereichen eröffnen sich für den deutschen Gesetzgeber keine Regelungsspielräume.

Die Videoüberwachung wird daher weitgehend verbindlich durch die Datenschutz-Grundverordnung geregelt. Hier bestehen aber keine speziellen, sondern nur die allgemeinen Zulässigkeitstatbestände der Art. 5 und 6 DSGVO.

Ausblick

Es bleibt spannend, wie sich die Rechtsprechung in dem Bereich zukünftig entwickeln und zu einer Konkretisierung der allgemeinen Normen beitragen wird.

AKTUELLE URTEILE

9 Social-Media-Nutzung durch Arbeitgeber: Facebook-Auftritt nur mit Zustimmung des Betriebsrats

Von Michael Fuhlrott

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

Auf Social Media Plattformen präsent zu sein, ist besonders für größere Arbeitgeber heute oft eine Selbstverständlichkeit. Dabei hat der Betriebsrat nach einer Entscheidung des BAG jedoch ein gutes Wörtchen mitzureden.

Das Bundesarbeitsgericht (BAG, Beschl. v. 13.12.2016, Az. 1 ABR 7/15) hatte sich am Dienstag zur arbeitsrechtlichen Zulässigkeit der Facebook-Präsenz eines bundesweit vertretenen Transfusionszentrums mit rund 1.300 Mitarbeitern zu äußern. Konkret ging es um die Frage, ob das Betreiben der Internetseite mit Kommentarfunktion, Gästebuch und abrufbaren Informationen durch den Arbeitgeber Beteiligungsrechte des Betriebsrats gem. § 87 Abs. 1 Betriebsverfassungsgesetz (BetrVG) auslöst.

Dies machte der Betriebsrat mit einem Unterlassungsbegehren geltend. In dem Betrieb der Seite erblickte er einerseits eine mitbestimmungspflichtige Verhaltenssteuerung der Arbeitnehmer (§ 87 Abs. 1 Nr. 1 BetrVG); andererseits fürchtete er, dass damit eine Überwachung des Leistungsverhaltens der Arbeitnehmer (§ 87 Abs. 1 Nr. 6 BetrVG) einhergehen könne. Das BAG gab ihm damit nun Recht und hob die noch anders lautende Entscheidung der Vorinstanz auf.

Facebook-Präsenz als Werbemedium

Worum ging es genau? Der sich mit seinem Betriebsrat streitende Arbeitgeber nutzte seine Facebook-Präsenz als Kommunikationsplattform zu Kunden. So wurde online etwa über anstehende Blutspendetermine informiert, über besondere Aktionen berichtet, für die Abgabe von Blutspenden geworben und Abläufe einer Blutspende und deren Notwendigkeit für die medizinische Versorgung in Deutschland erläutert.

Die Mitarbeiter wurden über die bestehende Facebook-Präsenz durch ein Rundschreiben des Arbeitgebers informiert. Ein den Arbeitnehmern ausgehändigter Leitfaden „Wie stelle ich das DRK dar" hielt sie zudem zur Wahrung der „Rotkreuzgrundsätze" und der Netiquette an. Die Pflege der Facebook-Seite nahm der Arbeitgeber mit einem Team von rund 10 Arbeitnehmern wahr, die die Inhalte der Seite jeweils aktualisieren und insbesondere Gästebucheinträge kommentieren sollten.

Mitarbeitersteuerung durch Nutzerkommentare?

Nachdem es Einträge über das Verhalten bestimmter Mitarbeiter gab („Ich war am 14.4.2013 in N. mein kostbares abzapfen lassen. Gehe schon spenden seit ich 18 bin. Muss aber sagen die gestern die Nadel gesetzt hat, solle es noch lernen. Stechen kann die nicht"), und Mitarbeiter ihre Bedenken gegenüber dem Betriebsrat äußerten, verlangte dieser vom Arbeitgeber die Abschaltung der Seite.

Der Betriebsrat sah die Gefahr, dass der Arbeitgeber gezielt nach Arbeitnehmern mit häufigen negativen Bewertungen suchen und diese dann sanktionieren könne. Jedenfalls müsse der Arbeitgeber aber mit dem Betriebsrat die Inhalte der Seite abstimmen, wenn er diese weiter nutzen wolle. Der Arbeitgeber lehnte dies ab und betrieb die Seite weiterhin. Das daraufhin vom Betriebsrat angerufene Arbeitsgericht Düsseldorf (Beschl. v. 27.06.2014, Az. 14 BV 103/13) gab der Arbeitnehmervertretung Recht und verpflichtete den Arbeitgeber zur Abschaltung der Seite. Dem kam der Arbeitgeber nicht nach und legte gegen die erstinstanzliche Entscheidung Berufung zum Landesarbeitsgericht Düsseldorf (Beschl. v. 12.1.2015, Az. 9 Ta BV 51/14) ein, das wiederum dem Arbeitgeber Recht gab.

LAG: Keine Überwachung durch Kommentarfunktion

Insbesondere konnte das LAG Düsseldorf kein Beteiligungsrecht gem. § 87 Abs. 1 Nr. 6 BetrVG erkennen. Nach dieser Vorschrift ist der Betriebsrat zu beteiligen, wenn der Arbeitgeber eine technische Einrichtung betreibt, die eine Überwachung des Verhaltens oder der Leistung des Arbeitnehmers ermöglicht. Klassische Anwendungsfälle sind nach der Rechtsprechung etwa Stempeluhren oder Zugangskontrollsysteme. Aber auch die Nutzung bestimmter Office-Software, die die Zugriffs- und Bearbeitungszeitpunkte protokolliert oder selbst eine im Lagerbereich installierte Videokamera, die Arbeitnehmer bei der Arbeit filmt, kann der Norm unterfallen.

Facebook hingegen sei keine solche technische Einrichtung, die der Mitbestimmung bedürfe. Voraussetzung hierfür sei nämlich, dass die Überwachung durch die technische Einrichtung selbst erfolge. Hieran fehle es aber, wenn der Arbeitgeber bei Mitarbeitern mit den Facebook-eigenen Möglichkeiten gezielt nach negativen Einträgen suche, so das LAG.

LAG: Facebook-Präsenz tangiert betriebliche Ordnung nicht

Auch ein vom Betriebsrat gerügtes Beteiligungsrecht gem. § 87 Abs. 1 Nr. 1 BetrVG konnten die Richter nicht erkennen. Um dies zu bejahen, müsse das Verhalten der Arbeitnehmer im Betrieb betroffen sein, also Fragen des betrieblichen Zusammenlebens und Zusammenwirkens der Arbeitnehmer im Betrieb.

Die Rechtsprechung trennt hierbei zwischen dem sog. mitbestimmungspflichtigen Ordnungsverhalten und dem mitbestimmungsfreien Leistungsverhalten. Fragen wie Rauchverbote im Betrieb, die Nutzung von Radios im Büro oder das Tragen einer Uniform sind Ordnungsverhalten. Mitbestimmungsfreies Leistungsverhalten betrifft hingegen die Ausfüllung der Arbeitspflicht. Der Betrieb der Facebook-Präsenz tangiere das Ordnungsverhalten nicht, hinsichtlich der Anweisungen an die Administratoren zur Pflege der Seite liege reines Leistungsverhalten vor.

BAG gibt Betriebsrat auf ganzer Linie Recht

Das Bundesarbeitsgericht schlug sich mit seiner heutigen, bislang nur in Kurzform als Pressemitteilung vorliegenden Entscheidung auf die Seite des Betriebsrats. Zwar könne der Arbeitgeber das Facebook-Profil weiterbetreiben. Allerdings dürfe er die Funktion

„Besucher-Beiträge" so lange nicht nutzen, bis mit dem Betriebsrat hierüber eine Einigung erzielt worden sei.

Mitbestimmungspflichtig sei nämlich die Entscheidung des Arbeitgebers, Postings der Besucher unmittelbar zu veröffentlichen. Diese Entscheidung sei geeignet, das Verhalten oder die Leistung der Arbeitnehmer zu beeinflussen. Damit liege eine Überwachung der Arbeitnehmer durch eine technische Einrichtung i.S.v. § 87 Abs. 1 Nr. 6 BetrVG vor, die der betrieblichen Mitbestimmung unterliege.

Homepage mit oder ohne Interaktionsmöglichkeit

Die aktuelle Entscheidung beweist, dass es auf die jeweiligen Einzelfallumstände der Internetpräsenz ankommt. So ist eine Arbeitgeber-Homepage ohne Interaktionsmöglichkeit betriebsverfassungsrechtlich regelmäßig nicht zu beanstanden. Soweit eine Interaktion zulässig und durch Einträge oder sonstige Anmerkungen eine Beeinflussung des Verhaltens einzelner Arbeitnehmer möglich ist, greifen jedoch auch die Beteiligungsrechte des Betriebsrats ein.

Daher wäre z.B. ein „Abstimmungstool" im Internet zur Wahl eines Mitarbeiters des Monats oder zur allgemeinen Mitarbeiterbewertung zweifellos als technische Einrichtung zur Überwachung des Arbeitsverhaltens zu werten. Diese dürfte ein Arbeitgeber nicht ohne Beteiligung des Betriebsrats nutzen.

Auch ohne Betriebsrat: Keine „Narrenfreiheit" für Arbeitgeber im Internet

Unabhängig davon besteht natürlich auch in Unternehmen ohne Betriebsrat keine „Narrenfreiheit" für Arbeitgeber.

Das Datenschutzrecht und das Persönlichkeitsrecht gelten auch dort, wo es keinen Betriebsrat gibt. Daher müssen Fotos, Filme oder Aufnahmen von Arbeitnehmern im Internet generell vom Arbeitnehmer freigegeben werden. Dies folgt bereits aus datenschutzrechtlichen Vorgaben, wonach der Arbeitnehmer der Nutzung von eigenen Fotos ausdrücklich zustimmen muss.

Zum Autor: Der Autor Prof. Dr. Michael Fuhlrott ist Professor für Arbeitsrecht und Studiendekan Wirtschaftsrecht an der Hochschule Fresenius sowie Fachanwalt für Arbeitsrecht und Partner bei der Römermann Rechtsanwälte AG in Hamburg.

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