DOSB FÜHRUNGS AKADEMIE

FA Datenschutzportal

DSP Info-Brief

Nr. 47 / Juni 2017

INHALT

DATENSCHUTZPORTAL INTERN

IN DER DISKUSSION – NEUIGKEITEN RUND UM DEN DATENSCHUTZ

MEDIEN –TECHNIK – SICHERHEIT

GESETZGEBUNG

AKTUELLE URTEILE

Herausgeber
Führungs-Akademie des DOSB

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

Technische Umsetzung
Führungs-Akademie des DOSB

Redaktion
Toni Niewerth / Robert Graf

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

DATENSCHUTZPORTAL INTERN

Die Themen im Live-Chat vom 30.06.2017

1.1 Fragen zur rechtssicheren Archivierung von E-Mails

Seit 1.1.2017 besteht laut GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff) eine laut GoBD Archivierungspflicht für alle E-Mails. Was bedeutet das konkret für Sportvereine?

F 1 Müssen alle eingehenden und ausgehenden E-Mails rechtssicher archiviert werden oder nur bestimmte?

AW R. Graf
Laut GoBD müssen alle steuerrechtlich relevanten E-Mails revisionssicher archiviert werden. Diese Regelung gab es bereits seit 2001 (GdPdU nach §§ 146 und 147 AO) und wird in den GoBD ebenfalls gefordert.

Bitte beachten Sie auch, dass die GoBD nur die steuerrechtlichen Aspekte der Archivierung von Daten im Allgemeinen und E-Mails im Besonderen aufgreift. Daneben gilt es, die Archivierungsvorgaben weiterer gesetzlicher Regelungen zu beachten, so z.B. aus dem BDSG, dem Zivil- oder Arbeitsrecht.

Im Verein wird es vermutlich eine mehr oder minder große Anzahl von E-Mails geben, die steuerlich nicht relevant sind. Zu überlegen ist, wie hier eine saubere Trennung erfolgen kann. Möglicherweise ist hier der Einsatz einer automatisierten Software die am wenigsten aufwendige Lösung. Sollten Sie die Archivierung manuell auf der Basis eines Kriterienkatalogs vornehmen, ist es in jedem Falle ratsam, den vom Verein erstellten Kriterienkatalog von einem Steuerberater prüfen zu lassen.

F 2 Wie lange ist die Archivierungsdauer?

AW R. Graf
Die Archivierungsdauer von Daten / E-Mails richtet sich nach den dort verarbeiteten Inhalten und ist dementsprechend sehr unterschiedlich.

Im Portal finden Sie im Bereich „Dokumente" im Ordner *„Aufbewahrungs- und Löschfristen*" drei unterschiedlich ausgerichtete und unterschiedlich umfangreiche Dateien mit bis zu 1400 Aufbewahrungsfristen. Hier sollten Sie in jedem Falle fündig werden.

- ➔ CK_Aufbewahrungsfristen 1_Kleines ABC Aufbewahrungsfristen
- ➔ CK_Aufbewahrungsfristen 2_Medizinische Daten
- ➔ CK_Aufbewahrungsfristen_3_Longlist_2016

F3 Benötigen wir zur Datensicherung ein spezielles Archivierungstool?

AW R. Graf)
Eine revisionssichere Archivierung ohne eine entsprechende Software dürfte zumindest aufwendig sein. Es gibt inzwischen auch eine Reihe von ausgereiften und meist auch unabhängig zertifizierten Software-Lösungen (eine ist z.B. commvault). Viele dieser Lösungen bieten auch einfach zu bedienende 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.

ERGÄNZUNG 1

Ergänzende Informationen aus steuerlicher Sicht vom Steuerexperten Horst Lienig
(Lienig & Lienig Haller, Stuttgart)

Die Thematik geht weit über die Anfrage zur revisionssicheren Archivierung von E-Mails hinaus und betrifft alle steuerlich relevanten Datenbestände.

Seit 2001 haben Betriebsprüfer auf dreierlei Arten das Recht, Unternehmen – und damit auch Vereine und Verbände – zu prüfen.

- Variante 1:
  Zusendung sämtlicher Unterlagen an das Finanzamt; d. h. die Prüfung erfolgt auf dem Amt. Daten müssen in elektronischer Form bereitgestellt werden.
- Variante 2:
  Die Betriebsprüfung findet – dem Namen nach – beim Betrieb statt. Dem Prüfer müssen dann für seinen Laptop die prüfungsrelevanten Daten per CD oder Stick zur Verfügung gestellt werden, damit diese in das Prüfprogramm des Prüfers eingelesen werden können. Dazu bedarf es einer besonderen Schnittstelle in der jeweiligen Software.

  Dem Prüfer wird zudem eine Person im Unternehmen benannt, die auf Wunsch des Prüfers weitere Daten aus der EDV zieht.

- Variante 3:
  Der Prüfer setzt sich selbst an den PC und sucht sich die für ihn notwendigen Daten unmittelbar aus dem PC.

In allen drei Fällen ist es wichtig, dass ein Zugang nur zu den sog. „prüfungsrelevanten" Daten besteht. Zu den prüfungsrelevanten Daten gehört auch der Schriftverkehr, d. h auch E-Mails.

ERGÄNZUNG 2

Wir haben das Thema Archivierung von E-Mails nach den neuen Regelungen der GoBD bereits im Info-Brief 41 (Nov./Dez. 2016) aufgegriffen und auf das Ende der Übergangsfrist zum 31.12.2016 hingewiesen.

Um Ihnen eine schnelle Rückkopplung zum Text und zu den dort eingebundenen LINKS zu ermöglichen, haben wir den Text als Auszug auf der nachfolgenden Seite noch einmal aufgenommen.

„... Vorgaben zur E-Mail-Archivierung – Übergangsregel endet"

Auszug aus DSP Info-Brief 41 (Dez. 2016), S. 8

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 gestützten Erzeugung, beim Empfang, der Übermittlung und Verarbeitung *von buchungsrelevanten Daten*, wie Angeboten, Rechnungen etc.

Hintergrund der Regelung ist, dass Geschäftsvorfälle belegbar sein müssen, weshalb ein bloßes „Liegenlassen" der E-Mails im Eingangsordner den gesetzlichen Anforderungen nicht genügt. Steuerlich relevante E-Mails dürfen weder gelöscht noch verändert werden, und sie müssen 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 bedienende 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.

1.2 Auftragsdatenverarbeitung im Rahmen des DSOB Lizenzmanagement-systems

FRAGE:
Als Spitzenverband sind wir für die Verarbeitung und Weitergabe der personenbezogenen Daten der Trainer A-Lizenzen an den DOSB zuständig. Die Verarbeitung erfolgt zukünftig online über das vom DOSB bereitgestellte Lizenzmanagementsystem. Hierzu haben wir auch einen Vertrag zur Auftragsdatenverarbeitung (die Vorlage des Vertrags kam vom DOSB) mit dem DOSB abgeschlossen.

Die Bearbeitung aller weiteren Lizenzen (Trainer-B usw.) erfolgt ausschließlich in der Verantwortung unserer Landesverbände. Nur diese haben die entsprechenden Daten zur Verarbeitung und Weitergabe zur Verfügung, wir als Spitzenverband haben keinen Zugriff auf diese Daten.

Der DOSB stellt möchte nun auch den Landesverbänden die Möglichkeit zur Verfügung stellen, die Daten online im Lizenzmanagementsystem anzulegen und zu verarbeiten. Die Landesverbände haben dabei weiterhin die gesamte „Datenhoheit" und müssen die Lizenzen nach wie vor alleine verwalten. Aus meiner Sicht ist in diesem Fall der Landesverband die „verantwortliche Stelle".

Nach aktuellem Sachstand geht der DOSB davon aus, dass in dieser Konstellation nur ein Vertrag zur Auftragsdatenverarbeitung zwischen DOSB und uns als Spitzenverband notwendig ist. Es wird abgelehnt, Verträge mit jedem einzelnen unserer Landesverbände abzuschließen.

Da diese Daten von den Landesverbänden direkt an den DOSB weitergeleitet bzw. in die Datenbank eingetragen werden, kann ich mir nicht vorstellen, dass wir als Spitzenverband hierzu einen Vertrag zur Auftragsdatenverarbeitung abschließen müssen bzw. dass der bereits für unseren Zweck geschlossene Vertrag gleichzeitig für alle Landesverbände gilt. Ich gehe vielmehr davon aus, dass hierfür der jeweilige Landesverband als „verantwortliche Stelle" selbst verantwortlich ist und direkt mit dem DOSB einen Vertrag zur Auftragsdatenverarbeitung abschließen muss, soweit er das online Lizenzverwaltungssystem nutzen möchte.

AW R. Graf
Ich sehe das genauso wie Sie. Der DOSB ist sowohl Auftragsverarbeiter für den Spitzenverband als auch für die Landesverbände.

Dadurch dass die Landesverbände als verantwortliche Stellen die von Ihnen genannte Auftragsverarbeitung regeln müssen und der Spitzenverband keinen Zugriff auf die Daten hat, kommt der Spitzenverband als Auftragsverarbeiter auch nicht in Frage.

Die Verträge müssen zwischen den Landesverbänden und dem DOSB geschlossen werden.

Dass der Spitzenverband in die Kette zwischen DOSB und Landesfachverband eingefügt wird, kann ich nicht nachvollziehen.

1.3 Frage zur Einschätzung der Nutzung der Amazon Cloud Frankfurt

Gibt es in Sachen Datenschutz Erfahrungen mit der Amazon Cloud Frankfurt? Laut Anbieter unterliegen die Server dem "deutschen Datenschutz". Wie kann man sicher sein, dass dies bei einem amerikanischen Unternehmen wirklich zutrifft?

Hintergrund meiner Frage ist, dass wir derzeit erwägen, ein Online Kurssystem zu etablieren, welches dann auf eben jenen Servern gehostet wäre. Das muss dann aber natürlich entsprechend konform mit unseren Regularien sein.

Gibt es ggf. andere Anbieter, bei denen man diesbezüglich besser aufgehoben wäre?

AW R. Graf:
Das ist zugegeben eine schwierige Frage. Erfahrungsgemäß haben US-amerikanische Firmen ein anderes Verständnis von "deutschem Datenschutz" und dies führt dann in der Anwendung in Deutschland zu Problemen.

Ein gutes Beispiel hierfür ist die Geschichte der Microsoft Deutschland Cloud. Hier dauerte es auch einige Zeit bis der Zugriff von Microsoft Administratoren auf Daten bei der Telekom klar geregelt war. Erst am Ende dieses Anpassungsprozesses stand eine den deutschen Datenschutzregeln folgende Regelung, in der Microsoft eine Lösung des Problems in Form einer Datentreuhänderschaft festlegte. Sie besagt, dass nur Mitarbeiter der Telekom Zugriff auf die in Deutschland liegenden Daten haben. Somit erfolgt keine Datenübermittlung in die USA, auch nicht z. B. durch Fernwartung durch US-amerikanische Microsoft Mitarbeiter. Damit sichergestellt ist, dass Microsoft in keinem Fall Zugriff auf diese Daten hat, können auch die deutschen Mitarbeiter von Microsoft nicht auf diese Daten zugreifen.

Ich habe mir die Datenschutzregeln von Amazon angesehen, und hier fällt sofort auf, dass Amazon nicht diesen strikten Weg geht, den Microsoft eingeschlagen hat. LINK

Als Nachteil sehe ich, dass dem Kunden überlassen wird, die Region festzulegen, in der seine Daten liegen. Hier kann ich mir gut vorstellen, dass dies einige Kunden überfordert, da sie die entsprechenden Datenschutzregeln und Gesetze wenig bis gar nicht kennen und deswegen die falschen Schlüsse ziehen und datenschutzrechtlich falsche Einstellungen übernehmen.

Weitere Kritische Punkte sind folgende Formulierungen:

> *"Zugriff: Die Kunden verwalten den Zugriff auf ihre Inhalte sowie auf AWS-Services und -Ressourcen. Wir bieten fortschrittliche Funktionen für den Zugriff, die Verschlüsselung und die Anmeldung, damit sie dies effektiv tun können (z. B. AWS CloudTrail). Wir greifen nicht auf die Inhalte unserer Kunden zu oder verwenden sie – außer dies ist gesetzlich oder für die Wartung der AWS-Dienste und ihre Bereitstellung an unsere Kunden und ihre Endbenutzer erforderlich."*

und auch:

> ◦*Offenlegung von Kundeninhalten: Wir legen keine Kundeninhalte offen – außer wir müssen dies zur Einhaltung des Gesetzes oder einer gültigen und verpflichtenden Anweisung einer Regierungs- oder Regulierungsbehörde tun.*

In diesen Formulierungen wird deutlich, dass, sollte ein US-amerikanisches Gesetz oder ein Gericht Amazon die Offenbarung der Daten vorschreiben, Amazon diese Daten in die USA übertragen wird, obwohl dies gegen EU-Recht verstößt. Amazon wird sich somit dem US-Recht beugen.

Hier dürfte auch die Frage des US-amerikanischen "Patriot Act" eine Rolle spielen, der US-amerikanische Firmen zwingt, den Geheimdiensten Zugriff und Zugang auf Daten zu geben, ohne die Betroffenen darüber informieren zu dürfen.

Darüber hinaus kann auch zu Wartungszwecke auf die Daten der Kunden zugegriffen werden. Auch dies wird wieder eine Übermittlung von Daten in die USA beinhalten, denn ich kann mir bei schwierigen technischen Fragen nicht vorstellen, dass in der heutigen Zeit ein Techniker nach Frankfurt fliegt, um eine Wartung vor Ort durchzuführen, die er auch mittels Fernwartungsprogramm erledigen kann.

Auch wenn Amazon in seinen Ausführungen (vgl. den oben bereits angeführten Link), Wert darauf legt, dass Amazon den Datenschutz wertschätzt – das will ich Amazon auch gar nicht absprechen – unterliegt Amazon US-amerikanischen Gesetzen, die zu befolgen sind.

Ein interessanter Punkt ist die Möglichkeit des Kunden, seine Daten zu verschlüsseln. Das macht aber nur Sinn, wenn der Schlüssel ausschließlich beim Kunden liegt, da sonst die oben genannten Offenbarungsverpflichtungen wieder greifen. Leider habe ich auf diese Frage keine Antwort gefunden.

Ich habe auch keinen Auftragsdatenverarbeitungsvertrag von Amazon gefunden, der nähere Aufschlüsse über die getroffenen technisch organisatorischen Maßnahmen gibt.

Fazit:
US-amerikanische und ggf. auch zukünftig englische Firmen unterliegen gesetzlichen Anforderungen, die wir in Deutschland nicht überschauen bzw. einschätzen können. Ich würde einen Anbieter wählen, der ausschließlich in Deutschland die Daten verwaltet. Selbst dann bleiben beim Einsatz von Clouddiensten noch genügend Fragen offen, wie z. B. die Verfügbarkeit, die schwierig zu regeln ist.

1.4 Aushang zur Vorstellung von Mitarbeitern im Kursraum

Wir überlegen, für unsere Trainer im Kursraum einen Aushang zu platzieren, welche festen Mitarbeiter im Center zuständig sind (mit Foto und ausgeschriebenem Namen). Da es sich um den Kursraum handelt, können aber auch die Mitglieder Einsicht gelangen. Benötigen wir dazu die Einverständniserklärung der Mitarbeiter?

AW R. Graf:
Bitte Holen Sie die Einverständniserklärung ein. Es ist kein Problem, in Ihren Räumen die Namen der zuständigen festen Mitarbeiter aufzulisten (Verantwortungsbereich, Zuständigkeiten). Das dient der Erfüllung der Geschäftszwecke (§28 Abs. 1 BDSG), für das Bild wird es aber keine Rechtsgrundlage geben, auch nicht über den §32 BDSG.

Auch ist es nicht zwingend notwendig, das Bild zu zeigen, wie es z. B. bei einer notwendigen Personenkontrolle der Fall wäre. Aus diesem Grund bleibt nur die Einwilligung.

Sollten Trainer dies nicht wollen, müssen Sie leider auf das Bild des jeweiligen Betroffenen verzichten.

Bitte lassen Sie sich für die Einwilligung ein konkretes Bild geben und nicht pauschal für "Bilder" der Trainer, am besten einen sw Ausdruck des Bildes an die Einwilligung anheften.

IN DER DISKUSSION – NEUIGKEITEN RUND UM DEN DATENSCHUTZ

Fit für den Urlaub

Tipps des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur sicheren Netz-Kommunikation im Urlaub

Die Urlaubszeit naht und damit auch wieder die intensive Nutzung von Hotspots und öffentlichen und ungesicherten Internetzugängen. Hotels sollen gebucht, Tickets gekauft und alle möglichen Informationen zur Urlaubsgestaltung abgerufen werden. Und natürlich gilt es, die eigenen Eindrücke in Text und Bild mit Freunden und Verwandten zu teilen.

Nutzen Sie den Service des BSI zur Sensibilisierung Ihrer Kolleginnen und Kollegen

Unter den Überschriften „*Internetnutzung*", „*Internetcafés und öffentlich zugängliche Computer*", „*Mobile Netzwerke / Hotspots*", „*Schutz für Kinder*", „*Kommunikation über Mobiltelefone*", „*Soziale Netzwerke*" bietet die Website des BSI aktuell zahlreiche Informationen zum sicheren Surfen. Dabei beschränken sich die Informationen nicht nur auf die Zeit im Urlaub selbst, Hinweise erhält der Leser auch, was man in der Vorbereitung beachten und auch worauf man nach dem Urlaub achten sollte.

Eine kurze Checkliste mit den wichtigsten Kernpunkten und ein sehr leichtes Sicherheitsquiz: „Auf in den Urlaub – aber sicher" runden den Info-Urlaubs-Service ab. [LINK zur Website]

Wer seinen Kolleginnen und Kollegen hier etwas mehr mit an die Hand bzw. mit auf den Weg geben möchte, kann die Checkliste und das Quiz mit eigenen Fragen und Informationen ergänzen. *[TN]*

MEDIEN –TECHNIK – SICHERHEIT

Login-Daten: Unerlaubte Zugriffe auf Daten bei OneLogin

Quelle: https://www.golem.de/news/passwortmanger-kundendaten-von-onelogin-gehackt-1706-128189.html
Fundort: Buerger-Cert-Newsletter] SICHER • INFORMIERT vom 08.06.2017

Der Passwortmanager OneLogin verwaltet die Zugriffsrechte eines Nutzers oder einer Nutzerin auf deren genutzte Webapplikationen, unter anderem für Amazon Web Services, Microsoft Office 365, LinkedIn, Twitter und Google. Aus bisher ungeklärten Gründen verfügten am 31. März Angreifer aus dem Internet über den zentralen geheimen Verwaltungsschlüssel, den sogenannten AWS-Schlüssel des Unternehmens. Mit dem Schlüssel ist es laut Golem den Angreifern gelungen, sensible Kundendaten der zentralen Datenbank des Unternehmens abzugreifen. Darunter könnten unter anderem Nutzernamen, Notizen und Schlüssel der Kunden und auch von den Kunden verwendete Apps ausspioniert worden sein. Ob diese Daten durch eine Verschlüsselung geschützt waren, hat OneLogin noch nicht veröffentlicht. Die Firma hat jedoch angekündigt, betroffene Nutzerinnen und Nutzer zu informieren und fordert alle Kunden auf, ihr Zugangspasswort zu ändern sowie neue Schlüssel zu generieren.

Account geknackt? Wie kann ich prüfen, ob die eigene Adresse betroffen ist?

Quelle: Checked4You: Das Online-Jugendmagazin der Verbraucherzentrale Nordrhein-Westfalen
Fundort: Buerger-Cert-Newsletter] SICHER • INFORMIERT vom 23.06.2017

Ob der eigene E-Mail-Account von einem Angriff betroffen ist, kann man anhand von drei vom Online-Jugendmagazin checked4you der Verbraucherzentrale NRW empfohlenen sicheren Service-Seiten überprüfen. In einer übersichtlichen Tabelle werden die Funktionen und der Umfang der geprüften Datensätze vorgestellt. Betreiber der drei Websites sind das *Bundesamt für Sicherheit in der Informationstechnik*, das *Hasso-Plattner-Institut* der Uni Potsdam und eine Seite des Internet-Sicherheitsexperten und Blogger *Troy Hunt*. [Link zur Übersicht] [TN]

GESETZGEBUNG

Bundestag und Bundesrat beschließen Datenschutz-Anpassungs- und -Umsetzungsgesetz EU [DSAnpUG-EU]

1 Worum geht es?

Am 25. Mai 2018 wird die im April 2016 vom Europäischen Parlament beschlossene EU Datenschutzgrundverordnung [EU-DSGVO] in allen Mitgliedstaaten der Europäischen Union als unmittelbar geltendes Recht angewendet werden.

Ziel der Verordnung ist es, in allen Mitgliedstaaten ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten zu gewährleisten.

2 Was regelt das Gesetz

Mit Blick auf die sehr unterschiedlich ausgestalteten und differenzierten nationalen Datenschutzgesetze hat das EU Parlament eine Reihe von Öffnungsklauseln beschlossen, die es den Mitgliedstaaten erlaubt, nationale Regelungen in die EU-DSGVO zu integrieren. Gleichzeitig enthält die Verordnung verpflichtende Regelungsaufträge, die in der nationalen Gesetzgebung zwingend berücksichtigt werden müssen.

Mit dem vom Bundestag am 27. April und vom Bundesrat am 15. Mai beschlossenen Datenschutz-Anpassungs- und –Umsetzungsgesetz [DSAnpUG-EU] (*nachfolgend: Datenschutz-Anpassungsgesetz*) kommt der Gesetzgeber den Regelungsmöglichkeiten und -pflichten des EU-Parlaments nach.

Die Herausforderung für Datenschutzexperten wie für die Anwender – dies gilt für Unternehmen ebenso wie für Sportverbände und –vereine – wird sein, die vorhandenen Regelungen in den noch verbleibenden Monaten bis zur unmittelbaren Anwendung ab dem 25. Mai 2018 an die neue Verordnung anzupassen und umzusetzen. Vor dem Hintergrund des von Experten als „ausgesprochen komplex" charakterisierten Anpassungsgesetzes dürfte das für viele Organisationen keine leicht zu erfüllende und mit erheblichem Aufwand verbundene Aufgabe sein. Verstärkt wird der Druck zur termingerechten Umsetzung auf die Verantwortlichen noch dadurch, dass die EU-DSGVO im Vergleich zum bisherigen Bundesdatenschutzgesetz (BDSG) massiv erhöhte Bußgelder vorsieht.

Wie hoch der tatsächliche Aufwand zur Anpassung der bisherigen Regelungen an das Datenschutz-Anpassungsgesetz in den Sportvereinen und –verbänden sein wird, wird sich erst in den nächsten Wochen und Monaten nach der intensiven Erörterung in den einschlägigen Fachzirkeln abschätzen lassen.

Eine erste Orientierung zur Einschätzung möchten wir Ihnen mit diesem Beitrag liefern.

3 Wie wird das Gesetz eingeschätzt?

Einhellig begrüßt wird von den Kommentatoren die Tatsache, dass – über ein Jahr nach Verabschiedung der EU Datenschutzgrundverordnung – „endlich" ein Anpassungs- und Umsetzungsgesetz vorliegt, das zumindest in vielen zentralen Punkten den Rahmen des Datenschutzrechts in Deutschland ab dem 25. Mai 2018 absteckt und damit auch in vielen Punkten Planungssicherheit bietet. Gleichzeitig weisen zahlreiche Kommentatoren, wie z.B. auch der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD), darauf hin, dass das Datenschutzanpassungsgesetz immer noch eine Reihe „Fragen offen lasse".[LINK]

Ein zentraler Kritikpunkt richtet sich aus Sicht vieler Experten dagegen, dass mit dem Datenschutz-Anpassungsgesetz ein zu kompliziertes und wenig übersichtliches Konstrukt entstanden ist:

> *„Auch der neue Entwurf ist … wenig übersichtlich und erweist sich eher als ein komplexes Konstrukt schwer leserlicher Verweisungen, als als transparente und sinnvolle Ergänzung der Verordnung. Zukünftig werden Rechtsanwender, Unternehmen und Verbraucher neben dem Verordnungstext auch das neue BDSG sowie gegebenenfalls etwaige Spezialvorschriften zur Hand nehmen müssen, um die Rechtslage im Allgemeinen oder Rechte und Pflichten im Speziellen einschätzen zu können. Hinzu kommen Stellungnahmen der Datenschutzaufsichtsbehörden und spätestens ab Mai 2018 auch die Lektüre einschlägiger gerichtlicher Entscheidungen."* [LINK]

Absehbar ist darüber hinaus, dass gegen einige Formulierungen des Gesetzes, die aus der Sicht von Experten deutliche Abweichungen zu den Vorgaben der EU-Datenschutzverordnung enthalten,[LINK] Klagen vor dem Europäischen Gerichtshof eingereicht werden, sodass die Umsetzung der neuen Datenschutzgesetzgebung auch vor diesem Hintergrund noch mit einem gewissen Maß an Unsicherheiten verbunden bleiben dürfte.

Auch wenn es nach wie vor eine Reihe von Unwägsamkeiten und Unsicherheiten gibt, bleibt es die Aufgabe für alle – und damit auch für alle Vereine und Verbände – die Vorgaben der EU Datenschutzgrundverordnung und des Datenschutz Anpassungsgesetzes so zu organisieren, dass sie ab Ende Mai 2018 in der täglichen Praxis auch tatsächlich eingesetzt werden kann.

4 Welche Neuregelungen sollten bei der Abschätzung des Anpassungsbedarfs besonders beachtet werden

In einem Kommentar von Wybitul / Böhm / Ströbel [LINK] weisen die Autoren auf 10 Kernpunkte hin, die aus Ihrer Sicht eine zentrale Bedeutung bei der Anpassung und der Risikoabschätzung spielen sollten:

- ***Hohe Risiken bei Fehlern****: Bußgelder von bis zu 20 Millionen € oder 4 % des globalen Umsatzes – je nachdem, welcher Betrag höher ist. Nur Verstöße, die allein deutsches Recht betreffen, sind bei EUR 50.000 gedeckelt.*
- ***Schmerzensgeld****: Verbraucher (d.h. auch Arbeitnehmer) können Schadensersatzansprüche auch wegen Nichtvermögensschäden geltend machen. Das ist neu und führt*

zu erheblichen wirtschaftlichen Risiken für Unternehmen. Denn Verbraucher und Verbände haben Verbandsklagerechte, die ihnen die Geltendmachung tatsächlicher oder behaupteter Ansprüche erleichtern.

- ***Beweislastumkehr**: Der Arbeitgeber muss nachweisen können, dass er die geltenden datenschutzrechtlichen Vorgaben einhält. Hierfür muss das Unternehmen auch die umfassenden Dokumentationspflichten der DSGVO umsetzen.*
- ***Sonderregelungen**: Das Gesetz enthält Sonderregelungen zu einigen Spezialgebieten, wie etwa dem Datenschutz am Arbeitsplatz, Videoüberwachung oder Profiling.*
- ***Teile des bisherigen Datenschutzes bleiben**: Der deutsche Gesetzgeber versucht erkennbar, möglichst große Teile des bisherigen deutschen Beschäftigtendatenschutzes zu übernehmen.*
- ***Erschwerte Compliance-Kontrollen**: Die Aufklärung von Straftaten oder anderen Pflichtverstößen bleibt zulässig, muss aber strengen Anforderungen genügen – gerade bei der Transparenz der Datenverarbeitung.*
- ***Transparenz**: Es bleibt weitgehend bei den umfassenden Unterrichtungspflichten nach Art. 13 ff. DSGVO. Die in älteren Entwürfen zum BDSG vorgesehenen Einschränkungen der Betroffenenrechte wurden stark zurückgenommen.*
- ***Dokumentation**: Auch die sehr weitgehenden Dokumentationspflichten nach der DSGVO werden durch das BDSG nicht reduziert.*
- ***Betriebsräte und der neue Beschäftigtendatenschutz nach § 26 BDSG**: Auch die Datenverarbeitung durch Betriebsräte muss sich künftig an den Maßstäben des BDSG und der DSGVO messen lassen.*
- ***Betriebsvereinbarungen**: Kollektivvereinbarungen bleiben ein zulässiges Mittel zur Regelung erlaubter Datenverarbeitung. Sie müssen aber die Anforderungen von Art. 88 Abs. 2 DSGVO und § 26 BDSG erfüllen. Hierfür müssen auch viele geltende Betriebsvereinbarungen einzeln oder durch den Abschluss entsprechender Rahmenbetriebsvereinbarungen angepasst werden.* LINK

5 Der Fragebogen des Bayrischen Landesdatenschutzbeauftragten als erster Orientierungspunkt notwendiger Anpassungen?

Für die Frage, welche Datenschutz-Anpassungsprozesse notwendig werden können und mit welchem personellen und finanziellen Aufwand das (auch) für Vereine und Verbände verbunden sein könnte, ist auch ein Fragebogen des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) sehr aufschlussreich. [1]

Er wurde, um einen besseren Einblick in den derzeitigen Stand der Umsetzung der EU-Datenschutzgrundverordnung zu erhalten, an 150 Unternehmen versendet und kann durchaus auch als Anforderungskatalog für die Anpassungen des Datenschutzmanagements bis Mai 2018 gesehen werden. Er soll daher an dieser Stelle vorgestellt werden.

---

1 Download: Sie finden den Fragebogen unter: https://www.lda.bayern.de/de/index.html Es ist davon auszugehen, dass auchdie anderen Aufsichtsbehörden nicht wesentlich von dem im Fragebogen erkennbaren Anforderungskatalog abweichen werden. Darauf deutet auch hin, dass Zumal ab Mai 2018 davon ausgegangen werden kann, dass die Aufsichtsbehörden sehr viel enger abstimmen werden, als es in der Vergangenheit der Fall war.

Der Fragebogen ist in 6 Themenschwerpunkte gegliedert

I. Strukturen Verantwortlichkeit im Unternehmen
II. Übersicht der Verarbeitung
III. Einbindung externer
IV. Transparenz, Informationspflichten und Sicherstellung der Betroffenen rechte
V. Verantwortlichkeit, Umgang mit Risiken
VI. Datenschutzverletzungen.

Ein Thema, das im Fragebogen immer wiederkehrt bezieht sich auf Fragen zum Datenschutzmanagementsystem, sodass davon ausgegangen werden kann, dass die Aufsichtsbehörden bei ihren Prüfungen ihr Augenmerk insbesondere auf die Gesamtheit der zum Datenschutz angelegten und durchgeführten Maßnahmen richten werden.

Ein zentraler Bereich im Rahmen des Anpassungsprozesses, der in vielen Organisationen vermutlich auch die größten Probleme verursachen könnte, dürfte die im Kapitel „IV Verantwortlichkeit, Umgang mit Risiken" aufgeführte *Datenschutzfolgeabschätzung* sein. Im Prinzip ist die Datenschutzfolgeabschätzung mit der Vorabkontrolle aus dem BDSG vergleichbar. Schon dort wurde eine Risikoabschätzung bzw. Risikoanalyse bei Verarbeitung besonderer personenbezogener Daten gefordert. In der Datenschutzfolgeabschätzung wird diesem Aspekt allerdings eine deutlich stärkere Bedeutung beigemessen.

Was sind die Unterschiede zwischen der neuen Datenschutzfolgeabschätzung und der bisherigen Vorabkontrolle?

Ein wichtiger Unterschied bezieht sich auf die Rolle des Datenschutzbeauftragten (DSB). Während der DSB bei der Vorabkontrolle auch die Prüfung durchführen musste, ist er nun nur noch in beratender Tätigkeit gefordert. Sicher wird der DSB auch zukünftig derjenige sein, der die Organisation auf entsprechende Maßnahmen und Umsetzungen hinweisen muss, für die Prüfung der Maßnahmen ist er allerdings nicht mehr zuständig. Sie obliegt künftig dem Verantwortlichen, das dürfte in der Regel – wie schon aus dem alten BDSG bekannt – die Verantwortliche Stelle sein. Der Datenschutzbeauftragte kann und soll als Berater zur Verfügung stehen.

Neu ist auch, dass die Aufsichtsbehörden um Auskunft gebeten werden können, ob die ergriffenen Maßnahmen zum Schutz der personenbezogenen Daten ausreichend sind. Das wird bedeuten, dass der Kontakt zwischen Augenstein und Landesdatenschutzbeauftragten intensiver werden wird, als dies in der Vergangenheit erfolgt.

Zurzeit gibt es verschiedene Ansätze zur Datenschutzfolgeabschätzung. Um eine Risikoanalyse durchzuführen wird z.B. empfohlen, die Vorgehensweise aus der ISO 27.000 oder aus dem BSI Grundschutz abzuleiten. Dies dürfte insbesondere für kleinere Organisation zu einer großen Herausforderung werden, da zu vermuten ist, dass die hierfür notwendigen Fachkenntnisse vielerorts nicht vorhanden sein dürften. Inwieweit die angekündigte Unterstützung der Aufsichtsbehörden – Negativ- bzw. Positivlisten sollen die Organisationen bei der Klärung der Frage unterstützen, welche Prozesse bzw. Verarbeitung personenbezogener Daten einer Datenschutzfolgeabschätzung unterliegen – ausreicht, um vorhandene Defizite auszugleichen, wird sich erst in der praktischen Umsetzung erweisen.

Leitfaden zur Beurteilung der Folgen

Zur Abschätzung der Prozesse, für die Unternehmen, Organisationen und Institutionen eine Datenschutzfolgeabschätzung zu erstellen haben, hat die Artikel-29-Datenschutzgruppe (G29)[2] einen ersten Leitfaden ausgearbeitet, in dem 10 Kriterien zur Risikobewertung aufgeführt werden:

1. Bewertung und Einstufung (Scoring) einschließlich Prognosen und Profilerstellung
2. automatisch erfolgende Entscheidungen mit rechtlichen oder ähnlich signifikanten Auswirkungen für Betroffene
3. systematisches Monitoring
4. sensitive, insbesondere personenbezogene Daten
5. umfangreiche Datenmengen
6. Vergleich oder Kombination von Datensätzen
7. Daten ungeschützter Betroffener
8. Einsatz innovativer Technologien oder neuartiger organisatorischer Lösungen
9. Datentransfers in Länder außerhalb der EU
10. Verhinderung, dass die betroffene Person ein Recht ausüben oder eine Dienstleistung oder einen Vertrag ausführen kann

Entscheidende Voraussetzung für eine sachgerechte, gesetzeskonforme und alle Prozesse beinhaltende Erstellung von Datenschutzfolgeabschätzungen bleibt zuallererst die umfassende Erfassung aller im eigenen Unternehmen verarbeiteten personenbezogenen Daten.

6 Von der Gesetzesvorlage zur praktischen Umsetzung

Auch wenn nach Verabschiedung des Datenschutz Anpassungsgesetzes noch nicht alle Fragen geklärt sind, so liegt mit diesem Gesetz doch ein tragfähiger Handlungsrahmen vor, der es den Datenschutzbeauftragten der Vereine und Verbände ermöglichen sollte, bis zum Mai des nächsten Jahres die Voraussetzungen dafür zu schaffen, dass die neuen Regeln angewendet werden können. *In diesem Prozess wird Sie das Datenschutzportal in den nächsten Monaten natürlich auch unterstützen.*

Aktuell kann noch nicht eingeschätzt werden, in welchem Umfang die neuen Gesetze von den Datenschutzbehörden geprüft und in welchem Umfang die drastisch erhöhten Sanktionen mit Bußgeldandrohungen auch tatsächlich verhängt werden, trotzdem sind alle Verantwortlichen vermutlich gut beraten, dies nicht auf die leichte Schulter zu nehmen.

Allen Beteiligten sollte bewusst sein, dass mit den verschärften Bußgeldern nicht mehr nur das Prestige auf dem Spiel steht, sondern es im schlimmsten Fall auch um die Existenz gehen kann. [RG / TN]

2 Die G29 ist ein unabhängiges Beratungsgremium der Europäischen Kommission. Seine Aufgabe ist es, Informationen, Empfehlungen und Stellungnahmen zu Themen auszuarbeiten, die in puncto Datenschutz bei der Verarbeitung personenbezogener Daten in der Europäischen Gemeinschaft relevant sind.

AKTUELLE URTEILE

Im Telekommunikationsgesetz vorgesehene Vorratsdatenspeicherung verstößt gegen Unionsrecht

Keine anlasslose Speicherung von Daten

Quelle: *Oberverwaltungsgericht Nordrhein-Westfalen, Beschluss vom 22.06.2017; AZ: 13 B 238/17*
Fundort: *www. kostenlose-urteile.de (ra-online GmbH), Berlin, 23.06.2017; Dok.-Nr.: 24437*

Die im Dezember 2015 gesetzlich eingeführte und ab dem 1. Juli 2017 zu beachtende Pflicht für die Erbringer öffentlich zugänglicher Telekommunikationsdienste, die bei der Nutzung von Telefon- und Internetdiensten anfallenden Verkehrs- und Standortdaten ihrer Nutzer für eine begrenzte Zeit von 10 bzw. – im Fall von Standortdaten – 4 Wochen auf Vorrat zu speichern, damit sie im Bedarfsfall den zuständigen Behörden etwa zur Strafverfolgung zur Verfügung gestellt werden können, ist mit dem Recht der Europäischen Union nicht vereinbar. Dies entschied das Oberverwaltungsgericht Nordrhein-Westfalen.

Die Antragstellerin des zugrunde liegenden Falls, ein IT-Unternehmen aus München, das u.a. Internetzugangsleistungen für Geschäftskunden in Deutschland und in anderen EU-Mitgliedstaaten erbringt, hatte sich mit einem Antrag auf Erlass einer einstweiligen Anordnung an das Verwaltungsgericht Köln gewandt, um der Verpflichtung zur Vorratsdatenspeicherung vorläufig bis zur Entscheidung über die gleichzeitig erhobene Klage nicht nachkommen zu müssen.

Datenspeicherung zur Abwehr von Gefahren muss auf betroffenen Personenkreis beschränkt sein

Diesen Antrag hatte das Verwaltungsgericht abgelehnt. Der gegen diese Entscheidung erhobenen Beschwerde der Antragstellerin hat das Oberverwaltungsgericht Nordrhein-Westfalen nunmehr stattgegeben. Zur Begründung führte das Gericht aus, dass die Speicherpflicht in der Folge eines Urteils des Gerichtshofs der Europäischen Union vom 21. Dezember 2016 jedenfalls in ihren gegenwärtigen Ausgestaltung nicht mit Art. 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG vom 12. Juli 2002 vereinbar sei. Die Speicherpflicht erfasse pauschal die Verkehrs- und Standortdaten nahezu aller Nutzer von Telefon- und Internetdiensten. Erforderlich seien aber nach Maßgabe des Gerichtshofs jedenfalls Regelungen, die den von der Speicherung betroffenen Personenkreis von vornherein auf Fälle beschränkten, bei denen ein zumindest mittelbarer Zusammenhang mit der durch das Gesetz bezweckten Verfolgung schwerer Straftaten bzw. der Abwehr schwerwiegender Gefahren für die öffentliche Sicherheit bestehe. Dies könne etwa durch personelle, zeitliche oder geographische Kriterien geschehen. Nach dem Urteil des Gerichtshofs könne die anlasslose Speicherung von Daten insbesondere nicht dadurch kompensiert werden, dass die Behörden nur zum Zweck der Verfolgung schwerer Straftaten bzw. der Abwehr schwerwiegender Gefahren Zugang zu den gespeicherten Daten erhielten und strenge Maßnahmen zum Schutz der gespeicherten Daten vor Missbrauch ergriffen würden. [MEHR]

Keine Haftung des Domain-Registrars für persönlichkeitsverletzende Äußerungen auf einer Internetseite

Domain-Registrar hat nur eingeschränkte Prüfpflichten

Quelle: *Oberlandesgericht Frankfurt am Main, Beschluss vom 16.09.2015; AZ: 16 W 47/15*
Fundort: *www. kostenlose-urteile.de (ra-online GmbH), Berlin, 08.06.2017; Dok.--Nr.: 24360*

Ein Domain-Registrar haftet nur sehr eingeschränkt für persönlichkeitsverletzende Äußerungen auf einer von ihm registrierten Internetseite. Eine Handlungspflicht besteht für ihn nur, wenn die Persönlichkeitsverletzung offenkundig und unschwer feststellbar ist und der Zugang zu dem rechtsverletzenden Inhalt durch zumutbare Maßnahmen unterbunden werden kann. Letzteres ist für ein Domain-Registrar in der Regel nicht möglich. Dies geht aus einer Entscheidung des Oberlandesgerichts Frankfurt a.M. hervor.

In dem zugrunde liegenden Fall wurde ein Domain-Registrar für persönlichkeitsverletzende Äußerungen auf einer von ihm registrierten Internetseite haftbar gemacht. Das Landgericht Frankfurt a.M. hat eine Haftung des Registrars verneint. Nunmehr musste das Oberlandesgericht über den Fall entscheiden.

Eingeschränkte Prüfpflichten des Domain-Registrars

Das Oberlandesgericht Frankfurt a.M. führte zum Fall aus, dass ein Domain-Registrar hinsichtlich der Verantwortlichkeit für die unter einer Domain abrufbaren Inhalte einem Host-Provider nicht gleichzusetzen sei. Die Regelungen zur Störerhaftung des Host-Providers seien daher nicht anzuwenden. Einem Domain-Registrar kommen nur eingeschränkte Prüfpflichten zu, die eine Handlungspflicht nur dann auslösen, wenn die Persönlichkeitsverletzung offenkundig und für ihn unschwer feststellbar sei.

Haftung setzt Vorliegen von zumutbaren Maßnahmen voraus

Nach Funktion und Aufgabenstellung sei der Domain-Registrar nach Ansicht des Oberlandesgerichts mit einem Zugangsprovider vergleichbar. Die Inanspruchnahme eines Zugangsvermittlers setze voraus, dass er den Zugang zu rechtsverletzenden Inhalten durch zumutbare Maßnahmen unterbinden könne. Unzumutbar seien dabei Maßnahmen, wenn durch sie in erheblichem Umfang auch der Zugang zu anderen, legitimen Inhalten betroffen wäre oder der Zugang zu rechtsverletzenden Inhalten nicht effektiv unterbunden werden könne. [MEHR]

Kammergericht bekräftigt den hohen Schutz des Fernmeldegeheimnisses und stellt klar, dass es sich auch auf E-Mails erstreckt

Schutz des Fernmeldegeheimnisses steht dem Anspruch der Erben auf Einsicht in Facebook-Account entgegen

Quelle: *Kammergericht Berlin, Urteil vom 31.05.2017; AZ: 21 U 9/16*
Fundort: *www. kostenlose-urteile.de (ra-online GmbH), Berlin, 31.05.2017; Dok.--Nr.: 24330*

Das Kammergericht Berlin hat in zweiter Instanz zu Gunsten von Facebook entschieden und die Klage einer Mutter, die den Zugang zu dem Facebook-Account ihres verstorbenen Kindes zusammen mit dem Kindesvater aus Erbrecht durchsetzen wollte, abgewiesen.

Der Schutz des Fernmeldegeheimnisses stehe dem Anspruch der Erben entgegen, Einsicht in die Kommunikation der Tochter mit Dritten zu erhalten.

Das Kammergericht ließ offen, ob die Klägerin und der Kindesvater als Erben in den Vertrag eingerückt seien, den die verstorbene Tochter mit Facebook geschlossen hatte. Es sei zwar grundsätzlich möglich, dass die Erben in die Rechte und Pflichten dieses Vertrages eingetreten seien, und zwar nicht im Sinne der aktiven Fortführung dieses Vertrages, sondern um passive Leserechte zu erhalten.

In den von Facebook gestellten Nutzungsbedingungen sei nicht geregelt, ob Rechte aus dem Vertrag im Falle des Todes des Nutzers auf seine Erben übergehen könnten. Auch der Grundgedanke des Vertrages spreche nicht generell dagegen, dass er nicht vererblich sei. Facebook wolle den Nutzern nur eine Kommunikationsplattform zur Verfügung stellen und Inhalte vermitteln. Durch eine Änderung in der Person des Vertragspartners würden die Leistungen in ihrem Charakter nicht verändert.

Vererbbarkeit höchstpersönlicher Rechtspositionen nicht in BGB geregelt

Andererseits regele das Bürgerliche Gesetzbuch nicht, ob höchstpersönliche Rechtspositionen (ohne vermögensrechtliche Auswirkungen) vererbbar seien, sondern setze für eine Vererbung voraus, dass sie in irgendeiner Form im Eigentum des Verstorbenen verkörpert seien und nicht nur virtuell existierten. Um zu klären, ob es sich bei – nicht verkörperten – E-Mails um solche handele, die aufgrund ihres höchstpersönlichen Inhalts nicht vererbbar seien, oder um solche, die aufgrund ihres wirtschaftlichen Bezuges vererbbar seien, würde man in der Praxis auf erhebliche Probleme und Abgrenzungsschwierigkeiten stoßen.

Fernmeldegeheimnis erstreckt sich auch auf E-Mails

Das Gericht müsse jedoch die Frage der Vererbbarkeit des Facebook-Accounts nicht entscheiden. Selbst wenn man davon ausgehe, dass dieser Account in das Erbe falle und die Erbengemeinschaft Zugang zu den Account-Inhalten erhalten müsse, stehe das Fernmeldegeheimnis nach dem Telekommunikationsgesetz entgegen. Dieses Gesetz sei zwar ursprünglich für Telefonanrufe geschaffen worden.

Das Fernmeldegeheimnis werde jedoch in Art. 10 Grundgesetz geschützt und sei damit eine objektive Wertentscheidung der Verfassung. Daraus ergebe sich eine Schutzpflicht des Staates und auch die privaten Diensteanbieter müssten das Fernmeldegeheimnis achten. Nach einer Entscheidung des Bundesverfassungsgerichts vom 16. Juni 2009 erstrecke sich das Fernmeldegeheimnis auch auf E-Mails, die auf den Servern von einem Provider gespeichert seien. Denn der Nutzer sei schutzbedürftig, da er nicht die technische Möglichkeit habe, zu verhindern, dass die E-Mails durch den Provider weitergegeben würden. Dies gelte entsprechend für sonstige bei Facebook gespeicherten Kommunikationsinhalte, die nur für Absender und Empfänger oder jedenfalls einen beschränkten Nutzerkreis bestimmt sind. [MEHR]

SAVE THE DATE – ZUSATZTERMIN

DOSB FÜHRUNGS-AKADEMIE

Neu und Europäisch: Die EU Datenschutzgrundverordnung

Sem. 17-41 Freitag, 3. November 2017, 10:00 Uhr bis 17:00 Uhr

THEMA	Auf dem Weg zu einem einheitlichen, für alle Länder der EU verbindlichen europäischen Datenschutzrecht ist die vom EU Parlament im April 2016 verabschiedete europäische Datenschutzgrundverordnung (EU DSGVO) ein Meilenstein. Mit der Harmonisierung des europäischen Datenschutzrechtes verbunden sind gleichzeitig gravierende Änderungen und auch z.T. deutliche Verschärfungen rechtlicher Vorgaben. Auch wenn die genauen Regelungen in Detailfragen noch offen sind, ist schon jetzt erkennbar, dass die EU DSGVO auch in Deutschland mit einem erheblichen Anpassungsbedarf verbunden sein wird. Die rechtzeitige Überprüfung des Datenschutzes im eigenen Verein / Verband und die frühzeitige Ermittlung der für die Anpassung notwendigen zeitlichen und finanziellen Ressourcen sind auch deshalb von entscheidender Bedeutung, weil die DSGVO ab Mai 2018 ohne weitere Übergangsfristen sofort in Kraft tritt. Die im Vergleich zum Bundesdatenschutzgesetz (BDSG) deutlich verschärften Strafandrohungen stellen zudem ein erheblich gesteigertes Haftungsrisiko für Vereins- und Verbandsführungen dar. Auf Basis der bis September 2017 vorliegenden Novellierungen erfahren Sie in diesem Tagesseminar, was sich im Vergleich zum BDSG konkret ändert, welche Anforderungen auf Sie zukommen, mit welchen Zeitressourcen Sie rechnen müssen und wie Sie die notwendigen Anpassungen erfolgreich und termingetreu umsetzen können.
INHALT	▪ Die neuen Vorschriften der EU DSGVO: Was ändert sich im Vergleich zum BDSG und den weiteren im Datenschutz geltenden gesetzlichen Vorschriften? ▪ Welche Konsequenzen hat die DSGVO für Datenschutzbeauftragte? ▪ Welche Maßnahmen sind zur Umsetzung der DSGVO notwendig? ▪ Welche Haftungs- und Bußgeldrisiken sind mit der neuen Verordnung verbunden?
NUTZEN	▪ Sie lernen die neuen Anforderungen der EU DSGVO und ihre Unterschiede zu den Regelungen und Vorschriften des Bundesdatenschutzgesetzes kennen. ▪ Sie können die daraus abzuleitenden Anforderungen für Ihren eigenen Verein/Verband erkennen und rechtzeitig die notwendigen technisch-organisatorischen Anpassungsmaßnahmen einleiten. ▪ Mit den im Seminar vermittelten Inhalten und den erhaltenen Materialien können Mitarbeiter/innen und Ehrenamtliche über veränderte Vorgaben informieren, sie schulen und ihnen so rechtssicheres Handeln ermöglichen.
ZIELGRUPPE	▪ Datenschutzbeauftragte aus Verbänden und Vereinen, die sich einen Überblick verschaffen möchten, welche Anpassungen durch die EU-DSGVO im eigenen Verband/Verein notwendig werden ▪ Geschäftsführer(innen) und Vorstandsmitglieder von Vereinen u. Verbänden ohne Datenschutzbeauftragte(n), die die Konsequenzen und neuen Risiken der EU-DSGVO für sich selbst und den eigenen Verein / Verband abschätzen möchten.
REFERENT	▪ Dirk-Michael Mülot, Wirtschaftsinformatiker, Externer DSB und Freier Sachverständiger für Datenschutz, Datensicherheit u. IT-Forensik, Langenberg
LEITUNG	T. Niewerth, Führungs-Akademie DOSB
ORT	ACHTUNG: Der Ort konnte noch nicht abschließend geklärt werden Das Seminar findet entweder in Köln oder in Frankfurt statt
KOSTEN	Mitglieder 115 € /// Nicht-Mitglieder 175 € *[inkl. Materialien und Verpflegung]
ANMELDUNG	Anmeldeformular als Anlage: Fax: 0221 / 221 220 14; E-Mail: anmeldung@fuehrungs-akademie.de

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