



# **FA Datenschutzportal**

## **DSP Info-Brief**

**Nr. 48 / JULI 2017**

---

## INHALT

### DATENSCHUTZPORTAL INTERN

1	Die Themen im Live-Chat vom 28.07.2017.....	3
1.1	Online-Befragung: Datenschutzrechtliche Absicherung zur Nutzung und Weitergabe von erhobenen Daten	
1.2	Videoüberwachung eines Schießstandes	
2	Aktualisierung der im Portal eingestellten Dokumente.....	5
3	Unser Halbjahresservice als Anlagen: Aktualisierung aller Übersichten: .....	5
•	Alle Themen der Info-Briefe .....	A 1
•	Alle im Live-Chat thematisierten Fragen .....	A 2
•	Alle vorgestellten Urteile zum Datenschutz .....	A 3

### IN DER DISKUSSION – NEUIGKEITEN RUND UM DEN DATENSCHUTZ

4	Sind Sie auf sicherem Weg? Infos zur Umsetzung der EU-Datenschutzgrundverordnung .....	6
---	---	---

### MEDIEN –TECHNIK – SICHERHEIT

5	Akten digital archivieren: Das ist wichtig.....	10
---	---	----

### GESETZGEBUNG

6	Neu im Bundesgesetzblatt: Das neue Bundesdatenschutzgesetz, das am 25. Mai 2018 in Kraft tritt.....	11
7	Stellungnahmen der Landesdatenschutzbeauftragten zum Datenschutz Anpassungs- und Umsetzungsgesetz .....	11
8	Beschäftigtendatenschutz und das neue BDSG – Das ändert sich .....	12

### AKTUELLE URTEILE

9	Bundesgerichtshof erleichtert Verfolgung illegaler Uploads in Tauschbörsen.....	13
10	Antrag der Deutschen Telekom AG gegen Verpflichtung zur anlasslosen Speicherung von Telekommunikationsverkehrsdaten erfolglos.....	13
11	OLG Köln verbietet Klausel über Verwendung früherer Kundendaten zur "individuellen Kundenberatung" .....	14
12	Journalist macht sich mit Veröffentlichung eines ungepixelten Bildes eines vermeintlichen Ebola-Patienten strafbar .....	15
13	BAG: Daten aus Spähsoftware sind kein Kündigungsgrund .....	16

#### 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](http://www.fuehrungs-akademie.de)

[niewerth@fuehrungs-akademie.de](mailto:niewerth@fuehrungs-akademie.de)

#### Technische Umsetzung

Führungs-Akademie des DOSB

#### Redaktion

Toni Niewerth / Dirk-Michael Mülöt

#### Kontakt SVBG

Sachverständigenbürogemeinschaft Mülöt:Graf

Westfalenweg 2

33449 Langenberg

[www.muelot.de/](http://www.muelot.de/)

[d.muelot@muelot-Graf.de](mailto:d.muelot@muelot-Graf.de)

#### Copyright

© 2016 by SVBG MÜLOT:GRAF

**DATENSCHUTZPORTAL INTERN****1 Die Themen des Live-Chat vom 28.07.2017<sup>1</sup>****1.1 Online-Befragung: Datenschutzrechtliche Absicherung zur Nutzung und Weitergabe von erhobenen Daten**

- F 1** Spricht datenschutzrechtlich etwas gegen die Verwendung von Google Formulare<sup>1</sup> bzw. gibt es datenschutzrechtlich unbedenklichere Angebote?
- F 2** Die Befragung enthält folgende Formulierung: *"Der/die Ansprechpartner\*in der Schule/Kita ist damit einverstanden, dass der RSV NRW seine Daten" nutzt/ zugänglich macht".* " ja / " nein
- (a) Ist die Frage in dieser Allgemeinheit zulässig oder muss hier nicht formuliert werden, wozu die Daten genutzt bzw. wem sie zugänglich gemacht werden sollen?
- (b) Ist es datenschutzrechtlich ausreichend, dass der/die Befragte die Möglichkeit hat, der Nutzung der Daten bzw. der Weitergabe der Daten zu widersprechen oder ist sogar eine persönliche Befragung der Person notwendig?

**AW D.M. Mülöt****AW zu F1**

Grundsätzlich spricht nichts gegen eine Verwendung von „von Google Formulare“. Allerdings müsste der Verband als Ersteller des Fragebogens einen Vertrag zur Auftragsdatenverarbeitung mit Google abschließen, bei dem die Grundregeln des § 4a BDSG eingehalten werden müssen.

**AW zu F2 (a)**

Die Frage suggeriert, dass die Antwort auf den Fragebogen nicht anonym ist bzw. anonymisiert wird, sondern, dass die Antworten einer bestimmten Kita zugeordnet werden können und dass auch die weitergegebenen Daten einer bestimmten Institution zugeordnet werden können.

Da die Beantwortung des Fragebogens freiwillig ist, dürfte der Antwortgeber mit der Beantwortung der Fragen konkludent zustimmen, dass seine Antworten auch zur Auswertung genutzt werden. Wenn die Antworten einem Dritten zugänglich gemacht werden sollen und dabei auch die entsprechende Institution bestimmbar ist, müsste im Fragebogen oder im Anschreiben zur Befragung deutlich gemacht werden, an wen / an welche Stellen die Informationen zu welchem Zweck weitergegeben werden sollen. Auch hier sind die Grundregeln des § 4a BDSG zu beachten.

**AW zu F2 (b)**

Unter Berücksichtigung der vorhergehenden Antwort reicht die Möglichkeit der schriftlichen Befragung aus.

Wenn Sie sicher gehen wollen, dass etwaige Beschwerden vor Gericht keinen Erfolg haben, ist vorab die Konsultation eines Rechtsanwaltes zu empfehlen.

<sup>1</sup> Bitte beachten Sie, dass es sich bei den Diskussionen im Live-Chat nicht um eine Rechtsberatung oder „Rechtsdienstleistung“ im Sinne des RDG handelt. Hierzu müssen Sie einen entsprechend autorisierten Juristen konsultieren.

**Ergänzender Hinweis zu F1.**

Eine nicht kostenlose, aber kostengünstige (und zugleich leicht zu bedienende und auszuwertende) Alternative für Online-Befragungen ist vor einigen Wochen in einem Webinar auf der Website des Portals „[www.stifter-helfen.de/](http://www.stifter-helfen.de/)“ vorgestellt worden. Für 92 € kann bei QuestionPro eine Jahreslizenz erworben werden. [TN]

-----

**1.2 Videoüberwachung eines Schießstandes**

Ist es datenschutzrechtlich zulässig einen Schießstand, der an andere Vereine vermietet wird per Video zu überwachen, um sicherzustellen, dass der Stand nur für genehmigte Disziplinen genutzt wird?

Hintergrund ist, dass in der letzten Zeit auf Grund von Einschüssen in Decke und Deckung davon auszugehen ist, dass dies nicht immer der Fall war.

**AW D.M. Mülöt**

Grundsätzlich kann eine Videoüberwachung zur Wahrung des Hausrechts (BDSG §§ 28 Abs. 1 Nr. 2 i.V.m. § 6b Abs. 1 Nr. 2+3 ggf. auch § 6b Abs. 3) – auch aus datenschutzrechtlicher Sicht heraus – installiert werden.

Wichtig sind folgende, flankierende Maßnahmen:

1. Die Nutzer der Schießanlage müssen auf die Videoüberwachung sichtbar hingewiesen werden (BDSG § 6b Abs. 2 = Schild mit DIN-Piktogramm),
2. Eine Erläuterung zum Betrieb der Videoüberwachung ist hier äußerst ratsam (BDSG § 6b Abs. 3 z.B. Begründung: Nutzung nur für genehmigte Disziplinen und Nachweis von Schäden, bzw. Schadensverursachern)
3. Auf dem Schild muss die verantwortliche Stelle genannt sein (Wer betreibt die Videoanlage, Kontaktdaten, etc.),
4. Für die Videoüberwachung muss eine Verfahrensbeschreibung nach § 4e BDSG-alt angefertigt werden.
5. Die Löschfrist der Aufzeichnungen muss definiert werden (BDSG § 6b Abs. 5). Ich denke, dass hier die Frist kurz gehalten werden sollte. Frage: Wann ist die frühestmöglich Erkennung von Verstößen oder Schäden möglich? Dazu 24 Std. rechnen und Max-Speicherzeit festlegen.
6. Die Löschung muss technisch durch geeignete Verfahren sichergestellt werden.
7. Videoaufnahmen dürfen nicht veröffentlicht werden.
8. Die technisch-organisatorischen Maßnahmen gem. § 9 BDSG müssen eingehalten werden.

Das noch bis Mai 2018 geltende BDSG wird durch das neue BDSG abgelöst. Hier bleiben aber die Regeln identisch. In der EU-DSGVO ist die Videoüberwachung nicht geregelt.

-----

## 2 Aktualisierung der im Portal eingestellten Dokumente


Derzeit werden alle Dokumente, Infomaterialien und Checklisten im Datenschutzportal auf die Veränderungen der EU-Datenschutzgrundverordnung und des neuen Bundesdatenschutzgesetzes hin angepasst. Viele Details sind jedoch noch nicht ausreichend durch die Gesetzgeber und die eingesetzten Arbeitskreise sauber definiert. Demzufolge wird die Anpassung mit hoher Wahrscheinlichkeit erst Ende September 2017 finalisiert werden können. Daher bitten wir alle Portalnutzer noch um Geduld.

Über die aktuellen Entwicklungen halten wie Sie auch weiterhin in unseren Info-Briefen auf dem Laufenden. (DMM)

## 3 Unser Halbjahresservice als Anlagen: Aktualisierung aller Übersichten

Als Anlagen erhalten Sie mit diesem Info-Brief die aktualisierten Übersichten zu

- allen Themen der Info-Briefe Anlage 1
- Alle im Live-Chat thematisierten Fragen Anlage 2
- Alle vorgestellten Urteile zum Datenschutz Anlage 3

AUSGABE DATUM [JJJJ-MM]	RUBRIK	THEMA	Seite [Beginn]
2017-06	DATENSCHUTZPORTAL INTERN	Die Themen im Live-Chat vom 30.06.2017 3 1. Fragen zur rechtssicheren Archivierung von E-Mails 2. Auftragsdatenverarbeitung im Rahmen des DSOB Lizenzmanagementsystems 3. Frage zur Einschätzung der Nutzung der Amazon Cloud Frankfurt 4. Aushang zur Vorstellung von Mitarbeitern im Kursraum	3
2017-06	IN DER DISKUSSION: NEUES RUND UM DEN DATENSCHUTZ	Fit für den Urlaub – Tipps zur sicheren Netz-Kommunikation im Urlaub	9
2017-06	MEDIEN – TECHNIK – SICHERHEIT	Login-Daten: Unerlaubte Zugriffe auf Daten bei OneLogin	10
2017-06	MEDIEN – TECHNIK – SICHERHEIT	Account geknackt? Wie kann ich prüfen, ob die eigene Adresse betroffen ist?	10
2017-06	GESETZGEBUNG	Bundestag und Bundesrat beschließen Datenschutz-Anpassungs- und -Umsetzungsgesetz EU [DSAnUG-EU]	11
2017-06	AKTUELLE URTEILE	 <b>FA-DATENSCHUTZPORTAL – LIVE-CHAT-ARCHIV, 2013 – 2017 (JUNI)</b> <span style="float: right;">S. 1-(22)</span> Ihre Fragen – Unsere Antworten	
2017-06	AKTUELLE URTEILE		
Datum ALT DA	Schlagnote ALT TL	Frage ALT FR	Antwort ALT AW / ALT E1 / ALT N1 / ALT N2
30.06.17	(1) Fragen zur rechtssicheren Archivierung von E-Mails	<b>FRAGE:</b> → 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? <b>F1:</b> Müssen alle eingehenden und ausgehenden E-Mails rechtssicher archiviert werden oder nur bestimmte? <b>F2:</b> Wie lange ist die Archivierungsdauer?	<b>AW (zu F1):</b> → Laut GoBD müssen alle steuerrechtlich relevanten E-Mails revisionssicher archiviert werden. Diese Regelung gab es bereits seit 2001 (GdPdl 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. <b>AW (zu F2):</b> → 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 Löschrufen“ 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

**IN DER DISKUSSION – NEUIGKEITEN RUND UM DEN DATENSCHUTZ****4 Sind Sie auf sicherem Weg?****Infos zur Umsetzung der EU-Datenschutzgrundverordnung**

Am 25. Mai 2018 tritt die EU-DSGVO (Datenschutzgrundverordnung) verbindlich in Kraft. Hierdurch werden die noch gültigen Datenschutzgesetze der Länder, des Bundes und der Kirchen abgelöst und verlieren ihre Gültigkeit. Da die EU-DSGVO keine Übergangsfristen duldet, ist hier erhöhter Handlungsbedarf angesagt.

Bereits jetzt beginnen die Datenschutz-Aufsichtsbehörden der Bundesländer mit der Nachfrage bei Unternehmen jeglicher Art – und hierzu zählen auch die Vereine und Verbände – zum Umsetzungsstand auf die neue Datenschutzgrundverordnung.

Wir hatten bereits in der Juni-Ausgabe des Info-Briefes auf die wichtigsten Veränderungen im Vergleich zum bisherigen Bundesdatenschutzgesetz hingewiesen (S. 11-15) und dabei auch schon die Kernelemente des Fragebogens des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) genannt (S. 14f).

Da dieser Fragebogen nicht nur in Bayern relevant sein dürfte, sondern mit hoher Wahrscheinlichkeit in der einen oder anderen Form auch von den Aufsichtsbehörden anderer Bundesländer übernommen werden wird, um den aktuellen Status der Anpassung zu ermitteln, haben wir uns entschlossen, den Fragebogen nicht nur – wie im letzten Info-Brief – als Link, sondern als Dokument mit in den Info-Brief aufzunehmen (vgl. nachfolgende Seiten).

Mit der Beantwortung des Fragebogens und der internen Absprache über das weitere Vorgehen dürften Sie als Datenschutzbeauftragte(r) ebenso wie als verantwortliche Geschäftsführung / Vorstand optimal auf etwaige Anfragen von Landesdatenschutzbehörden vorbereitet sein.

**Fragebogen des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA)**

<b>I. Struktur und Verantwortlichkeit im Unternehmen</b>	
1	<ul style="list-style-type: none"> <li>• Gibt es das Bewusstsein im Unternehmen das Datenschutz Chefsache ist, beispielsweise durch</li> <li>• Vorhandensein einer Datenschutzleitlinie</li> <li>• Beschreibung der Datenschutzziele</li> <li>• Regelung der Verantwortlichkeiten</li> <li>• Bewusstsein über Datenschutzrisiken</li> <li>• Transparenz über Zielkonflikte (z. B. zwischen Marketing- und Rechtsabteilung)</li> </ul>
2	<ul style="list-style-type: none"> <li>• Verfügt Ihr Unternehmen über einen betrieblichen Datenschutzbeauftragten?</li> <li>• Wenn nein, warum nicht?</li> <li>• Wenn ja, ist geklärt, wann er von wem einzubeziehen ist?</li> <li>• Wenn ja, ist er schon gem. Art. 37 Abs. 8 DS-GVO der zuständigen Aufsichtsbehörde gemeldet?</li> </ul>
<b>III. Übersicht über Verarbeitungen</b>	
1	<ul style="list-style-type: none"> <li>• Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem. Art. 39 DS-GVO?</li> <li>• Wenn nein, warum nicht? Ist das dokumentiert?</li> <li>• Wie haben Sie sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Unternehmen Berücksichtigung finden (Privacy by Design-Art. 25 DS-GVO)?</li> </ul>
<b>IV. Einbindung Externer</b>	
1	<ul style="list-style-type: none"> <li>• Haben Sie ein Externe zur Erledigung Ihrer Arbeiten (Auftragsverarbeiter) eingebunden?</li> <li>• Wenn ja, haben Sie eine Übersicht über die Auftragsverarbeiter?</li> <li>• Wenn ja, haben Sie mit allen Ihren Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DS-GVO abgeschlossen?</li> </ul>
<b>V. Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte</b>	
1	<ul style="list-style-type: none"> <li>• Haben Sie Ihre Texte zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 DS-GVO angepasst?</li> <li>• Wenn nein, warum nicht?</li> </ul>
1	<ul style="list-style-type: none"> <li>• Haben Sie insbes. folgende Informationen neu aufgenommen, sofern nicht bereits vorher enthalten:             <ul style="list-style-type: none"> <li>• Kontaktdaten des Datenschutzbeauftragten</li> <li>• Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten</li> </ul> </li> <li>• Falls Sie die Verarbeitung mit ihren berechtigten Interessen oder berechtigten Interessen eines Dritten begründen. die berechtigten Interessen</li> </ul>

	<ul style="list-style-type: none"> <li>● Falls Sie Daten in Drittländer übermitteln: die von Ihnen zum Einsatz gebrachten geeigneten Garantien zum Schutz der Daten (z. B. Standarddatenschutzklauseln)</li> <li>● Dauern der Speicherung; sofern nicht möglich, die Kriterien für die Festlegung dieser Dauer</li> <li>● Bestehen der Rechte betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung auf Widerspruch aufgrund besonderer Situation einer betroffenen Personen sowie auf Datenportabilität</li> <li>● Sofern Verarbeitung auf Einwilligung beruht, das Recht zum jederzeitigen Widerruf der Einwilligung</li> <li>● Recht auf Beschwerde bei der Aufsichtsbehörde</li> <li>● Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist</li> <li>● sofern einschlägig: die Vornahme einer automatisierten Entscheidungsfindung einschließlich Profiling sowie - in diesem Fall - Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der Verarbeitung für die betroffene Personen</li> <li>● Sofern Sie die Daten nicht beider betroffenen Person erhoben haben: aus welcher Quelle die personenbezogenen Daten stammen und ggf. ob die aus öffentlich zugänglichen Quellen stammen.</li> <li>● Haben Sie Ihre Werbe-Einwilligungserklärungen für Kunden, Interessenten usw., an die Anforderungen von Art. 7 und 13 DS-GVO angepasst (Insbesondere: erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung)?</li> </ul>
2	<ul style="list-style-type: none"> <li>● Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 DS-GVO zeitnah und vollständig erfüllen zu können (Art. 12 Abs. 1 DS-GVO)?</li> </ul>
3	<ul style="list-style-type: none"> <li>● Haben Sie Verfahren eingerichtet, um Anträge auf Datenübertragbarkeit betroffener Personen erfüllen zu können (Art. 20 DS-GVO)?</li> </ul>

## VI. Verantwortlichkeit, Umgang mit Risiken

1	<ul style="list-style-type: none"> <li>● Gibt es für jede Verarbeitungstätigkeit Angaben mit der Sie die Rechtmäßigkeit Ihrer Verarbeitung nachweisen können, z. B. Bezüglich Zwecken, Kategorien personenbezogener Daten, Empfängern und/oder Löschristen (Art. 5 Abs. 2 DS-GVO)?</li> <li>● Haben Sie geprüft, ob die Einwilligungen, auf die Sie eine Verarbeitung stützten, noch den Voraussetzungen der Art. 7 und/oder 8 DS-GVIO entsprechen?</li> <li>● Können sie das Vorliegen der Einwilligung nachweisen?</li> </ul>
2	<ul style="list-style-type: none"> <li>● Haben Sie ein Datenschutzmanagementsystem installiert, um sicherzustellen und den Nachweis erbringen zu können, dass Ihre Verarbeitung gemäß der DS-GVO erfolgt (Art. 24 Abs. 1 DS-GVO)?</li> </ul>
3	<ul style="list-style-type: none"> <li>● Haben Sie Ihre bestehenden Prozesse zur Überprüfung der Sicherheit der Verarbeitung auf die neuen Anforderungen des Art. 32 DS-GVO angepasst?</li> <li>● Haben Sie insbesondere bestehende Checklisten zur Auswahl von technischen und organisatorischen Maßnahmen durch eine risikoorientierte Betrachtungsweise auf Basis von Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten ersetzt?</li> </ul>

	<ul style="list-style-type: none"> <li>• Wurde ein geeignetes Managementsystem zur regelmäßigen Überprüfung, Bewertung und Verbesserung der Security-Maßnahmen umgesetzt?</li> <li>• Wurden Schutzmaßnahmen wie Pseudonymisierung und der Einsatz von kryptographischen Verfahren zum Schutz vor unbefugten oder unrechtmäßigen Verarbeitungen sowohl bezüglich externer als auch interner „Angreifer“ umgesetzt?</li> </ul>
4	<ul style="list-style-type: none"> <li>• Haben Sie sich auf die evtl. Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung vorbereitet?</li> <li>• Haben Sie eine geeignete Methode zur Bestimmung der Frage, ob eine Datenschutz-Folgenabschätzung durchzuführen ist, in Ihrem Unternehmen eingeführt?</li> <li>• Haben Sie eine geeignete Risikomethode zur Durchführung einer Datenschutz-Folgenabschätzung in Ihrem Unternehmen eingeführt? Haben Sie sich für einen Prozess der Datenschutz-Folgenabschätzung entschieden; haben Sie diesen schon einmal getestet?</li> </ul>
<b>VII. Datenschutzverletzungen</b>	
1	<ul style="list-style-type: none"> <li>• Haben Sie gem. Art. 33 DS-GVO sichergestellt, dass die Meldung von Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden an die Aufsichtsbehörde möglich ist?</li> <li>• Haben Sie insbesondere sichergestellt, dass Datenschutzverletzungen in Ihrem Unternehmen erkannt werden können. Haben Sie dazu eine geeignete Methode zur Ermittlung eines Risikos bzw. eines hohen Risikos in Ihrem Unternehmen eingeführt?</li> <li>• Haben Sie einen Prozess aufgesetzt, wie mit potentiellen Verletzungen intern umzugehen ist?</li> <li>• Haben Sie festgelegt, wer, wann und wie mit der Datenschutzaufsichtsbehörde kommuniziert?</li> </ul>

.....

## MEDIEN – TECHNIK – SICHERHEIT

### 5 Akten digital archivieren: Das ist wichtig

Ergänzend zum Bericht der Juni-Ausgabe des Info-Briefes, in dem wir die Archivierung von E-Mails thematisiert haben, möchten wir in dieser Ausgabe die Frage der Archivierung von Akten mit einem zusammenfassenden Artikel aufgreifen, den die „[Deutsche Handwerks Zeitung – Die Wirtschaftszeitung für den Mittelstand](#)“ veröffentlicht hat.

Die digitale Archivierung gewinnt nicht erst seit der Diskussion rund um das Schlagwort „Industrie 4.0“ an Bedeutung. Die selbst in kleinen Institutionen kaum mehr zu überblickende Vielfalt an zu verwaltenden und zu archivierenden Dokumenten macht eine digitale Archivierung in vielen Fällen nahezu unumgänglich. Wer seine Datenbestände digital archivieren möchte, benötigt dazu nicht nur individuell abgestimmte (und schriftlich fixierte) Archivierungsregeln und -richtlinien, sondern hat darüber hinaus auch eine Reihe von gesetzlichen Vorschriften zu beachten. Der auf der Website der Deutschen Handwerks Zeitung veröffentlichte Text erläutert in knapper und übersichtlicher Form, welchen gesetzlichen Bestimmungen zu beachten sind. Er bezieht sich dabei auf die "Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)", in denen in 10 Punkten die gesetzlichen Vorgaben für die IT-gestützte Buchführung zusammengefasst sind. Dazu gehören unter anderem Kriterien wie Unveränderbarkeit, Vollständigkeit oder Nachvollziehbarkeit der Unterlagen:

1. Elektronische Archivierung ist technologieneutral
  2. Die Archivierung von Belegen muss zeitnah zu erfolgen
  3. Die elektronische Archivierung muss eine Unveränderbarkeit sicherstellen
  4. Archivierte Objekte müssen mit einem Index versehen werden
  5. Elektronisch archivierte Akten müssen lesbar und auswertbar bleiben
  6. Steuerrelevante Daten dürfen im elektronischen Archivsystem aufbewahrt werden
  7. Elektronisch archivierte Objekte unterliegen der Betriebsprüfung
  8. Das elektronische Archivsystem darf vom Betriebsprüfer genutzt werden
  9. Die elektronische Archivierung darf unter bestimmten Voraussetzungen auch im Ausland erfolgen
  10. Das elektronische Archivierungsverfahren ist zu dokumentieren. [[LINK zum vollständigen Text](#)]
-

## GESETZGEBUNG

## 6 Neu im Bundesgesetzblatt: Das neue Bundesdatenschutzgesetz, das am 25. Mai 2018 in Kraft tritt

Ab dessen Geltung ersetzt es das Bundesdatenschutzgesetz in der bisherigen Fassung. Neben dem Bundesdatenschutzgesetz wurden weitere Regelungen des Datenschutzes neu gefasst. Das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU) ist abrufbar unter [LINK zum Gesetz](#).

## 7 Das Datenschutz-Anpassungs- und -Umsetzungsgesetz aus der Sicht der Landesdatenschutzbehörden

Bis zum Zeitpunkt der Recherche (24.-26.7.2017) wurde das am 27.04.2017 abschließend verabschiedete DSAnpUG-EU auf den Webseiten der Landesdatenschutzbehörden inhaltlich noch nicht in größerem Umfang aufgegriffen.<sup>2</sup> Die meisten der Landesdatenschutzbehörden, die Bezug auf das Anpassungsgesetz nehmen, beziehen sich weiterhin auf den Entwurf der Bundesregierung aus dem Februar 2017, der aber im Verlauf der weiteren Beratungen und unter dem Einfluss zahlreicher kritischer Kommentare vor seiner Verabschiedung überarbeitet wurde. Lediglich auf den Webseiten der Landesdatenschutzbehörden von Niedersachsen und Nordrhein-Westfalen finden sich erste Hinweise. Während sich Nordrhein-Westfalen auf einen – allerdings unkommentierten – LINK zum Gesetzestext begnügt, hat die niedersächsische Landesdatenschutzbeauftragte, Barbara Thiel, einen ersten kritischen Kommentar veröffentlicht.

Das vom Bundestag beschlossene neue Datenschutzgesetz stellt, so die Landesdatenschutzbeauftragte Niedersachsens Niedersachsen und gegenwärtig Vorsitzende der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, „bewährte datenschutzrechtliche Standards in Frage und ist europarechtlich zweifelhaft“.

Aus Sicht B. Thiels missachte das Gesetz an einigen Stellen, so z.B. bei den „Vorgaben zur Verarbeitung besonders sensibler personenbezogener Daten wie Gesundheitsdaten oder genetischen Daten das Europarecht“. Auch schränke das Gesetz „die Informations-, Auskunfts- und Löschrechte der betroffenen Personen erheblich ein“. „Gegenüber dem gegenwärtigen Schutzniveau sei das, so Thiel weiter, „ein Rückschritt“.

„Nicht überzeugen“ kann aus Sicht Thiels „auch die Regelung zur Vertretung der Aufsichtsbehörden im Europäischen Datenschutzausschuss (EDSA), dem zukünftig eine zent-

---

<sup>2</sup> Explizit hinweisen möchten wir an dieser Stelle auf die Unterscheidung zwischen der EU Datenschutzgrundverordnung (EU-DSGVO), die auf den Websites der Landesdatenschutzbehörden aller Bundesländer dokumentiert und zum Teil auch sehr ausführlich kommentiert ist, und dem gerade verabschiedeten DSAnpUG der Bundesregierung, in dem es um die speziellen deutschen Regelungen geht, die aufgrund der Öffnungsklausen der EU-DSGVO von den nationalen Gesetzgebern verabschiedet werden können.

rale Bedeutung zukomme, da dieser Beschlüsse treffen könne, die für alle Datenschutz-Aufsichtsbehörden bindend seien. Thiel: „Hier werden die Länderinteressen unzureichend berücksichtigt. In Angelegenheiten, in denen allein die Aufsichtsbehörden der Bundesländer sachlich zuständig sind, sollte den Landesbehörden auch das Recht zur Vertretung auf europäischer Ebene zugestanden werden.“ [[Pressemitteilung vom 28.4.17](#)]

In den nächsten Wochen werden sich sicher auch andere Landesdatenschutzbehörden zum Datenschutz Anpassungsgesetz positionieren. Wir werden neben den Diskussionen in den diversen Datenschutzforen und den Kommentaren von Experten und -beratern ebenso auch die weitere Auseinandersetzung der Datenschutzbehörden verfolgen und in den kommenden Info-Briefen darüber berichten.

Neben den Diskussionen in Foren, Datenschutzbehörden und privaten Datenschutzunternehmen sind wir natürlich auch sehr interessiert zu erfahren, wie Sie mit dem Thema umgehen, ob und wie das Thema in Ihrem Verein / Verband diskutiert wird und nicht zuletzt auch, **welche Fragen Sie haben**. Das Portal bietet dazu sowohl in der Einrichtung eines eigenen Forums als auch mit den Live-Chats unterschiedliche Möglichkeiten der Unterstützung und des Austausches. **Wir würden uns freuen**, wenn Sie von diesen Möglichkeiten im Interesse aller Mitglieder des DS-Portals regen Gebrauch machen würden!!!

Wir werden in den nächsten Monaten auch einen Live-Chat unter dieses spezielle Motto stellen und Sie rechtzeitig über den Termin informieren, damit Sie zum einen den Termin rechtzeitig blocken können, Sie zum anderen genügend Zeit haben, Ihre speziellen Fragen zu stellen bzw. die spezifischen Probleme in Ihrem Verein / Verband zu schildern.

---

## 8 Beschäftigtendatenschutz und das neue BDSG – Das ändert sich

---

Der Beschäftigtendatenschutz (oder auch Arbeitnehmerdatenschutz) ist in der EU-Datenschutz-Grundverordnung nicht eigenständig geregelt worden. Vielmehr wurde die Regelungsbefugnis durch eine Öffnungsklausel an die Mitgliedsstaaten zurückgespielt. Von dieser hat die Bundesregierung Gebrauch gemacht und eine entsprechende Regelung zum Beschäftigtendatenschutz in das neu gefasste BDSG (BDSG-neu) aufgenommen.

Einen zusammenfassenden Beitrag, der die Kernelemente der von Bundestag und Bundesrat verabschiedeten Regelungen kommentierend vorstellt, haben die Autoren der Website „[Datenschutzbeauftragter Info – Informationen zum Datenschutz](#)“ veröffentlicht. Der Beitrag ist 6 Kapitel untergliedert (s.u.) und gibt einen guten Überblick über die neuen Regelungen und ihre Bedeutung für die Praxis.

- 1 Öffnungsklausel der Datenschutz-Grundverordnung
- 2 Vorgaben zum Arbeitnehmerdatenschutz im neuen Bundesdatenschutzgesetz
- 3 Bekannte Regelungen zum Beschäftigtendatenschutz
- 4 Neue Regelungen zum Arbeitnehmerdatenschutz
- 5 Worauf ist in Zukunft besonders zu achten?
- 6 Keine Reform des Arbeitnehmerdatenschutzes [[LINK zum vollständigen Artikel](#)]

## AKTUELLE URTEILE

## 9 Bundesgerichtshof (BGH) erleichtert Verfolgung illegaler Uploads in Tauschbörsen

Nutzerkennung und Anschrift dürfen ohne richterliche Genehmigung heraus gegeben werden

Quelle: *Bundesgerichtshof, Urteil vom 13.07.2017; Az. I ZR 193/16*

Fundort: [www.heise.de](http://www.heise.de)

In Internet-Tauschbörsen kursieren die neuesten Filme und Musikalben. Die Rechteinhaber betreiben viel Aufwand, um den Tätern auf die Schliche zu kommen. Ein Urteil räumt ihnen dabei einige Steine aus dem Weg. Das Nachsehen haben leichtsinnige Nutzer.

Der Bundesgerichtshof (BGH) macht es geschädigten Firmen leichter, illegale Uploads von Filmen, Musik oder Spielen in Internet-Tauschbörsen aufzuklären. Um für eine Abmahnung oder Schadenersatz-Klage herauszufinden, wer dahintersteckt, brauchen sie vom Internet-Anbieter die Nutzerdaten. Die Herausgabe muss ein Richter genehmigen. In dem Fall, der am Donnerstag in Karlsruhe entschieden wurde, lag eine solche Genehmigung nur für die Anfrage beim Netzbetreiber vor, hier bei der Deutschen Telekom.

### Eine Genehmigung für mehrere Anfragen

Kundin war die gesuchte Nutzerin aber beim Anbieter 1&1, der schließlich ohne weitere Genehmigung Namen und Anschrift herausgab. Umstritten war deshalb, ob die Daten vor Gericht gegen die Anschluss-Inhaberin verwendet werden dürfen. Die Frau, die über die Tauschbörse ein Computerspiel zur Verfügung gestellt haben soll, war in den Vorinstanzen ungestraft davongekommen. Nun muss ihr Fall neu verhandelt werden. Denn der BGH stellt klar: Eine Genehmigung reicht für beide Abfragen, bei Telekom und 1&1. (Az. I ZR 193/16)

Um die kostenlose Verbreitung ihrer Produktionen einzudämmen, suchen viele Rechteinhaber das Netz gezielt nach Filesharing-Verstößen ab. Mit der IP-Adresse versuchen sie zurückzuverfolgen, von welchem Internet-Anschluss aus die Datei angeboten wurde. Dafür braucht es aber die Unterstützung der Anbieter.

In dem Karlsruher Fall fand die Telekom heraus, dass die IP-Adresse über 1&1 vergeben wird, und teilte die Nutzerkennung mit. Anhand dieser Kennung ermittelte 1&1 im zweiten Schritt den Namen und die Adresse der gesuchten Kundin. [[Zum vollständigen Artikel](#)]

## 10 Antrag der Deutschen Telekom AG gegen Verpflichtung zur anlasslosen Speicherung von Telekommunikationsverkehrsdaten erfolglos

VG Köln lehnt Antrag mangels Rechtsschutzinteresses ab

Quelle: *Verwaltungsgericht Köln, Urteil vom 30.06.2017; AZ: 9 L 2085/17*

Fundort: [kostenlose-urteile.de](http://kostenlose-urteile.de) (ra-online GmbH), Berlin 03.07.2017, Dok.-Nr.: 24486

Das Verwaltungsgericht Köln hat einen Antrag der Deutschen Telekom AG abgelehnt, mit dem diese die Feststellung begehrt hat, nicht zur anlasslosen Speicherung von Telekommunikationsverkehrsdaten (Vorratsdatenspeicherung) verpflichtet zu sein.

Im zugrunde liegenden Fall hatte die Deutsche Telekom AG zunächst beantragt, festzustellen, dass sich die Speicherpflicht nach § 113 b Abs. 3 TKG nicht auf Internetverbindungen erstreckt, die unter Einsatz des sogenannten NAPT-Verfahren insbesondere bei öffentlichen Hotspots und im Mobilfunkbereich hergestellt werden. Nachdem das Obergerverwaltungsgericht Nordrhein-Westfalen mit Beschluss vom 22. Juni 2017 vorläufig festgestellt hatte, dass die dortige Antragstellerin insgesamt nicht verpflichtet sei, Verkehrsdaten ihrer Kunden, denen sie den Internetzugang vermittelt, zu speichern [[LINK zum Fundort / \(kostenlose-urteile.de v. 23.6.17\)](#)] und dies mit der Europarechtswidrigkeit der Norm begründet hatte, veröffentlichte die Bundesnetzagentur auf ihrer Internetseite eine Erklärung, wonach sie bis zum rechtskräftigen Abschluss eines Hauptsacheverfahrens gegenüber allen Telekommunikationsunternehmen davon absehen werde, Maßnahmen wegen des Verstoßes gegen die Speicherpflicht nach § 113 b TKG zu ergreifen. ...

Diesen Antrag lehnte das Verwaltungsgericht Köln nun mangels Rechtsschutzinteresses ab. Zur Begründung führte das Gericht aus, dass die Erklärung der Bundesnetzagentur im Rahmen des auf einstweiligen Rechtsschutz gerichteten Verfahrens ausreichend sei. Der von der Antragstellerin darüber hinaus erstrebte Schutz vor Einleitung strafrechtlicher Ermittlungen wegen des Unterlassens der Speicherung sei im vorliegenden Verfahren nicht zu erreichen. Eine Entscheidung wirke nur im Verhältnis zwischen den Beteiligten und nicht auch gegenüber den Strafverfolgungsbehörden. [[Zum vollständigen Artikel](#)]

---

## 11 OLG Köln verbietet Klausel über Verwendung früherer Kundendaten zur "individuellen Kundenberatung"

Vorformulierte Einwilligungserklärung der Telekom Deutschland GmbH unzulässig

*Quelle:* Oberlandesgericht Köln, Urteil vom 02.06.2017 - 6 U 182/16 -

*Fundort:* [© kostenlose-urteile.de \(ra-online GmbH\), Berlin 05.07.2017, Dok.-Nr.: 24496](#)

Das Oberlandesgericht Köln hat eine Einwilligungs-erklärung der Telekom Deutschland GmbH über die Nutzung von Vertragsdaten für Werbenachrichten oder -anrufe zur "individuellen Kundenberatung" nach Vertragsende untersagt.

Im zugrunde liegenden Rechtsstreit konnten Verbraucher beim Abschluss eines Telefonvertrags auf der Webseite der Telekom Deutschland GmbH per Klick in die Nutzung ihrer Vertragsdaten zur "individuellen Kundenberatung" bis zum Ende des auf die Kündigung folgenden Kalenderjahres einwilligen. Das Unternehmen wollte seine ehemaligen Kunden über neue Angebote und Services per E-Mail, Telefon, SMS oder MMS informieren und beraten. Ein späterer Widerruf war jederzeit möglich.

### Verbraucherzentrale rügt unangemessene Benachteiligung von Verbrauchern

Der Bundesverband der Verbraucherzentralen sah in der Klausel eine unangemessene Benachteiligung von Verbrauchern, weil sie mehrere Werbekanäle in einer Einwilligungserklärung zusammenfasse und die Kontaktaufnahme für einen unzumutbar langen Zeitraum nach Vertragsende erlaube. Nach Auffassung der Verbraucherzentrale könnten nicht alle Verbraucher wissen, worauf sich die Befugnis genau beziehe. Später müssten

sie auch noch selbst die Initiative ergreifen, um ihre ungestörte Privatsphäre wieder herzustellen.

### **Klausel verstößt gegen Verbot belästigender Werbung**

Das Oberlandesgericht Köln sah die vorformulierte Einwilligungserklärung ebenfalls als unzulässig an und hob das Urteil der Vorinstanz auf. Demnach verstoße die Werbefähigkeit gegen das Verbot belästigender Werbung. Sie erlaube dem Unternehmen, Vertragsdaten eines Verbrauchers in erheblichem Umfang zur "individuellen Kundenberatung" am Telefon zu verwenden. [[Zum vollständigen Artikel](#)]

---

## **12 Journalist macht sich mit Veröffentlichung eines ungepixelten Bildes eines vermeintlichen Ebola-Patienten strafbar**

Weitergabe der Bilddatei ohne jegliche Verfremdung stellt massive Beeinträchtigung des allgemeinen Persönlichkeitsrechts des Patienten dar

*Quelle:* Oberlandesgericht Köln, Beschluss vom 02.06.2017 - III -

*Fundort:* [www.kostenlose-urteile.de](http://www.kostenlose-urteile.de) (ra-online GmbH), Berlin 07.07.17; Dok.-Nr.: 24518

---

### **Worum geht es?**

Das Oberlandesgericht Köln hat entschieden, dass sich ein Fotojournalist strafbar machen kann, wenn er Fotos eines Krankenhauspatienten gegen dessen Willen fertigt und an eine Redaktion weitergibt, ohne auf eine Unkenntlichmachung der Bilder hinzuwirken.

Im zugrunde liegenden Fall arbeitete ein Fotojournalist an einer Fernsehdokumentation über Ebola. Er bemerkte im Klinikum Aachen einen dunkelhäutigen Patienten, der von Mitarbeitern des Klinikums mit Mundschutz und Handschuhen versorgt und aufgefordert wurde, von den anderen Patienten Abstand zu halten. Der Journalist schnappte außerdem u.a. das Wort "Ebola" auf. Daraufhin fertigte er ungefragt Fotos des Patienten und folgte diesem mit seinem Fotohandy ins Behandlungszimmer. Obwohl der Patient erklärte, dass er keine Fotos von sich wolle, obwohl die behandelnde Ärztin den Journalisten bat, die Fotos zu löschen und obwohl die Ärztin ihm mitteilte, dass sich der Ebola-Verdachtsfall nicht bestätigt habe, konnte weder diese noch die hinzugerufene Polizei den Journalisten zum Löschen der Bilder bewegen. Vielmehr bot er die Fotos zusammen mit einer inhaltlichen Information über die Vorkommnisse im Klinikum mehreren Redaktionen an. Eine Redaktion übernahm die Fotos. Dabei wurde nicht darüber gesprochen, ob der fotografierte Patient unkenntlich zu machen sei. In der Onlineausgabe der Zeitung erschien daraufhin ein ungepixeltes Foto des Patienten mit Mundschutz und Handschuhen und der Bezeichnung als "Ebola-Verdächtiger". In der Printausgabe erschienen Bilder, bei denen der Patient teilweise unkenntlich gemacht worden war.

### **Verbreitung von Bildern ohne Einwilligung des Betroffenen unzulässig**

Das Amtsgericht hatte den Journalisten wegen unbefugten Verbreitens eines Bildnisses zu einer Geldstrafe von 25 Tagessätzen verurteilt. Auf die Berufung der Staatsanwaltschaft hat das Landgericht Aachen die Strafe auf 40 Tagessätze erhöht. Die Revision des

Journalisten gegen seine Verurteilung blieb ohne Erfolg. Das Oberlandesgericht Köln bestätigte die Verurteilung wegen unbefugten Verbreitens eines Bildnisses gem. §§ 33 Abs. 1 Nr. 1, 22, 23 Kunsturhebergesetz (KunstUrhG). Nach dieser Vorschrift ist es strafbar, Bilder ohne Einwilligung des Betroffenen zu verbreiten. Bilder aus dem Bereich der Zeitgeschichte dürfen nur verbreitet werden, wenn dadurch kein berechtigtes Interesse des Abgebildeten verletzt wird.

### **Weitergabe der Bilddatei stellt strafbares Unrecht dar**

Das Gericht führte aus, dass die Berichterstattung über den Umgang mit Ebolaverdachtsfällen zwar der Zeitgeschichte zugeordnet werden könne. Die Weitergabe der Bilddatei ohne jegliche Verfremdung bzw. Unkenntlichmachung sei aber eine massive Beeinträchtigung des allgemeinen Persönlichkeitsrechts des Patienten. [[Zum vollständigen Artikel](#)]

-----

## **13 Daten aus Spähsoftware sind kein Kündigungsgrund**

Eine Firma ließ die Computer ihrer Mitarbeiter heimlich überwachen - und kündigte einem Angestellten, weil dieser den Rechner während der Arbeitszeit privat nutzte. Zu Unrecht, wie nun das Bundesarbeitsgericht urteilte.

*Quelle:* Bundesarbeitsgericht in Erfurt, Beschluss vom 02.06.2017 – AZ: 2 AZR 681/16

*Fundort:* <http://www.spiegel.de/karriere/bundesarbeitsgericht-daten-aus-spaehsoftware-sind-kein-kuendigungsgrund-a-1159968.html>

Das Bundesarbeitsgericht in Erfurt hat entschieden, dass Erkenntnisse aus Überwachungssoftware nicht für eine Kündigung genutzt werden dürfen - zumindest nicht, wenn die Software heimlich und ohne schwerwiegende Gründe installiert wurde. Der Einsatz von Keyloggern ist unzulässig, wenn "kein auf Tatsachen beruhender Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung gegeben ist" (Aktenzeichen 2 AZR 681/16). Die Software prüft die Tastatureingaben und macht regelmäßig Fotos von den Computerbildschirmen.

In dem verhandelten Fall hatte ein Webentwickler aus Nordrhein-Westfalen 2015 seine Arbeitszeit teilweise genutzt, um private Dinge zu erledigen. Der Vorgesetzte entdeckte das Fehlverhalten, nachdem er einen Keylogger installiert hatte, mit dem er seinen Computer ausspähen konnte.

Zuvor hatte er den Angestellten per E-Mail mitgeteilt, dass "sämtlicher Internet Traffic und die Benutzung der Systeme mitgelogged und dauerhaft gespeichert wird". [[LINK zum vollständigen Artikel](#)]

-----



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

Tel. 0221/221 220 13  
Fax: 0221/221 220 14  
[info@fuehrungs-akademie.de](mailto:info@fuehrungs-akademie.de)  
[www.fuehrungs-akademie.de](http://www.fuehrungs-akademie.de)