ISSN 0178-8930
HZ201947

G 20 141

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

RDV

6/2019

Recht der Datenverarbeitung

Herausgegeben von

Peter Gola · Andreas Jaspers · Rolf Schwartmann · Gregor Thüsing
in Kooperation mit der
Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

Aufsätze

PILTZ/HÄNTSCHEL, Der Datenschutzbeauftragte – Anwalt, Berater, Haftungsobjekt?

BENEDIKT, ePrivacy-VO – Was lange währt, wird endlich gut?

THIEL, Prüfung der LfD Niedersachsen zur Umsetzung der DS-GVO in Unternehmen – die Ergebnisse

Kurzbeiträge

GOLA, Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (44): Der ThürLfDI zu Foto- und Filmaufnahmen mit und ohne Einwilligung

CLAUS/REIF, Praxisfälle zum Datenschutz II: Musterfalllösung zur Kundendatenverwaltung im Konzern

Rechtsprechung

Aus dem Inhalt

BAG, Zulässigkeit offener Videoüberwachung und Beweisverwertungsverbot

OLG DRESDEN, Heimliche Videoaufnahme zur Aufdeckung von Missständen im Pflegeheim (Ls)

OLG FRANKFURT/M., Freiwilligkeit einer Einwilligung zur Werbung bei Koppelung mit Gewinnspielteilnahme

LAG SACHSEN, Amt des Datenschutzbeauftragten neben dem Amt als Vorsitzenden des Betriebsrats möglich

LSG THÜRINGEN, Nichtigkeit der Abtretung ärztlicher Forderung bei Verletzung der Schweigepflicht

OVG SAARLOUIS, Zum Zeitpunkt der Beurteilung datenschutzbehördlicher Anordnungen (Ls)

35. Jahrgang
Dezember 2019
Seiten 275–324

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

GDD-FORUM

Fortbildungsveranstaltung gem.
Art. 38, Abs. 2 DS-GVO/§§ 5, 6, 38 BDSG

GEMEINSAME VERANTWORTLICHKEIT:

Die neue Auftragsverarbeitung?

Einordnung, Praxisbeispiele, Haftungsrisiken und Vertragsmuster

SCHWERPUNKTE

- Überblick: Wann liegt eine gemeinsame Verantwortlichkeit vor?
- Was bedeuten die EuGH Entscheidungen zu Facebook Fanpages, Zeugen Jehovas und Fashion ID?
- Andere Social Media und Online-Services als gemeinsame Verantwortlichkeit?
- Was gilt für Tracking-Tools wie Google Analytics?
- Wie kann die Auftragsverarbeitung abgegrenzt werden?
- Wie kann die frühere Funktionsübertragung abgegrenzt werden?
- Checkliste für die Abgrenzung zwischen den verschiedenen Konstellationen

12. März 2020 in Berlin
1. September 2020 in Frankfurt/M.

Referenten:
Andreas Jaspers, Sascha Kremer,
Prof. Dr. Rolf Schwartmann

890 € zzgl. gesetzl. MwSt.
(für GDD-Mitglieder 790 € zzgl. MwSt.)

Weitere Infos unter: datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Zeitschrift für
Datenschutz–, Informations-
und Kommunikationsrecht

35. Jahrgang 2019
Heft 6
Seiten 275–324

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial 275

Veranstaltungen 276

Aufsätze

Dr. Carlo PILTZ/Sandra HÄNTSCHEL
Der Datenschutzbeauftragte – Anwalt, Berater, Haftungsobjekt? **277**

Kristin BENEDIKT
ePrivacy-VO – Was lange währt, wird endlich gut? **283**

Barbara THIEL
Prüfung der LfD Niedersachsen zur Umsetzung der DS-GVO in Unternehmen – die Ergebnisse **291**

Kurzbeiträge

Prof. Peter GOLA
Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (44): Der ThürLfDI zu Foto- und Filmaufnahmen mit und ohne Einwilligung **295**

Miriam CLAUS, LL.B./RAin Yvette REIF, LL.M.
Praxisfälle zum Datenschutz II: Musterfalllösung zur Kundendatenverwaltung im Konzern **299**

Rechtsprechung

Zulässigkeit offener Videoüberwachung und Beweisverwertungsverbot
(BAG, Urteil vom 28.03.2019) **303**

Heimliche Videoaufnahme zur Aufdeckung von Missständen im Pflegeheim (Ls)
(OLG Dresden, Urteil vom 24.09.2019) **309**

Freiwilligkeit einer Einwilligung zur Werbung bei Koppelung mit Gewinnspielteilnahme
(OLG Frankfurt/M., Urteil vom 27.07.2019) **310**

Amt des Datenschutzbeauftragten neben dem Amt als Vorsitzenden des Betriebsrats möglich
(LAG Sachsen, Urteil vom 19.08.2019) **310**

Nichtigkeit der Abtretung ärztlicher Forderung bei Verletzung der Schweigepflicht
(LSG Thüringen, Beschluss vom 26.08.2019) **313**

Zum Zeitpunkt der Beurteilung datenschutzbehördlicher Anordnungen (Ls)
(OVG Saarlouis, Beschluss vom 10.09.2019) **313**

Rechtsverletzung durch Betrieb von Google Analytics ohne „anonymizeIP“
(LG Dresden, Urteil vom 11.01.2019) **314**

Zur Veröffentlichung eines Lehrerfotos im Schuljahrbuch
(VerwG Koblenz, Urteil vom 06.09.2019) **317**

Zur Wahrung der Vertraulichkeit eines behördlichen Informanten (Ls)
(VerwG Minden, Urteil vom 26.08.2019) **318**

Information des Personalrats über die Anordnung gesundheitlicher Untersuchungen nur in anonymisierter Form (Ls)
(VerwG Darmstadt, Beschluss vom 30.07.2019) **318**

Berichte, Informationen, Sonstiges

EuGH: Das Setzen von Cookies erfordert die aktive Einwilligung des Internetnutzers **320**

DSK positioniert sich zu Personenkennzeichen **320**

Bitkom: Das digitale Büro erobert den Mittelstand **320**

Literaturhinweise

Buchbesprechungen

Katharina Höhne, Auswirkungen der unionsrechtlichen Öffnungsklausel (REDAKTION) **321**

Christina-Maria Leeb, Digitalisierung, Legal Technology und Innovation (REDAKTION) **321**

Jürgen Taeger (Hrsg.), Die Macht der Daten und der Algorithmen – Regulierung von IZ, IoT und KI (GOLA) **322**

Neuerscheinungen

Aufsätze **323**

Nachgefasst **324**

Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

Prof. Dr. Rolf SCHWARTMANN, Leiter der Kölner Forschungsstelle für Medienrecht, Technische Hochschule Köln

Prof. Dr. Gregor THÜSING, LL.M. (Harvard), Universität Bonn

in Kooperation mit der
Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

Herausgeberbeirat

Prof. Dr. Ralf Bernd ABEL, Rechtsanwalt, Hamburg

Dietrich BOEWER, Vorsitzender Richter am Landesarbeitsgericht Düsseldorf i.R.

Prof. Dr. Alfred BÜLLESBACH, Universität Bremen

Prof. Dr. Horst EHMANN, Universität Trier

Dr. Joachim W. JACOB, Bundesbeauftragter für den Datenschutz a.D.

Prof. Dr. Friedhelm JOBS, Richter am Bundesarbeitsgericht a.D.

Prof. Dr. Tobias O. KEBER, Hochschule der Medien, Stuttgart

Prof. Dr. Karl LINNENKOHL, Universität Kassel

Dr. Alexander OSTROWICZ, Präsident des Landesarbeitsgerichts Schleswig-Holstein a.D.

Prof. Dr. Michael RONELLENFITSCH, Hessischer Datenschutzbeauftragter

Prof. Dr. Friedhelm ROST, Vorsitzender Richter am Bundesarbeitsgericht a.D.

Peter SCHAAR, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit a.D.

Prof. Dr. Mathias SCHWARZ, Rechtsanwalt, München

Prof. Dr. Dres. h.c. Spiros SIMITIS, Universität Frankfurt

Prof. Dr. Jürgen TAEGER, Universität Oldenburg

PD Dr. Irini VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis: GDD-Mitteilungen 6/2019; DATAKONTEXT, Frechen; C.H. Beck, München

Manuskripte:
Zuschriften und Manuskriptsendungen, die den Inhalt der Zeitschrift betreffen, werden an die Schriftleitung erbeten. Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. Beiträge werden grundsätzlich nur angenommen, wenn sie nicht einer anderen Zeitschrift zur Veröffentlichung angeboten wurden. Mit der Annahme zur Veröffentlichung erwirbt der Verlag vom Autor alle Rechte, insbesondere das Recht der weiteren Vervielfältigung zu gewerblichen Zwecken mit Hilfe fotomechanischer oder anderer Verfahren.

Urheber- und Verlagsrechte:
Sie sind einschließlich der Veröffentlichung als PDF im Online-Archiv vorbehalten. Sie erstrecken sich auch auf die veröffentlichten Gerichtsentscheidungen und deren Leitsätze; diese sind geschützt, soweit sie vom Einsender oder von der Schriftleitung erstellt oder bearbeitet sind. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen: Diese bedürfen zur Auswertung einer Genehmigung des Verlages.
Der Verlag gestattet in der Regel die Herstellung von Fotokopien zu innerbetrieblichen Zwecken, wenn dafür eine Gebühr an die VG Wort, Abteilung Wissenschaft, Goethestraße 49, 80336 München, entrichtet wird, von der die Zahlungsweise zu erfragen ist.

Schriftleitung
Prof. Peter Gola (federführend)
RA Dr. Georg Wronka
RA Andreas Jaspers
RDV-Schriftleitung@gdd.de

Redaktionsanschrift
Birgit Koppitsch
Heinrich-Böll-Ring 10, 53119 Bonn
Telefon: (02 28) 96 96 75-00
Telefax: (02 28) 96 96 75-25
RDV-Redaktion@gdd.de

Erscheinungsweise
6 x jährlich

Bezugspreis

Jahresabonnement	€ 139,–
Einzelheft	€ 25,–

MwSt. im Preis enthalten
jeweils zzgl. Versandkosten

Vertrieb:
Jürgen Weiß
Telefon: (02234) 989 49-71
weiss@datakontext.com

Abo-Service:
Telefon: 089-2183-7110
Telefax: 089-2183-32
aboservice@hjr-verlag.de

Abbestellungen
Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.

Verlag
DATAKONTEXT GmbH, Frechen
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-30
Telefax: (0 22 34) 9 89 49-32
www.datakontext.com
Geschäftsführung: Dr. Karl Ulrich;
Hans-Günter Böse
HRB 337678

Satz
alka mediengestaltung gmbh
Willmuthstraße 30, 53332 Bornheim-Sechtem

Druck
AZ Druck und Datentechnik GmbH
Heisinger Straße 16, 87437 Kempten

Anzeigenverwaltung
DATAKONTEXT GmbH, Frechen
Wolfgang Scharf
Telefon: (0221) 25 08-60 71
wolfgang.scharf@agentur-8020.de
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Zeitschrift für
Datenschutz–, Informations- und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
35. Jahrgang 2019 Heft 6
Seiten 275 – 324

RDV
Recht der Datenverarbeitung

35. Jahrgang · Dezember 2019 · Seiten 275 – 324

Editorial

Status im Schwebestand: Die Mitarbeitervertretung

Nach Inkraftreten der DS-GVO steht die Frage im Raum, ob Betriebs-und Personalräte „datenschutzrechtlich" weiterhin Teil der „verantwortlichen Stelle", also Teil ihres Unternehmens oder ihrer Behörde sind. Dies war bis dato weitgehend einhellige Meinung von Rechtsprechung (anders bereits das LAG Sachsen-Anhalt, Beschl. v. 10.12.2018 – 4 ToB 19 17 Rn. 51) und Literatur. Gleichwohl hatte jedoch das BAG (Beschl. v. 11.11.1997 – ABR 217/97; und v. 12.08.2009 – ABR 15/08) den Betriebsrat auf Grund seiner betriebsverfassungsrechtlichen Eigenständigkeit vom Kontrollrecht des „als Organ des Arbeitgebers" eingestuften betrieblichen Datenschutzbeauftragten ausgenommen.

Eindeutig ist zunächst, dass diese Auffassung nicht mehr haltbar ist. Art. 38 Abs. 2 DS-GVO weist dem DSB ein uneingeschränktes Kontrollrecht zu, das durch nationale Gesetzgebung oder Rechtsprechung nicht eingeschränkt werden kann (z.B. Kort, ZD 2017, 3 (6)). Gleichwohl bleibt die Frage, ob für die Ausübung des Kontrollrechts der betriebliche/behördliche DSB oder ein von der Mitarbeitervertretung zu bestellender eigener Beauftragter zuständig ist.

Ausgangspunkt der Überlegung ist, dass die DS-GVO in Art. 4 Nr. 7 neben natürlichen oder juristischen Personen, Personenvereinigungen des privaten Rechts oder Gesellschaften auch „andere Stellen" als Verantwortliche kennt. Voraussetzung ist, dass diese über die Verarbeitung personenbezogener Daten und darüber entscheiden, welche Zwecke und Mittel der Verarbeitung eingesetzt werden. Während einige Aufsichtsbehörden diese Kriterien bei der Mitarbeitervertretung bejahen (LfDI Baden-Württemberg, 34. TB (2018), Abschnitt 1.6.1 Nr. 3; ThürLfDI, 1. TB (2018), Abschnitt 5.12; i.E. wohl ablehnend Kranig, ZD 2019, 1) halten die Kommentarmeinungen und durchweg die Literatur (Baumgartner/Hansch, ZD 2019, 256; Stück, ZD 2019, 143 (146); Brahms/Möhrle, ZD 2018, 570; Lücke, NZA 2019, 658) an der Rolle des Betriebsrats als Teil der verantwortlichen Stelle fest. (Brunk/Joos NZA 2019, 1395)

In Thüringen hat der Gesetzgeber für den öffentlichen Bereich insoweit entsprechend der Auffassung des ThürLfDI eine andere, klare Rechtslage in § 80 Abs. 1 ThürPersVG geschaffen. Hiernach hat die Personalvertretung einen eigenen Datenschutzbeauftragten zu bestellen, wobei der Gesetzgeber der Personalvertretung und der Dienststelle quasi empfiehlt, im Einvernehmen einen gemeinsamen Datenschutzbeauftragten zu bestellen.

Nicht erkennbar ist, ob neben Thüringen und Bayern (vgl. BayLFD, Aktuelle Kurzinformation Nr. 23, 8.9.2019) auch andere Gesetzgeber eine diesbezügliche Gesetzgebung im Blick haben. Zu erwarten ist auch, dass Aufsichtsbehörden wegen der Unterschiedlichkeit ihrer Meinungen diese zunächst nicht mit Bußgeldandrohungen durchsetzen werden, wobei fraglich ist, ob ein Betriebsrat mangels Benennung eines DSB mit einem Bußgeld belegt werden kann. Somit besteht für Unternehmen und Behörden sowie deren Mitarbeitervertretungen noch kein unmittelbarer Handlungsbedarf. Gleichwohl können Unternehmen versuchen, durch freiwillige Vereinbarungen mit der Mitarbeitervertretung vorbeugend tätig zu werden.

Prof. Peter Gola

Prof. Peter Gola
Mitherausgeber und federführender Schriftleiter der Fachzeitschrift RDV sowie Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn.

Termin	Thema	Ort	Kontakt
09.01.2020	Repetitorium GDDcert. EU	Köln	GDD e.V. und DATAKONTEXT
15.01.2020	Die Aufgaben und der Tätigkeitsbericht des betrieblichen DSB praxisnah im Unternehmen	Frankfurt/M.	GDD e.V. und DATAKONTEXT
22.01.2020	Zertifizierung zum betrieblichen Datenschutzbeauftragten (GDDcert. EU)	Köln	GDD e.V. und DATAKONTEXT
27.-28.01.2020	GDD-Winter-Workshop	Garmisch-Partenkirchen	GDD e.V. und DATAKONTEXT
05.02.2020	Datenschutzverletzungen richtig behandeln	Frankfurt/M.	GDD e.V. und DATAKONTEXT
10.-14.02.2020	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V. und DATAKONTEXT
18.02.2020	Die ePrivacy-Verordnung im Zusammenspiel mit der DS-GVO	Frankfurt/M.	GDD e.V. und DATAKONTEXT
18.02.2020	Teleworking unter Beachtung von Datenschutz und Sicherheit	Köln	GDD e.V. und DATAKONTEXT
27.02.2020	Hacker-Tools für Datenschutzbeauftragte	Frankfurt/M.	GDD e.V. und DATAKONTEXT
02.03.2020	Planung und Umsetzung der Überwachungsaufgabe des DSB	Frankfurt/M.	GDD e.V. und DATAKONTEXT
03.03.2020	Datenschutz und IT-Sicherheit bei der Nutzung	Frankfurt/M.	GDD e.V. und DATAKONTEXT
04.03.2020	Der Brexit und seine datenschutzrechtlichen Folgen	Frankfurt/M.	GDD e.V. und DATAKONTEXT
05.03.2020	Big Data-Analysen nach DS-GVO und BDSG	Berlin	GDD e.V. und DATAKONTEXT
09.-10.03.2020	Datenschutz Kompakt	Köln	GDD e.V. und DATAKONTEXT
11.03.2020	Mobile Endgeräte im Zeitalter von DS-GVO und ePrivacy-Verordnung	Berlin	GDD e.V. und DATAKONTEXT
10.-12.03.2020	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Köln	GDD e.V. und DATAKONTEXT
12.03.2020	GDD-Forum Joint Controller – Gemeinsame Verantwortlichkeit: Die neue Auftragsverarbeitung?	Berlin	GDD e.V. und DATAKONTEXT
16.03.2020	Verteidigung gegen Bußgelder bei Datenschutzverstößen	Köln	GDD e.V. und DATAKONTEXT
16.03.2020	Datenlöschung und andere SAP-Funktionen für den Datenschutz	Berlin	GDD e.V. und DATAKONTEXT
17.03.2020	Strategischer Umgang mit Bußgeldbescheiden	Köln	GDD e.V. und DATAKONTEXT
18.03.2020	Datenschutz-Management light	Köln	GDD e.V. und DATAKONTEXT
19.03.2020	ISO 27001 und Datenschutz	Frankfurt/M.	GDD e.V. und DATAKONTEXT
26.03.2020	Löschen nach DS-GVO	Köln	GDD e.V. und DATAKONTEXT
30.03.2020	Websites datenschutzkonform gestalten	Köln	GDD e.V. und DATAKONTEXT
02.04.2020	Beschäftigtendatenverarbeitung nach DS-GVO und BDSG	Köln	GDD e.V. und DATAKONTEXT
02.04.2020	DS-GVO-konforme Verarbeitung personenbezogener Daten mit SAP-Systemen	Berlin	GDD e.V. und DATAKONTEXT

Datakontext GmbH, www.datakontext.com, Tel. 0 22 34 / 9 89 49 40

Aufsätze

Dr. Carlo Piltz/Sandra Häntschel

Der Datenschutzbeauftragte – Anwalt, Berater, Haftungsobjekt?

Datenschutzbeauftragte (DSB) sind seit Anwendbarkeit der DS-GVO begehrte Dienstleister. Jedoch existiert, abgesehen von den Anforderungen der DS-GVO an die Qualifikationen, keine offizielle staatlich gesteuerte oder überwachte Ausbildung. In der Praxis bieten die Dienstleistung als DSB daher Personen mit den verschiedensten beruflichen Hintergründen an. Seit dem 25. Mai 2018 war ein exponentielles Wachstum der Anzahl an Datenschutzexperten zu verzeichnen. Auch viele Rechtsanwälte sind als DSB tätig. Dies lässt sich eventuell auch damit begründen, dass sich durch die DS-GVO die Aufgaben von DSB mehr und mehr in den Bereich der rechtlichen Beratung entwickelt haben. So obliegt dem DSB nach Art. 39 DS-GVO die Aufgabe der Unterrichtung und Beratung gegenüber Unternehmen und deren Beschäftigten hinsichtlich ihrer Rechtspflichten nach der DS-GVO und sonstigen geltenden Datenschutzvorschriften. Auch können sich betroffene Personen nach Art. 38 Abs. 4 DS-GVO mit allen Fragen, welche die Verarbeitung ihrer personenbezogenen Daten und die Wahrung ihrer Rechte nach der DS-GVO betreffen, an den DSB wenden.[1] Möchte sich ein als Rechtsanwalt zugelassener Jurist zum DSB benennen lassen, muss er dabei jedoch eine Reihe von Aspekten beachten.[2]

I. Mindestaufgaben des Datenschutzbeauftragten nach Art. 39 Abs. 1 DS-GVO

Die Kernaufgaben des DSB sind gesetzlich vorgeschrieben und zwar über die DS-GVO unmittelbar bindend in jedem Mitgliedstaat der Europäischen Union. Die Aufgaben in Art. 39 Abs. 1 DS-GVO enthalten einen nicht national-staatlich reduzierbaren Mindestaufgabenkatalog.[3] Der Erfüllung der Aufgaben ist der risikobasierte Ansatz der DS-GVO zugrunde gelegt. Danach muss der DSB dem mit der Verarbeitung verbundenen Risiko gebührend Rechnung tragen (Art. 39 Abs. 2 DS-GVO).[4]

1. Unterrichtung und Beratung

Nach Art. 39 Abs. 1 lit. a DS-GVO hat der DSB die Pflicht zur „Unterrichtung" und „Beratung". Die Begriffe der Unterrichtung und Beratung haben grundsätzlich eine unterschiedliche Zielrichtung. „Unterrichtung" meint insbesondere, den Verantwortlichen und seine Beschäftigten allgemein über datenschutzrechtlich relevante Vorgänge zu informieren und sie für diese zu sensibilisieren.[5] Dies umfasst allgemeine Mitteilungen und Hinweise zu relevanten rechtlichen Themen und Entwicklungen, beispielweise neuen gesetzlichen Vorgaben und neuer Rechtsprechung, aber auch neuen technischen Entwicklungen, die zu Datenschutzrisiken führen können oder umgekehrt zusätzliche Schutzinstrumente eröffnen.[6] Die Aufgabe der „Beratung" bezieht sich demgegenüber auf eine konkrete Arbeitssituation und eine damit einhergehende datenschutzrechtliche Frage- oder Problemstellung. Ziel der Unterrichtung und Beratung ist es, dem Verantwortlichen oder Auftragsverarbeiter sowie den konkret tätigen Mitarbeitern zu vermitteln, was bei einer Datenverarbeitung nach den einschlägigen Datenschutzbestimmungen zu beachten ist, sodass im Ergebnis eine datenschutzkonforme Handhabung durch die betreffende Stelle möglich wird.[7]

2. Überwachung

Der DSB berät und unterrichtet allerdings nicht nur; ihm kommt auch eine Überwachungsfunktion zu.[8] So überträgt Art. 39 Abs. 1 lit. b DS-GVO dem DSB die Pflicht zur Überwachung der Einhaltung der DS-GVO. Erwägungsgrund 97 DS-GVO gibt zudem vor, dass „der Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der internen Ein-

1 BayLfD, Orientierungshilfe: Der behördliche Datenschutzbeauftragte, S. 12; Baumgartner/Hansch, ZD 2019, 99, 99 f.

2 Bortz, in: Specht/Mantz, Handbuch europäisches und deutsches Datenschutzrecht, § 11, Rn. 98; Kazemi, NJW 2018, 443, 444; vgl. zudem unten, Ziff. IV.

3 Baumgartner/Hansch, ZD 2019, 99, 99; Moos, in: BeckOK Datenschutzrecht, 26. Ed. 2017, Art. 39, Rn. 1.

4 Baumgartner/Hansch, ZD 2019, 99, 100; Art.-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243, S. 22.

5 BayLfD, Orientierungshilfe: Der behördliche Datenschutzbeauftragte, S. 10; Moos, in: BeckOK Datenschutzrecht, 26. Ed. 2017, Art. 39, Rn. 3.

6 Drewes, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 39, Rn. 7; Voigt, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 39, Rn. 19.

7 Drewes, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 39, Rn. 9; BayLfD, Orientierungshilfe: Der behördliche Datenschutzbeauftragte, S. 10.

8 BayLfD, Orientierungshilfe: Der behördliche Datenschutzbeauftragte, S. 11; Voigt, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 39, Rn. 20.

haltung der Bestimmungen dieser Verordnung von weiteren Personen unterstützt werden" sollte. Angesprochen ist mit dieser Person der DSB. Überwachung der Einhaltung bedeutet jedoch wohl nicht, dass der DSB im Fall der Nichteinhaltung der DS-GVO-Vorgaben durch den Verantwortlichen oder Auftragsverarbeiter persönlich zur Verantwortung gezogen werden kann (vgl. hierzu nachfolgend unter V.).

3. Zusammenarbeit mit und Anlaufstelle für Aufsichtsbehörden

Zur Erfüllung seiner Aufgaben ist der DSB verpflichtet, mit den Aufsichtsbehörden gemäß Art. 39 Abs. 1 lit. d DS-GVO zusammenzuarbeiten.[9] Wie diese Pflicht in der Praxis konkret ausgestaltet ist, bleibt jedoch unklar. Es wird aber davon ausgegangen, dass der DSB zumindest den Zugang der Aufsichtsbehörden zu Dokumenten und Informationen zur Erfüllung ihrer Aufgaben gewährleistet, um die Ausübung ihrer Untersuchungs-, Abhilfe-, Genehmigungs- und beratenden Befugnisse zu erleichtern.[10] Die Kooperationspflicht umfasst hingegen nicht, Datenschutzverstößen sofort gegenüber der Aussichtsbehörde zu melden.[11] Die Pflicht der Zusammenarbeit hat also auch Grenzen, und man wird den DSB nicht als verlängerten Arm der Aufsichtsbehörde ansehen können. Rein bildlich gesprochen, steht er im Lager des Verantwortlichen oder Auftragsverarbeiters.

Nach Art. 39 Abs. 1 lit. e DS-GVO fungiert der DSB darüber hinaus als Anlaufstelle (Mittler) der Aufsichtsbehörde.[12] Die Behörde ist befugt, unmittelbar gezielt Auskünfte von dem DSB als fachkundiger Person einzuholen, ohne erst den Weg über den Verantwortlichen bzw. den Auftragsverarbeiter und die Geschäftsleitung einschlagen zu müssen.[13]

II. Übernahme weiterer Aufgaben

In der Praxis endet das von dem DSB abgeforderte Pflichtenkontingent jedoch nicht an dieser Stelle. Vielfach wird er mit weiteren Aufgaben betraut. Eine Delegation weiterer, über Art. 39 Abs. 1 DS-GVO hinausgehender Aufgaben, kann durch Verantwortliche und Auftragsverarbeiter – nicht aber die Mitgliedsstaaten, da Art. 39 DS-GVO keine Öffnungsklausel enthält – erfolgen. Die Mitgliedsstaaten sind nach Art. 37 Abs. 4 DS-GVO lediglich befugt, die Pflicht für die Benennung eines DSB um weitere Fallgestaltungen zu ergänzen, insoweit sind sie aber auch an die Vorschriften des Art. 37, 38 und 39 DS-GVO gebunden.[14] Die Aufgabenübertragung muss deshalb (dienst- bzw. arbeitsvertraglich) durch den Verantwortlichen bzw. den Auftragsverarbeiter, also etwa das Unternehmen oder die Behörde, erfolgen. Der Gesetzeswortlaut des Art. 39 Abs. 1 DS-GVO („zumindest") lässt jedenfalls den Schluss zu, dass dem DSB weitere Aufgaben übertragen werden können. Verdeutlicht wird die nicht abschließende Aufgabenzuweisung mit der Erwähnung des DSB im Zusammenhang mit internen verbindlichen Datenschutzregeln in Art. 47 Abs. 2 lit. h DS-GVO und der in Erwägungsgrund 77 DS-GVO erwähnten Hinweisfunktion.[15] Die Zulässigkeit der Übernahme weiterer Aufgaben steht jedoch unter der Voraussetzung, dass die ordnungsgemäße Erfüllung der nach Art. 39 Abs. 1 lit. a bis e DS-GVO in jedem Fall wahrzunehmenden Aufgaben und die Stellung des DSB durch die Übernahme nicht beeinträchtigt werden. Auch müssen die dazu erforderlichen zusätzlichen Ressourcen zur Verfügung gestellt werden (Art. 38 Abs. 2 DS-GVO). Eine weitere Bedingung ist, dass diese zusätzlichen Aufgaben nicht zu einem Interessenkonflikt (Art. 38 Abs. 6 S. 2 DS-GVO), also einem Missverhältnis zwischen Durchführungsverantwortung einerseits und Kontrollpflicht andererseits, führen.[16] Die Problematik des Interessenkonflikts zwischen Durchführungs- und Überwachungsverantwortung manifestiert sich unter anderem bei der Frage, ob der DSB in einer aktiven Rolle an der Datenschutz-Folgeabschätzung mitwirken darf.[17]

1. Die Funktion des Datenschutzbeauftragten bei einer Datenschutz-Folgeabschätzung

Gegen die Zulässigkeit der Erstellung einer Datenschutz-Folgeabschätzung (DSFA) als alleinige Aufgabe des DSB im Sinne des Art. 39 DS-GVO spricht, dass eine solche Aufgabenzuweisung aufgrund des damit verbundenen Arbeits- und Zeitaufwandes zu einer Beeinträchtigung der ordnungsgemäßen Erfüllung der Pflichtaufgaben führen könnte. Darüber hinaus ist die DSFA ausdrücklich dem Verantwortlichen zugewiesen. Unabdingbar ist danach, dass der DSB die ordnungsgemäße Durchführung der in Art. 35 DS-GVO geregelten DSFA überwacht. Die Wahrnehmung als Aufgabe würde folglich zu einem Interessenkonflikt führen, in welchem sich der DSB selbst überwachen würde.[18] Neben der Überwachungspflicht obliegt dem DSB jedoch eine Pflicht zur aktiven Beratung. Der Verantwortliche hat dafür Sorge zu tragen, dass der DSB bei der DSFA zu Rate gezogen wird (Art. 35 Abs. 2 DS-GVO).[19] Art. 39 Abs. 1 lit. c DS-GVO überträgt des Weiteren dem DSB die Pflicht, „Beratung – auf Anfrage – im Zusammenhang mit der [DSFA] und Überwa-

9 Baumgartner/Hansch, ZD 2019, 99, 100; Klug, ZD 2016, 315, 319.

10 Art.-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243, S. 21; Heberlein, in: Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 39, Rn. 18; Kirchberg-Lennartz, in: Gierschmann/Schlender/Stentzel/Veil, Datenschutzgrundverordnung, Art. 39, Rn. 20.

11 Paal, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 39, Rn. 8; Heberlein, in: Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 39, Rn. 19.

12 Heberlein, in: Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 39, Rn. 17; Jaspers/Reif, RDV 2016, 61, 67; Kirchberg-Lennartz, in: Gierschmann/Schlender/Stentzel/Veil, Datenschutzgrundverordnung, Art. 39, Rn. 22.

13 Heberlein, in: Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 39, Rn. 17; Moos, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 39, Rn. 8.

14 Heberlein, in: Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 39, Rn. 20; Baumgartner/Hansch, ZD 2019, 99, 99; Paal, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 39, Rn. 4.

15 Klug, in: Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 39, Rn. 4; Paal, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 39, Rn. 4.

16 Baumgartner/Hansch, ZD 2019, 99, 99; Heberlein, in: Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 39, Rn. 20.

17 Baumgartner/Hansch, ZD 2019, 99, 100; Klug, in: Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 39, Rn. 4 f.

18 Heberlein, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 39, Rn. 21.

19 Klug, in: Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 39, Rn. 5; Kirchberg-Lennartz, in Gierschmann/Schlender/Stentzel/Veil, Datenschutzgrundverordnung, Art. 39, Rn. 20.

chung ihrer Durchführung gemäß Art. 35 DS-GVO" zu leisten.[20] Mit Blick auf die Pflicht zur frühzeitigen Einbindung des DSB (Art. 38 Abs. 1 DS-GVO), seine Hinweisfunktion nach Erwägungsgrund 77 DS-GVO und die auch nach Art. 39 Abs. 2 DS-GVO gebotene Risikoorientierung, erscheint eine Beteiligung des DSB schon bei der Ermittlung der Notwendigkeit einer DSFA sinnvoll.[21] Wo in der Praxis genau die Grenze zwischen einer alleinigen Durchführung der DSFA einerseits und einer aktiven Beratung andererseits verlaufen, ist sicherlich kaum vorab fest darstellbar, sondern sollte stets anhand der Gegebenheiten der jeweiligen DSFA festgelegt werden.

2. Die Funktion des Datenschutzbeauftragten bei der Führung von Verzeichnissen

Ob der DSB auch mit der Aufgabe betraut werden darf, das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO zu führen, ist zumindest in der Literatur umstritten.

a) Übertragung der Aufgabe des Führens des Verzeichnisses möglich

Die Art.-29-Datenschutzgruppe nennt in den „Leitlinien in Bezug auf Datenschutzbeauftragte" das Führen des Verzeichnisses von Verarbeitungstätigkeiten als eine sinnvollerweise dem DSB zuzuweisende Aufgabe.[22] So erstellen die DSB nach Ansicht der Aufsichtsbehörden in der Praxis oftmals Inventarlisten und führen Register der Verarbeitungsvorgänge auf der Grundlage der Informationen, die ihnen von den verschiedenen für die Verarbeitung personenbezogener Daten zuständigen Bereichen ihrer Einrichtung vorgelegt werden. Auf diesen Inventarlisten aufbauend, könnte folglich das Verzeichnis geführt werden. Aus dem Wortlaut des Art. 39 Abs. 1 DS-GVO („zumindest") ergibt sich darüber hinaus eine Liste von Aufgaben, die der DSB als Mindestanforderungen wahrzunehmen hat. Den Verantwortlichen bzw. den Auftragsverarbeiter hindert somit nichts daran, dem DSB die Aufgabe zu übertragen, unter der Verantwortlichkeit (!) des Verantwortlichen oder des Auftragsverarbeiters ein Verzeichnis der Verarbeitungsvorgänge zu führen. Jene Listen sind als eines der Instrumente anzusehen, die den DSB in die Lage versetzen, die ihm in Bezug auf die Überwachung der Vorschrifteneinhaltung und die Unterrichtung und Beratung des Verantwortlichen bzw. des Auftragsverarbeiters obliegenden Aufgaben wahrzunehmen.[23]

b) Übertragung der Aufgabe des Führens des Verzeichnisses nicht möglich

Eine andere Auffassung vertritt hingegen, dass die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten in Art. 30 DS-GVO ausdrücklich dem Verantwortlichen und Auftragsverarbeiter zugewiesen ist. Insbesondere die Erarbeitung sowie die Erstellung der einzelnen Beschreibungen der Verarbeitungstätigkeiten kann daher nicht auf den DSB delegiert werden.[24] Historisch betrachtet wurde in der Datenschutzrichtlinie 95/46/EG die Aufgabe zur Führung der Verarbeitungsverzeichnisse ausdrücklich als Aufgabe des DSB hervorgehoben.[25] Der Umstand, dass die DS-GVO allerdings diese Aufgabe nicht in den Aufgabenkatalog übernommen hat, spreche dafür, die Führung der Verarbeitungsverzeichnisse nicht an den DSB zu übertragen. Die Einhaltung der Verpflichtung unterliegt darüber hinaus der Überwachung durch den DSB, was bei Bearbeitung durch ihn selbst einen Interessenkonflikt hervorrufen würde.[26]

c) Vermittelnde Ansicht

Dazwischen wird als vermittelnde Lösung jedoch vertreten, dass der DSB bei der Führung des Verzeichnisses unterstützen kann, ohne, dass eine vollständige Übertragung der Aufgabe erfolgt. Wird das Verzeichnis der Verarbeitungstätigkeit, wie von der Art.-29-Datenschutzgruppe empfohlen, von dem DSB geführt, müssten die Verzeichniseinträge oder die Verzeichnisdatensätze die Letztverantwortlichkeit des Verantwortlichen oder Auftragsverarbeiters eindeutig erkennen lassen.[27] Damit wäre eine notwendige Aufgabentrennung zwischen Fachverantwortlichem und dem DSB gewahrt, um eine schleichende Verlagerung der Verantwortung für die Inhalte der Verarbeitungsübersichten zu vermeiden.[28] Es wird jedoch auch empfohlen, die erstmalige Erarbeitung sowie die Erstellung der einzelnen Beschreibungen der Verarbeitungstätigkeiten nicht auf den DSB zu delegieren. Dieser sollte vielmehr den Erstellungsprozess beratend, gegebenenfalls koordinierend beiseitestehen und zugleich dessen ordnungsgemäße Durchführung überwachen.[29]

III. Rechtsanwalt als Datenschutzbeauftragter – die ewige Diskussion

Es war umstritten, ob ein Syndikusrechtsanwalt in seiner Hauptaufgabe als DSB eines Unternehmens agieren darf.

20 Art.-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243, S. 20; BayLfD, Orientierungshilfe: Der behördliche Datenschutzbeauftragte, S. 13; LfDI BaWü, Praxisratgeber: Die/der Beauftragte für den Datenschutz Teil II, S. 32; Kirchberg-Lennartz, in: Gierschmann/Schlender/Stentzel/Veil, Datenschutzgrundverordnung, Art. 39, Rn. 20.

21 BayLfD, Orientierungshilfe: Der behördliche Datenschutzbeauftragte, S. 13; Klug, in: Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 39, Rn. 5; Art.-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243, S. 20 f.

22 Art.-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243, S. 22; so auch LfDI BaWü, Praxisratgeber: Die/der Beauftragte für den Datenschutz Teil II, S. 33.

23 Art.-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243, S. 22.

24 BayLfD, Orientierungshilfe: Der behördliche Datenschutzbeauftragte, S. 13; Heberlein, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 39, Rn. 21; Kirchberg-Lennartz, in: Gierschmann/Schlender/Stentzel/Veil, Datenschutzgrundverordnung, Art. 39, Rn. 30.

25 Art. 18 Abs. 2 zweiter Spiegelstrich, zweiter Unterabschnitt DS-RL 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995.

26 Heberlein, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 39, Rn. 21; Kirchberg-Lennartz, in Gierschmann/Schlender/Stentzel/Veil, Datenschutzgrundverordnung, Art. 39, Rn. 30.

27 Art.-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243, S. 22; vermittelt dazu BayLfD, Orientierungshilfe: Der behördliche Datenschutzbeauftragte, S. 13.

28 Kirchberg-Lennartz, in: Gierschmann/Schlender/Stentzel/Veil, Datenschutzgrundverordnung, Art. 39, Rn. 30.

29 BayLfD, Orientierungshilfe: Der behördliche Datenschutzbeauftragte, S. 13; Kirchberg-Lennartz, in: Gierschmann/Schlender/Stentzel/Veil, Datenschutzgrundverordnung, Art. 39, Rn. 30.

Der BGH urteilte kürzlich,[30] dass dies, bezogen auf den Einzelfall, durchaus möglich ist. Mit anderen Worten: auch ein zugelassener Rechtsanwalt kann als DSB tätig sein.

In dem konkreten Sachverhalt wollte eine Mitarbeiterin des öffentlichen Rundfunks, zusätzlich zu der bereits bestehenden Rechtsanwaltszulassung, im Rahmen einer Beschäftigung als DSB die Zulassung als Syndikusrechtsanwältin bei der örtlichen Anwaltskammer durchsetzen. Die Rechtsanwaltskammer lehnte die Zulassung unter anderem mit der Begründung ab, dass die Tätigkeit im öffentlichen Dienst als DSB nicht mit dem Beruf des Rechtsanwalts, insbesondere seiner Stellung als unabhängiges Organ der Rechtspflege, vereinbar sei, ohne dass das Vertrauen in die Unabhängigkeit der anwaltlichen Tätigkeit gefährdet sein könne.[31]

Der BGH nahm jedoch an, dass die Tätigkeit als DSB nach den Umständen des Einzelfalls die Voraussetzungen einer Anwaltstätigkeit im Sinne des § 46 Abs. 3 BRAO erfüllen kann.[32] Danach liegt eine anwaltliche Tätigkeit vor, wenn die auszuübende Tätigkeit durch die Prüfung von Rechtsfragen (§ 46 Abs. 3 Nr. 1 BRAO), die Erteilung von Rechtsrat (§ 46 Abs. 3 Nr. 2 BRAO), die Ausrichtung der Tätigkeit auf die Gestaltung von Rechtsverhältnissen (§ 46 Abs. 3 Nr. 3 BRAO) sowie die Befugnis, nach außen verantwortlich aufzutreten (§ 46 Abs. 3 Nr. 4 BRAO) geprägt ist. Begründet wird die Annahme einer Anwaltstätigkeit mit der Änderung der Aufgaben des DSB mit der Einführung der DS-GVO. So ist laut dem BGH die Komplexität der mit der DS-GVO verbundenen rechtlichen Fragen gestiegen.[33] Der Kern und der Schwerpunkt der Tätigkeit eines DSB lägen grundsätzlich in der Auslegung und Anwendung der datenschutzrechtlichen Vorgaben sowie in der Überwachung und Einhaltung dieser datenschutzrechtlichen Vorgaben.[34] Dass der DSB nicht nur rechtliches Wissen, sondern vielmehr tiefgreifendes Verständnis im Datenschutz beherrschen muss, spreche dabei nicht gegen die Annahme einer anwaltlichen Tätigkeit, sodass ein DSB im Einzelfall auch als Syndikusanwalt zugelassen sein darf.[35]

Fraglich und bislang höchstrichterlich nicht geklärt ist, wie sich diese Begründung des BGH auf einen Rechtsanwalt in einer Kanzlei auswirkt, der als externer DSB für ein Unternehmen tätig werden möchte. Grundsätzlich ist dem Anwalt ein Zweitberuf erlaubt, wenn gem. § 14 Abs. 2 Nr. 8 BRAO der gewählt Beruf mit dem Anwaltsberuf vereinbar und das Vertrauen in seine Unabhängigkeit nicht gefährdet ist. Nach dem oben zitierten Urteil des BGH ist aber schon fraglich, ob die Tätigkeit als (externer) DSB überhaupt als ein Zweitberuf anzusehen ist, sondern nicht vielmehr als originäre anwaltliche Tätigkeit. Denn der Kern und der Schwerpunkt der Tätigkeit eines DSB liegen grundsätzlich in der Auslegung und Anwendung der datenschutzrechtlichen Vorgaben sowie in der Überwachung der Einhaltung dieser Vorgaben.[36] Eine Abgrenzung kann im Einzelfall sicher schwierig sein. Im Hinblick auf § 3 Abs. 1 BRAO wird bei Rechtsangelegenheiten im Zweifel aber eine anwaltliche Tätigkeit anzunehmen sein.[37] Und der Datenschutz wird vom BGH zur Rechtsangelegenheit des Verantwortlichen (etwa eines Unternehmens) gezählt.[38]

Geht man von einem Zweitberuf aus, darf der Anwalt gemäß § 45 Abs. 1 Nr. 4 BRAO in seinem Zweitberuf nicht in Angelegenheiten tätig werden, in denen er bereits beruflich tätig war. Interessenkonflikte können dabei die notwendige Unabhängigkeit beeinträchtigen.[39] Denkbar sind solche Interessenkonflikte nach Ansicht der Art.-29-Datenschutzgruppe, wenn Rechtsanwälte zu DSB benannt werden und diese den Verantwortlichen gleichzeitig in datenschutzrelevanten Angelegenheiten vor Gericht vertreten. Dabei ist jedoch immer auf den Einzelfall abzustellen.[40] Eine Beratung des Verantwortlichen durch eine Anwaltskanzlei, die gleichzeitig den externen DSB stellt, führt somit nicht automatisch zu einem relevanten Interessekonflikt.[41] Teilweise wird zwar in der der Literatur ein Interessenkonflikt mit der Verpflichtung externer Berater zur Wahrnehmung von Mandatsinteressen begründet,[42] diese Auffassung überzeugt jedoch nicht in der Hinsicht, dass Rechtsanwälte als Organ der Rechtspflege zu einer objektiven Beratung geeignet und verpflichtet sind.[43] Insbesondere, wenn auf Seiten der externen Berater eine klare Aufgabenzuweisung an einzelne Mitarbeiter sowie eine personelle Trennung zwischen der Beratungstätigkeit und der Aufgabe als externer DSB existiert, spricht nichts gegen eine solche Tätigkeit. So hat die Art.-29-Datenschutzgruppe aus gutem Grund die möglichen Interessenkonflikte auf den Fall einer gerichtlichen Tätigkeit eines Rechtsanwalts in datenschutzrechtlichen Angelegenheiten beschränkt.[44]

Folglich ist der Anwaltsberuf grundsätzlich mit der Tätigkeit als DSB vereinbar und verstößt nicht gegen die „Stellung als unabhängiges Organ der Rechtspflege“ im Sinne von § 7 Nr. 8 BRAO.[45] Eventuell ist sogar davon auszugehen, dass eine Tätigkeit als externer DSB als Anwalt wahrgenommen werden kann und keinen Zweitberuf darstellt. Neben etwaigen Interessenkonflikten ist jedoch ratsam, auch das erweiterte Haftungsrisiko des Anwalts aufgrund

30 BGH, Urt. v. 15.10.2018, AnwZ (Brfg) 20/18, NJW 2018, 3701.

31 BGH, Urt. v. 15.10.2018, AnwZ (Brfg) 20/18, NJW 2018, 3701, 3701 ff.

32 BGH, Urt. v. 15.10.2018, AnwZ (Brfg) 20/18, NJW 2018, 3701, 3710, Rz. 84.

33 BGH, Urt. v. 15.10.2018, AnwZ (Brfg) 20/18, NJW 2018, 3701, 3708, Rz. 70.

34 BGH, Urt. v. 15.10.2018, AnwZ (Brfg) 20/18, NJW 2018, 3701, 3708, Rz. 71.

35 BGH, Urt. v. 15.10.2018, AnwZ (Brfg) 20/18, NJW 2018, 3701, 3708, Rz. 71.

36 BGH, Urt. v. 15.10.2018, AnwZ (Brfg) 20/18, NJW 2018, 3701, 3708, Rz. 71.

37 Träger, in: Feuerich/Weyland, Bundesrechtsanwaltsordnung: BRAO, 9. Aufl. 2016, § 45 BRAO, Rn. 29.

38 BGH, Urt. v. 15.10.2018, AnwZ (Brfg) 20/18, NJW 2018, 3701, 3710 f., Rz. 93; BGH Urt. v. 2.7.2018. AnwZ (Brfg) 49/17, NJW 2018, 3100, 3104, Rz. 44.

39 Baumgartner/Hansch, ZD 2019, 99, 102.

40 Art.-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243 rev. 01, S. 19; Baumgartner/Hansch, ZD 2019, 99, 103.

41 Baumgartner/Hansch, ZD 2019, 99, 103.

42 Bezugnehmend auf Art.-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243 rev. 01, S. 19: Heberlein, in: Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 38, Rn. 25.

43 Haag, in: Forgó/Helfrig/Schneider, Betrieblicher Datenschutz, 2. Aufl. 2018, Kapitel 3, Rn. 67; Baumgartner/Hansch, ZD 2019, 99, 103.

44 Art.-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243 rev. 01, S. 19; Baumgartner/Hansch, ZD 2019, 99, 103.

45 Bortz, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 11, Rn. 98.

des umfangreicheren Pflichtenkreises zu beachten. Außerdem werden nach der bisher wohl herrschenden Ansicht externe DSB gewerblich tätig, sodass eine klare Abgrenzung zwischen Anwaltsberuf und der Tätigkeit als DSB für nicht als Kapitalgesellschaft organisierte Einheiten empfehlenswert ist, damit die Umsätze der Tätigkeit als Anwalt nicht gewerbesteuerlich belegt werden.[46]

IV. Haftung des Datenschutzbeauftragten

Aus der DS-GVO geht klar hervor, dass es Sache des Verantwortlichen ist, „geeignete technische und organisatorische Maßnahmen [umzusetzen], um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt" (Art. 24 Abs. 1 DS-GVO). Die Einhaltung datenschutzrechtlicher Bestimmungen fällt somit in den Aufgabenbereich des Verantwortlichen und nicht des DSB.[47] Damit scheidet eine persönliche Haftung des DSB, im Falle der Nichteinhaltung der DS-GVO-Vorschriften durch den Verantwortlichen, aus.[48]

Der DSB kann aber als Täter, Mittäter oder Anstifter handeln und so gegen §§ 41, 42 BDSG verstoßen. Dies ist etwa der Fall, wenn er sich über seine Befugnisse hinwegsetzt. Eine eigene Strafbarkeit kommt insbesondere auch wegen Verstoßes gegen § 203 StGB in Betracht. Derartige Verstöße des DSB dürften in der Praxis aber eher die Ausnahme darstellen.[49] Bei Realisierung eines Schadens, kommt jedoch ein Haftungsrückgriff des Verantwortlichen auf den DSB nach den allgemeinen Vorschriften des BGB in Betracht.[50]

1. Vertragliche bzw. dienstliche Haftung

Eine zivilrechtliche Haftung gegenüber dem Verantwortlichen kann sich daraus ergeben, dass eine falsche, unvollständige oder zu späte Unterstützung oder Beratung erfolgt. Dasselbe gilt bei einer unterbliebenen oder mangelhaft durchgeführten unternehmens- oder behördeninternen Überwachung.[51] Dabei bedarf es jedoch einer zusätzlichen Prüfung, inwiefern eine konkrete Pflichtverletzung vorliegt, also eine vertragliche oder dienstliche Pflicht betroffen ist, da der DSB grundsätzlich in der Aufgabenwahrnehmung frei und unabhängig ist. Seine besondere Stellung wirkt sich folglich auch auf seinen Pflichtenkreis aus.[52] Bei einem internen DSB sind des Weiteren die Grundsätze der beschränkten Arbeitnehmerhaftung anwendbar.[53] Danach ist das betrieblich veranlasste Schadensrisiko grundsätzlich beim Arbeitgeber anzusiedeln, da es sich um eine betrieblich veranlasste Tätigkeit handelt und die Haftung des Arbeitnehmers abhängig vom Grad des Verschuldens zu betrachten ist.[54]

Die Pflichten des DSB gegenüber betroffenen Personen nach Art. 38 Abs. 4 DS-GVO weisen keinen Charakter einer schuldrechtlichen Sonderverbindung auf. Damit lässt sich aus der weiteren Formulierung des Art. 38 Abs. 4 DS-GVO auch nicht entnehmen, dass der DSB vertragliche Schutzpflichten zugunsten der betroffenen Person zu beachten hätte. Vertragliche Ansprüche von Dritten gegenüber dem DSB scheiden damit von vorn herein aus.[55]

2. Deliktische Haftung

Deliktische Haftungsfälle des DSB können vorliegen, wenn der Verstoß unmittelbar auf den DSB zurückzuführen ist. Dies kann etwa bei Verstößen gegen die Verschwiegenheitspflicht, die aktive Falschberatung der benennenden Stelle oder das Unterlassen von Überwachungsmaßnahmen nach Art. 39 Abs. 1 lit. b DS-GVO gegeben sein.[56] Keine Haftung ist hingegen anzunehmen, wenn der DSB datenschutzrechtliche Defizite in einem Verfahren nicht erkannt hat und daher der Verantwortliche keine Veranlassung sah, Korrekturen am Datenverarbeitungsprozess vorzunehmen. In diesen Fällen wird darauf abgestellt, ob es dem DSB möglich war entsprechende Defizite zu erkennen. Dies setzt allerdings voraus, dass der Verantwortliche dem DSB alle erforderlichen Unterlagen zur Bewertung zur Verfügung gestellt hat und er auch über die notwendigen organisatorischen und personellen Mittel verfügt.[57] Auch müsste bei Vornahme der gebotenen Handlung der tatbestandliche Erfolg mit an Sicherheit grenzender Wahrscheinlichkeit ausgeblieben sein. Die Pflichtverletzung des DSB muss demnach für die eingetretene Rechtsgutverletzung kausal gewesen sein und die Rechtsgutverletzung den Schaden verursacht haben.[58] In der Praxis dürfte es jedoch schwerfallen, eine Datenschutzverletzung eines Betroffenen auf eine fehlende, oberflächliche oder unter fachlichen Mängeln leidende Kontrolltätigkeit eines DSB zurückzuführen. So dürfte es schon fraglich sein, ob ohne den aufdeckenden Kontrollbericht die jeweilige Verarbeitungstätigkeit verändert oder unterlassen worden wäre.[59]

3. Haftung wegen Unterlassen

Praxisrelevanter ist die Frage, ob eine Strafbarkeit des DSB wegen Beteiligung durch Unterlassen in Betracht kommt. Eine Teilnahme, welche für die Beteiligung an einem Unter-

46 Bortz, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 11, Rn. 98.

47 Art.-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243, S. 20.

48 LfDI BaWü, Praxisratgeber: Die/der Beauftragte für den Datenschutz Teil II, S. 28.

49 Drewes, in: Simitis/Hornung/Spiecker, Datenschutzrecht 2019, Art. 39, Rn. 58; Scheja, in: Teuger/Gabel, DS-GVO BDSG, Art. 38, Rn. 27.

50 Haag, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Kapitel 3, Rn. 75; Paal, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 39, Rn. 12.

51 Drewes, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 39, Rn. 43; Bergt, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 37, Rn. 53.

52 Drewes, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 39, Rn. 43; Paal, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 39, Rn. 12.

53 Drewes, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 39, Rn. 45.

54 Moos, in: BeckOK Datenschutzrecht, 23. Ed. 2015, § 4 g, Rn. 42; Eßer/Steffen, CR 2018, 289, 293.

55 Bergt, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 37, Rn. 52; Moos, in: BeckOK Datenschutzrecht, 23. Ed. 2015, § 4 g, Rn. 43.

56 Drewes, in: Simitis/Hornung/Spiecker, Datenschutzrecht 2019, Art. 39, Rn. 48 ff; Paal, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 39, Rn. 12; Scheja, in: Teuger/Gabel, DS-GVO BDSG, Art. 38, Rn. 12 ff.

57 Drewes, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 39, Rn. 48.

58 Drewes, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 39, Rn. 48; Eßer/Steffen, CR 2018, 289, 292.

59 Scheja, in: Teuger/Gabel, DS-GVO BDSG, Art. 38, Rn. 14.

lassungsdelikt ursächlich ist, kann sich etwa daraus ergeben, dass der DSB nicht die gebotenen Prüfungen im Unternehmen durchführt oder die Führungskräfte nicht auf aktuelle datenschutzrechtliche Entwicklungen hingewiesen hat. Eine Strafbarkeit durch Unterlassen setzt nach § 13 StGB voraus, dass der DSB eine Garantenstellung einnimmt.[60]

Der BGH entschied, dass eine Garantestellung des Compliance-Officers aus seiner Verpflichtung, Rechtsverstöße zu verhindern, resultiert.[61] Im Rahmen des BDSG a.F. wurde diesbezüglich diskutiert, ob die BGH-Rechtsprechung zur Garantenstellung und Haftung eines Compliance-Officers auf den DSB übertragbar ist.[62] Dies ist im Rahmen der DS-GVO von den Pflichten des DSB abhängig. In Bezug auf eine Garantenstellung muss hinterfragt werde, ob der DSB verpflichtet ist, Rechtsverstöße zu verhindern.[63] Gemäß Art. 39 Abs. 1 lit. a und b DS-GVO obliegt dem DSB primär eine beratende und überwachende Funktion und explizit keine Compliance-Verantwortung, welche grundsätzlich der Geschäftsleitung im Unternehmen zukommt.[64] Allerdings hat der DSB kraft Gesetzes im Rahmen des unternehmerischen Compliance-Management-Systems seinen Beitrag zur Compliance des Unternehmens zu leisten. Dies gilt beispielweise für unternehmerische Informationspflichten. So besteht die Verpflichtung des DSB zur Unterrichtung über datenschutzrechtliche Pflichten nicht nur gegenüber dem Unternehmen, sondern auch gegenüber den Beschäftigten.[65] Allerdings richten sich die Vorgaben zur Erfüllung der Informations- und Betroffenenrechte der Art. 13 ff. DS-GVO ausschließlich an den Verantwortlichen.[66] Von wesentlicher Bedeutung ist darüber hinaus, dass die Überwachungspflicht auch die Organisations-, die Informations- und die diesbezüglichen Überprüfungspflichten des Unternehmens umfasst. Der DSB wird damit zum Kontrolleur des unternehmerischen Compliance-Management-Systems, allerdings ohne selbst Verantwortung dafür zu tragen.[67] Folgerichtig sind daher auch in den Regelungen der Art. 82 ff. DS-GVO keine eigenen Haftungsregelungen für den DSB vorgesehen.[68] Zuletzt wird die Abgrenzung der Verantwortung der Geschäftsleitung von der Beratungs- und Überwachungsfunktion des DSB mit Blick auf die DSFA deutlich. Im Rahmen dieser wird der DSB lediglich beratend, überwachend und nur auf Anfrage hinzugezogen, währenddessen der Verantwortliche selbst verpflichtet ist, den Rat des DSB einzuholen, sodass die Verantwortung für dessen Einbeziehung beim verantwortlichen Unternehmen liegt.[69] Die Pflichten des Compliance-Officers sind daher deutlich von der Beratungs- und Überwachungsfunktion des Datenschutzbeauftragen abzugrenzen. Ein aktives Eingreifen zur Beseitigung oder Verhinderung einzelner Verstöße liegt hingegen nicht im Pflichtenkreis des DSB. So muss der Verantwortliche die entsprechenden Maßnahmen ergreifen, damit das Unternehmen datenschutzkonform arbeitet,[70] sodass eine entsprechende Verhinderungspflicht und damit eine Garantenstellung zu verneinen ist.[71]

V. Fazit

Ein DSB (ggfs. auch als Rechtsanwalt) wird wohl nicht in vergleichbarer Funktion wie ein Compliance-Officer tätig, sondern beratend und überwachend. Dabei erstreckt sich sein Haftungspotenzial auf Pflichtverstöße, die aus einer Verletzung dieser beratenden bzw. überwachenden Funktion erwachsen. Eine aktive Verhinderungspflicht von Rechtsverstößen ist ihm gerade nicht zuzuschreiben.

Artikel der DS-GVO	Inhalt der Pflicht
Art. 37 Abs. 5	Besitz von beruflicher Qualifikation und insbesondere Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis
Art. 38 Abs. 3	Der DSB berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters.
Art. 38 Abs. 5	Der DSB ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.
Art. 39 Abs. 1 lit. a	Dem DSB obliegt die Aufgabe, den Verantwortlichen oder Auftragsverarbeiter und deren Beschäftigte, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten zu unterrichten und zu beraten.
Art. 39 Abs. 1 lit. b	Dem DSB obliegt die Aufgabe die Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sen-

60 Drewes, in: Simitis/Hornung/Spiecker, Datenschutzrecht 2019, Art. 39, Rn. 58 ff.

61 BGH NJW 2009, 3173, 3175, Rz. 27.

62 BGH Urt. v. 17.07.2009 – 5 StR 394/08 zur Garantenstellung eines Compliance-Officers aufgrund seiner Verpflichtung, Rechtsverstöße zu verhindern; zur Garantenstellung ablehnend Schmitz/Thoma, in: Gierschmann/Saeugling, Syst. Praxis-Kommentar, § 4f, Rn. 45.

63 Krätschmer, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 6, Rn. 1; LfDI BaWü, Praxisratgeber: Die/der Beauftragte für den Datenschutz Teil II, S. 28; Drewes, in: Simitis/Hornung/Spiecker, Datenschutzrecht 2019, Art. 39, Rn. 62.

64 Krätschmer, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 6, Rn. 8; Jung, ZD 2018, 208, 209.

65 Jung, ZD 2018, 208, 209; Krätschmer, in: Specht/Mantz, Handbuch europäisches und deutsches Datenschutzrecht, § 6, Rn. 9.

66 Lantwin, ArbRAktuell 2017, 508, 511.

67 Krätschmer, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 6, Rn. 5.

68 Lantwin, ArbRAktuell 2017, 508, 511.

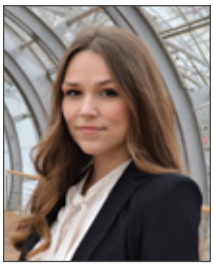
69 Krätschmer, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 6, Rn. 10; Lantwin, ArbRAktuell 2017, 508, 511.

70 Döhmann, in: Simitis/Hornung/Spiecker, Datenschutzrecht 2019, Art. 39, Rn. 62.

71 LfDI BaWü, Praxisratgeber: Die/der Beauftragte für den Datenschutz Teil II, S. 28; Krätschmer, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 6, Rn. 9; Lantwin, ArbRAktuell 2017, 508, 508; Jung, ZD 2018, 208, 209.

	sibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen zu überwachen.
Art. 39 Abs. 1 lit.c	Dem DSB obliegt die Aufgabe, – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35 zu beraten.
Art. 39 Abs. 1 lit. d	Dem DSB obliegt die Aufgabe, mit der Aufsichtsbehörde zusammen zuarbeiten.
Art. 39 Abs. 1 lit.e	Dem DSB obliegt die Aufgabe, für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36, zu allen sonstigen Fragen als Anlaufstelle tätig zu werden und gegebenenfalls zu beraten.
Art. 39 Abs. 2 DS-GVO	Der DSB trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Dr. Carlo Piltz
Rechtsanwalt, Salary Partner, reuschlaw Legal Consultans, Berlin



Sandra Häntschel
Wiss. Mitarbeitern, reuschlaw Legal Consultants, Berlin

Kristin Benedikt

ePrivacy-VO – Was lange währt, wird endlich gut?

Seit Beginn des Gesetzgebungsverfahrens sorgt die ePrivacy-VO für Furore. Die Entwürfe zur ePrivacy-VO sind zum Teil derart umstritten, dass immer wieder Stimmen laut werden, die bisherigen Entwürfe seien grundsätzlich zu überdenken[1] oder gar das Gesetzgebungsverfahren einzustellen. Auch Parlamentarier beklagen, dass das Verhandeln um die ePrivacy-VO zu einer der massivsten Lobby-Kampagnen geworden sei.[2] Dies mag mitunter einer von vielen Gründen sein, weshalb das Gesetzgebungsverfahren seit den Entwürfen der Kommission vom 10.01.2017[3] und des Parlaments vom 23.10.2017[4] ins Stocken geraten ist.

I. Aktueller Stand des Gesetzgebungsverfahrens

Nachdem längere Zeit kein Fortschritt zu verzeichnen war, veröffentlichte die Working Party Tele unter der Finnischen Ratspräsidentschaft im Oktober 2019 gleich drei Entwürfe zur ePrivacy-VO.[5] Das Gesetzgebungsverfahren hat folglich wieder Fahrt aufgenommen. Damit rückt die ePrivacy-VO immer näher. Nach vorsichtigen Prognosen ist mit einem Inkrafttreten der neuen Verordnung jedoch nicht vor Ende 2020 zu rechnen.[6] Ob es wie bei der DS-GVO eine Übergangsfrist von 24 Monaten geben wird, ist noch unklar. Die Vorschläge im Gesetzgebungsverfahren reichen von 12 bis 24 Monaten. Im Zweifel ist jedoch von einer kürzeren Übergangsfrist auszugehen. Übergangsfristen dienen in erster Linie dazu, den Mitgliedsstaaten einen ausreichenden Zeitraum einzuräumen, um die mitgliedsstaatlichen Regelungsgebote und -spielräume umzusetzen. Doch dieser Spielraum ist nach den Entwürfen

1 Verbändebrief zur ePrivacy-Verordnung, Time to rethink ePrivacy, vom 08.10.2019, abrufbar unter: https://www.bvdw.org/fileadmin/bvdw/upload/dokumente/recht/e_privacy_verordnung/Verbaendeschreiben_ePrivacy_Oktober_2019.pdf.

2 Corporate Europe Observatory, Big Data is watching you 17.10.2017, arufbar unter https://corporateeurope.org/en/power-lobbies/2017/10/big-data-watching-you.

3 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)v. 10.01.2017, COM/2017/010 final -2017/03 (COD).

4 Vorschlag der Europäischen Kommission vom 10. Januar 2017, (COM(2017) final 2017/0003 (COD); Entwurf einer legislativen Entschließung des Europäischen Parlaments vom 23.10.2017, A8-0324/2017.

5 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)v. 04.10.2019 RAT: 12633/19; v. 17.10.2019, RAT: 13080/19.

6 BVDW, Aktuelle Informationen zur ePrivacy-Verordnung, abrufbar unter: https://www.bvdw.org/fileadmin/bvdw/upload/dokumente/recht/e_privacy_verordnung/Zeitstrahl_eVP_20190521_02.pdf.

der ePrivacy-VO[7] äußerst gering. Im Vergleich zur DS-GVO, die den Mitgliedsstaaten eine Vielzahl an Regelungsgeboten und -spielräumen einräumt[8], enthalten die Entwürfe zur ePrivacy-VO lediglich 3 Öffnungsklauseln.[9]

Doch auch eine 2-jährige Übergangsfrist vermag die Hürden bei der Umsetzung der neuen Verordnung nicht schmälern. Die Erfahrungen mit der DS-GVO haben gezeigt, dass auch eine Übergangsfrist von zwei Jahren bei weitem nicht ausreicht, um alle Anforderungen zum Stichtag umzusetzen. Umso wichtiger erscheint es, sich frühestmöglich mit den neuen Anforderungen der ePrivacy-Verordnung vertraut zu machen.

Auch wenn einige Regelungen kontrovers diskutiert werden, so sind die bereits veröffentlichten Entwürfe derart konkret, dass klare Tendenzen erkennbar sind.

II. Sinn und Zweck

Die DS-GVO fordert den Gesetzgeber auf, die bisher geltende ePrivacy-RL[10] zu überarbeiten, um Kohärenz mit der DS-GVO zu gewährleisten.[11]

Die ePrivacy-VO soll die DS-GVO ergänzen und präzisieren. Die neue Verordnung enthält Vorschriften zum Schutz von Grundrechten und Grundfreiheiten natürlicher und juristischer Personen bei der Bereitstellung und Nutzung elektronischer Kommunikationsdienste und regelt insbesondere die Rechte auf Achtung des Privatlebens und der Kommunikation gem. Art. 7 GRCh und den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten gem. Art. 8 GRCh.[12]

Voreilig wird die ePrivacy-VO als lex specialis zur DS-GVO bewertet.[13] Dabei wird verkannt, dass die ePrivacy-VO in vielerlei Hinsicht über den Anwendungsbereich der Grundverordnung hinausgeht und einen eigenständigen Regelungsbereich enthält. Dies ergibt sich unter anderem daraus, dass die ePrivacy-VO nicht nur natürliche Person schützt, sondern den Schutzbereich auch auf juristische Personen erweitert.[14] Darüber hinaus ist die ePrivacy-VO nicht nur auf die Anwendung personenbezogener Daten beschränkt, sondern umfasst auch nicht personenbezogenen Daten z.B. bei der Maschine-zu-Maschine-Kommunikation.[15]

Viel zu häufig wird die Diskussion um die ePrivacy-VO auf das Einwilligungserfordernis bei der Einbindung von Dritteninhalten beschränkt. Der sachliche Anwendungsbereich der ePrivacy-VO geht weit über den der DS-GVO hinaus, indem sie nicht nur für die Verarbeitung von elektronischen Kommunikationsdaten gilt, sondern auch Regelungen für den Umgang mit Informationen auf Endeinrichtungen enthält.

III. Kein ausreichender Schutz durch DS-GVO

Zu Beginn des Gesetzgebungsverfahrens führte die EU-Kommission eine Konsultation durch, bei der die beteiligten Akteure u.a. dazu Stellung nehmen sollten, ob es neben der DS-GVO überhaupt noch einer weitergehenden Regelung für den Bereich der elektronischen Kommunikation bedarf. Die Konsultation ergab, dass spezielle Regelungen für den Bereich der elektronischen Kommunikation erforderlich sind. Die Regelungen der DS-GVO seien nicht ausreichend, um die Vertraulichkeit der Kommunikation zu gewährleisten.[16]

Darüber hinaus ergab das Konsultationsverfahren, dass Vorschriften zum Schutz der elektronischen Kommunikation in Form einer Richtlinie ungeeignet sind. Die Gründe dafür liegen nicht nur in einer unzureichenden und teils unterschiedlichen Umsetzung durch die Mitgliedsstaaten.[17]

Auch die Vollzugspraxis der zuständigen Aufsichtsbehörden war in der Vergangenheit uneinheitlich.[18] Ein harmonisierter Rechtsrahmen für den Bereich der elektronischen Kommunikation bestand nicht.

Doch der Zweck der neuen Verordnung besteht nicht nur darin, einen einheitlichen Rechtsrahmen und Vollzug für den Bereich der elektronischen Kommunikation sicherstellen.

Die bisher geltenden Regelungen der ePrivacy-Richtlinie werden der rasanten technologischen Entwicklung nicht mehr gerecht. Nicht nur internetbasierte Kommunikationsdienste, so genannte Over-The-Top-Dienste (OTT-Dienste), wie Messenger oder E-Mail sind vom Anwendungsbereich der Richtlinie ausgenommen. Auch weitere neuartige Anwendungsbereiche wie Connected Car oder Internet of Things, insbesondere Smart-Home-Anwendungen werden vom An-

7 Kühling/Martini et al. DS-GVO und das nationale Recht; 2016; S. 1

8 Übersicht über Regelungsgebote und -spielräume der Mitgliedsstaaten bei, Kühling/Martini et. al., Die DS-GVO und das nationale Recht, 2016 S. 14 ff.

9 Art. 11, 13, 16 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 10.01.2017, COM/2017/010 final -2017/03 (COD).

10 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L 337 v. 18.12.2009, 11; Sofern im Folgenden eine Vorschrift der ePrivacy-RL genannt wird, ist immer geänderte Fassung der Richtlinie 2009/136/EG gemeint.

11 Vgl. Erwägungsgrund 173.

12 Art. 1 der ePrivacy-VO (E) Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 10.01.2017, COM/2017/010 final -2017/03 (COD).

13 Schmitz, in: Spindler/Schmitz, Telemediengesetz, 2. Aufl. 2018, Rn. 25.

14 Erwägungsgrund 3, 8, 31, 32 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)v. 10.01.2017, COM/2017/010 final -2017/03 (COD).

15 Erwägungsgrund 12 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 10.01.2017, COM/2017/010 final -2017/03 (COD).

16 Synopsis report of the public consultation on the evaluation and review of the ePrivacy Directive, S. 4 f. abrufbar unter: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40777.

17 European Commission, Directorate-General of Communications Networks, Content & Technology, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulationv. 31.01.2015, Contract number: 30-CE-0629642/00-85, SMART 2013/0071, doi:10.2759/411362.

18 Synopsis report of the public consultation on the evaluation and review of the ePrivacy Directive, S. 4 f. abrufbar unter: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40777.

wendungsbereich der ePrivacy-RL bisher nicht erfasst. Dies führt zu gravierenden Schutzlücken für die Anwender, sodass auch vor diesem Hintergrund eine Anpassung der ePrivacy-RL an die technologische Fortentwicklung geboten ist.

IV. Kapitel 1 – Allgemeine Bestimmungen

1. Schutzbereich

Art. 1 der ePrivacy-VO regelt nicht nur den Datenschutz, in dem die Verordnung Regelungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten gem. Art. 8 GRCh trifft. Sie enthält auch Vorschriften zum Schutz von Grundrechten und Grundfreiheiten natürlicher und juristische Personen bei elektronischen Kommunikationsdiensten. Dazu zählt insbesondere das Recht auf Achtung des Privatlebens und die Vertraulichkeit der Kommunikation gem. Art. 7 GRCh.

Bereits an dieser Stelle ist der wesentliche Unterschied zur DS-GVO erkennbar. Die ePrivacy-VO soll die Vertraulichkeit der Kommunikation gewährleisten. Sämtliche Kommunikationspartner müssen darauf vertrauen können, dass Dritte nicht unbefugt Kenntnis vom Inhalt oder den Umständen, dass Dritte der Kommunikation erlangen.

Die Bedeutung des in Art. 7 GRCh verankerten Grundrechts ergibt sich insbesondere bei der Betrachtung konkreter Einzelfälle. Geschäftsgeheimnisse eines Unternehmens, die Recherche eines investigativen Journalismusverbands oder ein Telefonat zwischen einem Mandanten und einem Rechtsanwalt sind nur wenige Beispiele, bei denen offensichtlich ist, dass der persönliche Schutzbereich der Vertraulichkeit der Kommunikation nicht nur natürliche Personen umfasst, sondern auch juristische Personen. Die genannten Beispiele verdeutlichen zugleich, dass die Vertraulichkeit der Kommunikation unabdingbar für die Wahrung anderer Grundrechte ist. Weder Grundrechte wie die unternehmerische Freiheit gem. 16 GRCh noch die Freiheit der Meinungsäußerung und Informationsfreiheit gem. Art. 11 GRCh können umfassend gewahrt werden, wenn die Grundrechtsträger nicht darauf vertrauen können, dass die Inhalte und Umstände ihrer Kommunikation Dritten verborgen bleiben.

2. Räumlicher Anwendungsbereich

Der räumliche Anwendungsbereich entspricht dem der DS-GVO. Auch der ePrivacy-VO liegt das Marktortprinzip zugrunde. Der räumliche Anwendungsbereich ist eröffnet, wenn der Anbieter elektronischer Kommunikationsdienste innerhalb der EU niedergelassen ist oder sich der elektronische Kommunikationsdienst an einen Endnutzer in die Union richtet.

Dies hat in der Praxis weitreichende Konsequenzen. Internetbasierte Kommunikationsdienst wie z.B. Messenger oder E-Mail sind in der privaten wie auch geschäftlichen Kommunikation nicht mehr wegzudenken, weil Nutzer zu geringen Kosten oder sogar kostenlos auf der ganzen Welt miteinander verbunden sind.

Das Marktortprinzip der neuen Verordnung führt dazu, dass die Anforderungen der ePrivacy-VO von nahezu jedem Betreiber von Kommunikationsdiensten weltweit zu beachten ist. Für die Anwendbarkeit genügt es bereits, dass nur ein Kommunikationsteilnehmer innerhalb der EU einen Messenger verwendet, um beispielsweise mit einem Nutzer in Asien oder Afrika Nachrichten zu senden. Im Ausland beliebte Messenger wie Viper, Kakao Talk oder WeChat[19] unterliegen somit künftig den Anforderungen der ePrivacy-VO.

Dies erscheint durchaus ein erstrebenswertes Ergebnis zu sein, um zu verhindern, dass Schutzlücken bei der elektronischen Kommunikation bestehen. Die Kehrseite dieses überbordenden Anwendungsbereichs wird in erster Linie Defizite im Vollzug sein. Zwar erklärt die ePrivacy-VO die Regelungen zur Zusammenarbeit und Kohärenz der DS-GVO für anwendbar. Dies hilft jedoch nicht über den Vollzug bei Staaten außerhalb der EU hinweg. Bereits die förmliche Zustellung eines Beschlusses in einen Drittstaat dauert in der Regel mehrere Monate. In Drittstaaten ohne Vollzugsabkommen mit der EU oder einzelnen Mitgliedsstaaten scheint die Durchsetzung der ePrivacy-VO nahezu aussichtslos. Diese Problematik ist jedoch nicht spezifisch für die ePrivacy-VO. Dieselben Schwierigkeiten ergeben sich schon heute beim Vollzug der DS-GVO.

3. Definitionen

Die ePrivacy-VO enthält in den Entwürfen lediglich 43 Erwägungsgründe und 29 Art.. Damit ist sie im Gegensatz zur DS-GVO im Hinblick auf den Umfang eine überschaubare Verordnung. Der geringe Umfang der ePrivacy-VO ist zugleich auch eine ihrer Schwächen. Die neue Verordnung enthält nur wenige Definitionen und verweist im Wesentlichen auf die Begriffsbestimmungen der DS-GVO sowie auf den Kodex für die elektronische Kommunikation.[20] Dies führt dazu, dass die Verordnung aus sich heraus schwerfällig zu lesen ist.

V. Kapitel 2 – Schutz der elektronischen Kommunikation

Das Kapitel 2 enthält die Kernvorschriften der neuen Verordnung. Um die besondere Bedeutung der Vertraulichkeit der Kommunikation zu betonen, greift Art. 5 ePrivacy-VO (E) den Grundsatz auf und verbietet jede Art von Eingriffen in die elektronische Kommunikation wie z.B. das Mithören, Abhören, Speichern oder jede andere Art des Abfangens oder Überwachens der Kommunikation. Dies gilt nicht nur für die Verarbeitung von Kommunikationsdaten, sondern auch für Daten, die sich auf Endeinrichtungen beziehen oder in ihnen verarbeitet werden. Damit erweitert die ePrivacy-VO den Schutzbereich erneut, indem auch Daten, die sich im Herrschaftsbereich des Nutzers befinden, geschützt werden. Daraus folgt, dass nicht nur der Verarbeitungsvorgang, sondern auch die Integrität des Endgeräts geschützt wird.

19 Mathias Brandt, „1,3 Milliarden nutzen WhatsApp“ vom 17.01.12018, abrufbar unter: https://de.statista.com/infografik/10309/monatlich-aktive-nutzer-von-messenger-diensten/.

20 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation, ABl. L321/36 v. 17.12.2018.

1. Rechtmäßige Verarbeitung elektronischer Kommunikationsdaten

Die Verarbeitung von elektronischen Kommunikationsdaten ist in Art. 6 ePrivacy-VO (E) geregelt. Die Vorschrift richtet sich nur an Betreiber von Kommunikationsdiensten. Wer keine Kommunikationsdienste anbietet, kann sich nicht auf die Rechtsgrundlagen des Art. 6 berufen, mit der Folge, dass jede Verbreitung von Kommunikationsdaten verboten ist.

Die Vorschrift zur rechtmäßigen Verarbeitung umfasst nur Kommunikationsdaten. Darunter fallen sowohl Kommunikationsinhalts- als auch Metadaten. Zu den Metadaten gehören alle Daten, die für die Diensterbringung notwendig sind und Rückschluss auf die Umstände der Kommunikation erlauben, wie z.B. angerufene Nummern, besuchte Websites, der geografische Standort, Uhrzeit, Datum und Dauer eines von einer Person getätigten Anrufs. Nach dem Willen des Gesetzgebers sind Metadaten ebenso schützenswert wie die Inhalte der Kommutation, da sich aus den Metadaten präzise Schlussfolgerungen über das Privatleben der Kommunikationspartner ziehen lassen, z.B. in Bezug auf ihre sozialen Beziehungen, Gewohnheiten und Lebensalltag oder Interessen.[21]

Aufgrund des hohen Schutzbedarfs der Kommunikationsdaten, ist eine Verarbeitung nur unter engen Voraussetzungen zulässig. So ist die Verarbeitung im Wesentlichen nur rechtmäßig, wenn dies zur Diensterbringung, Abrechnung, Betrugsprävention oder aus Gründen der Datensicherheit erforderlich ist oder eine Einwilligung vorliegt. Eine Verarbeitung aufgrund berechtigter Interessen ist nicht vorgesehen.

Für die Anforderungen der Einwilligung verweist die ePrivacy-VO auf die Vorschriften der DS-GVO. Die ohnehin schon großen Hürden bei der Einholung einer wirksamen Einwilligung werden bei der Verarbeitung von Kommunikationsinhaltsdaten noch weiter erhöht. Für den Fall, dass keine Rechtgrundlage in Betracht kommt und der Betreiber Kommunikationsinhaltsdaten verarbeiten will, bedarf es der Einwilligung aller Kommunikationsteilnehmer.

Dies dürfte in der Praxis nur dann keine besonderen Schwierigkeiten verursachen, wenn beispielsweise der Betreiber einen Messenger-Dienst als App anbietet und eine Kommunikation unter den Nutzern nur über diese App möglich ist.

Anders hingegen wären Fälle bei unterschiedlichen Webmaildiensten zu beurteilen. Will der Betreiber des Webmaildienstes Inhaltsdaten aufgrund einer Einwilligung verarbeiten, gelingt es ihm zwar ohne weiteres, eine Einwilligung bei dem Nutzer einzuholen, der bei ihm ein Webmailkonto z.B. bei Gmail führt. Die Kommunikationspartner des Nutzers, die nicht zugleich auch Nutzer desselben Webmaildienstes sind, weil sie z.B. ein E-Mail-Konto bei T-Online führen, können nicht ohne weiteres eine Einwilligung erteilen. Auch diese Konstellation zeigt, dass die Umsetzung der ePrivacy-VO keinesfalls leicht gelingen dürfte.

Soweit die ePrivacy-VO spezielle Regelungen für die Verarbeitung von personenbezogenen Daten, insbesondere von Kommunikationsdaten enthält, genießt sie als lex specialis Anwendungsvorrang gegenüber der DS-GVO.[22]

Ein Rückgriff auf die allgemeinen Rechtsgrundlagen gem. Art. 6 DS-GVO, insbesondere der Interessenabwägung gem. Art. 6 Abs. 1 lit. f) DS-GVO, bleibt verwehrt.

2. Speicherung und Löschung

Nach den Vorschriften zum rechtmäßigen Umgang mit Kommunikationsdaten enthält die ePrivacy-VO konkrete Regelungen zur Speicherung und Löschung elektronischer Kommunikationsdaten. Nach Art. 7 der Entwürfe ist der Betreiber eines elektronischen Kommunikationsdienstes verpflichtet, die Kommunikationsdaten zu löschen oder zu anonymisieren, sobald die Daten für die Bereitstellung des Dienstes nicht mehr benötigt werden.

Wie auch die DS-GVO enthält die ePrivacy-VO keine Definition zum Begriff der Anonymisierung. Eine Begriffsdefinition wäre jedoch zur Klarstellung und Bestimmtheit der Anforderungen erforderlich. Im Zusammenhang mit der Verarbeitung von elektronischen Kommunikationsdaten unterliegen einige Betreiber und Verantwortliche nach wie vor dem Irrglauben, dass das Entfernen von Klardaten oder eindeutigen Meinungen des Nutzers in jedem Fall zu einer Anonymisierung des Datensatzes führe.

Das Entfernen von Klardaten, aber auch die Kürzung der IP-Adresse oder der Mac-Adresse, führen nicht zu einer Anonymisierung des kompletten Datensatzes. Zwar könne isoliert betrachtet ein einzelnes Datum durch Kürzung oder Anwendung eines Hash-Verfahrens unter bestimmten Voraussetzungen derart verändert werden, dass der Nutzer nur unter unverhältnismäßigen Aufwand identifiziert werden kann. Bei der Beurteilung, ob personenbezogene Daten anonymisiert wurden und somit aus dem Anwendungsbereich der DS-GVO und ePrivacy-VO fallen, genügt nicht die isolierte Betrachtung eines Datums. Ein Datensatz besteht nicht nur aus einer IP-Adresse oder der MAC-Adresse, sondern in der Regel aus einer Vielzahl von Nutzungsdaten.[23] Enthält ein Datensatz weitere eindeutige Kennungen, so genügt es nicht, ein einzelnes Datum zu anonymisieren. Entscheidend ist, ob der gesamte Datensatz anonym ist.

3. Opt-In oder Opt-Out

Neben den restriktiven Vorschriften zur Verarbeitung von Kommunikationsdaten gehört Art. 8 zu den umstrittensten Regelungen der neuen Verordnung.

Hiernach ist grundsätzlich jede Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer, auch über deren Software und Hardware unter-

21 Erwägungsgrund 2 ePrivacy-VO (E) Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 10.01.2017, COM/2017/010 final – 2017/03 (COD).

22 Schwartmann/Benedikt/Jacquemain, Die ePrivacy-VO kommt: Reichweitenmessung und Nutzungsprofile über Cookies zwischen DS-GVO und ePrivacy-VO, PinG 04/2018, 150, 151.

23 Benedikt, Buckel, Mammen, Web-Tracking nach DS-GVO, Praxishilfe zum Datenschutz im Online-Marketing inklusive Compliance-Nachweis und Checkliste zum Tracking bei Websites, 1. Aufl. 2019, S. 20f.

sagt. Welche Ausnahmen von diesem Grundsatz gelten werden, ist derzeit noch nicht absehbar.

Der Entwurf der Kommission sah vor, dass Informationen auf Endeinrichtungen lediglich verarbeitet werden dürfen, wenn dies zur Durchführung eines elektronischen Kommunikationsvorgangs oder zur Bereitstellung eines Dienstes der Informationsgesellschaft nötig ist, der Nutzer seine Einwilligung erteilt hat oder dies zur Reichweitenmessung erforderlich ist.

Der Entwurf des Parlaments griff diese restriktiven Regelungen auf und konkretisierte die Bedingungen für eine rechtmäßige Reichweitenmessung. Demnach ist eine Reichweitenmessung ausschließlich eine statistische Analyse, die nur vom Betreiber selbst oder einer unabhängigen Webanalyseagentur durchgeführt werden darf. Dabei ist sicherzustellen, dass die Daten nur in aggregierter Form verarbeitet werden und Dritte keinen Zugang zu den Daten haben. Jede weitergehende Verarbeitung, die nicht den abschließend genannten Zwecken dient, bedarf einer Einwilligung.

Auch die Entwürfe der WP Tele führen die strenge Einwilligungslösung fort.

Die praktischen Folgen dieser Opt-In-basierten Lösung sind weitreichend. Nahezu jede Form der individualisierten oder zielgruppenorientierten Werbung bei Online-Angeboten wäre in der heutigen Form kaum denkbar. Dies hat unmittelbare Auswirkungen auf Werbenetzwerken aber auch Werbetreibende, deren Geschäftsmodelle ganz oder überwiegend von der Werbefinanzierung abhängen.

Sinn und Zweck der Einwilligungslösung ist es, dem Nutzer die Entscheidungsbefugnis über sein Nutzungsverhalten zurückzugeben. Der Nutzer soll frei entscheiden können, ob und wenn ja, in welcher Form er für welche Zwecke bei der Verwendung von Apps, Websites, Messenger und sonstigen web-basierten Angeboten verfolgt wird.

Der Gesetzgeber wählt offensichtlich den Weg des Opt-In und verlangt bei einer Vielzahl von Datenverarbeitungen im Web die Einwilligung des Nutzers. Unbestritten ist, dass die derzeitige Praxis der „Cookie-Banner", intransparenten Datenverarbeitung und aggressiven Erstellung von Nutzungsprofilen eine enorme Beeinträchtigung der Nutzer darstellt.

Der Nutzer hat unter den derzeit praktizierten Verfahren weder eine reale Chance, den weitreichenden Umfang des dienst- oder geräteübergreifenden Tracking zu erfassen, noch hat er eine Chance, sich der Verarbeitung zu entziehen.

Dennoch ist fraglich, ob die ePrivacy-VO diesen Umstand mit den Mitteln einer harten Opt-In-Lösung zugunsten des Nutzers verbessern wird.

Unabhängig davon, wie die endgültige Fassung des Art. 8 ePrivacy-VO formuliert sein wird, kann der Konflikt zwischen den Interessen und Bedürfnissen des Nutzers auf der einen Seite und denen der Verantwortlichen und Betreibers auf der anderen Seite nicht aufgelöst werden.

Der Nutzer ist es gewohnt, kostenlose Inhalte im Web zu konsumieren, ohne auf Benutzerfreundlichkeit zu verzichten. Die permanente Abfrage einer Einwilligung oder der Einsatz von Tracking-Walls laufen diesen Interessen zuwider.

Auch der Betreiber wird in der Regel aus wirtschaftlichen Gesichtspunkten nicht auf Tracking-Tools oder die Einbindung sonstiger Drittanbieter verzichten.

Dies gilt unabhängig davon, ob das Recht ein Opt-In oder Opt-Out vorsieht.

4. Einwilligung über Browsereinstellungen

Um dennoch ansatzweise einen Ausgleich zwischen den Interessen der Nutzer und denen der Betreiber zu erzielen, sah der Vorschlag des Parlaments in Art. 10 vor, dass der Nutzer seine Einwilligung einmalig für die gesamte Nutzung über seine Privatsphäre-Einstellungen geben könne.

Diese Regelung wurde in den Entwürfen des Rats ersatzlos gestrichen.

Dabei wäre eine Lösung über die Einstellungen des Browsers oder über das Betriebssystem für beide Seiten vorteilhaft gewesen.

Der Nutzer würde aus seiner „Klick-Routine" befreit werden und einmalig entscheiden, ob und wenn ja für welche Zwecke er ein Tracking zulässt.

Der Betreiber hingegen könne auf „Cookie-Banner" verzichten, die den Nutzer überfrachten und teils ohnehin leerlaufen, weil Datenverarbeitungen stattfinden, bevor der Nutzer eine freie Entscheidung treffen konnte.[24]

Doch genau an dieser Stelle zeigt sich, welche Interessenkonflikte in der digitalen Welt bestehen.

Softwareanbieter, die über Nutzereinstellungen eine wirksame Einwilligung für einen anderen Betreiber einholen, profitieren in keiner Weise davon. Es fehlt ein Anreiz, um diese Regelungen durchzusetzen. Auch offenbart ein Blick über den Tellerrand des Datenschutzes hinaus, dass es im Kern der Diskussion um kartellrechtliche Fragestellungen geht, die mit den Mitteln des Datenschutzes nur bedingt zu lösen sind.

Solange es einige wenige Unternehmen gibt, die sowohl ein eigenes Werbenetzwerk betreiben, als auch Betreiber einer Suchmaschine sind, zugleich aber auch Anbieter eines Browsers und Betriebssystemhersteller sind, wird es in absehbarer Zeit kein Marktgleichgewicht geben. Wer das Internet beherrscht, sei es durch die Bereitstellung von Inhalten oder das Betreiben von Cloud-Computing-Services, entscheidet auch über die Spielregeln des Marktes.

5. Regelungen zum Beschäftigtendatenschutz

Eine weitere Besonderheit der ePrivacy-VO sind Vorschriften für besondere Verarbeitungssituationen. So enthält der Entwurf des Parlaments eine Vorschrift zum Beschäftigtendatenschutz. Hiernach darf der Arbeitgeber Informationen auf Endeinrichtungen der Arbeitnehmer verarbeiten, wenn dies zur Erfüllung der arbeitsrechtlichen Pflichten des Arbeitnehmers erforderlich ist und keine Überwachung des Arbeitnehmers erfolgt.[25] Würde diese Regelung verbindliches Recht

24 Vgl. Ergebnis der Website-Prüfung des Bayerischen Landesamts für Datenschutzaufsicht, Sicher im Internet – Digitale Dienste im Datenschutzcheck am Safer Internet Day 2019, abrufbar unter: https://www.lda.bayern.de/media/sid_ergebnis_2019.pdf.

25 Art. 8 Abs. 1 db) i) ePrivacy-VO (E) Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)v. 10.01.2017, COM/2017/010 final -2017/03 (COD).

werden, wäre die Rechtsprechung in Bezug auf die Stellung des Arbeitsgebers als TK-Anbieter[26] endgültig überholt.

6. Offline-Tracking

Darüber hinaus enthält die ePrivacy-VO eine Regelung zum Offline-Tracking. Beim Offline-Tracking können Standorte, Laufwege, Verweildauer und weitere Informationen über Besucher im Einzelhandel, in Fußgängerzonen oder Veranstaltungsgeländen erfasst werden. Dies gelingt über unterschiedliche Tracking-Technologien wie z.B. das Wifi- oder Bluetooth-Tracking, bei dem Signale des mobilen Endgeräts eines Besuchers verarbeitet werden.

In vielen Einsatzszenarien wird weder über die Datenverarbeitung informiert, noch erfolgt das Offline-Tracking aufgrund einer Rechtsgrundlage oder einer Einwilligung. Diesen Missstand erkannte der Gesetzgeber und formulierte Anforderungen für ein rechtmäßiges Offline-Tracking. Hiernach ist das Offline-Tracking nur zulässig, wenn der Besucher hinreichend informiert wird und das Tracking ausschließlich zum Zweck einer statistischen Zählung erfolgt.

VI. Kapitel 3 – Kontrolle über die elektronische Kommunikation

Das 3. Kapitel der ePrivacy-VO enthält Regelungen, die im Wesentlichen nur für Betreiber von klassischen Telekommunikationsdiensten relevant sind. Darunter fallen Vorschriften zur Anzeige der Rufnummer des Anrufers, die Rufnummernunterdrückung, die Sperrung eingehender Anrufe oder öffentlich zugängliche Verzeichnisse wie z.B. das Telefonbuch oder die Gelben Seiten in Deutschland.

1. Direktwerbung

Von besonderer Relevanz ist hingegen die Vorschrift zur unerbetenen Kommunikation. Art. 16 der Entwürfe regelt Telefonanrufe und die Nutzung elektronischer Kommunikationsdienste für Werbezwecke.

Nach den Entwürfen ist Direktwerbung über elektronische Nachrichten nur nach voriger Einwilligung des Nutzers zulässig. Dies gilt sowohl für natürliche als auch juristische Personen. Einer Einwilligung bedarf es nicht, wenn nur für eigene Produkt oder Dienstleistung geworben wird, die Kontaktdaten im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung erhalten wurden und der Kunde der Nutzung seiner Daten für Werbezwecke nicht widersprochen hat, obwohl er zuvor auf sein Widerspruchsrecht hingewiesen wurde.

Im Hinblick auf Direktwerbeanrufe sehen die Entwürfe zur ePrivacy-VO eine Öffnungsklausel für die Mitgliedsstaaten vor. Im Falle von Direktwerbeanrufen können die Mitgliedsstaaten Abweichungen zum Einwilligungserfordernis vorsehen. Demnach wären Direktwerbeanrufe bei Nutzern zulässig, die dem Erhalt solcher Kommunikation nicht widersprochen haben. Die Mitgliedsstaaten müssen sicherstellen, dass der Nutzer die Möglichkeit hat, über eine Robinson-Liste Direktwerbeanrufen zu widersprechen. Über eine einheitliche Widerspruchsliste soll gewährleistet werden, dass der Nutzer nur ein einziges Mal sein Widerspruchsrecht ausüben muss.

Diese Regelung steht im Widerspruch zur bisherigen Praxis in Deutschland, nach der für Direktwerbeanrufe bei Verbrauchern und sonstigen Marktteilnehmern gem. Art. 7 Abs. 2 Nr. 2 UWG die Einwilligung erforderlich ist.

Die vorgeschlagenen Regelungen der ePrivacy-VO zum Direktmarketing entsprechen im Wesentlichen Art. 13 ePrivacy-RL.

Neu ist, dass die Vorschriften zur Direktwerbung nicht nur auf elektronische Post, d.h. E-Mails, beschränkt ist, sondern jede Form von Nachrichten erfasst, die über elektronische Kommunikationsmittel erschickt werden. Dazu gehören auch Nachrichten über Messenger oder Push-Nachrichten in Apps.

2. Informationspflicht bei Sicherheitsrisiken

Die Entwürfe zur ePrivacy-VO enthalten auch eine zusätzliche Informationspflicht gem. Art. 17 ePrivacy-VO (E) über anerkannte Sicherheitsrisiken, die für Betreiber von elektronischen Kommunikationsdiensten gilt. Hiernach ist der Betreiber von elektronischen Kommunikationsdiensten verpflichtet, den Nutzer über Sicherheitsrisiken zu informieren. Diese Informationspflicht geht über die allgemeinen Hinweise zur Verarbeitung von Daten gemäß Art. 12 ff. DS-GVO hinaus und soll die Nutzer beispielsweise im Falle von Angriffswellen wie bei der Schadsoftware Emotet warnen und den Nutzern Hinweise zum Selbstschutz geben.[27]

Diese spezielle Informationspflicht ist vor dem Hintergrund der zunehmenden Bedrohungslage bei elektronischen Kommunikationsdiensten durchaus gerechtfertigt.

Unklar bleibt jedoch für den Rechtsanwender das Verhältnis zu den weiteren Transparenzanforderungen, insbesondere den Melde- und Benachrichtigungspflichten, gemäß Art. 33, 34 DS-GVO. Art. 17 ePrivacy-VO (E) enthält weder Mindestanforderungen zum Inhalt der Informationspflicht noch eine konkrete Frist, innerhalb derer die Information zu erteilen ist. Auch eine Definition des Begriffs Sicherheitsrisiko fehlt, sodass der Betreiber elektronischer Kommunikationsdienste aufgrund der unbestimmten Norm seiner Verpflichtung nur schwer nachkommen dürfte. Damit läuft die Vorschrift in der Praxis leer. Diese Problematik wurde im Arbeitsentwurf der WP Tele[28] erkannt, mit der Folge, dass die Informationspflicht bei Sicherheitsrisiken ersatzlos gestrichen wurde.[29]

VII. Kapitel 4 – Aufsichtsbehörden

Kapitel vier regelt die unabhängigen Aufsichtsbehörden und die Durchsetzung der Regelungen. Für die Überwachung und

26 Beschluss des Oberlandesgerichts Karlsruhe vom 10.01.2005, 1 Ws 152/0.

27 In Deutschland ist es u.a. Aufgabe des BSI, über Gefahren und Sicherheitsrisiken zu informieren. Der Betreiber wird in der Regel nicht über die erforderlichen Informationen verfügen, um eine valide Einschätzung der Bedrohungslage abgeben zu können.

28 Ratsarbeitsgruppe "Telekommunikation und Informationsgesellschaft".

29 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 17.10.2019, RAT: 13080/19.

Durchsetzung der ePrivacy-VO sollen die unabhängigen Aufsichtsbehörden zuständig sein, die auch für den Vollzug der DS-GVO zuständig sind.

Um eine einheitliche Rechtsanwendung und einen einheitlichen Vollzug zu gewährleisten, sollen die Aufsichtsbehörden zusammenarbeiten. Darüber hinaus findet das Kohärenz-Verfahren der DS-GVO Anwendung. Auf den ersten Blick erscheint es folgerichtig, die Regelungen der DS-GVO zur Zusammenarbeit und Kohärenz der Aufsichtsbehörden entsprechend anzuwenden.

Bei näherer Betrachtung wird jedoch deutlich, dass Konflikte im Vollzug unausweichlich sind.

Dies gilt beispielsweise in Mitgliedstaaten mit föderalen Strukturen und sektoralen Aufsichtsbehörden wie Deutschland. Neben der Vielzahl an Datenschutzaufsichtsbehörden des Bundes und der Länder, zählen auch die spezifischen Aufsichtsbehörden u.a. für den Rundfunk und die Kirchen zu den zuständigen Aufsichtsbehörden nach der ePrivacy-VO. Im Bereich der elektronischen Kommunikation wäre darüber hinaus auch die Bundesnetzagentur als Aufsichtsbehörde im Sinne der ePrivacy-Verordnung zuständig.

Der nationale Gesetzgeber wäre erneut verpflichtet, umfassende Zuständigkeitsbestimmungen im nationalen Recht zu schaffen, um sicherzustellen, dass bei der Vielzahl der Aufsichtsbehörden Zuständigkeitskonflikte vermieden werden und die Handlungsfähigkeit der Behörden gewährleistet ist. Insbesondere bedarf es einer geänderten Vorschrift zur sachlichen Zuständigkeit des BfDI.

1. Zuständige Behörden innerhalb Deutschlands

Grundsätzlich sind die Landesaufsichtsbehörden gem. Art. 83 f. GG für den Vollzug der ePrivacy-VO zuständig. Für den Bereich der Telekommunikation wurde der Vollzug gem. § 115 Abs. 4 TKG bisher dem BfDI übertragen. Diese Zuständigkeitsregelung des BfDI dürfte für den Vollzug der ePrivacy-VO nicht ohne weiteres übertragbar sein.[30] Schon heute ergeben sich Zuständigkeitskonflikte beim Vollzug der DS-GVO, der ePrivacy-RL und dem TKG in Bezug auf OTT-Dienste.

Zuletzt hatte die Entscheidung des EuGH in Sachen Gmail Auswirkungen auf die Zuständigkeit der deutschen Aufsichtsbehörden. Der EuGH äußerste sich in Sachen GMail zu der Frage, ob es sich bei Webmaildiensten um Telekommunikationsdienste i. S. d. TKG handelt und verneinte diese Frage.[31] Dies hat zur Folge, dass – mangels Anwendbarkeit des TKG – die Zuständigkeitsregel des § 115 Abs. 4 TKG nicht greift und es bei dem Grundsatz verbleibt, dass die Datenschutzaufsichtsbehörden der Länder für den Vollzug zuständig sind.[32]

Der EuGH führte in seiner Entscheidung aus, dass der von GMail erbrachte Dienst "nicht ganz oder ganz überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht".[33] Diese Erwägungen sind auch auf andere OTT-Dienste, wie z.B. Messenger übertragbar, da sie auf technischer Ebene der Funktionsweise von Webmaildiensten entsprechen. Daraus ergibt sich bereits nach geltendem Recht die Zuständigkeit der Datenschutzaufsichtsbehörden der Länder. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) beurteilte dies anders und kam zu dem Ergebnis, dass Messenger auch nach der Entscheidung des EuGH als Telekommunikationsdienste i.S.d. TKG angesehen werden können. Die hat zur Folge, dass der BfDI für Messenger-Dienste weiterhin zuständig ist (§ 115 Abs. 4 TKG).[34]

Zusammenfassend ergibt sich bereits nach heutiger Rechtslage, das komplexe Zuständigkeitsgefüge der nationalen Aufsichtsbehörden innerhalb Deutschlands anzupassen.

2. Unabhängige Aufsichtsbehörden

Wie auch die DS-GVO hebt die ePrivacy-VO die unabhängige Stellung der Aufsichtsbehörden hervor. Die Unabhängigkeit ist nur gewährleistet, wenn die Aufsichtsbehörden gem. Art. 52 Abs. 2 DS-GVO völlig weisungsfrei handeln können. Nur eine völlige Weisungsfreiheit garantiert, dass die Aufsichtsbehörden ihre Befugnisse ohne direkte oder indirekte Beeinflussung wahrnehmen können.[35]

Die Unabhängigkeit dürfte jedenfalls im Hinblick auf die Bundesnetzagentur zu überprüfen sein. Sowohl das Bundesministerium für Wirtschaft und Energie als auch das Bundesministerium für Verkehr und digitale Infrastruktur können der Bundesnetzagentur Weisungen erteilen, § 117 TKG. Darüber hinaus unterliegt die Bundesnetzagentur der parlamentarischen Kontrolle. Das Gesetz über die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen sieht in § 5 vor, dass ein Beirat einzuberufen ist. Der Beirat besteht aus jeweils 16 Mitgliedern des Deutschen Bundestages und 16 Vertretern oder Vertreterinnen des Bundesrates und wirkt gem. § 120 TKG an Entscheidungen der Bundesnetzagentur mit.

Es bleibt abzuwarten, wie der nationale Gesetzgeber die Zuständigkeit künftig regeln und die Unabhängigkeit der Aufsichtsbehörden sicherstellen wird.

VIII. Kapitel 5 – Rechtsbehelfe, Haftung und Sanktionen

Um einen Einklang mit der DS-GVO zu gewährleisten, verweist die ePrivacy-VO vollständig auf die Vorschriften des 8. Kapitels der DS-GVO zu Rechtsbehelfen, Haftung und Sanktionen.

Demnach stehen jedem Endnutzer sowie jeder Einrichtung oder Organisation unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs die Rechte gemäß Art. 77 ff. DS-GVO zu. Der Endnutzer hat das Recht, bei einer Aufsichtsbehörde eine Beschwerde einzureichen.

30 Engeler/Felber: Entwurf der ePrivacy-VO aus Perspektive der aufsichtsbehördlichen Praxis, ZD 2017, 251, 257.

31 EuGH, Urt. v. 13.06.2019, Az. C-193/18.

32 Bei konsequenter Betrachtung war der BfDI zu keinem Zeitpunkt sachlich zuständige Aufsichtsbehörde für E-Mail-Provider. Mangels Anwendbarkeit des TKG sind die Aufsichtsbehörden der Länder zuständig. Ob die Entscheidung auch auf andere OTT-Dienste übertragbar ist, wurde unter den Aufsichtsbehörden kontrovers diskutiert.

33 EuGH, Urt. v. 13.06.2019, Az. C-193/18 Rn. 35.

34 DSK, Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12.09.2019 zur sachlichen Zuständigkeit für E-Mail und andere Over-the-top (OTT)-Dienste, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20190912_beschluss_zu_ott_diensten.pdf.

35 Selmayr, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 52, Rn. 16 f.

Befasst sich die Aufsichtsbehörde nicht mit der Beschwerde oder informiert sie den Beschwerdeführer nicht innerhalb von drei Monaten über den Stand der Bearbeitung der Beschwerde, so unterliegt dies einer gerichtlichen Überprüfung.

1. Interessenskollision im Vollzug

Das Beschwerderecht kann im Einzelfall zu Interessenskollisionen bei den Aufsichtsbehörden führen, was anhand folgenden Beispiels verdeutlicht wird:

Ein Unternehmen bietet für die Kontaktaufnahme mit Kunden die Kommunikation über einen Messenger an. Der verwendete Messenger-Dienst nutzt die Kommunikationsdaten u.a. für Werbezwecke und behält sich vor, die Daten auch an Dritte weiterzuleiten. Für diese Verarbeitungstätigkeiten liegt weder eine Rechtsgrundlage noch eine wirksame Einwilligung aller Kommunikationsteilnehmer vor. Dennoch entscheidet sich das Unternehmen bewusst dafür, den Messenger-Dienst wegen der hohen Verbreitung weiter zu nutzen.

Die Kunden des Unternehmens sind nicht nur Nutzer des Messenger-Dienstes und unterliegen somit dem Schutzbereich der ePrivacy-VO. Sie sind zugleich Betroffene nach der DS-GVO. Der Unternehmer fällt ebenfalls in den Schutzbereich der ePrivacy-VO und kann sein Beschwerderecht wegen unzulässiger Verarbeitung der Kommunikationsdaten gegenüber den Aufsichtsbehörden geltend machen.

Andererseits ist das Unternehmen auch Verantwortlicher i.S.d. DS-GVO im Hinblick auf die verwendeten Kommunikationsmitteln.

Der Unternehmer muss sicherstellen, dass seine Kommunikation zum Betroffenen die Vorschriften der DS-GVO und der ePrivacy-VO erfüllt.

Bei einem vergleichbaren Fall kam die zuständige Aufsichtsbehörde zu dem Ergebnis, dass ein Unternehmen gegen die DS-GVO verstößt, wenn es einen rechtswidrigen Messenger-Dienst verwendet.[36]

In dem Fallbeispiel ist der Unternehmer einerseits Verantwortlicher nach der DS-GVO und Adressat der datenschutzrechtlichen Vorgaben, deren Verstoß sanktioniert werden kann. Zugleich ist der Verantwortliche durch die ePrivacy-VO geschützter Kommunikationsteilnehmer. Wie dieser Konflikt in der aufsichtlichen Vollzugspraxis aufgelöst werden kann, bleibt abzuwarten.

2. Aufgaben und Befugnisse

Wie auch die DS-GVO regelt die ePrivacy-VO, dass der europäische Datenschutzausschuss, bestehend aus Vertretern der Aufsichtsbehörden eines jeden Mitgliedstaates, für die einheitliche Anwendung der ePrivacy-VO zuständig ist. Der europäische Datenschutzausschuss soll Leitlinien entwickeln. Zudem soll er im Fall widersprüchlicher Standpunkte zwischen mehreren zuständigen Aufsichtsbehörden verbindliche Beschlüsse erlassen.

Für die Durchsetzung der ePrivacy-VO stehen den Aufsichtsbehörden die Befugnisse der DS-GVO zu. Auch der Bußgeldrahmen entspricht dem der DS-GVO, sodass bei einem Verstoß eine Geldbuße von bis zu 20 Millionen € oder im Fall eines Unternehmens von bis zu 4 % des weltweit erzielten Jahresumsatzes verhängt werden kann.

IX. Fazit

Dass ein weiterer Rechtsrahmen neben der DS-GVO erforderlich ist, um einen umfassenden Schutz bei digitalen Diensten gewährleisten, dürfte unbestritten sein.

Die große Herausforderung ist es dabei, ein Gesetz zu verfassen, welches flexibel genug ist, um auch in Zukunft mit dem technologischen Fortschritt mithalten zu können, aber auch kein allzu starres Korsett darstellt, durch das digitale Entwicklungen erschwert oder gar unmöglich werden.

Zumindest die bereits veröffentlichten Entwürfe zur ePrivacy-VO scheinen diese Herausforderung nicht zu meistern.

Es fehlt an klaren Definitionen sowie an Vorschriften, die unmissverständlich das Verhältnis zum europäischen und nationalen Recht regeln.

An welchen Stellen die ePrivacy-VO spezielleres Recht ist und die DS-GVO verdrängt, in welchen Fällen sie einen eigenständigen Regelungsbereich enthält, oder ob ein Verweis auf die Vorschriften der DS-GVO erfolgt, ist für den Rechtsanwender nach dem aktuellen Stand des Gesetzgebungsverfahrens völlig unklar.

Das wirft unzählige Fragen auf: Wenn der Anwendungsbereich für juristische Personen eröffnet ist, sind dann auch Betroffenenrechte zu gewährleisten? Gelten die Anforderungen der DS-GVO zu gemeinsam Verantwortlichen und Auftragsverarbeitern? Immerhin wirken im digitalen Bereich stets eine Vielzahl von Akteuren an der Verarbeitung von Daten mit.

Und wie soll künftig sichergestellt werden, dass Europa jedenfalls faktisch die Chance hat, im digitalen Wettstreit mitzuhalten? Die DS-GVO greift diesen Gedanken zumindest in den Erwägungsgründen auf und privilegiert die Verarbeitung zu wissenschaftlichen Zwecken.

Die ePrivacy-VO verliert kein Wort über nicht mehr wegzudenkende Technologien wie Blockchain und Künstliche Intelligenz. Darin zeigt sie ihre womöglich größte Schwäche. Ein Rechtsrahmen, der BigData-Anwendungen schlicht unmöglich macht, ist schon heute überholt und veraltet, noch bevor er überhaupt gilt.

Kristin Benedikt
Kristin Benedikt ist Leiterin des Bereichs Internet beim Bayerischen Landesamt für Datenschutzaufsicht.

36 Entscheidung der Rumänischen Datenschutzaufsichtsbehörde vom 09.10.2019 zum Einsatz von WhatsApp, abrufbar unter: https://www.dataprotection.ro/?page=Comunicat_Presa_09_10_2019&lang=ro.

Barbara Thiel

Prüfung der LfD Niedersachsen zur Umsetzung der DS-GVO in Unternehmen – die Ergebnisse

Es ist erst wenige Jahre her, dass die Wirtschaft in den Kontrolltätigkeiten der Landesbeauftragten für den Datenschutz (LfD) Niedersachsen eine eher untergeordnete Rolle spielte. Unternehmen und ihre immensen Datenströme waren kaum im Fokus der Aufsichtsbehörde. Doch das hat sich in den vergangenen fünf Jahren geändert: Inzwischen hat die Aufsicht über die Wirtschaft ein mindestens genau so großes Gewicht wie jene über den öffentlichen Bereich. So war es nur folgerichtig, dass die LfD Niedersachsen unmittelbar nach Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO) eine groß angelegte Prüfung zu deren Umsetzung in niedersächsischen Unternehmen initiierte.

50 große und mittelgroße Unternehmen mit Hauptsitz in Niedersachsen sollten in der sogenannten Querschnittsprüfung darlegen, ob und wie sie die Regelungen der DS-GVO in der betrieblichen Praxis mit Leben füllten. Hierfür sollten sie Fragen zu zehn Komplexen beantworten, welche die wesentlichen Bereiche der DS-GVO abdeckten. In der Auswertung der Antworten wurde jedem Fragenkomplex eine Ampelfarbe zugeordnet, die zeigte, ob es in diesem Bereich keinen bzw. kaum (grün), normalen (gelb) oder erheblichen Handlungsbedarf (rot) gab. Ausgehend von diesen Einzelergebnissen erhielt jedes Unternehmen eine Gesamtbewertung, ebenfalls in Rot, Gelb oder Grün (Anmerkung der Verfasserin: *Eine ausführliche Darstellung der Prüfungsplanung und -auswertung findet sich in RDV-Heft 2/2019)*.

Nun liegen die Ergebnisse dieser bislang umfassendsten Prüfung in der Geschichte der LfD Niedersachsen vor. Sie liefern wertvolle Erkenntnisse sowohl für die datenschutzrechtlichen Erfordernisse in Wirtschaftsunternehmen als auch für die weitere aufsichtsbehördliche Tätigkeit.

I. Ergebnisse im Überblick – neun Unternehmen bleiben rot

Die meisten der geprüften Unternehmen hatten sich intensiv auf die DS-GVO vorbereitet, die größeren in der Regel im Rahmen eines 2017 gestarteten unternehmensweiten Projektes. Die Ergebnisse der Querschnittsprüfung waren dennoch zunächst ernüchternd. Gerade einmal 5 der 50 geprüften Unternehmen konnte die LfD Niedersachsen nach der Auswertung der ersten Antworten mit „Grün" bewerten. Nur bei diesen fünf wurde in keinem der zehn Fragenkomplexe ein erheblicher Handlungsbedarf festgestellt. Bei weiteren 15 Unternehmen musste „nur" ein Komplex mit dem Prädikat „Rot" versehen werden, diese wurden deshalb insgesamt mit „Gelb" bewertet. Auffällig war hier, dass dieser eine mit Rot bewertete Fragenkomplex entweder den technisch-organisatorischen Datenschutz oder die Datenschutzfolgenabschätzung (DSFA) betraf – dazu später mehr.

30 von 50 Unternehmen erhielten zunächst die Gesamtbewertung „Rot". Bei ihnen wurde in mehr als einem Fragenkomplex erheblicher Handlungsbedarf festgestellt. Auch hier bereiteten die Bereiche des technisch-organisatorischen Datenschutzes und der DSFA die mit Abstand größten Schwierigkeiten.

Für die insgesamt mit Grün und mit Gelb bewerteten Unternehmen war die Prüfung beendet, sobald sie ihr schriftliches Ergebnis erhalten hatten. Darin schlüsselte die LfD Niedersachsen anhand eines Katalogs von über 200 Einzelkriterien genau auf, wie es zur Bewertung der einzelnen Komplexe gekommen war. So sollten die Unternehmen zum einen möglichst transparent über die Auswertung ihrer Antworten informiert werden. Zum anderen gab die LfD dadurch Hinweise, wo und wie der Datenschutz im jeweiligen Unternehmen noch zu verbessern war.

Auch die mit Rot bewerteten Unternehmen erhielten ihr Ergebnis in dieser Form. Sie wurden aber gleichzeitig zu einer weiteren Stellungnahme aufgefordert. Mit dieser zweiten Abfrage wollte die LfD Niedersachsen ihnen die Gelegenheit geben, sich im Gesamtergebnis noch zu verbessern. Schließlich war es auch möglich, dass die Unternehmen den Erwartungshorizont der Behörde in ihren ersten Antworten falsch eingeschätzt und nur deshalb unzureichende Auskünfte gegeben hatten.

Tatsächlich gelang es 4 der 30 Unternehmen im Zuge des zweiten Prüfungsschrittes, sich von Rot auf Grün zu verbessern. Durch ihre ergänzenden Antworten musste nun keiner der Fragenkomplexe mehr mit Rot bewertet werden. Dieser große Sprung in der Bewertung lässt sich auf zwei Faktoren zurückführen: Zum einen resultierten rote Bewertungen teilweise daraus, dass die Unternehmen den Erwartungshorizont der LfD Niedersachsen hinsichtlich der Antworttiefe nicht richtig eingeschätzt hatten. Zum anderen befanden sich einige Unternehmen zu Beginn der Querschnittsprüfung noch in der Umsetzungsphase zur DS-GVO. Zum Zeitpunkt ihrer zweiten Stellungnahme konnten sie aber eine aktualisierte Antwort geben, aus der hervorging, dass die Anforderungen zwischenzeitlich umgesetzt worden waren. Das wurde in der Bewertung berücksichtigt.

Weitere 17 Unternehmen verbesserten sich auf Gelb, standen somit noch bei einem Fragenkomplex auf Rot.

Bei den übrigen neun Unternehmen blieb es bei der Gesamtbewertung Rot. Sie hatten also trotz der ergänzenden

Stellungnahme weiterhin mehr als einen „roten" Fragenkomplex. Alle neun Unternehmen standen beim technisch-organisatorischen Datenschutz auf Rot, sechs auch bei der DSFA. Darüber hinaus gab es rote Bewertungen bei den Einwilligungserklärungen (5), beim Prozess zur Meldung von Datenpannen (3) sowie bei den Betroffenenrechten, der Bestellung von Datenschutzbeauftragten und der Auftragsverarbeitung (je 1). Insgesamt standen nach zwei Prüfungsschritten also 9 Unternehmen auf Grün, 32 auf Gelb und 9 auf Rot.

Gesamtbewertung nach erstem Prüfungsschritt

Gesamtbewertung nach zweitem Prüfungsschritt

Am wenigsten Schwierigkeiten bereiteten den Unternehmen die Bereiche Auftragsverarbeitung, Datenschutzbeauftragte (DSB), Meldepflichten von Datenschutzverletzungen und Dokumentation. Hier wurden nur gelegentlich Defizite festgestellt. Etwas häufiger bemängeln musste die LfD Niedersachsen die Antworten in den Komplexen Verzeichnis von Verarbeitungstätigkeiten, Einwilligungen und Betroffenenrechte. Verbreitet erhebliche Defizite lagen, wie bereits angedeutet, bei den Themen technisch-organisatorischer Datenschutz und DSFA vor. Besonders gravierend: Nicht selten wurde bei der Risikoeinschätzung der Fokus auf die (finanziellen) Risiken für das Unternehmen gelegt statt – wie im Datenschutz nötig – auf die Risiken für die Betroffenen.

II. Ergebnisse im Detail

1. Fragenkomplex 1 – Vorbereitung auf die DS-GVO

„Wie haben Sie sich als Unternehmen auf die DS-GVO vorbereitet?" Mit dieser weit gefassten, einleitenden Frage wollte die LfD Niedersachsen einen Überblick sowohl über die unterschiedlichen Herangehensweisen der Unternehmen erhalten als auch über deren Selbsteinschätzung hinsichtlich ihres Umsetzungsstandes. Bei der Auswertung achtete die LfD besonders darauf, ob jeweils alle Unternehmensbereiche, die personenbezogene Daten verarbeiten, in die Planungen und Maßnahmen zur Umsetzung der DS-GVO involviert waren. Dies war bei nahezu allen der Fall, nur sehr vereinzelt blieb hier etwas unklar. Erfreulich war auch, dass die Unternehmen überwiegend Schulungen für ihre Beschäftigten durchgeführt oder noch kurzfristig geplant hatten.

2. Fragenkomplex 2 – Verzeichnis von Verarbeitungstätigkeiten

Das Verzeichnis von Verarbeitungstätigkeiten (VVT) ist das Herzstück jedes Datenschutzkonzeptes. Es dient als wesentliche Grundlage für eine strukturierte Dokumentation und als Nachweis der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO. Deshalb müssen Verantwortliche dafür Sorge tragen, dass das VVT vollständig ist, regelmäßig überprüft und falls nötig auch aktualisiert wird. Auch in diesem Bereich waren die Unternehmen überwiegend gut aufgestellt. Nur gelegentlich konnten die Prüferinnen und Prüfer der LfD den zur Verfügung gestellten Übersichten nicht entnehmen, dass alle Standardverfahren wie z.B. das Personal- und Bewerbermanagement oder das Betreiben der Website dokumentiert waren. Vereinzelt fehlten auch die Kontaktdaten des DSB. Insgesamt stellte die LfD hier aber bei keinem Unternehmen erheblichen Handlungsbedarf fest.

3. Fragenkomplex 3 – Zulässigkeit der Verarbeitung

Die Verarbeitung personenbezogener Daten ist nur auf Basis einer gültigen Rechtsgrundlage zulässig. Maßgeblich ist hier besonders Art. 6 Abs. 1 DS-GVO. In diesem Fragenkomplex erwartete die LfD Niedersachsen eine vollständige und plausible Nennung aller für die verschiedenen Verfahren einschlägigen Rechtsgrundlagen. Mehrfach fiel in den Antworten die Aussage, dass keine Datenverarbeitung auf Basis von Einwilligungen erfolge. Zugleich musste aber auf der jeweiligen Webseite der Nutzung von Cookies zugestimmt werden. Oder es ergab sich aus den sonstigen Antworten, dass Newsletter auf Einwilligungsbasis verschickt wurden.

Die LfD Niedersachsen weist beim Thema Einwilligungen immer wieder darauf hin, dass sie in der Regel nicht eingeholt werden sollten, wenn die Verarbeitung auf eine andere Rechtsgrundlage gestützt werden kann. Zudem muss die betroffene Person vor Abgabe der Einwilligung von ihrem Recht auf jederzeitigen Widerruf in Kenntnis gesetzt werden. Da der Widerruf so einfach wie die Erteilung der Einwilligung sein muss, ist u.a. unbedingt anzugeben, an welche Stelle der Widerruf zu richten ist. Dies war bei den Antworten der Unternehmen häufiger nicht klar zu erkennen. Insgesamt stellte die LfD in diesem Fragenkomplex bei fünf Unternehmen erheblichen Handlungsbedarf fest.

4. Fragenkomplex 4 – Betroffenenrechte

Dieser Komplex umfasste besonders die Informationspflichten aus Art. 13 und 14 DS-GVO, das Auskunftsrecht (Art. 15 DS-GVO), die Rechte auf Berichtigung und Löschung (Art. 16 und 17 DS-GVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) sowie das Recht auf Datenübertragbarkeit aus Art. 20 DS-GVO. Die ganz grundsätzlichen Erwartungen der LfD ergaben sich aus Art. 12 DS-GVO, wonach alle Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zu übermitteln sind. Die Unternehmen sollten außerdem für alle Rechte entsprechende Verfahren implementiert haben, um den Anforderungen der DS-GVO form- und fristgerecht zu genügen.

Bei den Informationspflichten war bei der Hälfte der geprüften Unternehmen die Darstellung des Prozesses nicht oder nur teilweise nachvollziehbar beschrieben worden. Ebenfalls bei der Hälfte war das berechtigte Interesse gar nicht beschrieben worden, sofern eine Verarbeitung nach Art. 6 Abs. 1 lit. f DS-GVO erfolgte. Bei einem weiteren Viertel war die Beschreibung nur beispielhalft oder es fehlte die Abwägung mit den Betroffeneninteressen. Ganz überwiegend konnte den Antworten nicht entnommen werden, dass bei einer beabsichtigten Zweckänderung sichergestellt ist, dass die betroffene Person vor dieser Weiterverarbeitung Informationen über den anderen Zweck und alle anderen maßgeblichen Informationen erhält.

Bezogen auf das Auskunftsrecht war die Darstellung des entsprechenden Prozesses bei fast allen Unternehmen nachvollziehbar. Die übrigen Betroffenenrechte wurden von den meisten Unternehmen allerdings trotz expliziter Erwähnung in der Fragestellung nicht näher beschrieben.

Insgesamt sah die LfD in diesem Bereich bei zwei Unternehmen erheblichen Handlungsbedarf.

5. Fragenkomplex 5 – technisch-organisatorischer Datenschutz

Die Fragen zum technisch-organisatorischen Datenschutz waren ausschließlich als Verständnisfragen formuliert. Sie zielten also nicht auf die konkrete Umsetzung technisch-organisatorischer Maßnahmen (TOM) in einzelnen Verfahren ab. Das überdurchschnittlich schlechte Abschneiden der geprüften Unternehmen zu diesem Themenkomplex lässt sich nur in Teilen mit der mangelnden Vertrautheit mit der neuen Rechtslage begründen. So waren beispielsweise der Stand der Technik oder das Rechte-/Rollenkonzept (in Form der Zugangs- und Zugriffskontrolle) schon in der Anlage zu § 9 Satz 1 des alten Bundesdatenschutzgesetzes (BDSG) zu beachten.

Die Fragen der LfD Niedersachsen zielten hier zum Beispiel auf die Gewährleistung eines angemessenen Schutzniveaus und auf die Anpassung der TOM an den jeweiligen Stand der Technik ab. Die Antworten waren überwiegend nicht zufriedenstellend, weshalb 41 Unternehmen in der ersten Prüfungsrunde mit Rot bewertet wurden.

Die Systematik des Art. 25 DS-GVO wurde häufig nicht umgesetzt, Schutzziele nicht benannt, Schutzbedarfe gar nicht erst erkannt. Einige Unternehmen verwiesen auf verbindliche Vorschriften zur IT-Sicherheit als maßgeblich für den Datenschutz. Die Beachtung der datenschutzrechtlichen Anforderungen und damit der Blick auf die Risiken für Betroffene blieben hingegen weitgehend offen. Zum Stand der Technik wurde teilweise lediglich auf jährliche Audits und regelmäßige Erneuerungen per Hardware- sowie Software-Updates verwiesen. Der Stand der Technik bezieht sich aber auf die bestmöglichen marktfähigen Techniken, die aktuell einen hohen Sicherheitsstandard aufweisen, selbst wenn sich ihr Einsatz in der Praxis (noch) nicht durchgesetzt hat. Was „Stand der Technik" ist, ist dynamisch zu betrachten. Nach unten grenzt er sich von den „anerkannten Regeln der Technik" (z.B. DIN-Normen) ab, nach oben vom „Stand von Wissenschaft und Technik" (neueste technische und wissenschaftliche Erkenntnisse).[1]

Mangelhaft waren auch Rechte- und Rollenkonzepte, die zum Teil lediglich der Informationssicherheit i. S. d. ISO/IEC 27001 dienten. Damit unterblieben an dieser Stelle datenschutzrechtliche Betrachtungen bspw. unter dem Aspekt der Datensparsamkeit.

In Bezug auf Privacy by Design und by Default ließ sich aus den übersandten Leitfäden zwar erkennen, dass diese Prinzipien in den Unternehmen bekannt und bei der Implementierung von Verarbeitungsvorgängen zu beachten sind. Welche konkreten Anforderungen hier zu stellen und wie diese umzusetzen sind, blieb jedoch unklar.

6. Fragenkomplex 6 – Datenschutz-Folgenabschätzung

Auch in diesem Bereich musste die LfD Niedersachsen häufig das Prädikat „rot" vergeben, nämlich 29 Mal im ersten Prüfungsschritt. Da es zur DSFA aber auch einige wenige hervorragende Ergebnisse gab, waren die Erwartungen der Aufsichtsbehörde offenbar nicht überzogen.

Bei vielen Unternehmen war nicht erkennbar, dass sie die Tatbestände prüfen, die sich aus den Normen des Art. 35 DS-GVO ergeben. Schon deren Nennung hätte sich positiv ausgewirkt, da sie gezeigt hätte, dass sich die Verantwortlichen umfassend mit den gesetzlichen Vorgaben auseinandergesetzt hatten.

Die deutschen Aufsichtsbehörden haben gemäß Art. 35 Abs. 4 DS-GVO eine Liste von Verarbeitungstätigkeiten erstellt, für die eine DSFA durchzuführen ist (Muss-Liste). Immer wieder weisen die Behörden ausdrücklich darauf hin, dass diese Liste nicht abschließend ist. Trotzdem antworteten mehrere Unternehmen, sie hätten keine DSFA durchgeführt, weil ihre Verarbeitungsverfahren nicht auf der Muss-Liste gestanden hätten.

Bei zahlreichen der kontrollierten Unternehmen war zudem keine methodische Herangehensweise an die Prüfung von Art. 35 Abs. 1 DS-GVO erkennbar, was nachvollziehbare Ergebnisse quasi unmöglich macht. Die Aufsichtsbehörden machen hier keine explizite Vorgabe, welche Methodik anzuwenden ist. Entscheidend ist letztlich, dass die jeweils zuständige Aufsicht die Prüfung und deren Ergebnisse nachvollziehen kann. Die LfD Niedersachsen hat zur Unterstützung von Verantwortlichen den „Prozess zur Auswahl angemessener Sicherungsmaßnahmen" (ZAWAS) entwickelt. Dieser Prozess ist u.a. dafür geeignet, bei der Durchführung einer DSFA die möglichen Risiken und die für deren Eindämmung notwendigen TOM systematisch herzuleiten.

Schließlich gab es weder in allen Unternehmen klare Zuständigkeiten für die DSFA-Prüfung noch eine umfassende Dokumentation derselben.

1 Der Stand der Technik wird in Art. 25 Abs. 1 DS-GVO erwähnt. Zwar gibt es zu diesem Begriff keine Legaldefinition. Er ist aber – vor allem im datenschutzrechtlichen Kontext – insbesondere unter Heranziehung des Kalkar I-Beschlusses des Bundesverfassungsgerichts (BVerfG, Beschluss vom 8.8.1978 – 2 BvL 8-77, BVerfGE 49, 89 – Kalkar I) sowie der Drei-Stufen-Theorie auszulegen.

7. Fragenkomplex 7 – Auftragsverarbeitung

An dieser Stelle wollte die LfD Niedersachsen zunächst wissen, inwieweit bestehende Auftragsverarbeitungsverträge an die neuen Regelungen nach Art. 28 DS-GVO angepasst worden waren. Bei knapp der Hälfte der Unternehmen war dieser Anpassungsprozess noch nicht vollständig abgeschlossen. Zudem prüfte die LfD die übersandten Muster und Beispielverträge dahingehend, ob sie den rechtlichen Anforderungen entsprechen, was überwiegend der Fall war. Insgesamt musste deshalb nur bei einem Unternehmen ein dringender Handlungsbedarf festgestellt werden.

8. Fragenkomplex 8 – Datenschutzbeauftragte

Die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten ergibt sich aus Art. 37 DS-GVO sowie aus § 38 BDSG. Die Bestellung erfolgt auf Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens im Bereich des Datenschutzrechts und der Datenschutzpraxis sowie auf Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 DS-GVO genannten Aufgaben. Diese Fachkunde ist im Rahmen der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO umfassend nachzuweisen. Auch zu diesem Fragenkomplex waren die Ergebnisse erfreulich. Ein Interessenskonflikt stand nur bei einem Unternehmen im Raum, bzgl. der erforderlichen Fachkunde wurde nach dem zweiten Prüfungsschritt ebenfalls nur noch in einem Fall dringender Handlungsbedarf festgestellt.

9. Fragenkomplex 9 – Meldepflichten

Rechtsgrundlage bilden hier die Art. 33 und 34 DS-GVO. Zur Umsetzung sollten Unternehmen einen Prozess zur Meldung von Datenschutzverstößen implementieren. In einer nachvollziehbaren Darstellung sollten insbesondere die Verantwortlichkeiten und Abläufe klar geregelt sein und allen Beschäftigten bekannt gemacht werden.

Im ersten Prüfungsschritt wurde bei circa einem Drittel der Unternehmen der Meldeprozess nicht oder nur teilweise nachvollziehbar dargestellt. Zudem fehlte es bei einem Drittel der Unternehmen an einer klaren Regelung der Verantwortlichkeit und an einer erkennbaren Berücksichtigung der 72-Stunden-Meldefrist. Nach dem zweiten Prüfungsschritt stellte die LfD nur noch bei drei Unternehmen erheblichen Handlungsbedarf beim Meldeprozess fest.

10. Fragenkomplex 10 – Dokumentation

Jeder Verantwortliche muss nachweisen können, dass er den Pflichten, die ihm die DS-GVO auferlegt, nachkommt. Daher prüfte die LfD Niedersachsen abschließend, inwiefern sich aus der Antwort zu diesem Komplex sowie aus der Summe der übrigen Antworten ergab, dass eine Dokumentation zu jeder der abgefragten Pflichten vorhanden ist. Ganz überwiegend konnte die LfD hier nachvollziehen, dass die Unternehmen eine entsprechende Dokumentation vorhalten. Bei sieben Unternehmen wurde hier nur geringer Anpassungsbedarf festgestellt, erheblicher Bedarf bei keinem.

III. Schlussfolgerungen

Aus der branchenübergreifenden Querschnittsprüfung haben sich für die LfD Niedersachsen Erkenntnisse ergeben, die sowohl ihre Vollzugsaufgaben berühren als auch ihre Pflicht zu Aufklärung und Sensibilisierung der Verantwortlichen. Was den Vollzug betrifft, so war die Prüfung zwar auch für die Unternehmen beendet, die nach der zweiten Stellungnahme immer noch mit Rot bewertet worden waren. Allerdings wurden fünf von Ihnen mit der Mitteilung des Ergebnisses gleichzeitig darüber informiert, dass bei ihnen aufgrund der gravierenden Defizite noch in diesem Jahr weitergehende Kontrollen in separaten Prüfungen folgen werden. Nicht auszuschließen ist, dass es auch zur Verhängung von Bußgeldern kommen kann. Dabei wird die LfD Niedersachsen u.a. berücksichtigen, wie schwerwiegend ein möglicherweise vorliegender Verstoß ist und wie das Unternehmen damit umgegangen ist. Zudem wird die LfD verstärkt weitere themen- und branchenbezogene anlasslose Kontrollen durchführen, um ihrer Aufgabe als Aufsichtsbehörde angemessen nachzukommen.

Zugleich wird die Behörde den eingeschlagenen Weg fortsetzen, das Beratungs- und Informationsangebot auf ihrer Webseite an die identifizierten Bedarfe anzupassen. Die Querschnittsprüfung hat deutlich gezeigt, dass die größten Schwierigkeiten in der Umsetzung der DS-GVO in den Bereichen technisch-organisatorischer Datenschutz und Datenschutz-Folgenabschätzung liegen. Deshalb hat die LfD Niedersachsen beschlossen, Handlungsempfehlungen zu den Themen „Stand der Technik“, „Rollen- und Berechtigungskonzepte“, „Privacy by Design und by Default“ sowie zur Schwellwertprüfung bei der DSFA zu veröffentlichen.

Barbara Thiel
ist seit dem 1. Januar 2015 die Landesbeauftragte für den Datenschutz Niedersachsen. Nach ihrem beruflichen Einstieg bei der Stadt Salzgitter, dem Jurastudium in Göttingen und dem Referendariat war sie unter anderem im Niedersächsischen Innenministerium, beim Niedersächsischen Landesrechnungshof sowie beim Landkreis Wolfenbüttel tätig.

Kurzbeiträge

Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (44): Der ThürLfDI zu Foto- und Filmaufnahmen mit und ohne Einwilligung

Zusammengestellt und erläutert von Prof. Peter Gola*

Der Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit(ThürLfDI) befasst sich in seinem „Tätigkeitsbericht zum Datenschutz nach der DS-GVO 2018“ (Abschnitt 5.21) ausführlich mit der von ihm festgestellten großen Verunsicherung hinsichtlich der rechtlichen Grundlagen für die Erstellung und auch die anschließende Veröffentlichung von Film- und Fotoaufnahmen, wobei er darauf verweist, dass die Aufsichtsbehörden inzwischen die bei der Handhabe privater Fotoalben oder der Veröffentlichung von Foto-und Filmaufnahmen durch Fotografen oder Vereine zu beachtenden Vorgaben praxisnah beschrieben haben. Seine diesbezüglichen Hinweise werden hier zusammengefasst dargestellt.

I. Grundsätzliches

1. Fotos sind regelmäßig personenbezogene Daten

Der LfDI macht zunächst deutlich, dass es sich bei Fotos auch dann um personenbezogene Daten handelt, wenn die fotografierte Person dem Fotografen nicht bekannt ist oder bei Aufnahmen, auf denen viele Personen zu sehen sind, diese nicht identifiziert oder kontaktiert werden können.

„Personenbezogene Daten liegen gemäß Art.4 Ziff.1 DS-GVO vor, wenn sie sich auf „eine identifizierbare natürliche Person beziehen“. Identifizierbar ist eine Person, wenn diese „direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind“. Eine solche Identifizierbarkeit sei hier gegeben. An dieser prinzipiellen Identifizierbarkeit ändere auch der Umstand nichts, dass der einzelne Fotograf in den meisten Fällen keine Zuordnung einzelner Gesichter zu anderen Daten dieser Personen herstellt bzw. herstellen kann. Auf die individuellen Möglichkeiten des einzelnen Fotografen sei bei abstrakter Betrachtung, ob es sich um personenbezogene Daten handelt, nicht abzustellen. Es reiche aus, dass eine Personenbeziehbarkeit der Daten prinzipiell möglich ist, was angesichts der hohen Auflösung von Digitalbildern in Bezug auf Bildaufnahmen und der Verfügbarkeit von Gesichtserkennungssoftware angenommen werden muss. Auch wenn man auf die individuellen Möglichkeiten des einzelnen Fotografen abstellen würde, also einen relativen Begriff der personenbezogenen Daten vertrete, sei es schwierig zu argumentieren, dass körperliche Merkmale einer Person, insbesondere die individuellen Gesichtszüge, wenn sie ausreichend erkennbar sind, nicht geeignet sind, um eine Person eindeutig zu identifizieren. Es handele sich daher bei ausreichend aufgelösten oder auflösbaren Bildaufnahmen, die eine oder mehrere Personen gut erkennbar zeigen, immer um personenbezogene Daten.

Bei der Bewertung der rechtlichen Anforderungen ist dann zunächst zwischen der Erstellung und der Veröffentlichung der Fotoaufnahmen zu unterscheiden.

Sodann wird aufgezeigt, dass trotz der automatisierten Erhebung personenbezogener Daten bei zwei Konstellationen die DS-GVO gleichwohl nicht anwendbar ist und dies wenn die Verarbeitung unter das Haushaltsprivileg oder das Medienprivileg fällt. Dazu führt der ThürLfDI u.a. wie folgt aus:

2. Das Haushaltsprivileg

Der Anwendungsbereich der DS-GVO greift nur dann, wenn die Erstellung und Verarbeitung von Film-und Fotoaufnahmen nicht ausschließlich persönlichen oder familiären Zwecken dient. Das sogenannte „Haushaltsprivileg“ in Art. 2 Abs. 2 lit. c DS-GVO ermöglicht die Erstellung und Verwendung von Fotos für den privaten und familiären Gebrauch. Urlaubsfotos, Fotoalben und Erinnerungsfotos sind daher weiterhin möglich, ohne die Voraussetzungen, die die DS-GVO für die Datenverarbeitung aufstellt, erfüllen zu müssen. Zu beachten ist hierbei nur, dass diese Ausnahme einen sehr beschränkten Anwendungsbereich hat. Die Verarbeitung darf keinen Zusammenhang oder Bezug zu einer beruf-

* Der Autor ist Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn.

lichen oder wirtschaftlichen Tätigkeit haben. Auch bei der Veröffentlichung solcher Aufnahmen ist Vorsicht geboten. Sollen die Fotos in einem sozialen Netzwerk eingestellt werden, ist bei einer durch Nutzernamen und Passwort geschützten Gruppe oder Forum auf einer Webseite davon auszugehen, dass es gerade noch unter das Haushaltsprivileg fällt, da dieses restriktiv, also sehr eng ausgelegt wird. Wenn die Aufnahmen jedoch einem unbeschränkten Personenkreis zugänglich gemacht werden, beispielsweise durch die Bereitstellung der Aufnahmen auf einer frei zugänglichen Webseite, fällt dies nicht mehr unter das Haushaltsprivileg, da es sich dann nicht mehr um eine rein familiäre oder persönliche Tätigkeit handelt. Hier findet die DS-GVO mit allen Voraussetzungen Anwendung.

3. Das Medienprivileg

Erfolgt die Erstellung und Veröffentlichung zu journalistisch-redaktionellen Zwecken, steht dem Verantwortlichen das sogenannte „Medienprivileg" zur Seite. Für diesen Fall ist in Art. 85 Abs. 1 der DS-GVO den Mitgliedsstaaten die Möglichkeit eingeräumt worden, nationale Regelungen zu treffen, um den Datenschutz und das Recht auf freie Meinungsäußerung und Informationsfreiheit sowie der Verarbeitung von Daten für journalistische Zwecke in Einklang zu bringen. Eine derartige Regelung findet sich für öffentliche und nicht-öffentliche Stellen in Thüringen in § 25 Thüringer Datenschutzgesetz (ThürDSG). Danach sind Unternehmen sowie Hilfsunternehmen der Presse weitgehend frei von datenschutzrechtlichen Vorgaben für die Zulässigkeit der Erhebung und Verarbeitung der Daten. In diesem Fall werden nur die Art. 5 Abs. 1 lit. f, sowie die Art. 24, 32 und 33 DS-GVO für anwendbar erklärt. Damit wird dem Recht auf freie Meinungsäußerung und Informationszugang Genüge getan. Zu beachten bleiben allerdings weiterhin das Thüringer Pressegesetz, das allgemeine Persönlichkeitsrecht des Einzelnen und das Urheberrecht. Eine Entbindung von den Vorgaben der DS-GVO, geeignete technische und organisatorische Maßnahmen zur Datensicherheit zu treffen, gibt es aber auch für die journalistische Tätigkeit nicht.

II. Das Herstellen und Verwenden von Fotoaufnahmen

Sodann greift der ThürLfDI die Anwendung der DS-GVO bei der Herstellung und Verwendung von Fotos auf, wobei er folgende Fallkonstellationen unterscheidet:

1. Konkrete Personen oder überschaubare Gruppen als Betroffene

Die Herstellung des Bildes

Die Erstellung von Fotos, auf denen die abgebildete Person im Vordergrund steht, ist ausschließlich nach Art. 6 Abs.1 DS-GVO zu bewerten. Für die Erstellung der Fotos kann auch nicht das Kunsturhebergesetz (KUG) herangezogen werden, da sich dessen Anwendungsbereich allein auf die Veröffentlichung, also die Verbreitung und öffentliche Zurschaustellung von Fotos bezieht. Die Erstellung von Fotoaufnahmen dieser Art ist daher zulässig, wenn sie zur Erfüllung eines Vertrages notwendig ist. Das ist beispielsweise bei einem beauftragten Fotografen für eine Hochzeit der Fall, wenn er das Brautpaar ablichtet, von dem er beauftragt wurde. Die Fotos des Vertragspartners, hier des Brautpaares, sind aufgrund des bestehenden Werkvertrages mit dem Fotografen gemäß Art. 6 Abs. 1 S. 1 lit. b DS-GVO zulässig erstellt.

Wenn der Fotograf während der Feier auch Gäste ablichtet oder Gäste zusammen mit dem Brautpaar fotografiert, kann er sich nicht mehr allein auf seine Vertragserfüllung berufen. Als rechtliche Grundlagen kommen hier aber die Einwilligung oder ein berechtigtes Interesse des Verantwortlichen oder eines Dritten gemäß Art. 6 Abs. 1 S. 1 lit. f DS-GVO in Frage. Hier haben das Brautpaar (Dokumentation der Veranstaltung) und auch der Fotograf (Berufs-und Kunstfreiheit) ein berechtigtes Interesse an der Erstellung der Fotos, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten Betroffener überwiegen. Bei der Prüfung der Interessenlage sind auch die vernünftigen Erwartungen der betroffenen Personen zu berücksichtigen, die im Falle einer Einladung zu einer Hochzeitsfeier davon ausgehen können, dass zu diesem Anlass auch Fotos erstellt werden. Dies ist ein gebräuchlicher und allseits akzeptierter Umstand. Auch bei Teilnahme an einer anderen Veranstaltung auf Einladung eines Veranstalters geht die Erwartungshaltung der Gäste und auch des Veranstalters zumeist dahin, dass eine Dokumentation der Veranstaltung auch anhand von Fotografien stattfindet. Anders wäre die Interessenlage zu bewerten, wenn die Aufnahmen verdeckt oder heimlich erstellt werden würden, die Fotos die Intimsphäre des Abgebildeten erfasst oder die Aufnahmen diskreditierend sind oder die Gefahr einer Diskriminierung bergen.

Von einer überwiegenden Schutzbedürftigkeit der Betroffenen ist auch bei Aufnahmen von Kindern auszugehen, weshalb hier ein Rückgriff auf ein berechtigtes Interesse wohl sehr genau zu prüfen ist und in solchen Fällen grundsätzlich eine Einwilligung für die Erstellung von Bildern bei den Sorgeberechtigten einzuholen ist. Die Interessenabwägung wird auch im Fall von Fotos, die Rückschlüsse auf besondere Kategorien personenbezogener Daten zulassen, also u.a. Religion, Gesundheit, Sexualleben und sexuelle Orientierung, immer zu Gunsten der betroffenen Person ausgehen. Für diese Fälle ist dann auch eine Einwilligung in die Erstellung der Aufnahme gemäß Art. 7 DS-GVO notwendig.

Die Verwendung des Bildes

Das größte Interesse der Verantwortlichen liegt jedoch nicht in der Erstellung der Fotos, sondern in der anschließenden Verarbeitung oder Veröffentlichung der Bilder. Dies findet zumeist auf Webseiten statt oder in Informationsmaterialien wie Vereinszeitschriften. Für die Verbreitung und öffentliche Zurschaustellung von Fotos war bisher auf §§ 22f. des Kunsturhebergesetzes (KUG) abzustellen. Ob das

Kunsturhebergesetz neben der Datenschutz-Grundverordnung anwendbar ist oder bleibt, ist derzeit noch mangels entsprechender Öffnungsklausel in der DS-GVO umstritten (vgl. aber Urteil LG Frankfurt, 13. 09. 2018, 2-030283/18 u.a.). Eine Anwendung kann sich nur aus Art. 85 Abs. 1 DS-GVO im Hinblick auf die Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken ergeben.

Ungeachtet dieser Diskussion ist das Ergebnis in der praktischen Auswirkung mit und ohne direkte Anwendung des KUG aber ähnlich, da die Wertungen des KUG im Rahmen der Interessensabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO einfließen. Das KUG regelt insbesondere drei Fälle, bei denen es keiner Einwilligung der abgebildeten Person für die Verbreitung der Aufnahmen bedarf. Dies gilt für Bildnisse der Zeitgeschichte, Bilder bei denen Personen nur als Beiwerk neben einer Landschaft oder einer Örtlichkeit erscheinen und für Bilder von Versammlungen, Aufzügen u.Ä., an denen die abgebildete Person teilgenommen hat. Wenn das KUG nicht unmittelbar anwendbar wäre, würde die Verbreitung derartiger Aufnahmen nach Art. 6 Abs. 1 S. 1 lit. f zu prüfen sein, denn auch hinsichtlich der Veröffentlichung von Fotos ist die weitere Verwendung an eine Rechtsgrundlage gebunden. Hier stehen sowohl die Einwilligung sowie Art. 6 Abs. 1 S. 1 lit. f DS-GVO, also berechtigte Interessen, zur Verfügung. Während aus Sicht des Verantwortlichen eine Einwilligung immer die „schlechtere" Verarbeitungsgrundlage ist, weil sie jederzeit widerrufen werden kann, ist im Rahmen von Veröffentlichungen oftmals zwingend auf diese zurückzugreifen. Hinsichtlich ihrer Voraussetzungen wird auf das WP259 (Guidelines on Consent) der Art. 29 Gruppe verwiesen (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051), das nun auch in deutscher Sprache vorliegt (https://www.tlfdi.de/tlfdi/europa/artikel29gruppe/).

Erforderlichkeit einer Einwilligung

Sofern eine Einwilligung einzuholen ist, muss dies vor der Fotoaufnahme geschehen. Dies kann auch mündlich erfolgen, allerdings muss der Verantwortliche gemäß Art. 7 Abs. 1 DS-GVO im Zweifel das Vorliegen einer Einwilligung nachweisen können. Es wird daher empfohlen, die Einwilligungen wenigstens in Textform einzuholen. Es muss vor der Einwilligung immer über wesentliche Umstände informiert werden, auf die sich die Einwilligung bezieht, vor allem:

- die Identität des für die Verarbeitung Verantwortlichen,
- für welchen Zweck die Fotos angefertigt werden,
- ob und, wenn ja, wo eine Veröffentlichung geplant ist
- an wen sich der Betroffene bei Datenschutzfragen (z.B. Widerspruch, Löschung) wenden kann,
- dass die betroffene Person das Recht hat, ihre Einwilligung jederzeit zu widerrufen und dass durch den Widerruf der Einwilligung die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt wird (Art. 7 Abs. 3 DS-GVO).

Der Grund für den Rückgriff auf die Einwilligung im Rahmen von Veröffentlichungen liegt in der oftmals zu Lasten der Verantwortlichen ausgehenden Interessensabwägung im Rahmen des Art. 6 Abs. 1 S. 1 lit. f. DS-GVO. Es stehen sich hier die Interessen des Verantwortlichen z.B. an der Information und Werbung für Vereinsaktivitäten und die der betroffenen Personen gegenüber. Die Veröffentlichung hat grundsätzlich das Potential, einen schweren Eingriff in die Rechte des Betroffenen darzustellen, weil die Bilder des Betroffenen einer unüberschaubaren Anzahl an Personen zum Zugriff bereitstehen und einer relativ schwer bis nicht kontrollierbaren Vervielfältigung ausgesetzt werden.

2. Aufnahmen von unüberschaubarer Menge an Personen

Anders beurteilt der ThürLfDI ist die Verwertung von Aufnahmen, auf denen sich eine Vielzahl von Personen häufig als sogenanntes Beiwerk oder im Rahmen von Übersichtsaufnahmen befinden, z.B. Zuschauerränge bei Sportveranstaltungen, Publikumsaufnahmen im Hintergrund künstlerischer Darbietungen, da auf der einen Seite auch bei übersichtsartigen Bildaufnahmen nahezu immer personenbeziehbare Daten vorlägen; es auf der anderen Seite aber regelmäßig nicht möglich sei, jede einzelne Person zu identifizieren oder zu kontaktieren. Da somit die Einholung einer Einwilligung oder die Information der Abgelichteten über Ihre Rechte nahezu unmöglich sei, könne die Rechtmäßigkeit der Verarbeitung in Form der Erhebung nur nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO zur Wahrnehmung berechtigter Interessen erfolgen, sofern die dort genannten Voraussetzungen vorliegen.

Auszugehen sei dabei davon, dass regelmäßig keine schutzwürdigen Interessen der Bildherstellung und Nutzung entgegenstehen, wenn eine Ansammlung von Personen dargestellt wird, ohne dass eine Person oder wenige Personen im Fokus des Motivs stehen, weil dann nur ihre Sozialsphäre, nicht aber ihre Persönlichkeitssphäre betroffen sei.

Bei Kindern und Jugendlichen müsse diese Abwägung jedoch zu Gunsten der Kinder ausfallen, so dass schon die Erstellung solcher Fotografien nur auf eine Einwilligung der sorgeberechtigten Person/en gestützt werden könne.

III. Informationspflichten

Der ThürLfDI zeigt sodann auf, dass auch bzw. insbesondere wenn die Verarbeitung der Fotos ohne Einwilligung erfolgt, grundsätzlich die vorherige Information des Abgebildeten erforderlich ist.

Die Informationspflichten nach der DS-GVO (Art. 12 ff) seien umfassend und grundsätzlich gegenüber jedem Abgebildeten zu erfüllen. Hierzu sind u.a. Angaben hinsichtlich des Zweckes, für den die Fotos erstellt werden, notwendig und die Angabe zu dem hierzu berechtigten Interesses. Der zur Abbildung Vorgesehene muss Angaben dazu erhalten, ob und wo eine Veröffentlichung der Fotos geplant ist und an wen er sich hinsichtlich datenschutz-rechtlicher Fragestellungen wenden kann.

Hierbei gilt jedoch eine Ausnahme (Art. 11 Abs. 1 DS-GVO), wenn eine größere Menschenmenge ohne erkennbaren Fokus abgebildet ist.

Ein Verantwortlicher ist nämlich nicht verpflichtet, zur bloßen Einhaltung der DS-GVO, zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren, falls für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich ist. Keine Anwendung soll Art. 11 Abs. 1 DS-GVO allerdings bei kleineren, überschaubaren Personengruppen oder gar einzelnen Personen finden. Hier sei eine Information nach Art. 13 Abs. 1 DS-GVO notwendig, die beispielsweise durch gut sichtbare Aushänge am jeweiligen Veranstaltungsort und/oder beim Karten(ver)kauf erfolgen könne. Auf Nachfrage müsse der Fotograf auch in der Lage sein, die vollständige Information nach Art.13 DS-GVO bereitzustellen.

IV. Besondere Verarbeitungssituationen

Um der Vielfalt der Nutzungsmöglichkeiten von Fotoaufnahmen gerecht zu werden, geht der ThürLfDI sodann auf eine Reihe von besonderen Verarbeitungssituationen ein.

Das Beschäftigungsverhältnis

„Die Datenverarbeitung innerhalb des Beschäftigungsverhältnisses ist an strengen Maßstäben orientiert. Personenbezogene Daten von Beschäftigten durften und dürfen im Beschäftigungskontext nur dann verarbeitet werden, wenn dies zur Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses erforderlich ist (§ 26 Abs. 1 BDSG, § 27 Abs. 1 ThürDSG in Verbindung mit den §§ 79 bis 87 des Thüringer Beamtengesetzes, soweit der öffentliche Dienst betroffen ist. Die Veröffentlichung von Fotos von Mitarbeitern hält der LfDI jedoch nach diesen Vorschriften regelmäßig nicht für erforderlich, da die Interessenabwägung im Beschäftigtenverhältnis nicht in gleicher Weise greife. Eine Einwilligung für die Nutzung von Mitarbeiterfotos ist daher schriftlich einzuholen und insbesondere im Hinblick auf ihre Freiwilligkeit zu prüfen."

Bilder im Rahmen der Öffentlichkeitsarbeit

Bei der Verarbeitung von Fotos im Rahmen der Öffentlichkeitsarbeit von verantwortlichen Stellen sei zunächst die Anwendung des Medienprivilegs (Art. 85 DS-GVO) zu prüfen. Die Nutzung für journalistische Zwecke könne danach für Pressemappen oder für die Erstellung eigener Zeitschriften oder Zeitungen zulässig sein. Wenn die Verarbeitung allerdings der reinen Werbung und Darstellung für die Stelle diene, seien bei nicht-öffentlichen Stellen die oben dargestellten Ausführungen zu beachten. Möglicherweise könne sich die Stelle auch auf das berechtigte Interesse hinsichtlich der Öffentlichkeitsarbeit und einer damit einhergehenden Veröffentlichung von Bildmaterial stützen. Bezüglich der öffentlichen Stellen, stehe dem allerdings der Art. 6 Abs. 1 S. 2 DS-GVO entgegen, wonach der Rückgriff auf Art. 6 Abs. 1 S. 1 lit. f DS-GVO für Behörden in Erfüllung ihrer Aufgaben nicht gilt. Hier muss als Rechtsgrundlage der Art. 6 Abs. 1 S. 1 lit. e DS-GVO in Verbindung mit den Landes- und Spezialgesetzen herangezogen werden. Hierbei ist ausschlaggebend, was für die Organisationskommunikation jeweils erforderlich ist.

Sowohl für öffentliche als auch für nicht-öffentliche Stellen bleibe aber festzuhalten, dass kein relevanter Unterschied zur früheren Rechtslage zu erkennen sei, da auch hier nur selten die Ausnahmen des § 23 KUG einschlägig gewesen seien. „Denn nicht jede Veranstaltung ist ein Ereignis der Zeitgeschichte und auch nicht jedes Fest eine Versammlung!"

Vereine

Zu Bildherstellungen in Vereinen wird dann wie folgt ausgeführt: „Besonders die Arbeit der Vereine lebt oftmals von der Veröffentlichung von Fotoaufnahmen. Hier sind insbesondere Wettkämpfe, Mannschaftsfotos, Jubiläen, Jahrestage oder andere Vereinsfeierlichkeiten eingeschlossen. Doch auch diese Dokumentationen unterliegen der DS-GVO und bedürfen zu ihrer Verarbeitung einer rechtlichen Grundlage. Zwar kann sich diese zunächst aus dem Vereinszweck ergeben, also auf vertraglicher Grundlage im Rahmen einer Satzung beruhen, jedoch ist zur Durchführung der Mitgliedschaft, eine Verarbeitung von Fotos wohl regelmäßig nicht erforderlich. Die Veröffentlichung kann aber auf Art. 6 Abs. 1 S. 1 lit. f DS-GVO gestützt werden, da der Verein ein berechtigtes Interesse daran hat, über das Vereinsgeschehen zu informieren. Hierfür können beispielsweise Mannschaftsfotos zur Dokumentation der Mannschaftsaufstellung eines Sportvereins auf der vereinseigenen Webseite eingestellt werden. Die gleichzeitige Veröffentlichung bei sozialen Netzwerken schließt dieses berechtigte Interesse jedoch nicht zwangsläufig mit ein. Weiterhin ist es über die Anwendung des Art. 6 Abs. 1 S. 1 lit. f DS-GVO auch möglich, Fotos von offiziellen Vereinsveranstaltungen, Sportveranstaltungen oder Wettkämpfen zu veröffentlichen, da auch hier ein berechtigtes Interesse der Vereine daran besteht, über das Vereinsgeschehen zu berichten. Es muss sich allerdings um Fotos handeln, auf denen das Spielgeschehen als solches oder die Veranstaltung als solche erkennbar ist und nicht einzelne im Vordergrund stehende Personen. Sobald eine Person im Fokus steht, gelten die Vorschriften zu Einzelaufnahmen und deren Veröffentlichung.

Bezüglich der vereinsinternen Aktivitäten, wie interne Vereinsfeiern, Ausflüge, Geburtstage von Mitgliedern u.Ä.ist eine Veröffentlichung von Fotos nicht mehr von einem berechtigten Interesse des Vereins gedeckt. Hier gehen die Erwartungen der Mitglieder keinesfalls dahin, dass mit einer Veröffentlichung auf der Vereinsseite zu rechnen ist. Da die Veröffentlichung eine fortwährende Form der Verarbeitung darstellt, ist eine Interessensabwägung über die Fortführung der Veröffentlichung erneut durchzuführen, wenn für widerstreitende Interessen Anhaltspunkte vorliegen. Dies

kann beispielsweise dann der Fall sein, wenn eine Person sich mit der Bitte meldet, das veröffentlichte Foto zu entfernen, auch wenn er hierfür keine Gründe aufführt. Gerade bei älteren Bildern wird sich ein solcher Anspruch unmittelbar aus Art. 17 Abs.1 DS-GVO ableiten lassen. Bei Bildern jüngeren Datums ist vom Verantwortlichen zu prüfen, inwieweit die Veröffentlichung auch ohne Einwilligung zulässig wäre. Das kann nur dann der Fall sein, wenn ein berechtigtes Interesse des Vereins nach dem o.a. Grundsätzen besteht und die Interessenabwägung nicht aufgrund besonderer Umstände zugunsten des Abgebildeten zu treffen ist. Wenn das Interesse der betroffenen Person überwiegt, ist eine weitere Veröffentlichung nicht zulässig und das Foto muss entfernt oder die Person unkenntlich gemacht werden".

Kinder insbesondere in Kitas / Schulen

Dass Abbildungen von Kindern besonders restriktiv zu handhaben sind, wurde vorstehend schon angesprochen. Zur Situation in Kitas und Schulen stellt der ThürLfDI u.a. wie folgt fest:

„Die DS-GVO stellt den Schutz von Kindern bei der Verarbeitung ihrer Daten unter einen besonderen Vorbehalt. Dieser wird in Art. 6 Abs. 1 S. 1 lt. f der DS-GVO formuliert. Danach überwiegt stets das schutzwürdige Interesse der Kinder. Aus diesem Grund ist die Verarbeitung von Daten, wenn Kinder betroffen sind, nur aufgrund einer Einwilligung möglich, aufgrund einer vertraglichen Grundlage oder aufgrund gesetzlicher Regelungen. Für das Mannschaftsfoto im Verein, Aushänge in der Schule oder Kita gilt daher: Wenn Minderjährige erkennbar abgebildet werden, ist das Erstellen und auch das Veröffentlichen nur mit der Einwilligung der Sorgeberechtigten möglich. Dies ist jedoch für Bildnisse eines Spielablaufs/Veranstaltungsablaufs dann nicht der Fall, wenn nur das Spielgeschehen oder der Veranstaltungsablauf dargestellt werden sollen, ohne dass erkennbar Kinder im Vordergrund abgebildet sind oder diese nur als sogenanntes „Beiwerk" zu einer Übersichtsaufnahme erscheinen. Solche Aufnahmen werden zumeist zur Dokumentation von schulischen Veranstaltungen im Rahmen der Öffentlichkeitsarbeit erstellt. Sobald die Kinder jedoch erkennbar, einzeln oder in kleiner Gruppe und im Vordergrund abgebildet sind, das Bild also prägen, kann nicht mehr von Beiwerk ausgegangen werden, und eine Einwilligung ist notwendig.

Praxisfälle zum Datenschutz II:[1] Musterfalllösung zur Kundendatenverwaltung im Konzern

Miriam Claus, LL.B./RAin Yvette Reif, LL.M.*

I. Sachverhalt

In einem Konzern soll eine zentrale Kreditoren-/Debitoren-Stammdatenverwaltung eingeführt werden. Bei den Kreditoren/Debitoren handelt es sich um Unternehmen. In der Datenbank sollen aber auch Kontaktinformationen zu den jeweiligen natürlichen Ansprechpartnern bei den Unternehmen gespeichert werden.

Sind die mit der zentralen Kreditoren-/Debitoren-Stammdatenverwaltung verbundenen Datenverarbeitungen zulässig?

Wer trägt die datenschutzrechtliche Verantwortung für die Datenbank?

II. Lösung

1. Rechtsgrundlage für die Datenübermittlung im Konzern

Für die Verarbeitung personenbezogener Daten besteht ein Verbot mit Erlaubnisvorbehalt (vgl. Erwägungsgrund 40 DS-GVO). Demnach ist die Verarbeitung personenbezogener Daten verboten, es sei denn, diese ist über die Einwilligung der betroffenen Person, einen Erlaubnistatbestand in der DS-GVO oder eine sonstige zulässige unions- oder mitgliedstaats-rechtliche Rechtsgrundlage gestattet.

Bei den Ansprechpartnerdaten handelt es sich um personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO. Eine zentrale Kreditoren-/Debitoren-Stammdatenverwaltung innerhalb eines Konzerns, inklusive entsprechender Ansprechpartnerdaten im B2B Umfeld, hätte eine Übermittlung personenbezogener Daten zur Folge, die der Legitimation bedarf. Insbesondere existiert kein Konzernprivileg, und jede juristische Einheit eines Konzernverbunds ist als eigener datenschutzrechtlich Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-

* Miriam Claus, LL.B. ist Referentin bei der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. und schließt gerade ihr Masterstudium (LL.M.) an der TH Köln ab. RAin Yvette Reif, LL.M. ist stellvertretende Geschäftsführerin der GDD und Mitautorin des Werks Gola/Reif, Praxisfälle Datenschutzrecht, 2. Aufl. 2016.

1 Praxisfälle zum Datenschutz I (Einführung in die juristische Prüftechnik sowie Musterfalllösung zum Auskunftsbegehren von aktiven und ausgeschiedenen Mitarbeitern) finden Sie in der RDV 5/2019, S. 238 ff.

GVO anzusehen. Eine ggf. bestehende gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO (vgl. dazu nachstehend 2.) ließe das Erfordernis einer Rechtsgrundlage für die geplanten Datenweitergaben ebenso wenig entfallen. Denn auch die Übermittlung personenbezogener Daten unter gemeinsam Verantwortlichen ist ein eigener Verarbeitungsvorgang i.S.v. Art. 4 Nr. 2 DS-GVO und bedarf daher einer Rechtsgrundlage.[2]

Als Rechtsgrundlage für die Datenübermittlung kommt vorliegend Art. 6 Abs. 1 lit. f DS-GVO in Betracht (sog. Interessenabwägung). Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und gleichzeitig nicht die Interessen oder Grundrechte/Grundfreiheiten der betroffenen Person, die den Schutz seiner personenbezogenen Daten erfordern, überwiegen. Ein berechtigtes Interesse an der wechselseitigen Übermittlung personenbezogener Daten lässt sich insbesondere auf Erwägungsgrund (ErwG) 48 der DS-GVO stützen. Darin heißt es: „Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln." Auch wenn die DS-GVO also, wie gesagt, kein (umfassendes) Konzernprivileg enthält, so erkennt sie in ErwG 48 zumindest ein berechtigtes Interesse daran grundsätzlich an, dass innerhalb eines Konzerns personenbezogene Daten zu administrativen Zwecken übermittelt werden („kleines Konzernprivileg"). Mit der zentralen Kreditoren-/Debitoren-Stammdatenverwaltung wird hier ein solcher interner Verwaltungszweck i.S.v. ErwG 48 DS-GVO verfolgt. Ein Überwiegen schutzwürdiger Interessen der betroffenen Personen ist nicht ersichtlich. Insbesondere sind die personenbezogenen Daten, die sich aus der zentralen Datenbank ergeben werden, wenig sensibel, nämlich, dass die betroffenen Personen Ansprechpartner für ein bestimmtes Unternehmen sind und welche Kontaktdaten sie in diesem Zusammenhang haben. Die betroffenen Personen sind auch nur in der beruflichen und nicht in ihrer privaten Sphäre betroffen.

Folglich können die mit der zentralen Kreditoren-/Debitoren-Stammdatenverwaltung verbundenen Datenübermittlungen über Art. 6 Abs. 1 lit. f DS-GVO legitimiert werden.

Sollten die Datenübermittlung an ein Konzernunternehmen außerhalb der EU / des EWR stattfinden, so sind zusätzlich die Bestimmungen der Art. 44 ff. DS-GVO zu beachten. Innerhalb der EU / des EWR wird die Datenübermittlung wie eine Übermittlung im Inland behandelt.

2. Datenschutzrechtliche Verantwortung für die Datenbank

a) Allgemeines

Sind mehrere Stellen an einer Datenverarbeitung beteiligt, ist zunächst zu prüfen, ob alle Stellen datenschutzrechtlich Verantwortliche i.S.v. Art. 4 Nr. 7 DS-GVO sind oder ob Stellen ggf. nur als Auftragsverarbeiter i.S.v. Art. 28 DS-GVO fungieren. Gibt es mehrere datenschutzrechtlich Verantwortliche, ist sodann zu prüfen, ob es sich um eine alleinige oder gemeinsame Verantwortlichkeit i.S.v. Art. 26 DS-GVO handelt.

b) Abgrenzung zur Auftragsverarbeitung

Entscheidendes Kriterium für den Status als sog. Auftragsverarbeiter (Art. 28 DS-GVO) ist die Weisungsgebundenheit der datenverarbeitenden Stelle im Verhältnis zum Auftraggeber. Während datenschutzrechtliche Verantwortlichkeit voraussetzt, dass die betreffende Stelle einen steuernden und kontrollierenden Einfluss auf die Zwecke oder wesentlichen Mittel der Verarbeitung nimmt, unterwirft sich ein Auftragsverarbeiter im Hinblick auf die Datenverarbeitung den Weisungen des Verantwortlichen und wird lediglich als dessen „verlängerter Arm" tätig. Der Auftragsverarbeiter muss zur Legitimation der Verarbeitung lediglich einen Vertrag über die Auftragsverarbeitung (Art. 28 Abs. 3 DS-GVO) mit dem Verantwortlichen schließen. Der Verantwortliche ist verpflichtet, den Auftragsverarbeiter unter Berücksichtigung der von diesem gewährleisteten technischen und organisatorischen Maßnahmen sorgfältig auszuwählen und diesen während des laufenden Auftragsverarbeitungsverhältnisses angemessen zu kontrollieren.

Klassische Anwendungsbereiche für die Auftragsverarbeitung sind etwa die Auslagerung der Lohn- und Gehaltsabrechnung, Archivierungsvorgänge und Konvertierungen von Dokumenten, Verarbeitung von Kundendaten durch Call-Center ohne wesentliche eigene Entscheidungsspielräume oder die Datenträgerentsorgung.

Eine Auftragsverarbeitung i.S.v. Art. 28 DS-GVO scheidet vorliegend aus, da keines der beteiligten Konzernunternehmen Daten nur nach Weisung der jeweils anderen verarbeiten soll. Ein Auftragsverarbeiter darf außer dem finanziellen Interesse, für diese bezahlt zu werden, kein Eigeninteresse an der Datenverarbeitung haben und die verarbeiteten Daten nicht für eigene Zwecke verwenden. Die Informationen aus der gemeinsamen Kreditoren-/Debitoren-Stammdatenverwaltung sollen von den angeschlossenen Konzernunternehmen hier aber für deren eigene Zwecke, nämlich die Finanzbuchhaltung verwendet werden.

Anders wäre der Sachverhalt zu bewerten, wenn ein (Konzern-)Unternehmen die Kreditoren-/Debitoren-Stammdatenverwaltung als Dienstleister für die angeschlossenen Unternehmen betreibt, selber aber keinerlei Entscheidungsgewalt über Zwecke und Mittel der Verarbeitung innehat. Die an die zentrale Kreditoren-/Debitoren-Stammdatenverwaltung angeschlossenen Unternehmen müssten dann mit dem Dienstleister einen Vertrag zur Auftragsverarbeitung gemäß den Anforderungen des Art. 28 Abs. 3 S. 2 DS-GVO schließen.

2 Datenschutzkonferenz, Kurzpapier Nr. 16: Gemeinsam für die Verarbeitung Verantwortliche, Stand: 19.03.2018, S. 1.

c) Gemeinsame Verantwortlichkeit, Art. 26 DS-GVO

Zwei oder mehr Verantwortliche, die gemeinsam über die Zwecke und Mittel der Verarbeitung entscheiden, sind gemeinsam Verantwortliche (Art. 26 DS-GVO). Eine gemeinsame Entscheidung im vorgenannten Sinne setzt voraus, dass jeder der Beteiligten einen bestimmenden tatsächlichen Einfluss auf die Datenverarbeitung nimmt. Entscheidend ist die pluralistisch ausgeübte Kontrolle über die Datenverarbeitung.

Datenverarbeitungen durch gemeinsam Verantwortliche kommt keine „Privilegierungswirkung" zu.[3] Art. 26 stellt weder eine Rechtsgrundlage für eine Verarbeitung durch mehrere Verantwortliche dar, noch braucht es eine Rechtsgrundlage dafür, dass sich mehrere Verantwortliche zusammenschließen.[4] Der Zweck von Art. 26 DS-GVO ergibt sich insbesondere aus ErwG 79 DS-GVO, wonach es zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen – auch mit Blick auf die Überwachung und sonstigen Maßnahmen von Aufsichtsbehörden – einer klaren Zuteilung der Verantwortlichkeiten bedarf. Die betroffene Person soll nicht schlechter gestellt werden, weil mehrere Verantwortliche zusammenarbeiten,[5] und auch die Aufsichtsbehörde soll wissen, wer für welche (Phase einer) Verarbeitung verantwortlich ist.[6]

Praktische Konsequenz der gemeinsamen Verantwortlichkeit ist, dass eine Vereinbarung nach Art. 26 DS-GVO zu schließen ist. In dieser ist in transparenter Form festzulegen, wer von den gemeinsam Verantwortlichen welche in der DS-GVO geregelten Verpflichtungen erfüllt, insbesondere die Betroffenenrechte und die Informationspflichten nach Art. 13 und 14. Die Vereinbarung muss die tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen „gebührend widerspiegeln", und das „Wesentliche" der Vereinbarung muss betroffenen Personen zur Verfügung gestellt werden (Art. 26 Abs. 2 DS-GVO). „Wesentlich" sind nach Auffassung der nationalen Aufsichtsbehörden zumindest eine nachvollziehbare Beschreibung des Zusammenwirkens und der Rollen der Beteiligten und ihrer jeweiligen Beziehung zur betroffenen Person sowie die Angabe, welcher der gemeinsam Verantwortlichen welche Betroffenenrechte und Informationspflichten erfüllen soll.[7]

Von der gemeinsamen Verantwortlichkeit abzugrenzen sind Konstellationen, in denen Unternehmen mit Bezug auf die personenbezogene Datenverarbeitung kooperieren und ggf. auch personenbezogene Daten austauschen, ohne dass jedoch eine gemeinsame Festlegung der Zwecke und Mittel der Datenverarbeitung erfolgt. Insoweit bleibt es bei der alleinigen bzw. unverbundenen datenschutzrechtlichen Verantwortlichkeit. Dies gilt etwa, wenn Unternehmen personenbezogene Datensätze von anderen Stellen für eigene Werbezwecke erhalten. In diesem Fall trägt die Stelle, welche die Daten bereitstellt, die alleinige Verantwortung für die Datenübermittlung, die werbende Stelle die alleinige Verantwortung für die mit der Werbeaktion verbundene personenbezogene Datenverarbeitung.

Die beteiligten Konzernunternehmen verfolgen vorliegend mit der Gewährleistung der Richtigkeit und Aktualität ihrer Kreditoren- bzw. Debitorendaten einen gemeinsamen Zweck. Zur Erreichung dieses Zwecks wollen die Unternehmen über die geplante gemeinsame Datenbank auch die gleichen personenbezogenen Daten verwenden. Das Konzept für die Stammdatenverwaltung wurde gemeinsam von den beteiligten Unternehmen entwickelt, die auch gemeinsam über die wesentlichen Elemente der Datenverarbeitung entscheiden, wie z.B. „Welche Daten werden verarbeitet?" oder „Wer hat Zugang zu den Daten?".

Im Ergebnis ist damit eine gemeinsame Verantwortlichkeit i.S.v. Art. 26 DS-GVO für die geplante zentrale Kreditoren-/Debitoren-Stammdatenverwaltung anzunehmen.

3 Datenschutzkonferenz, Kurzpapier Nr. 16: Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO, Stand: 19.03.2018, S. 1.

4 Datenschutzkonferenz, ebenda.

5 Dovas ZD 2016, 512 (514).

6 Piltz in: Gola, DS-GVO, 2. Aufl., Art. 26 Rn. 2.

7 Datenschutzkonferenz, a.a.O., S. 4.

E-LEARNING
IT-SICHERHEIT

DATENSICHERHEIT

Geschulte Mitarbeiter machen den Unterschied!

Schulen Sie alle Mitarbeiter via E-Learning in den Grundlagen der IT-Sicherheit und erhöhen Sie so den Schutz für Ihre Daten.

- ✓ Moderation in TV-Studioqualität
- ✓ moderne Didaktik
- ✓ Dauer: 45 Minuten
- ✓ praxisnah und interaktiv
- ✓ auch in englischer Sprache verfügbar

Jetzt informieren: datakontext.com/eLearning

UNIVADO

DATAKONTEXT

Rechtsprechung

Zulässigkeit offener Videoüberwachung und Beweisverwertungsverbot

(**Bundesarbeitsgericht**, Urteil vom 28. März 2019 – 8 AZR 421/17 –)

Zu den Kriterien, unter denen eine offene Videoüberwachung unverhältnismäßig ist.

(nicht amtlicher Leitsatz)

Sachverhalt:

Die Parteien streiten im Revisionsverfahren noch darüber, ob die Klägerin dem Beklagten Schadensersatz iHv. insgesamt 9.840,27 € schuldet.

Die Klägerin war seit dem 1. September 2014 bei dem Beklagten als Verkäuferin in einer Lottoannahmestelle zu einem Stundenlohn von 9,00 € brutto beschäftigt. Ihre monatliche Arbeitszeit betrug 120 Stunden. In der Lottoannahmestelle, die sich im Gebäude eines Markts in S befindet, werden neben den Artikeln des Lottogeschäfts insbesondere Tabakwaren und Zeitungen verkauft. Außer der Klägerin waren dort – in verschiedenen Schichten – drei weitere Verkäuferinnen tätig. Von den drei weiteren Mitarbeiterinnen waren zwei seit September 2015 beim Beklagten beschäftigt. Eine weitere Mitarbeiterin war erst zu einem späteren Zeitpunkt eingestellt worden.

Das Ladenlokal der Lottoannahmestelle wird von drei für jedermann deutlich erkennbar positionierten Videokameras, den Kameras Nr. 1, Nr. 2 und Nr. 4 überwacht. Im Eingangsbereich macht ein auffälliges gelbes Hinweisschild auf die Überwachung, die den Arbeitnehmerinnen bekannt ist, aufmerksam. Die Kameras im Ladenlokal sind so angebracht, dass die Kamera Nr. 1 und die Kamera Nr. 2 die Zeitungs-, Presse- und Tabakregale aus unterschiedlichen Perspektiven erfassen, wobei die Kamera Nr. 2 zudem den Bereich auf zeichnet, in dem die Kunden die Lottoscheine ausfüllen und sich etwas länger aufhalten können. Die Kamera Nr. 4 filmt den Kassenbereich mit Fokus auf den Thekenbereich und die davor stehenden Kunden sowie die Tasten der Kasse und deren Bedienung. Eine weitere Kamera, die Kamera Nr. 3, überwacht den im hinteren Bereich der Lottoannahmestelle liegenden, dem Publikumsverkehr nicht zugänglichen Büroraum, der zum Geldzählen und zum Deponieren des Geldbestands in einem dort befindlichen Tresor genutzt wird. Sämtliche Aufnahmen werden mittels eines in einem verschlossenen Metallbehälter aufbewahrten Festplattenvideorekorders aufgezeichnet.

Aufgrund stichprobenartiger Ermittlungen der Warenaufschläge durch die Innenrevision wurde nach dem Vorbringen des Beklagten erstmals Anfang Dezember 2015 festgestellt, dass Waren – insbesondere Rubbellose und Tabakwaren – in deutlicher Menge fehlten. Nachdem auch für Januar 2016 erhebliche Fehlmengen zu verzeichnen waren, entnahm der Beklagte am 15. Februar 2016 das Videogerät mit den Aufzeichnungen aus der Filiale und analysierte die Aufnahmen in seiner Verwaltungszentrale in G.

Mit Schreiben vom 24. Februar 2016 kündigte der Beklagte das Arbeitsverhältnis mit der Klägerin fristlos. Die Klägerin hat gegen die Kündigung zunächst Kündigungsschutzklage erhoben und ausstehende Vergütung für den Monat Februar 2016 iHv. 918,00 € nebst Zinsen eingeklagt. Im Termin zur mündlichen Verhandlung vor dem Arbeitsgericht am 23. Juni 2016 hat sie ihre Kündigungsschutzklage zurückgenommen und nur noch ihren Zahlungsantrag – der nicht Gegenstand des Berufungs- und des Revisionsverfahrens geworden ist – weiterverfolgt.

Der Beklagte hat die Klägerin mit einer Widerklage auf Zahlung von Schadensersatz iHv. insgesamt 9.840,27 € in Anspruch genommen.

Er hat behauptet, eine Analyse der am 15. Februar 2016 entnommenen Videoaufzeichnungen habe ergeben, dass die Klägerin am 17. Dezember 2015, am 19. Dezember 2015, am 8. Januar 2016, am 13. Januar 2016, am 23. Januar 2016 sowie am 29. Januar 2016 Zigarettenverkäufe nicht ordnungsgemäß abgerechnet, Diebstähle von Zigaretten begangen, unberechtigt Gelder entnommen und Rubbellose genutzt habe, ohne diese zu bezahlen. Hierdurch sei ihm ein Schaden iHv. insgesamt 976,20 entstanden. Der gerichtlichen Verwertung der Videoaufnahmen vom 17. Dezember 2015, 19. Dezember 2015, 8. Januar 2016, 13. Januar 2016, 23. Januar 2016 sowie vom 29. Januar 2016 stehe kein Beweisverwertungsverbot entgegen. Die Videoüberwachung sei nach dem BDSG zulässig.

Darüber hinaus schulde die Klägerin ihm einen weiteren Schadensersatz iHv. 8.864,07 €. Die Innenrevision habe für den Zeitraum vom 1. November 2015 bis zum 31. Januar 2016 einen Warenschwund iHv. 9.177,88 € festgestellt. Dieser berechne sich aus der Gewinnmarge, die in diesem Zeitraum, abweichend von den üblichen etwa 10 Prozent, lediglich 2,5 Prozent betragen habe. Bei den Rubbellosen sei im selben Zeitraum eine Differenz iHv. 1.818,00 zwischen eingescannten und verkauften Losen aufgetreten. Von dem Gesamtbetrag iHv. 10.995,88 € seien der schon einbehaltene Lohn iHv. 715,97 € sowie weitere 439,64 € wegen einer von einer anderen Mitarbeiterin begangenen Stornomanipulation und der Betrag iHv. 976,20 € in Abzug zu bringen, so dass sich sein Gesamtschaden insoweit auf 8.864,07 € belaufe. Auch insoweit sei von einer Täterschaft der Klägerin auszugehen. Die Auswertung der Videoaufzeichnungen einzelner Tage habe im Hinblick auf die anderen Mitarbeiterinnen – mit Ausnahme der von einer anderen Mitarbeiterin begangenen Stornomanipulation iHv. 439,64 € – nichts ergeben. Die Kunden gelangten wegen der bestehenden räumlichen Trennung nicht an die Tabakwaren. Das Ladenlokal werde auch außerhalb der Öffnungszeiten videoüberwacht. Die Warenanlieferung werde ebenfalls durch Mitarbeiter kontrolliert. Anhand der einzelnen analysierten Arbeitstage der Klägerin am Anfang, in der Mitte und gegen Ende des Zeitraums vom 1. November 2015 bis zum 31. Januar 2016 ergebe sich ein so dichtes Bild, dass eine Schadensschätzung möglich sei. Einer Videoanalyse des gesamten Zeitraums bedürfe es nicht. Eine solche Analyse würde, da die Aufnahmen in Echtzeit vorlägen, einen unzumutbaren Zeitaufwand bedeuten.

Der Beklagte hat widerklagend beantragt, die Klägerin zu verurteilen, an ihn 9.840,27 € nebst Zinsen iHv fünf Prozentpunkten über dem Basiseinsatz seit dem 29. März 2016 zu zahlen.

Die Klägerin hat beantragt, die Widerklage abzuweisen.

Sie hat in Abrede gestellt, sich unrechtmäßig Geld oder Waren angeeignet zu haben. Sie hat behauptet, soweit sie unzutreffende Beträge in die Kasse eingetippt habe, sei dies zum Ausgleich vorher aufgetretener Stornos erfolgt. Dies sei erforderlich gewesen, da die Kasse keine einfache technische Vorkehrung für einen Stornovorgang aufgewiesen habe. Das Kassensystem sei zudem nicht in der

Lage gewesen, den Abverkauf von Tabakwaren spezifiziert zu erfassen. Ein etwaiger Fehlbestand könne auch auf ein Verhalten von Kunden oder der übrigen Mitarbeiterinnen zurückzuführen sein. Im Übrigen erscheine die Annahme ihrer Täterschaft schon deshalb nicht nachvollziehbar, weil sie vor der Einstellung der zwei weiteren Mitarbeiterinnen im September 2015 bereits ein Jahr für den Beklagten gearbeitet habe, ohne dass es zu Beanstandungen gekommen sei. Jedenfalls dürften die vom Beklagten gefertigten Videoaufzeichnungen nicht zu Beweiszwecken herangezogen werden, insoweit bestehe ein Beweisverwertungsverbot. Der Beklagte habe zum Zeitpunkt der Erstellung der Aufzeichnungen keinen diese Maßnahme rechtfertigenden hinreichend konkreten Verdacht gehabt. Zudem hätten die Aufzeichnungen im Kassenbereich lediglich der Überwachung der dort tätigen Mitarbeiter gedient. Darüber hinaus wirke sich aus, dass Arbeitnehmer im nicht öffentlich zugänglichen Büroraum grundsätzlich einen weitergehenden Schutz ihrer Privatsphäre erwarten dürften.

Das Arbeitsgericht hat den Beklagten zur Zahlung von 918,00 nebst Zinsen verurteilt und die Widerklage abgewiesen. Das Landesarbeitsgericht hat die gegen die Abweisung der Widerklage gerichtete Berufung des Beklagten zurückgewiesen. Mit seiner Revision verfolgt dieser sein Widerklagebegehren weiter. Die Klägerin beantragt die Zurückweisung der Revision.

Aus den Gründen:

Die zulässige Revision des Beklagten hat nur teilweise Erfolg, im Übrigen war sie zurückzuweisen. Das Landesarbeitsgericht hat die Berufung des Beklagten insoweit zu Recht als unbegründet zurückgewiesen, als dieser von der Klägerin einen weiteren Schadensersatz iHv. 8.864,07 € wegen angeblicher Pflichtverletzungen der Klägerin im Zeitraum vom 1. November 2015 bis zum 31. Januar 2016 mit Ausnahme am 17. und 19. Dezember 2015 sowie am 8., 13., 23. und 29. Januar 2016 angeblich begangener Pflichtverletzungen fordert. Soweit der Beklagte von der Klägerin die Zahlung von Schadensersatz iHv. 976,20 € wegen der aufgrund der Auswertung der Videoaufnahmen vom 17. und 19. Dezember 2015 sowie vom 8., 13., 23. und 29. Januar 2016 angeführter Pflichtverletzungen der Klägerin begehrt, ist die Revision dagegen begründet. Das Landesarbeitsgericht durfte die Widerklage insoweit nicht mit der von ihm gegebenen Begründung abweisen. Aufgrund der vom Landesarbeitsgericht bislang getroffenen Feststellungen kann der Senat nicht abschließend beurteilen, ob und ggf. in welchem Umfang die Widerklage insoweit begründet ist. Dies führt zur Aufhebung des angefochtenen Urteils (§ 562 Abs. 1 ZPO) im Kostenpunkt und im Übrigen insoweit, als das Landesarbeitsgericht die Widerklage des Beklagten wegen des von diesem begehrten Schadensersatzes iHv. 976,20 € wegen angeblicher Pflichtverletzungen der Klägerin am 17. und 19. Dezember 2015 sowie am 8., 13., 23. und 29. Januar 2016 abgewiesen hat, und im Umfang der Aufhebung zur Zurückverweisung der Sache zur neuen Verhandlung und Entscheidung an das Landesarbeitsgericht (§ 563 Abs. 1 Satz 1 ZPO).

A. Soweit der Beklagte mit seiner Widerklage Schadensersatz iHv. 8.864,07 € wegen der von ihm behaupteten Pflichtverletzungen der Klägerin im Zeitraum vom 1. November 2015 bis zum 31. Januar 2016 mit Ausnahme am 17. und 19. Dezember 2015 sowie am 8., 13., 23. und 29. Januar 2016 angeblich begangener Pflichtverletzungen begehrt, hat das Landesarbeitsgericht die Berufung des Beklagten zu Recht zurückgewiesen. Insoweit ist die Widerklage unbegründet. Der Beklagte kann – wie das Landesarbeitsgericht zutreffend angenommen hat – von der Klägerin insoweit weder nach § 280 Abs. 1 Satz 1 BGB noch nach § 823 Abs. 1 und Abs. 2 BGB iVm. § 242 Abs. 1, § 246 Abs. 1 oder § 266 Abs. 1 StGB Schadensersatz verlangen, da es bereits an einem schlüssigen Vorbringen des Beklagten zu den Voraussetzungen eines Schadensersatzanspruchs nach diesen Bestimmungen fehlt.

I. Das Landesarbeitsgericht hat seine die Widerklage insoweit abweisende Entscheidung zum einen tragend darauf gestützt, der Beklagte habe schon nicht schlüssig dargelegt, dass in den drei Monaten von November 2015 bis Januar 2016 in der streitgegenständlichen Lottoannahmestelle tatsächlich bei den Waren außerhalb des Lottogeschäfts ein Schwund/Fehlbetrag iHv. 9.177,88 € und bei den Rubbellosen ein Schwund/Fehlbetrag iHv. 1.818,00 € zu verzeichnen gewesen sei. Zur Begründung einer konkret zu beziffernden Schadensersatzforderung hätte der Beklagte – über den gehaltenen Vortrag hinaus – zudem vortragen müssen, dass der körperliche Warenbestand der Filiale in die Betrachtung einbezogen wurde. Nur dann hätten andere Erklärungen für eine unerwartet niedrige Marge hinreichend zuverlässig ausgeschlossen werden können.

Zum anderen und unabhängig davon, ob die Klägerin an den sechs konkret bezeichneten Tagen Unredlichkeiten begangen habe, habe der Beklagte eine Täterschaft und Verantwortlichkeit der Klägerin für einen Schaden iHv. 8.864,07 € nicht schlüssig dargetan. Weder der Beklagte noch sonstige Personen hätten unerlaubte Handlungen der Klägerin an weiteren Tagen beobachtet. Dass weitere belastende Videoaufzeichnungen vorgelegen hätten, habe der Beklagte nicht behauptet. Eine bloße Schlussfolgerung aus einem Fehlbestand auf eine Täterschaft der Klägerin sei nicht zwingend. Es könne nicht ausgeschlossen werden, dass andere Umstände als ein Fehlverhalten der Klägerin zu einem Warenschwund/Fehlbetrag geführt hätten. So könnten Kunden oder auch sonstige Dritte Waren weggenommen haben. Auch eine Täterschaft der anderen Mitarbeiterinnen des Beklagten könne nicht sicher ausgeschlossen werden. Unbestimmte Vermutungen und ein mehr oder weniger dringender Verdacht einer Pflichtverletzung der Klägerin reichten als Grundlage eines Schadensersatzanspruchs nicht aus.

II. Es kann offenbleiben, ob der Beklagte – wie das Landesarbeitsgericht mit seiner ersten selbständig tragenden Begründung angenommen hat – einen entsprechenden Vermögensschaden nicht schlüssig dargelegt hat, weshalb auch die Frage, ob eine Schadensschätzung nach § 287 Abs. 1 ZPO möglich wäre, keiner Entscheidung bedurfte. Die Annahme des Landesarbeitsgerichts, die Widerklage sei insoweit auch deshalb abzuweisen, weil der Beklagte eine Täterschaft und Verantwortlichkeit der Klägerin für den von ihm behaupteten Schaden iHv. 8.864,07 € nicht schlüssig dargetan habe, ist frei von Rechtsfehlern.

1. Zwar dürfen, wenn das schädigende Ereignis näher am Arbeitnehmer als am Arbeitgeber gelegen hat, an die Darlegungslast des Arbeitgebers keine allzu hohen Anforderungen gestellt werden. Vielmehr hat sich der Arbeitnehmer im Sinne einer abgestuften Darlegungslast substantiiert zu äußern (vgl. BAG 28. Oktober 2010 – 8 AZR 647/09 – Rn. 51; 2. Dezember 1999 – 8 AZR 386/98 – zu III 2 b der Gründe; 17. September 1998 – 8 AZR 175/97 – zu B II 2 c aa der Gründe, BAGE 90, 9). Das kann dazu führen, dass ein Arbeitgeber nicht jede einzelne Handlung des Arbeitnehmers mit Datum und Uhrzeit benennen muss, solange ein bestimmter Fehlbetrag feststeht und die Verantwortlichkeit gerade des Arbeitnehmers für den geltend gemachten Schaden substantiiert dargelegt ist.

2. Hieran fehlt es. Der Beklagte hat schon keine ausreichenden Umstände für ein haftungsbegründendes Fehlverhalten der Klägerin vorgetragen. Sein Vorbringen lässt diese Schlussfolge-

rung nicht zu, weil – wie das Landesarbeitsgericht zutreffend angenommen hat – auch andere Umstände in gleicher Weise zu dem behaupteten Schaden geführt haben könnten. Denn unstreitig hätten auch Kunden Waren entwenden oder zB durch Trickbetrügereien einen Kassenfehlbestand verursachen können. Ebenso wenig ist es auszuschließen, dass ein Fehlverhalten von Lieferanten für einen Warenfehlbestand ursächlich war. Darüber hinaus hatten auch die Kolleginnen der Klägerin Zugriff auf die Kasse und den Warenbestand. Das Landesarbeitsgericht hat in diesem Zusammenhang zutreffend angenommen, dass der Beklagte nicht hinreichend dargelegt hat, warum die Fehlbestände nicht durch deren Verhalten entstanden sein können. Der Beklagte hat die Fehlbestände nicht jeweils einer bestimmten Schicht zugeordnet, während derer allein die Klägerin tätig war, sondern nur den Gesamtschwund während des Zeitraums vom 1. November 2015 bis zum 31. Januar 2016 angegeben, in dem unstreitig auch die weiteren Arbeitnehmerinnen in der Lottoannahmestelle tätig waren. Dass eine Täterschaft dieser Arbeitnehmerinnen nicht ausgeschlossen werden kann, gilt umso mehr, als der Beklagte selbst ausdrücklich vorgetragen hat, dass auch im Hinblick auf die Kolleginnen der Klägerin nur stichprobenartige Prüfungen durchgeführt worden seien und diese Prüfungen ergeben hätten, dass eine Kollegin der Klägerin eine Stornomanipulation begangen habe, die zu einem Schaden iHv. 439,64 € geführt habe. Demnach bleiben im Ergebnis nur Vermutungen bzw. ein Verdacht, dass die Fehlbestände auf Pflichtverletzungen der Klägerin zurückzuführen sind. Hierauf kann ein Schadensersatzanspruch jedoch nicht gestützt werden (vgl. BAG 2. Dezember 1999 – 8 AZR 386/98 – zu III 2 b der Gründe; 17. September 1998 – 8 AZR 175/97 – zu B II 2 c aa der Gründe, BAGE 90, 9).

B. Soweit der Beklagte mit der Widerklage Schadensersatz iHv. 976,20 € wegen behaupteter Pflichtverletzungen der Klägerin am 17. und 19. Dezember 2015 sowie am 8., 13., 23. und 29. Januar 2016 begehrt, ist die Revision dagegen begründet. Das Landesarbeitsgericht durfte die Widerklage insoweit nicht mit der von ihm gegebenen Begründung abweisen. Aufgrund der vom Landesarbeitsgericht bislang getroffenen Feststellungen kann der Senat nicht abschließend beurteilen, ob und ggf. in welchem Umfang die Klage insoweit begründet ist. Dies führt zur Aufhebung des angefochtenen Urteils (§ 562 Abs. 1 ZPO) im Kostenpunkt und im Übrigen insoweit, als das Landesarbeitsgericht die Widerklage des Beklagten wegen des von diesem begehrten Schadensersatzes iHv. 976,20 € abgewiesen hat, sowie im Umfang der Aufhebung zur Zurückverweisung der Sache zur neuen Verhandlung und Entscheidung an das Landesarbeitsgericht (§ 563 Abs. 1 Satz 1 ZPO).

I. Das Landesarbeitsgericht hat seine die Widerklage (auch) insoweit abweisende Entscheidung darauf gestützt, der Beklagte habe keinen zulässigen Beweis für die Richtigkeit des von ihm behaupteten und von der Klägerin bestrittenen Fehlverhaltens der Klägerin angetreten. Sowohl für die Beweisführung durch Inaugenscheinnahme der Videosequenzen als auch für die Beweisführung durch Vernehmung der Mitarbeiterin, die die Videoaufzeichnungen ausgewertet habe, als Zeugin bestehe ein Beweisverwertungsverbot aus Gründen des Daten- und Persönlichkeitsrechtsschutzes.

Das Landesarbeitsgericht hat angenommen, die von dem Beklagten ab dem 15. Februar 2016 begonnene Auswertung des mit der Kamera Nr. 4 (sog. Kassenkamera) aufgezeichneten Arbeitsverhaltens der Klägerin im Kassenbereich verstoße gegen § 6b Abs. 5 BDSG in der bis zum 24. Mai 2018 geltenden Fassung (im Folgenden BDSG aF). Der Beklagte habe mit dem Vorhalten der Videoaufzeichnungen des Kassierverhaltens der Klägerin im Zeitraum von November 2015 bis Januar 2016 bis zum 15. Februar 2016 gegen seine Pflicht zur unverzüglichen Löschung verstoßen. Hieraus resultiere nach Abwägung der wechselseitigen Interessen ein Beweisverwertungsverbot. Auch wenn der Beklagte ein Interesse daran habe, Schadensersatzforderungen wegen eines rechtswidrigen Verhaltens realisieren zu können, erwarte der Gesetzgeber von der verantwortlichen Stelle eine alsbaldige Prüfung des Videomaterials zur Bedarfsklärung. Auf der Seite der Klägerin sei zu berücksichtigen, dass diese durch das Vorgehen des Beklagten in gravierender Weise in ihrem Recht auf informationelle Selbstbestimmung beschränkt werde. Die Kassenkamera habe jeden einzelnen Kassiervorgang während etlicher Arbeitswochen – weit rückwirkend in den Dreimonatszeitraum – aufgezeichnet. Zudem wirke sich aus, dass auch das Verhalten der Klägerin an anderen Stellen des Ladenlokals und zudem ihr Verhalten in dem nicht öffentlich zugänglichen Büroraum, insb. auch an dem dort befindlichen Sitzplatz durchgängig aufgezeichnet worden sei. Eine Videoüberwachung des Arbeitnehmers in seinem Arbeitsbereich während der gesamten Dauer seiner Arbeitszeit stelle einen intensiven Eingriff in das Persönlichkeitsrecht dar. Es komme hinzu, dass die lückenlose Dokumentation des Arbeitsverhaltens der Klägerin über Wochen bzw. über Monate hinaus gespeichert geblieben sei.

Etwas anderes folge nicht aus § 32 Abs. 1 Satz 2 BDSG aF. Ein Vorgehen nach dieser Bestimmung setze voraus, dass der Arbeitgeber Straftaten aufdecken wolle. Zudem müssten zumindest tatsächliche Anhaltspunkte für begangene Straftaten vorliegen. Der konkrete Tatverdacht müsse aktenkundig gemacht werden. Diese Voraussetzungen seien nicht erfüllt. Ein Verdacht sei bei dem Beklagten erst entstanden, nachdem er rückwirkend den Dreimonatszeitraum November 2015 bis Januar 2016 betriebswirtschaftlich ausgewertet habe.

Der Beklagte könne – so das Landesarbeitsgericht – die fraglichen Videoaufzeichnungen auch nicht nach § 32 Abs. 1 Satz 1 BDSG aF rechtfertigen. Insoweit sei anerkannt, dass diese Bestimmung eine permanente Überwachung des Arbeitsverhaltens wegen des zu beachtenden Verhältnismäßigkeitsgrundsatzes nicht zulasse.

Ein Beweisverwertungsverbot bestehe auch, soweit der Beklagte die Wegnahme von 200,00 € durch die Klägerin im Büroraum am 23. Januar 2016 mit Videosequenzen der Kamera Nr. 3 (sog. Bürokamera) beweisen wolle. Der Büroraum sei kein öffentlich zugänglicher Raum iSv. § 6b BDSG aF, so dass eine Videoüberwachung dieses Raums nach dieser Vorschrift nicht in Betracht komme. Die Zulässigkeitsvoraussetzungen nach § 32 Abs. 1 Sätze 1 und 2 BDSG aF seien aus den bereits dargelegten Gründen nicht erfüllt. Ein Rückgriff auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG aF führe zu keinem anderen Ergebnis.

II. Mit dieser Begründung durfte das Landesarbeitsgericht die Widerklage wegen der vom Beklagten behaupteten Pflichtverletzungen der Klägerin am 17. und 19. Dezember 2015 sowie am 8., 13., 23. und 29. Januar 2016 nicht abweisen. Zwar hat das Landesarbeitsgericht zu Recht geprüft, ob zugunsten der Klägerin ein Beweisverwertungsverbot eingreift. Entsprechende Anhaltspunkte bot schon der Vortrag des Beklagten. Dieser hat sich zur Rechtfertigung seines Schadensersatzverlangens auf die Videoaufzeichnungen vom 17. und 19. Dezember 2015 sowie vom 8., 13., 23. und 29. Januar 2016 gestützt. Die Klägerin, die die ihr gegenüber erhobenen Vorwürfe bestritten hat, hat auch nicht auf die Geltendmachung möglicher Persönlichkeitsrechtsverletzungen verzichtet, sondern sich – ohne dass

dies erforderlich gewesen wäre – ausdrücklich auf ein Beweisverwertungsverbot berufen (vgl. BAG 23. August 2018 – 2 AZR 133/18 – Rn. 17 mwN, BAGE 163, 239). Das Landesarbeitsgericht hat allerdings zum einen die Grundsätze, die für das Eingreifen eines Beweisverwertungsverbots gelten, falsch angewendet. Insoweit fehlt es bereits an einer gesonderten Prüfung, inwieweit die Verwertung der – nach Auffassung des Landesarbeitsgerichts – datenschutzrechtlich unzulässig gewonnenen Erkenntnisse oder Beweismittel durch das Gericht im Einzelfall einen Grundrechtsverstoß darstellt. Zum anderen tragen die bisherigen Feststellungen des Landesarbeitsgerichts seine Würdigung, die Erhebung der Daten sei nicht nach § 32 Abs. 1 Satz 1 BDSG aF zulässig, weil diese Bestimmung wegen des zu beachtenden Verhältnismäßigkeitsgrundsatzes eine permanente Überwachung des Arbeitsverhaltens der Klägerin nicht erlaube, nicht.

1. Für ein eventuelles Beweisverwertungsverbot kommt es auf die Frage an, ob ein Eingriff in das Recht der Klägerin auf informationelle Selbstbestimmung vorliegt und ob dieser Eingriff zulässig ist. Sofern die Datenerhebung und -verwertung nach den Bestimmungen des BDSG aF erfolgen durfte, kommt ein Beweisverwertungsverbot nicht in Betracht. Ist dies nicht der Fall, muss im Einzelfall geprüft werden, ob die Verwertung der so gewonnenen Beweismittel durch das Gericht im Einzelfall einen Grundrechtsverstoß darstellt. Dies entspricht der Rechtsprechung des Zweiten Senats des Bundesarbeitsgerichts (vgl. BAG 23. August 2018 – 2 AZR 133/18 – BAGE 163, 239), der der erkennende Senat sich anschließt.

a) Weder die Zivilprozessordnung noch das Arbeitsgerichtsgesetz enthalten Bestimmungen, die die Verwertbarkeit von Erkenntnissen oder Beweismitteln einschränken, die eine Arbeitsvertragspartei rechtswidrig erlangt hat. Ein Verwertungsverbot kann sich allerdings aus einer verfassungskonformen Auslegung des Verfahrensrechts ergeben. Da der Anspruch auf rechtliches Gehör aus Art. 103 Abs. 1 GG aber grundsätzlich gebietet, den Sachvortrag der Parteien und die von ihnen angebotenen Beweise zu berücksichtigen, kommt ein „verfassungsrechtliches Verwertungsverbot“ nur in Betracht, wenn dies wegen einer grundrechtlich geschützten Position einer Prozesspartei zwingend geboten ist (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 14 mwN, BAGE 163, 239). Dies setzt in aller Regel voraus, dass bereits durch die Informations- oder Beweisbeschaffung das allgemeine Persönlichkeitsrecht der Partei verletzt worden ist, ohne dass dies durch überwiegende Belange der anderen Partei gerechtfertigt gewesen wäre. Überdies müssen die betroffenen Schutzzwecke des bei der Gewinnung verletzten Grundrechts der Verwertung der Erkenntnis oder des Beweismittels im Rechtsstreit entgegenstehen. Die prozessuale Verwertung muss selbst einen Grundrechtsverstoß darstellen. Das ist der Fall, wenn das nach Art. 1 Abs. 3 GG unmittelbar an die Grundrechte gebundene Gericht ohne Rechtfertigung in eine verfassungsrechtlich geschützte Position einer Prozesspartei eingriffe, indem es eine Persönlichkeitsrechtsverletzung durch einen Privaten perpetuierte oder vertiefte. Insofern kommt die Funktion der Grundrechte als Abwehrrechte gegen den Staat zum Tragen. Auf eine nicht gerechtfertigte Beeinträchtigung des Persönlichkeitsrechts durch einen Privaten darf kein verfassungswidriger Grundrechtseingriff durch ein Staatsorgan „aufgesattelt“ werden. Nicht abschließend geklärt ist, ob die Gerichte jenseits der sie treffenden Pflicht, ungerechtfertigte Grundrechtseingriffe zu unterlassen, wegen einer verfassungsrechtlichen Schutzpflicht gehalten sein können, einer Verletzung des allgemeinen Persönlichkeitsrechts durch Private aktiv zu begegnen und Sachvortrag oder Beweisantritte einer Partei aus Gründen der Generalprävention außer Acht zu lassen. Dafür wäre jedenfalls Voraussetzung, dass die verletzte Schutznorm in den betreffenden Fällen ohne ein prozessuales Verwertungsverbot leerliefe (vgl. BAG 23. August 2018 – 2 AZR 133/18 – aaO).

b) Obgleich die Vorschriften des BDSG aF nicht die Zulässigkeit von Parteivorbringen und seine Verwertung im Verfahren vor den Gerichten für Arbeitssachen begrenzen, und obwohl es für das Eingreifen eines Verwertungsverbots darauf ankommt, ob bei der Erkenntnis- oder Beweisgewinnung das allgemeine Persönlichkeitsrecht verletzt worden ist, sind die einfachrechtlichen Vorgaben insofern nicht ohne Bedeutung. Die Bestimmungen des BDSG aF über die Anforderungen an eine zulässige Datenerhebung, -verarbeitung und -nutzung konkretisieren und aktualisieren für den Einzelnen den Schutz seines Rechts auf informationelle Selbstbestimmung und am eigenen Bild (§ 1 Abs. 1 BDSG aF). Sie regeln, in welchem Umfang im Anwendungsbereich des Gesetzes Eingriffe durch öffentliche oder nicht-öffentliche Stellen iSd. § 1 Abs. 2 BDSG aF in diese Rechtspositionen erlaubt sind (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 15 mwN, BAGE 163, 239).

aa) War die betreffende Maßnahme nach den Vorschriften des BDSG aF zulässig, liegt insoweit keine Verletzung des allgemeinen Persönlichkeitsrechts in Gestalt des Rechts auf informationelle Selbstbestimmung und am eigenen Bild vor. Ein Verwertungsverbot scheidet von vornherein aus. So liegt es namentlich, wenn die umfassende Abwägung der widerstreitenden Interessen und Grundrechtspositionen im Rahmen der Generalklauseln des § 32 Abs. 1 BDSG aF zugunsten des Arbeitgebers ausfällt (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 15, BAGE 163, 239).

bb) Nur dann, wenn die fragliche Maßnahme nach den Bestimmungen des BDSG aF nicht erlaubt war, muss gesondert geprüft werden, ob die Verwertung von im Zuge dieser Maßnahme gewonnenen Erkenntnissen oder Beweismitteln durch das Gericht einen Grundrechtsverstoß darstellen würde. Daran kann es zum einen fehlen, wenn die Unzulässigkeit der vom Arbeitgeber durchgeführten Maßnahme allein aus der (Grund-)Rechtswidrigkeit der Datenerhebung(en) gegenüber anderen Beschäftigten resultiert oder die verletzte einfachrechtliche Norm keinen eigenen „Grundrechtsgehalt“ hat. Zum anderen kann es sein, dass die gerichtliche Verwertung weder einen ungerechtfertigten Grundrechtseingriff darstellt noch aufgrund einer verfassungsrechtlichen Schutzpflicht zu unterlassen ist, weil durch sie die ungerechtfertigte „vorprozessuale“ Verletzung des allgemeinen Persönlichkeitsrechts einer Prozesspartei nicht perpetuiert oder vertieft würde und der Verwertung auch Gründe der Generalprävention nicht entgegenstehen (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 15 mwN, BAGE 163, 239).

c) Sofern danach ein Beweisverwertungsverbot wegen eines Verstoßes gegen das allgemeine Persönlichkeitsrecht besteht, erfasst dieses nicht allein das unrechtmäßig erlangte Beweismittel selbst, sondern steht auch einer mittelbaren Verwertung, wie der Vernehmung von Zeugen über den Inhalt des Beweismittels entgegen (vgl. BVerfG 31. Juli 2001 – 1 BvR 304/01 – zu II 1 b bb der Gründe; BAG 20. Oktober 2016 – 2 AZR 395/15 – Rn. 19, BAGE 157, 69). Falls im vorliegenden Verfahren ein Beweisverwertungsverbot eingreift, dürfte also weder eine Inaugenscheinnahme der Videoaufnahmen erfolgen, noch dürfte das Gericht dem weiteren Beweisangebot des Beklagten auf Vernehmung der mit der Auswertung der Aufnahmen betrauten Personen als Zeugen nachgehen.

2. Danach durfte das Landesarbeitsgericht die Widerklage wegen der vom Beklagten behaupteten Pflichtverletzungen der

Klägerin am 17. und 19. Dezember 2015 sowie am 8., 13., 23. und 29. Januar 2016 nicht mit der von ihm gegebenen Begründung abweisen, wobei dahinstehen kann, ob das Landesarbeitsgericht § 6b Abs. 3 und Abs. 5 BDSG aF zutreffend angewendet hat. § 32 Abs. 1 Satz 1 BDSG aF stellt für die Verarbeitung und Nutzung personenbezogener Daten eines Beschäftigten, die der Arbeitgeber durch eine Videoüberwachung öffentlich zugänglicher Räume erlangt hat, eine eigenständige, von den Voraussetzungen des § 6b Abs. 3 BDSG aF unabhängige Erlaubnisnorm dar (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 23, BAGE 163, 239).

Soweit das Landesarbeitsgericht angenommen hat, die Erhebung der Daten sei nicht nach § 32 Abs. 1 Satz 1 BDSG aF erlaubt, weil diese Bestimmung wegen des zu beachtenden Verhältnismäßigkeitsgrundsatzes eine permanente Überwachung des Arbeitsverhaltens der Klägerin nicht zugelassen habe, fehlt es an einer daran anschließenden Prüfung, ob die Verwertung von im Zuge dieser Maßnahme gewonnenen Erkenntnissen oder Beweismitteln durch das Gericht einen Grundrechtsverstoß darstellen würde. Zudem tragen die vom Landesarbeitsgericht bislang getroffenen Feststellungen seine Würdigung, die Erhebung der Daten sei nicht nach § 32 Abs. 1 Satz 1 BDSG aF zulässig, nicht.

a) Nach § 32 Abs. 1 Satz 1 BDSG aF dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Dabei gehört zur Durchführung die Kontrolle, ob der Arbeitnehmer seinen Pflichten nachkommt, zur Beendigung iSd. Kündigungsvorbereitung die Aufdeckung einer Pflichtverletzung, die die Kündigung des Arbeitsverhältnisses rechtfertigen kann (BAG 27. Juli 2017 – 2 AZR 681/16 – Rn. 28, BAGE 159, 380; 29. Juni 2017 – 2 AZR 597/16 – Rn. 26, BAGE 159, 278).

aa) § 32 Abs. 1 Satz 2 BDSG aF entfaltet zwar keine „Sperrwirkung“ dergestalt, dass eine anlassbezogene Datenerhebung durch den Arbeitgeber ausschließlich zur Aufdeckung von Straftaten zulässig wäre und nicht nach § 32 Abs. 1 Satz 1 BDSG aF zulässig sein könnte. Der mit einer Datenerhebung verbundene Eingriff in das allgemeine Persönlichkeitsrecht des Arbeitnehmers muss aber auch im Rahmen von § 32 Abs. 1 Satz 1 BDSG aF einer Abwägung der beiderseitigen Interessen nach dem – dort gleichfalls verankerten – Grundsatz der Verhältnismäßigkeit standhalten. Dieser Grundsatz verlangt, dass der Eingriff geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den erstrebten Zweck zu erreichen (vgl. hierzu ausführlich BAG 27. Juli 2017 – 2 AZR 681/16 – Rn. 30 mwN, BAGE 159, 380). Es dürfen keine anderen, zur Zielerreichung gleich wirksamen und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränkenden Mittel zur Verfügung stehen. Die Verhältnismäßigkeit im engeren Sinne (Angemessenheit) ist gewahrt, wenn die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht. Die Datenerhebung, -verarbeitung oder -nutzung darf keine übermäßige Belastung für den Arbeitnehmer darstellen und muss der Bedeutung des Informationsinteresses des Arbeitgebers entsprechen. Danach muss im Fall einer der (verdeckten) Videoüberwachung vergleichbar eingriffsintensiven Maßnahme, die auf § 32 Abs. 1 Satz 1 BDSG aF gestützt werden soll, der auf konkrete Tatsachen begründete Verdacht einer schwerwiegenden, nicht notwendig strafbaren Pflichtverletzung bestehen. In einem solchen Fall ist eine Ermittlung „ins Blaue hinein“, ob ein Arbeitnehmer sich pflichtwidrig verhält, auch nach § 32 Abs. 1 Satz 1 BDSG aF unzulässig (BAG 27. Juli 2017 – 2 AZR 681/16 – aaO).

bb) Hieraus folgt zugleich, dass weniger intensiv in das allgemeine Persönlichkeitsrecht des Arbeitnehmers eingreifende Datenerhebungen nach § 32 Abs. 1 Satz 1 BDSG aF ohne Vorliegen eines durch Tatsachen begründeten Anfangsverdachts – zumal einer Straftat oder anderen schweren Pflichtverletzung – zulässig sein können. Das gilt vor allem für nach abstrakten Kriterien durchgeführte, keinen Arbeitnehmer besonders unter Verdacht stellende offene Überwachungsmaßnahmen, die der Verhinderung von Pflichtverletzungen dienen sollen. Solche präventiven Maßnahmen können sich schon aufgrund des Vorliegens einer abstrakten Gefahr als verhältnismäßig erweisen, wenn sie keinen solchen psychischen Anpassungsdruck erzeugen, dass die Betroffenen bei objektiver Betrachtung in ihrer Freiheit, ihr Handeln aus eigener Selbstbestimmung zu planen und zu gestalten, wesentlich gehemmt sind (dazu BAG 27. Juli 2017 – 2 AZR 681/16 – Rn. 31 mwN, BAGE 159, 380).

cc) Eine Unverhältnismäßigkeit der Datenerhebung nach § 32 Abs. 1 Satz 1 BDSG aF dürfte danach zwar dann anzunehmen sein, wenn es sich um eine verdeckte Videoüberwachung gehandelt hätte, ohne dass ein durch konkrete Tatsachen begründeter Verdacht einer schwerwiegenden Pflichtverletzung bestand. Unstreitig war der Klägerin jedoch bekannt, dass zumindest der öffentlich zugängliche Bereich der Lottoannahmestelle, insbesondere auch der Kassenbereich videoüberwacht wurde. Konkrete Anhaltspunkte dafür, dass ihr die Videoüberwachung im Büroraum, in dem sich der Tresor befand, nicht bekannt war, liegen nicht vor. Bei einer offenen Videoüberwachung käme es auch nicht darauf an, ob der Klägerin ausdrücklich eröffnet wurde, dass die Überwachung sich – auch – gegen sie richtete und ihr Verhalten an der Kasse, insb. die Eingabe bestimmter Beträge in die Kasse erfasste. Selbst wenn dies nicht geschehen sein sollte, wäre die damit verbundene Erhebung ihrer entsprechenden personenbezogenen Daten nicht allein aus diesem Grund unverhältnismäßig gewesen. Zwar stellt eine berechtigte Erwartung des Betroffenen in Bezug auf die Privatsphäre einen bedeutenden Faktor im Rahmen der Interessenabwägung dar. Von einer solchen „Privatheitserwartung“ konnte aber keine Rede sein, wenn die Klägerin angesichts ihres Wissens um die Überwachung des Kassenbereichs zumindest damit rechnen musste, dass mithilfe der Videoaufzeichnungen auch vorsätzliche Pflichtverletzungen durch Beschäftigte verhindert bzw. aufgedeckt und verfolgt werden konnten und sollten. In diesem Fall wäre die Klägerin nicht heimlich überwacht worden. Etwas anderes müsste allenfalls dann gelten, wenn der Beklagte die Klägerin – wofür nichts ersichtlich ist – in Bezug auf die Erfassung ihres Verhaltens an der Kasse und ihres sonstigen Arbeitsverhaltens „in Sicherheit gewiegt“ hätte (vgl. BAG 23. August 2018 – 2 AZR 133/18 – Rn. 44 mwN, BAGE 163, 239).

dd) Eine Unverhältnismäßigkeit der Datenerhebung nach § 32 Abs. 1 Satz 1 BDSG aF läge aber auch dann vor, wenn die Videoaufzeichnungen einen solchen psychischen Anpassungs- und Leistungsdruck erzeugt hätten, dass sie als eine der verdeckten Videoüberwachung vergleichbar eingriffsintensive Maßnahme anzusehen wären, ohne dass ein durch konkrete Tatsachen begründeter Verdacht einer schwerwiegenden Pflichtverletzung bestand. Dies wäre jedenfalls dann anzunehmen, wenn eine lückenlose, dauerhafte sowie sehr detaillierte Erfassung des Verhaltens der Klägerin während ihrer gesamten Arbeitszeit stattgefunden hätte, so dass sie davon ausgehen musste, dass jede ihrer Bewegungen überwacht wurde. In die-

sem Fall hätte für die Klägerin – vergleichbar mit der Situation einer verdeckten Überwachung – keine Möglichkeit einer unbewachten und ungestörten Wahrnehmung ihres Persönlichkeitsrechts bestanden.

b) Nach den bislang vom Landesarbeitsgericht getroffenen Feststellungen kann nicht beurteilt werden, ob durch die Videoüberwachung ein derartiger psychischer Anpassungs- und Leistungsdruck erzeugt wurde, dass die Klägerin bei objektiver Betrachtung in ihrer Freiheit, ihr Handeln aus eigener Selbstbestimmung zu planen und zu gestalten, wesentlich gehemmt wurde. Die bislang vom Landesarbeitsgericht getroffenen Feststellungen tragen die Annahme, die Videoüberwachung sei ohne Vorliegen eines konkreten Verdachts als unverhältnismäßig anzusehen, deshalb nicht.

Das Landesarbeitsgericht hat weder konkrete Feststellungen zur Größe der zur Lottoannahmestelle gehörenden Räumlichkeiten noch dazu getroffen, welcher räumliche Bereich der Lottoannahmestelle in welchem Umfang durch die einzelnen Videokameras konkret erfasst wurde. Es fehlt zudem an Feststellungen dazu, ob es – den Arbeitnehmerinnen bekannte – überwachungsfreie Zonen gab, in denen diese sich während der Arbeitsschichten aufhalten konnten, und wie groß diese Zonen ggf. waren. Unklar ist außerdem, ob alle oder nur ein Teil der von den Arbeitnehmerinnen ausgeführten Tätigkeiten erfasst wurden. Ferner hat das Landesarbeitsgericht keine Feststellungen dazu getroffen, wie oft und zu welchem Zweck der Büroraum betreten wurde. Darüber hinaus fehlen Feststellungen dazu, ob während der Arbeitsschichten – teilweise – mehrere Arbeitnehmerinnen gleichzeitig anwesend waren, wo die Mitarbeiterinnen ihre Ruhepausen (vgl. § 4 ArbZG) wahrgenommen haben und ob sie auch während dieser Pausen durch die Kameras überwacht wurden.

3. Aufgrund der vom Landesarbeitsgericht bislang getroffenen Feststellungen kann der Senat nicht abschließend beurteilen, ob und ggf. in welchem Umfang die auf Zahlung von Schadensersatz iHv. 976,20 € wegen angeblicher Pflichtverletzungen der Klägerin am 17. und 19. Dezember 2015 sowie am 8., 13., 23. und 29. Januar 2016 gerichtete Widerklage begründet ist. Dies führt zur Aufhebung des angefochtenen Urteils (§ 562 Abs. 1 ZPO) im Kostenpunkt und im Übrigen insoweit, als das Landesarbeitsgericht die Widerklage des Beklagten wegen des von diesem begehrten Schadensersatzes iHv. 976,20 € abgewiesen hat, sowie im Umfang der Aufhebung zur Zurückverweisung der Sache zur neuen Verhandlung und Entscheidung an das Landesarbeitsgericht (§ 563 Abs. 1 Satz 1 ZPO).

Für das fortgesetzte Berufungsverfahren sind folgende Hinweise veranlasst:

a) Das Landesarbeitsgericht wird dem Beklagten aufzugeben haben, eindeutig zu erklären, welche Handlungen der Klägerin am 17. und 19. Dezember 2015 sowie am 8., 13., 23. und 29. Januar 2016 aufgezeichnet wurden und welche konkreten Vorwürfe er insoweit gegen die Klägerin erhebt, wobei zu beachten sein wird, dass die Klägerin ausweislich der vom Beklagten mit Schriftsatz vom 21. April 2016 vorgelegten „Anlage zum Kassenrevisionsbericht“ am 8. Januar 2016 möglicherweise nicht gearbeitet hat, weil sich dort für beide Arbeitsschichten an diesem Tag in der Rubrik „Unterschrift“ der Name einer anderen Arbeitnehmerin findet.

Sodann wird die Klägerin sich zu den vom Beklagten erhobenen Vorwürfen zu erklären haben. Sofern die Klägerin behaupten sollte, Warenverkäufe immer ordnungsgemäß registriert und die vereinnahmten Gelder stets vollständig in die Kasse gelegt zu haben, könnte der Hinweis veranlasst sein, dass sie sich zu ihrer Entlastung mit der Inaugenscheinnahme der betreffenden Videosequenzen einverstanden erklären kann.

b) Das Landesarbeitsgericht wird zudem Feststellungen zu den unter Rn. 41 aufgeführten Umständen zu treffen haben. Insoweit wird den Parteien Gelegenheit zu entsprechendem Vorbringen zu geben sein.

c) Sollte das Landesarbeitsgericht danach die Datenerhebung nach § 32 Abs. 1 Satz 1 BDSG aF für zulässig halten, wird es Folgendes zu berücksichtigen haben:

aa) Sofern zulässig erhobene Daten den Verdacht einer Pflichtverletzung begründen, dürfen sie für die Zwecke und unter den Voraussetzungen des § 32 Abs. 1 Satz 1 BDSG aF auch verarbeitet und genutzt werden. Der Arbeitgeber darf deshalb grundsätzlich alle Daten speichern und verwenden, die er benötigt, um die ihm obliegende Darlegungs- und Beweislast in einem potentiellen Rechtsstreit um die Wirksamkeit einer Kündigung und/oder das Bestehen von Schadensersatzansprüchen zu erfüllen (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 22 mwN, BAGE 163, 239).

bb) Dabei kommt es auf die Frage, ob die rechtmäßige Erhebung von Daten (nur) auf § 32 Abs. 1 BDSG aF oder (zugleich) auf § 6b Abs. 1 Satz 1 Nr. 3 BDSG aF beruhte, nicht an. § 32 Abs. 1 Satz 1 BDSG aF stellt – wie bereits unter Rn. 33 dargestellt – auch für die Verarbeitung und Nutzung von personenbezogenen Daten eines Beschäftigten, die der Arbeitgeber durch eine Videoüberwachung öffentlich zugänglicher Räume erlangt hat, eine eigenständige, von den Voraussetzungen nach § 6b Abs. 3 BDSG aF unabhängige Erlaubnisnorm dar (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 23 mwN, BAGE 163, 239). Sofern nach § 32 Abs. 1 Satz 1 BDSG aF zulässig erhobene Daten den Verdacht einer Pflichtverletzung begründen, dürfen sie für die Zwecke und unter den Voraussetzungen des § 32 Abs. 1 Satz 1 BDSG aF auch verarbeitet und genutzt werden (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 22 mwN, aaO). Erst recht gilt das für die von § 6b BDSG aF nicht erfasste Datenerhebung im Bereich nicht öffentlich zugänglicher Räume (vgl. BAG 22. September 2016 – 2 AZR 848/15 – Rn. 43, BAGE 156, 370).

cc) Nach § 32 Abs. 1 Satz 1 BDSG aF hängt auch die Frage, ob personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet oder genutzt werden dürfen – ebenso wie die Zulässigkeit der Datenerhebung – davon ab, ob dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach der Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Auch die Verarbeitung und Nutzung der Daten steht unter dem Vorbehalt der Verhältnismäßigkeit, dh. sie muss geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen sein, um den erstrebten Zweck zu erreichen. Es dürfen keine anderen, zur Zielerreichung gleich wirksamen und das Persönlichkeitsrecht der Betroffenen weniger einschränkenden Mittel zur Verfügung stehen. Die Verhältnismäßigkeit im engeren Sinne (Angemessenheit) ist gewahrt, wenn die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht. Die Datenverarbeitung und -nutzung darf keine übermäßige Belastung für die Betroffenen darstellen und muss der Bedeutung des Informationsinteresses des Arbeitgebers entsprechen. Dies beurteilt sich ggf. für jedes personenbezogene Datum gesondert (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 24 mwN, BAGE 163, 239).

dd) Der bei der Anwendung von § 32 Abs. 1 Satz 1 BDSG aF herangezogene Verhältnismäßigkeitsgrundsatz genügt dem durch die Richtlinie 95/46/EG des europäischen Parlaments und

des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie Art. 7 der Charta der Grundrechte der europäischen Union und Art. 8 der europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten garantierten Schutzniveau für die von einer Datenerhebung Betroffenen (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 25 mwN, BAGE 163, 239).

ee) Ferner wird das Landesarbeitsgericht zu beachten haben, dass ausschließlich die Verarbeitung der relevanten Sequenzen zu beurteilen ist und nicht diejenige von Passagen, die nicht in den Rechtsstreit eingeführt werden sollen (vgl. BAG 23. August 2018 – 2 AZR 133/18 – Rn. 26, BAGE 163, 239).

(1) Die Speicherung von Bildsequenzen, die geeignet sind, den mit einer rechtmäßigen Videoaufzeichnung verfolgten Zweck zu fördern, bleibt, weil es sich oft um die einzigen, regelmäßig aber um die „zuverlässigsten" Erkenntnis- und Beweismittel handelt, grundsätzlich erforderlich, bis der Zweck entweder erreicht oder aufgegeben oder nicht mehr erreichbar ist. Die Eignung beurteilt sich objektiv. Sie besteht oder besteht nicht, unabhängig davon, ob der Arbeitgeber sie erkannt hat. Eine etwaige Pflicht, das gesamte Bildmaterial zeitnah zu sichten, würde allein dazu dienen, die – eindeutig – nicht zweckrelevanten Passagen zu identifizieren und zu löschen. Ihre Missachtung ließe den Bedarf an den zweckrelevanten Passagen nicht entfallen. Diese dürften auch nach einer „Bedarfsklärung" – zumindest vorerst – gespeichert bleiben (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 27 mwN, BAGE 163, 239).

(2) Das Landesarbeitsgericht hat bislang keine Tatsachen festgestellt, die den Schluss zuließen, dem Beklagten sei es mit der Speicherung der Videoaufzeichnungen am 17. und 19. Dezember 2015 sowie am 8., 13., 23. und 29. Januar 2016 nicht – mehr – darum gegangen, seine Rechte gegenüber der Klägerin aufgrund möglicher Pflichtverletzungen durchzusetzen. Es hat – im Gegenteil – selbst angenommen, dieser habe das Bildmaterial zu eben diesem Zweck bis in den Februar 2016 aufbewahrt. Der Zweck war auch nach wie vor erreichbar. Etwaige Kündigungsrechte waren noch nicht verwirkt und mögliche Schadensersatzansprüche weder verjährt noch – soweit ersichtlich – verfallen. Damit blieb die Speicherung der relevanten Sequenzen erforderlich.

(3) Eine noch erforderliche Speicherung von Aufzeichnungsteilen, die vorsätzliche Handlungen gegen das Eigentum oder das Vermögen des Arbeitgebers belegen (sollen), ist nur ganz ausnahmsweise unangemessen und damit nicht verhältnismäßig im engeren Sinne. Auch insoweit schließt sich der erkennende Senat den Ausführungen des Zweiten Senats des Bundesarbeitsgerichts in seinem Urteil vom 23. August 2018 (- 2 AZR 133/18 – Rn. 29 ff., BAGE 163, 239) an.

(a) Der rechtmäßig gefilmte Vorsatztäter ist in Bezug auf die Aufdeckung und Verfolgung seiner materiell-rechtlich noch verfolgbaren Tat nicht schutzwürdig. Er wird dies auch nicht durch bloßen Zeitablauf. Das allgemeine Persönlichkeitsrecht kann nicht zu dem alleinigen Zweck in Anspruch genommen werden, sich vor dem Eintritt von Verfall, Verjährung oder Verwirkung der Verantwortung für vorsätzlich rechtswidriges Handeln zu entziehen. Zugleich verliert das in Bezug auf vorsätzliche Schädigungshandlungen beträchtliche, durch Art. 12 und Art. 14 GG geschützte Verarbeitungs- und Nutzungsinteresse des Arbeitgebers nicht an Gewicht, solange die Rechtsverfolgung materiell-rechtlich nicht ausgeschlossen ist. Darüber hinaus ist zu beachten, dass gedeihliche Arbeitsvertragsbeziehungen von beiderseitigem Vertrauen getragen sein müssen. Dem widerspräche es, wenn der Arbeitgeber gezwungen wäre, die Aufzeichnungen aus einer offenen, vorrangig zu präventiven (Verhinderung von Pflichtverletzungen) und nur bei Verfehlung dieses Primärziels zu repressiven Zwecken (Aufklärung und Verfolgung von Pflichtverletzungen) eingesetzten Videoüberwachung laufend vollumfänglich einzusehen, um relevante Sequenzen weiterverarbeiten zu dürfen. Das hielte ihn zu ständigem Misstrauen an. Zugleich würde durch einen faktischen Zwang zu zeitnaher Aufdeckung und „Sanktionierung" von Pflichtverletzungen der Arbeitnehmerschutz durch die Vorgaben des Datenschutzrechts in sein Gegenteil verkehrt. Die Speicherung – nach wie vor – erforderlicher Sequenzen kann deshalb nur unangemessen sein, wenn das Verhalten des Arbeitgebers objektiv den Schluss zulässt, er wolle diese Passagen nicht allein zur Rechtsverfolgung verwenden. Es muss die greifbare Gefahr eines Missbrauchs personenbezogener Daten bestehen (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 30 mwN, BAGE 163, 239).

(b) So kann es zwar auch liegen, wenn Anhaltspunkte dafür bestehen, der Arbeitgeber wolle sich mögliche Kündigungsgründe oder zum Schadensersatz verpflichtende Sachverhalte „aufsparen", um dadurch den Arbeitnehmer unter Druck zu setzen (BAG 23. August 2018 – 2 AZR 133/18 – Rn. 31 mwN, BAGE 163, 239). Das Landesarbeitsgericht hat bislang keine Tatsachen festgestellt, die auf eine solche Absicht des Beklagten hindeuten könnten. Hierfür genügt es nicht, dass er mit der Auswertung der Videoaufzeichnungen vom 17. und 19. Dezember 2015 sowie vom 8., 13., 23. und 29. Januar 2016 gewartet hat, bis er dazu nach stichprobenartigen Überprüfungen der Warenaufschläge einen Anlass sah. Das gilt umso mehr, als er nach der Feststellung eines Warenschwunds „ohne Umschweife" mit der Analyse des Bildmaterials begonnen und anschließend unverzüglich die Beendigung des Arbeitsverhältnisses mit der Klägerin betrieben hat.

Heimliche Videoaufnahme zur Aufdeckung von Mißständen im Pflegeheim (Ls)

(**Oberlandesgericht Dresden**, Urteil vom 24. September 2019 – 4 U 1401/19 –)

1. **Bei heimlichen Bild- und Tonaufnahmen spricht eine Vermutung für deren Unzulässigkeit. Im Einzelfall kann aber das Interesse, auf einen Missstand hinzuweisen dem Anspruch der Betroffenen auf Schutz ihrer Rechte am Bild und am gesprochenen Wort vorrangig sein.**

2. **Wird in einem Altenheim eine rechtswidrige Verabreichung von Medikamenten in verpixelter Form und unter Verfremdung der Stimme dokumentiert und anschließend bei einem Fernsehsender publiziert, kann das auf Grund des Interesses, auf diesen offensichtlichen Missstand hinzuweisen, berechtigt sein. Die betroffene Mitarbeiterin ist in der konkreten Situation nicht vergleichbar schutzbedürftig wie ein Bewohner der Einrichtung, zumal sie nicht erkennbar dargestellt wird.**

(nicht amtliche Leitsätze)

Freiwilligkeit einer Einwilligung zur Werbung bei Koppelung mit Gewinnspielteilnahme

(**Oberlandesgericht Frankfurt/M.**, Urteil vom 27. Juli 2019 – 6 U 6/19 –)

Ist die Teilnahme an einem Gewinnspiel von der Einwilligung in den Erhalt künftiger E-Mail-Werbung abhängig gemacht worden, bestehen gegen die Wirksamkeit dieser Einwilligung jedenfalls dann keine Bedenken, wenn der Verbraucher der Werbung durch nicht mehr als acht konkret bezeichnete Unternehmen zugestimmt hat und der Geschäftsbereich des werbenden Unternehmens hinreichend klar beschrieben worden ist (im Streitfall: „Strom & Gas"). Die Einwilligung in die Werbung dieses Unternehmens ist auch unabhängig davon wirksam, ob der Geschäftsbereich der anderen bezeichneten Unternehmen ausreichend klar beschrieben worden ist.

Aus den Gründen:

„Freiwillig" ist gleichbedeutend mit „ohne Zwang" iSd des Art. 2 lit. h RL 95/46/ EG (engl. beide Male „freely"). Der Betroffene muss also eine echte oder freie Wahl haben und somit in der Lage sein, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (Erwägungsgrund 42 DS-GVO). Insbesondere darf auf den Betroffenen kein Druck ausgeübt werden. Ein bloßes Anlocken durch Versprechen einer Vergünstigung, etwa – wie hier – einer Teilnahme an einem Gewinnspiel, reicht dafür aber nicht aus (Köhler/Bornkamm/Feddersen/Köhler, 37. Aufl. 2019, UWG § 7 Rn. 149 f.) Einer Freiwilligkeit steht nach der Rechtsprechung des Senats (vgl. GRUR-RR 2016, 421 – Überschaubare Partnerliste, juris-Rn. 18; GRUR-RR 2016, 252 – Partnerliste, juris-Rn. 24) nicht entgegen, dass die Einwilligungserklärung mit der Teilnahme an einem Gewinnspiel verknüpft ist. Der Verbraucher kann und muss selbst entscheiden, ob ihm die Teilnahme die Preisgabe seiner Daten „wert" ist.

Amt des Datenschutzbeauftragten neben dem Amt als Vorsitzender des Betriebsrats möglich

(**Landesarbeitsgericht Sachsen**, Urteil vom 19. August 2019 – 9 Sa 268/18 n. rk. –)

1. **Die Anweisung einer Datenschutzaufsichtsbehörde kann nur Wirkung entfalten für in ihrem Zuständigkeitsgebiet ansässige Verantwortliche. Mit dem „Verlangen der Aufsichtsbehörde" i. S. d. § 4 f Abs. 3 Satz 4 BDSG a. f. kann daher nur das Verlangen der zuständigen Aufsichtsbehörde gemeint sein.**
2. **Wird jemand infolge von Mehrfachbestellungen als sog. Konzerndatenschutzbeauftragter tätig, wäre die – gegen den Willen des Beauftragten erfolgte – Beendigung von einen Teil der Bestellungen und damit die Beendigung des Konzepts eines konzerneinheitlichen Datenschutzbeauftragten kein wichtiger Grund, auch die anderen Bestellungen zu beenden.**
3. **Im Anschluss an die Rechtsprechung des BAG zum Verhältnis von Datenschutzbeauftragten und Betriebsratsmitgliedschaft sieht das Gericht keine Inkompatibilität zwischen den Ämtern auch dann, wenn der Datenschutzbeauftragte die Funktion des Betriebsratsvorsitzen wahrnimmt.**

(nicht amtliche Leitsätze)

Sachverhalt:

Zwischen den Parteien besteht Streit darüber, ob der Kläger unter dem Datum des 16.06.2015 wirksam als Beauftragter für Datenschutz bei der Beklagten bestellt wurde oder die Rechtsstellung als Beauftragter für Datenschutz durch den Widerruf der Beklagten vom 01.12.2017 bzw. vorsorgliche Abberufung vom 25.05.2018 beendet wurde.

Der am ...1972 geborene Kläger ist seit dem 01.01.2009 bei der Beklagten beschäftigt. Die Betriebszugehörigkeit ist seit dem 01.11.1993 anerkannt worden. Der Kläger ist in der Funktion als freigestellter Betriebsratsvorsitzender der Beklagten sowie als stellvertretender Gesamtbetriebsratsvorsitzender in allen drei ... Unternehmen in ... tätig.

Die Beklagte ist Teil des ... Konzerns und 100%ige Tochtergesellschaft der ... GmbH (vormals AG), welche wiederum eine 100%ige Tochtergesellschaft der ... mit Sitz in ... ist. Vorstand der ... ist Herr ..., der zugleich auch Vorstandsvorsitzender der ... (... AG) mit Sitz in ... ist, der Muttergesellschaft der Beklagten.

Der Kläger wurde von der Beklagten und den weiteren in Deutschland ansässigen Gesellschaften ... GmbH, ... GmbH und ... GmbH mit Wirkung zum 01.06.2015 zum Datenschutzbeauftragten bestellt mit dem Ziel, einen konzerneinheitlichen Datenschutzstandard zu erreichen. Aus diesen Gründen erfolgte die Bestellung des Klägers als betrieblicher Datenschutzbeauftragter bei der Beklagten und als externer Datenschutzbeauftragter bei der ... GmbH (vormals AG), der ... GmbH und der ebenfalls in ... ansässigen ... GmbH.

In Auswertung der Umfrage bei Unternehmen mit mehr als 50 Arbeitnehmern zum Thema Datenübermittlung ins außer europäische Ausland und zum betrieblichen Datenschutzbeauftragten richtete sich der .Thüringer Landesbeauftragte für Datenschutz und Informationsfreiheit (TLfDI) mit Schreiben vom 04.09.2017 an die Muttergesellschaft der Beklagten – die ... GmbH (vormals AG) – unter Bezug auf § 4 f Abs. 2 BSDG mit dem Hinweis, dass bei der Bestellung des betrieblichen Datenschutzbeauftragten beachtet werden müsse, dass der Kandidat die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitze. Aufgrund der hauptberuflichen Tätigkeit des Datenschutzbeauftragten als Betriebsratsvorsitzender wurde die Auffassung vertreten, dass Zweifel bestünden hinsichtlich der Zuverlässigkeit aufgrund bestehender Interessenkollisionen. Hierzu hat die ... GmbH (vormals AG) mit Schreiben vom 27.09.2017 Stellung genommen und unter Bezug auf das Urteil des BAG vom 23.03.2011 – 10 AZR 562/09 – die Auffassung vertreten, dass keine Inkompatibilität seitens des Klägers vorliege und von einer Eignung als betrieblicher Datenschutzbeauftragter auszugehen sei.

Daraufhin hat der TLfDI mit Schreiben vom 24.11.2017 unter Bezug auf § 4 f BDSG nunmehr die Feststellung getroffen, dass der Kläger nicht über die notwendige Zuverlässigkeit verfüge, die für die Bestellung eines betrieblichen Datenschutzbeauftragten notwendig sei. Es wird ausgeführt, eine Inkompatibilität mit dem Amt des Betriebsratsvorsitzenden liege vor. Hervorgehoben durch Fettschrift wird erklärt: „Herr ... ist nicht wirksam als betrieblicher Da-

tenschutzbeauftragter bestellt worden. ... AG hat demnach seit dem 01.06.2015 keinen bDSG." Es wurde nochmals die Gelegenheit gegeben, bis zum 03.01.2018 zum Sachverhalt Stellung zu nehmen. Des Weiteren wird in dem Schreiben erklärt, dass mit Ablauf dieser Frist der Betrieb damit rechnen müsse, dass der Landesbeauftragte die verantwortliche Stelle verpflichte, einen nach § 4 f BDSG geeigneten betrieblichen Datenschutzbeauftragten zu bestellen. Ferner wurde darauf hingewiesen, dass nach § 43 Abs. 1 BDSG ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 4 f Abs. 1 Satz 1 oder 2 einen Beauftragten für Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt. Diese Ordnungswidrigkeit könne mit einer Geldbuße bis 50.000,00 € geahndet werden.

Im Anschluss an dieses Schreiben wurde dem Kläger mit Schreiben vom 01.12.2017 unter Bezugnahme auf die Erklärung der Landesbehörde mitgeteilt, dass eine wirksame Bestellung als betrieblicher Datenschutzbeauftragter zu keinem Zeitpunkt gegeben gewesen sei und zur Vermeidung eines Bußgeldes der Aufforderung des TLfDI unverzüglich Folge geleistet und ein geeigneter Datenschutzbeauftragter bestellt werde. Hilfsweise wurde die Bestellung des Klägers zum Datenschutzbeauftragten vom 16.06.2015 nach § 4 f Abs. 3 Satz 4 BDSG für alle vier Unternehmen mit sofortiger Wirkung zum 01.12.2017 widerrufen. Der Kläger hat den Empfang des Schreibens am 01.12.2017 durch Unterschrift bestätigt.

Als neue Datenschutzbeauftrage ist sodann mit Wirkung zum 01.12.2017 Frau .XX.. für alle deutschen Standorte der Unternehmen bestellt worden.

Nach dem Inkrafttreten der DS-GVO wurde der Kläger mit einem weiteren Schreiben der Beklagten vom 25.05.2018 aus betriebsbedingten Gründen gemäß Art. 38 Abs. 3 Satz 2 DS-GVO vorsorglich als Datenschutzbeauftragter abberufen.

Hiergegen wendet sich der Kläger mit vorliegender Klage.

Er hat erstinstanzlich die Auffassung vertreten, am 16.06.2015 wirksam zum Datenschutzbeauftragten bestellt und durch die Schreiben vom 01.12.2017 und vom 25.05.2018 auch nicht wirksam abberufen worden zu sein.

Der Kläger hat erstinstanzlich zuletzt beantragt,

1. festzustellen, dass seine Rechtstellung als Beauftragter für den Datenschutz der Beklagten nicht durch den Widerruf der Beklagten vom 01.12.2017 beendet worden ist,

2. festzustellen, dass seine Rechtstellung als Beauftragter für den Datenschutz der Beklagten auch nicht durch den Widerruf der Beklagten vom 25.05.2018 beendet worden ist.

Die Beklagte hat beantragt, die Klage abzuweisen.

Sie hat erstinstanzlich die Ansicht vertreten, dass sich die durch die für die Kontrolle der Durchführung des Datenschutzes zuständige Aufsichtsbehörde getroffene Feststellung, dass der Kläger nicht wirksam als betrieblicher Datenschutzbeauftragter bestellt worden sei, der arbeitsgerichtlichen Überprüfung entziehe. Weder die Parteien noch die Arbeitsgerichte seien zur Überwachung und Einhaltung des Bundesdatenschutzgesetzes berufen.

Im Übrigen sei der Ansicht des Landesbeauftragten, demzufolge dem Kläger als Betriebsratsvorsitzender die Zuverlässigkeit als Datenschutzbeauftragter fehle, beizutreten. Da der Kläger als Betriebsratsvorsitzender nach § 80 Abs. 1 BetrVG den betrieblichen Datenschutz zu überwachen habe, er jedoch auch gleichzeitig konzernweiten Datenschutz entwickeln müsse, verstoße dies gegen den Grundsatz, dass niemand „Richter in eigener Sache“ sein dürfe.

Unabhängig von der Wirksamkeit der Bestellung sei eine solche durch das Schreiben vom 01.12.2017 aber jedenfalls wirksam widerrufen worden. Das im Schreiben des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit vom 24.11.2017 zum Ausdruck gebrachte Abberufungsverlangen stelle einen wichtigen Grund für die Abberufung dar. Der Umstand, dass nicht die sächsische Aufsichtsbehörde, sondern der thüringische Datenschutzbeauftragte die Abberufung verlangt habe, sei irrelevant, da die Thüringer Behörde die für die Muttergesellschaft zuständige Behörde sei. Ein weiterer wichtiger Grund sei darin zu sehen, dass der Wegfall des Klägers als betrieblicher Datenschutzbeauftragter für die ...er Gesellschaften des ... Konzerns wegen des Verlangens der Aufsichtsbehörde dazu geführt habe, dass die Muttergesellschaft keinen konzernweiten einheitlichen Datenschutzbeauftragten mehr habe und dieses Ziel deshalb nicht mehr umgesetzt werden könne.

Sofern man auch dies anders sehen wolle, so sei der Kläger aber jedenfalls spätestens durch das Schreiben vom 25.05.2018 wirksam als Datenschutzbeauftragter abberufen worden. Nach Art. 38 Abs. 3 Satz 2 der am 25.05.2018 in Kraft getretenen DS-GVO dürfe ein Datenschutzbeauftragter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Im Umkehrschluss folge hieraus, dass ein Datenschutzbeauftragter aus betriebsbedingten Gründen sehr wohl abberufen werden dürfe. Das Arbeitsgericht XX. habe zwischenzeitlich entschieden, dass der Kläger bei der ...er Muttergesellschaft und der Schwestergesellschaft X jedenfalls am 01.12.2017 wirksam als Datenschutzbeauftragter abberufen worden sei. Deshalb lasse sich der strategische Ansatz der Bestellung eines konzerneinheitlichen Datenschutzbeauftragten in Person des Klägers nicht mehr verwirklichen. Dies stelle einen betriebsbedingten Grund für die Abberufung des Klägers als Datenschutzbeauftragter auch bei der Beklagten dar.

Mit Urteil vom 27.06.2018 hat das Arbeitsgericht Dresden nach den Klageanträgen erkannt. Wegen der Einzelheiten dieser Entscheidung wird auf das Urteil (Bl. 127 bis 136 d. A.) Bezug genommen.

Gegen das ihr am 19.07.2018 zugestellte Urteil des Arbeitsgerichts hat die Beklagte am 23.07.2018 Berufung eingelegt und diese – nach Verlängerung der Berufungsbegründungsfrist bis zum 19.10.2018 – mit am 08.10.2018 beim Landesarbeitsgericht eingegangenem Schriftsatz begründet.

Unter Vertiefung ihres erstinstanzlichen Vortrags greift die Beklagte das Urteil des Arbeitsgerichts im Wesentlichen mit Rechtsausführungen an.

Es verbleibe dabei, dass der Kläger bereits nicht wirksam zum Datenschutzbeauftragten bestellt worden sei. Der betriebliche Datenschutzbeauftragte könne nicht kraft gesetzlichen Auftrags auf der einen Seite als Berater des Arbeitgebers als für den Datenschutz verantwortliche Stelle agieren und auf der anderen Seite als Betriebsratsmitglied die Einhaltung des Datenschutzes überwachen. Unterrichtung und Beratung der i. S. d. Datenschutzrechts verantwortlichen Stelle einerseits und Überwachung der für den Datenschutz verantwortlichen Stelle andererseits würden sich ausschließen, da der Kläger ansonsten als Mitglied des Betriebsrats selbst zu prüfen habe, ob aufgrund seiner Unterrichtung und Beratung implementierte Datenschutzregelungen rechtskonform seien. Entgegen der Ansicht des Arbeitsgerichts liege damit sehr wohl eine Inkompatibilität vor.

Eine entgegen dem soeben Gesagten doch wirksame Bestellung des Klägers zum betrieblichen Datenschutzbeauftragten habe dann aber jedenfalls durch den Widerruf vom 01.12.2017 sein Ende gefunden. Es liege ein wichtiger Grund i. S. d. § 626 BGB vor und zudem auch ein Abberufungsverlangen durch die ... Aufsichtsbehörde i. S. d. § 4 f Abs. 3 Satz 4 BDSG a. f.

Unabhängig hiervon sei der Kläger von seiner Stellung als Datenschutzbeauftragter der Beklagten dann aber jedenfalls durch den Widerruf vom 25.05.2018 abberufen worden. Zu Unrecht stelle das Arbeitsgericht insoweit darauf ab, dass gemäß den §§ 38 Abs. 2, 6 Abs. 4 Satz 1 BDSG n. f. auch nach Inkrafttreten der DS-GVO eine Abberufung des Datenschutzbeauftragten nur in entsprechender Anwendung des § 626 BGB zulässig sei. Richtig sei vielmehr, dass nach Art. 38 Abs. 3 Satz 2 DS-GVO bereits ein betriebsbedingter Grund für die Abberufung des Klägers ausreiche

und ein solcher, da sich die von Anfang an verfolgte Intention der Bestellung eines konzerneinheitlichen Datenschutzbeauftragten nunmehr nicht mehr aufrechterhalten lasse, zweifelsfrei auch gegeben sei.

Die Beklagte beantragt, das Urteil des Arbeitsgerichts Dresden vom 27.06.2018 – 10 Ca 234/18 – abzuändern und die Klage abzuweisen.

Der Kläger beantragt, die Berufung zurückzuweisen.

Den Überlegungen des Arbeitsgerichts in der angefochtenen Entscheidung pflichtet er bei, den Ausführungen der Beklagten im Berufungsrechtszug tritt er entgegen.

Aus den Gründen:

Die gemäß § 64 Abs. 1 und 2 ArbGG statthafte, gemäß den §§ 66 Abs. 1, 64 Abs. 6 Satz 1 ArbGG, 519, 520 ZPO form- und fristgerecht eingelegte und begründete, insgesamt daher zulässige Berufung der Beklagten hat in der Sache keinen Erfolg. Zu Recht und mit im Wesentlichen zutreffender Begründung hat das Arbeitsgericht nach den Klageanträgen erkannt. Der Vortrag der Beklagten im Berufungsrechtszug rechtfertigt auch in seiner Gesamtheit keine andere Beurteilung. Zusammenfassend gilt insoweit Folgendes:

1. Mit Schreiben vom 16.06.2015 wurde der Kläger wirksam zum Datenschutzbeauftragten der Beklagten bestellt.

Hieran bestehen für die Kammer keine ernsthaften Zweifel. Der Einwand der Beklagten, die Unwirksamkeit der Bestellung des Klägers als Datenschutzbeauftragter folge daraus, dass dieser nicht über die notwendige Zuverlässigkeit verfüge, die für die Bestellung notwendig sei, insoweit liege eine Inkompatibilität mit dem Amt des Betriebsratsvorsitzenden vor, überzeugt dagegen nicht. Das Bundesarbeitsgericht hat mit Urteil vom 23.03.2011 (– 10 AZR 562/09 [BB 2011, 2683 m. BB-Komm. Wybitul] –, AP Nr. 3 zu § 4 f BDSG m. w. N.) ausdrücklich festgestellt, dass die bloße Mitgliedschaft im Betriebsrat diese Person für das Amt des Beauftragten für den Datenschutz nicht unzuverlässig macht und insoweit grundsätzlich keine Inkompatibilität zwischen diesen beiden Ämtern besteht, und diese Rechtsauffassung auch ausführlich begründet. Dieser höchstrichterlichen Rechtsprechung schließt sich die erkennende Kammer ausdrücklich an. Warum vorliegend etwas anderes gelten soll, nur weil der Kläger nicht „einfaches" Betriebsratsmitglied ist, sondern Betriebsratsvorsitzender, erschließt sich dem Gericht ebenfalls nicht. Warum dies einen Unterschied machen soll, wird auch weder von der Beklagten noch vom ... Landesbeauftragten für den Datenschutz und die Informationsfreiheit, der ebenfalls dieser Auffassung zu sein scheint, näher begründet.

2. Die hiernach wirksame Bestellung des Klägers zum betrieblichen Datenschutzbeauftragten hat auch nicht aufgrund des Widerrufs vom 01.12.2017 sein Ende gefunden. Nach alter, am 01.12.2017 geltender Rechtslage konnte gemäß § 4 f Abs. 3 Satz 4 BDSG a. f. die Bestellung zum Beauftragten für den Datenschutz entweder in entsprechender Anwendung von § 626 BGB oder bei nicht öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde widerrufen werden.

Weder von dem einen noch von dem anderen kann jedoch vorliegend ausgegangen werden.

a) Die Beklagte kann sich vorliegend nicht mit Erfolg darauf berufen, der Widerruf sei „auf Verlangen der Aufsichtsbehörde" erfolgt.

aa) Dabei kann dahingestellt bleiben, ob in dem Schreiben des ThürLfDI. an die Muttergesellschaft der Beklagten, also die .XX AG, ein solches Verlangen auf Widerruf der Bestellung hinreichend klar zum Ausdruck kommt. Wenn man dies – und hierfür sprechen gute Gründe – mit der Beklagten annehmen wollte, so bleibt gleichwohl zu konstatieren, dass ein solches Verlangen der Aufsichtsbehörde ausschließlich in Bezug auf die Schwestergesellschaft X und die Muttergesellschaft der Beklagten zum Ausdruck gebracht wurde, nicht hingegen gegenüber der Beklagten. Dies verwundert nicht, weil der TLfDI selbstredend nur für Thüringen zuständig ist, der Freistaat Sachsen hingegen über einen eigenen Datenschutzbeauftragten verfügt. Unstreitig hat dieser jedoch der Beklagten gegenüber kein Verlangen auf Widerruf der Bestellung des Klägers zum Datenschutzbeauftragten zum Ausdruck gebracht.

bb) Entgegen der Auffassung der Beklagten ist es auch nicht „aus Gründen der Rechtssicherheit" geboten, das vom ... Datenschutzbeauftragten gegenüber der in ... ansässigen Muttergesellschaft der Beklagten zum Ausdruck gebrachte Abberufungsverlangen – in welcher Form auch immer – auf die Beklagte zu übertragen.

Das Argument der Beklagten, was in ... auf Grundlage bundeseinheitlicher Regelung rechtmäßig sei, nämlich der Widerruf der Bestellung, könne in Sachsen auf Grundlage der identischen bundeseinheitlichen Regelung bei gleicher Sachverhaltskonstellation nicht unzulässig sein, greift zu kurz. Es gibt gerade keine gleiche Sachverhaltskonstellation, und dies bereits deshalb nicht, weil der Sächsische Datenschutzbeauftragte – im Gegensatz zu seinem Kollegen – ein Widerrufsverlangen unstreitig zu keiner Zeit auch nur im Ansatz geäußert hat. Man stelle sich nur mal vor, der Sächsische Datenschutzbeauftragte sei insoweit bewusst nicht aktiv geworden, weil er – in Übereinstimmung mit der Rechtsprechung des Bundesarbeitsgerichts und im Gegensatz zum ...Thüringer Datenschutzbeauftragten – eine grundsätzliche Inkompatibilität zwischen dem Amt des Datenschutzbeauftragten und dem des Betriebsratsvorsitzenden gerade nicht zu erkennen vermochte: Folgte man der Auffassung der Beklagten, so wäre auch in diesem Fall für die Beklagte mit Sitz in X nicht das fehlende Verlangen des Sächsischen Datenschutzbeauftragten, sondern das vom Kollegen aus Thüringen ausschließlich gegenüber den Mutter- bzw. Schwestergesellschaften der Beklagten zum Ausdruck gebrachte Verlangen maßgeblich. Dieses Beispiel zeigt, dass die Argumentation der Beklagten unmöglich richtig sein kann. Mit "Verlangen der Aufsichtsbehörde" i. S. d. § 4 f Abs. 3 Satz 4 BDSG a. f. kann daher nur das Verlangen der zuständigen Aufsichtsbehörde gemeint sein. Ein Verlangen des Sächsischen Datenschutzbeauftragten, die Bestellung des Klägers zum Datenschutzbeauftragten zu widerrufen, hat es gegenüber der Beklagten jedoch unstreitig zu keiner Zeit gegeben.

b) Für den Widerruf der Bestellung des Klägers zum Datenschutzbeauftragten vom 01.12.2017 kann sich die Beklagte auch nicht mit Erfolg auf eine entsprechende Anwendung von § 626 BGB berufen.

aa) Aufgrund der Verweisung in § 4 f Abs. 3 Satz 4 BDSG a. f. muss für die Abberufung ein wichtiger Grund vorliegen, der es der Beklagten aufgrund von Tatsachen und unter Berücksichtigung der Gegebenheiten des Einzelfalls sowie unter Abwägung der Interessen beider Vertragsteile unzumutbar macht, den Kläger als betrieblichen Datenschutzbeauftragten auch nur bis zum Ablauf der ordentlichen Kündigungsfrist weiterhin einzusetzen. Als wichtige Gründe kommen insbesondere solche in Betracht, die mit der Funktion und Tätigkeit des Datenschutzbeauftragten zusammenhängen und eine weitere Ausübung dieser Tätigkeit unmöglich machen oder sie zumindest erheblich gefährden, beispielsweise ein Geheimnisverrat oder eine dauerhafte Verletzung der Kontrollpflichten als Datenschutzbeauftragter (vgl. BAG, Urteil vom 23.03.2011 – 10 AZR 562/09 –, a. a. O. m. w. N.).

bb) Ein wichtiger Grund in diesem Sinne liegt nicht vor.

(1) Das Schreiben des ThürLfDI an die Muttergesellschaft der Beklagten vom 24.11.2017 stellt jedenfalls keinen wichtigen Grund dar. Insoweit kann auf obige Ausführungen auf den Seiten 10 f. verwiesen werden. Für die im Freistaat Sachsen ansässige Beklagte gibt es ein solches Verlangen nicht, und zwar bereits nicht vom Thüringer Landesbeauftragten und erst recht nicht vom Sächsischen Datenschutzbeauftragten.

(2) Ein wichtiger Grund ist auch nicht darin zu sehen, dass die Beklagte ihr Konzept eines konzerneinheitlichen Datenschutzbeauftragten nicht mehr verwirklichen kann.

Es mag sein, dass die Bestellung ein und desselben Datenschutzbeauftragten für alle in Deutschland ansässigen Gesellschaften des Konzerns zum Ziel hatte, konzerneinheitliche Datenschutzstandards zu erreichen, Datenschutzbestimmungen konzerneinheitlich zu verwirklichen und einheitliche Datenschutzkonzepte zu entwickeln und umzusetzen. Die Bestellung ein und derselben Person konzernweit mag insoweit wohl überlegt, sinnvoll und auch nützlich sein. Die Gefährdung dieses Ziels durch den Widerruf der Bestellung des Klägers als Datenschutzbeauftragten für die in ... ansässigen Gesellschaften stellt jedoch keinen wichtigen Grund dar, auch seine Bestellung zum Beauftragten für den Datenschutz für die Beklagte zu widerrufen. Zwar mag die Beklagte ihr ursprüngliches Ziel, nämlich durch Bestellung ein- und derselben Person als Datenschutzbeauftragten konzerneinheitliche Datenschutzstandards zu gewährleisten, nicht mehr erreichen. Dies hat jedoch nichts zu tun mit der Funktion und Tätigkeit des Klägers als Datenschutzbeauftragter für die Beklagte. Dass die Abberufung bei einigen Gesellschaften des Konzerns eine weitere Ausübung der Tätigkeit des Klägers als Datenschutzbeauftragter für die Beklagte unmöglich machen oder sie zumindest erheblich gefährden würde, ist nicht ersichtlich und wird auch von der Beklagten nicht behauptet.

3. Schließlich erweist sich auch der Widerruf der Bestellung vom 25.05.2018 nach § 38 Abs. 2 i. V. m. § 6 Abs. 4 BDSG n. f. als unwirksam.

a) Die Abberufung des Datenschutzbeauftragten ist in der DS-GVO nicht geregelt. In Art. 38 Abs. 3 Satz 2 findet sich lediglich der Verweis, dass der Datenschutzbeauftragte nicht wegen der Erfüllung seiner Aufgaben abberufen oder benachteiligt werden darf. Damit ist aber nicht geregelt, unter welchen Voraussetzungen eine Abberufung des Datenschutzbeauftragten tatsächlich erfolgen kann. Der deutsche Bundesgesetzgeber hat die Abberufung des betrieblichen oder behördlichen Datenschutzbeauftragten in Anlehnung an das bisherige Recht in § 6 Abs. 4 und § 38 Abs. 2 BDSG n. f. geregelt. Da die Art. 37 bis 39 DS-GVO keine Öffnungsklausel für die Mitgliedsstaaten enthalten, ist die Regelungskompetenz für dieses Vorgehen zwar nicht unproblematisch (ähnlich Drewes in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 37 Rn. 58). Mit dem Bundesgesetzgeber vertritt die Berufungskammer allerdings insoweit die Auffassung, dass es sich jedenfalls bei dem besonderen Abberufungs- und Kündigungsschutz eines betrieblichen, also nicht öffentlichen Datenschutzbeauftragten um eine arbeitsrechtliche Regelung handelt, die ergänzend zu den Vorgaben der Verordnung (EU) 2016/679 auch im BDSG n. f. beibehalten werden kann (vgl. hierzu auch BT-Drs. 18/11325 S. 82).

b) Nach § 6 Abs. 4 Satz 1 i. V. m. § 38 Abs. 2 BDSG n. f. ist die Abberufung eines privaten Datenschutzbeauftragten allerdings nur in entsprechender Anwendung des § 626 BGB zulässig. Wie oben auf den Seiten 12 f. bereits dargelegt, kann sich die Beklagte auf einen solchen wichtigen Grund jedoch nicht mit Erfolg berufen. Das Bestreben der Beklagten, durch Bestellung ein- und derselben Person als Datenschutzbeauftragten konzerneinheitliche Datenschutzstandards zu erreichen, mag einen betrieblichen Grund darstellen, aber keinen wichtigen Grund i. S. d. § 626 Abs. 1 BGB.

5. Nach § 72 Abs. 2 Nr. 1 ArbGG war für die Beklagte die Revision zuzulassen. Soweit ersichtlich ist insbesondere die Frage, ob § 6 Abs. 4 Satz 1 i. V. m. § 38 Abs. 2 BDSG n. f. mit Art. 38 Abs. 3 Satz 2 DS-GVO vereinbar ist, höchstrichterlich noch ungeklärt.

Nichtigkeit der Abtretung ärztlicher Forderung bei Verletzung der Schweigepflicht

(**Landessozialgericht Thüringen**, Beschluss vom 26. August 2019 – L 1 JVEG 691/19 –)

Die Abrechnung einer ärztlichen Begutachtung durch einen gerichtlichen Sachverständigen unter Heranziehung einer privatärztlichen Verechnungsstelle führt ohne Einwilligung des Betroffenen wegen Verstoßes gegen die ärztliche Schweigepflicht nach § 203 Abs. 1 Nr. 1 StGB zur Nichtigkeit der Abtretung (§ 134 BGB).

(nicht amtlicher Leitsatz)

Sachverhalt:

Mit Beweisanordnung vom 28. November 2018 beauftragte die Berichterstatterin des 3. Senats im Verfahren L 3 R 845/18 den Chefarzt der Klinik für Psychiatrie Dr. D. mit der Erstellung eines Sachverständigengutachtens. Eine testpsychologische Zusatzbegutachtung wurde genehmigt. Dr. D. erstattete am 7. März 2019 sein Gutachten.

Mit am 22. März 2019 beim Thüringer Landessozialgericht eingegangener „Rechnungserstellung im Auftrag von Herrn Dr. med. S. D." vom 21. März 20198 machte eine ärztliche Verrechnungsstelle, für das Gutachten einen Betrag i.H.v. 4.394,06 € geltend.

Aus den Gründen:

Der Anspruch auf Sachverständigenentschädigung nach dem JVEG steht dem beauftragten Sachverständigen zu. Eine Abtretung komm nur unter Beachtung der ärztlichen Schweigepflicht in Betracht. Insoweit bedürfte die Weitergabe von Behandlungsdaten an privatärztliche Verrechnungsstellen einer Einwilligung des begutachteten Betroffenen. Liegt diese nicht vor, führt dies nach § 134 des Bürgerlichen Gesetzbuches (BGB) zur Nichtigkeit der Abtretung.

Zum Zeitpunkt der Beurteilung datenschutzbehördlicher Anordnungen (Ls)

(**Oberverwaltungsgericht Saarlouis**, Beschluss vom 10. September 2019 – 2 A 174/18 –)

1. **Nach der Rechtsprechung des Bundesverwaltungsgerichts (Urteil vom 27.3.2019 – 6 C 2/18 – in NVwZ 2019, 1126 – 1132; juris) ist die Rechtmäßigkeit von**

Anordnungen zur Beseitigung datenschutzrechtlicher Verstöße nach § 38 Abs. 5 Satz 1 BDSG a.F. nach der Rechtslage zu beurteilen, die zum Zeitpunkt der letzten behördlichen Entscheidung gilt, und nachträgliche Rechtsänderungen sind nicht zu berücksichtigen.

2. **Dass in Bezug auf die Ermächtigungsgrundlage des § 38 Abs. 5 Satz 2 BDSG a.F. ausnahmsweise ein anderer rechtlicher Beurteilungszeitpunkt als bei der Vorschrift des § 38 Abs. 5 Satz 1 BDSG a.F. zugrunde zu legen wäre, erschließt sich nicht, denn sowohl Anordnungen nach § 38 Abs. 5 Satz 1 BDSG a.F. als auch Anordnungen nach § 38 Abs. 5 Satz 2 BDSG a.F. stehen gleichermaßen im Ermessen der zuständigen Aufsichtsbehörde.**

Rechtsverletzung durch Betrieb von Google Analytics ohne „anonymizeIP“

(**Landgericht Dresden**, Urteil vom 11. Januar 2019 – 1a O 1582/18 –)

Die Nutzung von Google Analytics ohne den Zusatz "anonymizeIP" verstößt gegen geltendes Datenschutzrecht. Der Betroffene kann untersagen, seine IP-Adresse zu speichern und an die Google Inc. zu übermitteln, wenn auf der vom ihm besuchten Webseite der Tracking-Dienst Google Analytics genutzt wird, ohne dabei gleichzeitig die Code-Erweiterung „anonymisiert“ zu verwenden.

(nicht amtlicher Leitsatz)

Sachverhalt:

Der Kläger begehrt Unterlassung und Erstattung von Rechtsanwaltskosten wegen unerlaubter Weitergabe personenbezogener Daten durch die Beklagte an Google Inc.

Die Beklagte bietet dem Internetportal (...) Dienste an und war Inhaberin des Google Analytics Kontos (...). Sie fügte in ihrem Internetauftritt den Tracking-Dienst Google Analytics ein.

Mit diesem Dienst werden Daten über Aktivitäten der Nutzer der Internetpräsenz überwacht und in Echtzeit dem Anbieter Google zur Auswertung zur Verfügung gestellt. Damit erhält der Anbieter Google auch die IP-Adressen der Webseitenbesucher. Weil die Übermittlung der IP-Adressen seit vielen Jahren von Datenschützern als unzulässig eingestuft wird, sieht der Tracking-Dienst Google Analytics die Möglichkeit vor, durch den Quellcode-Zusatz "anonymisiert" die letzten 8 Bit einer IP-Adresse zu löschen und dadurch die IP-Adressen zu anonymisieren.

Der Kläger besuchte am 24. März 2018 die Webpräsenz der Beklagten. Dabei stellte der Kläger fest, dass nicht nur der Tracking-Dienst Google Analytics eingebunden war, sondern dieser auch benutzt wurde, ohne den Quellcode-Zusatz "anonymisiert" zu verwenden.

Der Kläger verlangte von der Beklagten mit E-Mail vom 24. März 2018 (Anlage K 3) fruchtlos die Abgabe einer Unterlassungserklärung und verlangte Auskunft über die zu seiner Person gespeicherten Daten. Deshalb verlangte der Kläger mit anwaltlichem Schreiben vom 18. April 2018 (Anlage K 2) die Abgabe einer strafbewehrten Unterlassungserklärung, Auskunftserteilung und forderte die Beklagte auf, die anwaltlichen Kosten zu erstatten.

Die Beklagte gab weder eine Unterlassungserklärung ab, noch erteilt sie die Auskunft.

Der Kläger geht als Privatperson häufig gegen Datenschutzverstöße vor und verlangt, wie im vorliegenden Fall, zunächst ohne anwaltliche Hilfe eine Unterlassungserklärung.

Die Beklagte hat das Tool Google Analytics von der Webseite genommen.

Der Kläger behauptet, die Beklagte habe seine IP-Adresse bei seinem Webseitenbesuch bei der Beklagten vollständig an Google Inc. übermittelt. Die Beklagte als verantwortliche Stelle habe davon genaue Kenntnis gehabt und wusste, was sie zur Anonymisierung der IP-Adressen ihrer Webseitennutzer hätte unternehmen müssen. Er behauptet, es sei nicht möglich, die Webseite der Beklagten aufzusuchen, ohne dass er dabei eine auf seine Person beziehbare IP-Adresse verwendete. Webseitenbesuche sollen nur möglich sein, wenn der Internetnutzer eine IP-Adresse benutzt, da sonst die Datenpakete gar nicht adressiert werden könnten.

Dem Kläger seien außergerichtliche Rechtsanwaltskosten in Höhe von 571,44 € entstanden.

Der Kläger beantragt daher, die Beklagte zu verurteilen,

1. es bei Meidung eines für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes bis zu 250.000 €, ersatzweise Ordnungshaft, oder Ordnungshaft bis zu 6 Monaten zu unterlassen, eine IP-Adresse des Klägers zu speichern und an die Google Inc. zu übermitteln, indem die Beklagte auf der vom Kläger besuchten Webseite den Tracking-Dienst Google Analytics nutzt, ohne dabei gleichzeitig die Code-Erweiterung "anonymisiert" zu verwenden,

2. dem Kläger Auskunft zu erteilen, ob über den Kläger betreffende personenbezogene Daten verbreitet werden, sowie ggf. Auskunft zu erteilen, welche personenbezogenen Daten über den Kläger gespeichert werden und

3. an den Kläger vorgerichtliche Anwaltskosten in Höhe von 571,44 € zuzüglich Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit Rechtshängigkeit zu bezahlen.

Die Beklagte beantragt, die Klage abzuweisen.

Die Beklagte behauptet, die von dem Kläger genannte IP-Adresse sei nicht der Person des Klägers zugeordnet. Allein die Tatsache, dass im Quellcode nicht der Zusatz „anonymisiert“ angegeben wurde, bedeute nicht, dass IP-Daten des Klägers weitergegeben wurden. Vielmehr habe die Beklagte IP-Daten von Webseitenbesuchern verschlüsselt weitergegeben, sodass sie nicht verfolgbar seien und unabhängig davon, ob im Quellcode „anonymisiert“ angegeben wird oder nicht.

Der Kläger habe ein speziell von ihm entwickeltes IP-Tool eingesetzt, um massenhaft fehlende Hinweise auf eine Anonymisierung von IP-Adressen bei der Verwendung des Bausteins Google Analytics zu identifizieren.

Die Beklagte behauptet auch, es sei ohne Weiteres möglich, die eigene IP-Adresse zu unterdrücken oder anonym im Internet zu surfen. Zudem könne der Kläger mit technischen Mitteln ausschließen, dass seine IP-Adresse an Dritte weitergegeben wird, indem er eine entsprechende Einstellung an seinem Browser vornähme. Er hätte mit geringem technischem Aufwand seine IP-Adresse anonymisieren können, wenn er nicht gewollt hätte, dass seine IP-Adresse an Google weitergegeben werden sollte.

Wegen der weiteren Einzelheiten wird auf die zwischen den Parteien gewechselte Schriftsätze und das Protokoll der mündlichen Verhandlung vom 20. November 2018 verwiesen.

Aus den Gründen:

Die zulässige Klage ist begründet, da der Kläger einen Anspruch auf Unterlassen der Weitergabe personenbezogener Daten des Klägers an die Google Inc. hat.

Der Unterlassungsanspruch beruht auf §§ 823 Abs. 1 i. V. m. 1004 BGB analog.

Die unerlaubte Weitergabe personenbezogener Daten des Klägers durch die Beklagte an Google Inc. stellt eine Verletzung des allgemeinen Persönlichkeitsrechts des Klägers nach § 823 Abs. 1 BGB dar.

Das allgemeine Persönlichkeitsrecht leitet sich aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ab und stellt ein sonstiges Recht im Sinne des § 823 Abs. 1 BGB dar; auch der Datenbestand einer Person stellt ein solches sonstiges Recht dar (vgl. Palandt/Sprau, BGB, 77. Auflage 2018, § 823 Rn. 19).

Das allgemeine Persönlichkeitsrecht des Klägers – im speziellen das informationelle Selbstbestimmungsrecht – wurde verletzt, als die Beklagte die Daten des Klägers an Google Inc. weitergab.

Der Schutzbereich des § 823 Abs. 1 BGB umfasst das Recht des Einzelnen auf Achtung seiner personalen Identität. Damit kann der Inhaber des Rechts Angriffe abwehren; es währt ihm aber auch die aktive Handlungs- und Entschließungsfreiheit, die ihm das Recht gibt, selbstbestimmt zu handeln und sich frei zu entfalten (vgl. dazu Palandt/Sprau, aao. § 823 Rn. 86, 115).

Der Schutzbereich des Selbstbestimmungsrechts umfasst auch Daten, die gegenüber Dritten erkennbar einer Person zugeordnet sind. Dabei geht es um die Erhebung der Daten und um die Frage, ob und inwieweit diese Daten gespeichert werden.

IP-Adressen stellen personenbezogene Daten i. S. d. § 12 Abs. 1 und Abs. 2 TMG iVm. § 3 Abs. 1 BDSG dar, wenn diese von einem Anbieter von Online-Mediendiensten beim Zugriff auf Internetseiten gespeichert werden (BGH NJW 2017, 2416, zitiert nach juris, dort Rn. 18 ff.)

Die Beklagte verletzt auch das Recht des Klägers: Die Beklagte griff auch zum Nachteil des Klägers in die geschützte Sphäre des Klägers ein: Die Beklagte hat hier die IP-Adresse des Klägers an die Google Inc. weitergeleitet, ohne diese Adresse zu anonymisieren, als der Kläger die Webseite des Beklagten aufsuchte. Denn die Beklagte nutzte den sogenannten Tracking-Dienst Google Analytics, ohne dabei gleichzeitig den Quellcode-Zusatz „anonymisiert" zu verwenden. Dieser Quellcode-Zusatz hätte es ermöglicht, die IP¬Adressen zu anonymisieren.

Die Übermittlung der IP-Adresse des Klägers an Google Inc. war unzulässig, da die Verletzungshandlung rechtswidrig war. Denn die Weitergabe der IP-Adresse ist nach dem Datenschutzrecht ein unzulässiger Eingriff in das allgemeine Persönlichkeitsrecht des Klägers.

Der Kläger hat in diesem Eingriff auch nicht nach § 13 Abs. 2 TMG eingewilligt.

a) Nach § 12 TMG darf ein Dienstanbieter personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat. § 12 Abs. 1 TMG enthält damit grundsätzlich ein Verbot der Erhebung und Verwendung personenbezogener Daten zur Bereitstellung von Telemedien mit dem Erlaubnisvorbehalt, dass diese Handlungen zulässig sind, wenn das TMG oder andere Rechtsvorschriften sie erlauben oder der Nutzer darin einwilligt (Schreibauer, in: Auernhammer DS-GVO, BDSG, 5. Auflage, § 12 TMG Rn. 6).

Personenbezogene Daten dürfen nur erhoben oder verwendet werden, wenn der Betroffene einwilligt. § 13 Abs. 2 TMG ermöglicht unter den dort geregelten Voraussetzungen eine elektronische Einwilligung (Schreibauer, aaO., § 12 TMG, Rn. 10).

b) Nach § 13 Abs. 2 TMG kann die Einwilligung elektronisch erklärt werden, wenn der Dienstanbieter sicherstellt, dass der Nutzer seine Einwilligung bewusst und eindeutig erklärt hat, die Einwilligung protokolliert wird, der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

c) Anders als die Beklagte meint, kommt eine konkludente Einwilligung nach § 13 Abs. 2 TMG iVm. § 4a BDSG nicht in Betracht.

Der Einwilligungstatbestand § 13 Abs. 2 TMG stellt eine spezielle Regelung zur Form der Einwilligung im Anwendungsbereich der datenschutzrechtlichen Normen des TMG dar. Sie soll eine Erleichterung dadurch schaffen, dass eine Einwilligung in Schriftform, wie in § 4a BDSG vorgesehen ist, nicht erforderlich ist, sondern eine Einwilligung durch elektronische Form ermöglicht. Bei der Internetnutzung ist dies beispielsweise bei E-Mails oder per Mausklick ankreuzbaren Kästchen gewahrt.

d) Der Kläger hat keine Einwilligung nach § 13 Abs. 2 TMG erteilt, es fehlt insbesondere bereits an der bewussten und eindeutigen Erteilung nach § 13 Abs. 2 Nr. 1 TMG, weil es an der Erteilungshandlung des Klägers mangelt.

aa) Denn der Internetanbieter muss sicherstellen, dass die Einwilligung durch den Nutzer bewusst und eindeutig erteilt wurde. Dies setzt voraus, dass der Nutzer vom Erklärungsinhalt Kenntnis hat.

bb) Zwar schreibt das Gesetz eine spezielle Gestaltungsform dafür nicht vor, allerdings wird konkrete Einwilligungshandlung vorausgesetzt – durch Setzen eines Häkchens durch Anklicken oder Bestätigung eines Buttons mit der Aufschrift „ich akzeptiere und willige ein".

Nicht ausreichend ist ein bloßer Hinweis auf die AGB des Dienstanbieters, in denen ein Einwilligungstext enthalten ist. Denn dann fehlt es nach Ansicht des LG Dortmund – Urteil vom 23.02.2007 – Az.: 8 O 194/06 – bereits an einer bewussten und eindeutigen Handlung des Nutzers, mit der die Einwilligung erklärt wird (Schreibauer, aaO., § 13 T, Rn. 25,28-32,34).

cc) Der Kläger hat nur die Webseite der Beklagten aufgerufen. Darin kann keine – auch keine konkludente – Erteilungshandlung gesehen werden. Denn das bloße Aufrufen einer öffentlichen zugänglich gemachten Webseite begründet keine aktive Handlung i. S. d. § 13 Abs. 2 Nr. 1 TMG.

e) Die Voraussetzungen des § 13 Abs. 2 TMG sind somit nicht erfüllt, da es bereits an der Erteilung der Einwilligung nach § 13 Abs. 2 Nr. 1 TMG fehlt. Im Übrigen wäre die Beklagte für die wirksame Erteilung einer Einwilligung darlegungs- und beweispflichtig gewesen (Schreibauer, aaO., § 13 TMG, Rn. 39). Das Vorbringen der Beklagten bezüglich einer konkludenten erteilten Einwilligung ist dafür nicht konkret genug und wäre im Ergebnis auch nicht gelungen.

Auch der Erlaubnistatbestand des § 15 Abs. 2 TMG ist ebenfalls offensichtlich nicht erfüllt.

Die Speicherung und Übermittlung der IP-Adresse des Klägers an Google Inc. durch den Tracking-Dienst Google Analytics stellt einen unzulässigen, weil rechtswidrigen, Eingriff in das allgemeine Persönlichkeitsrecht des Klägers dar.

Bei einem sog. offenen Tatbestand – wie hier – muss die Rechtswidrigkeit nach Verneinung des Vorliegens eines Rechtfertigungsgrunds in jedem Einzelfall positiv festgestellt werden unter sorgfältiger Würdigung aller Umstände. Dazu ist eine Güter- und Interessenabwägung erforderlich, die das Schutzinteresse des Betroffenen dem des Schädigers gegenüberstellt. Rechtswidrigkeit wird bejaht, wenn das Schutzinteresse des Betroffenen die schutzwürdigen Belange der anderen Seite überwiegt. In der Abwägung einzubeziehen sind unter anderem die

Schwere des Eingriffs und das eigene Verhalten des Geschädigten (vgl. Paland/Sprau, aaO., § 823 Rn. 95, 97, 98).

Die Rechtswidrigkeit des Eingriffs in das allgemeine Persönlichkeitsrecht des Klägers ist nicht ausgeschlossen, es liegt insbesondere kein rechtsmissbräuchliches Verhalten i. S. von. § 242 BGB vor.

Allein das Aufsuchen und Aufrufen von Webseiten, wie die der Beklagten, Google Analytics ohne den Zusatz „anonymisiert" im Quellcode verwendet, um sodann auf die Rechtsverletzung aufmerksam zu machen, macht das Handeln des Klägers noch nicht rechtsmissbräuchlich.

Ein solcher Rechtsmissbrauch liegt nur vor, wenn das Vorgehen des Klägers wie in § 8 Abs. 4 UWG normiert – überwiegend sachfremde, für sich gesehen nicht schutzwürdige Interessen und Ziele verfolgt und diese als die eigentlichen Triebfeder und das beherrschende Motiv der Verfahrenseinleitung erscheinen (vgl. dazu etwa Köhler/Feddersen in Köhler/Bornkamm, UWG, 36. Auflage 2018, § 8 UWG Rn. 4.10).

Davon kann hier aber keine Rede sein: zum einen ist klar erkennbar, dass für den Kläger das Gebührenerzielungsinteresse nicht im Vordergrund steht (dazu Köhler/Feddersen, aaO., § 8 UWG, Rn. 4,12). Der Kläger schreibt Betreiber von Webseiten, die Google Analytics ohne den Zusatz "anonymisiert" im Quellcode verwenden, zunächst mit einer E-Mail an und verlangt keinen Kostenersatz, vielmehr nur die Abgabe einer strafbewehrten Unterlassungserklärung. Würde ein Betreiber einer Webseite hierauf reagieren, entstünden ihm keine Kosten durch den Verstoß. Daher ist hier die Gewinnerzielungsabsicht als beherrschendes Motiv der Verfahrenseinleitung nicht erkennbar (vgl. Schmitz-Fohrmann/Schwab, UWG, 3. Auflage, § 8 Rn. 145, 147, 148).

Darüber hinaus macht der Kläger gerichtlich nur die Rechtsanwaltskosten für das Gerichtsverfahren geltend und keinen darüber hinaus gehenden Schadensersatzanspruch. Dass kein rechtsmissbräuchliches Verhalten vorliegt, folgt auch aus dem Rechtsgedanken analog § 8 Abs. 4 UWG.

Insofern kann die Beklagte auch nicht geltend machen, der Kläger habe unter einer anderen Firma auch schon wegen Verstößen gegen das Datenschutzrecht abgemahnt.

Der Kläger war auch nicht verpflichtet, wie die Beklagte meint, zur Durchsetzung seiner Ansprüche seine eigene IP-Adresse zu verschleiern, bevor er die Webseite der Beklagten aufrief.

Die Beklagte meint, der Kläger hätte ohne Weiteres die Weiterleitung seiner IP-Adresse an Dritte ausschließen können, wenn er eine entsprechende Einstellung in seinem Browser vorgenommen hätte, mit denen seine IP-Adresse bereits vor dem Aufruf der Webseite der Beklagten anonymisiert wäre oder wenn er – wie die Beklagte im nicht nachgelassenen Schriftsatz vom 3. Dezember 2018 (Bl. 36 ff. dA) behauptet – seine IP-Adresse durch Verwendung von Werbeblockern, Nutzung eines Brave-Browsers oder Verschleierung der eigenen IP-Adresse durch Einsatz etwa eines VPN-Tunnels unkenntlich machen könnte.

Dies widerspricht jedoch den geltenden Grundsätzen und auch dem Zweck des Datenschutzrechts. Denn der Zweck der DS-GVO besteht u.a. darin, die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten, insbesondere die Wahrung des Schutzes personenbezogener Daten (vgl. von Lewinski, in: Auerhammer, aaO., M. 1 DS-GVO ErwGr2).

Durch die Datenschutzrechte soll vor Beeinträchtigungen des allgemeinen Persönlichkeitsrechts geschützt werden. Eine Verpflichtung dem Verletzten aufzuerlegen, sich vor einer vermuteten Rechtsverletzung selbst durch Vorkehrungen zu schützen, um eine tatsächliche Rechtsverletzung zu verhindern, widerspricht den vorgenannten Grundsätzen des Datenschutzes. Dies hätte zur Folge, dass der Datenschutz leerlaufen würde und sich die Dienstanbieter ihrer datenschutzrechtlichen Pflichten entziehen könnten.

Insofern kann dahinstehen, ob die von der Beklagten vorgeschlagenen Vorgehensweisen legal oder zumutbar sind: Die Beklagte muss ihre Webseite so einrichten, dass die Datenschutzrechte gewährleistet sind. Natürlich kann ein Nutzer seine Adresse schwer zugänglich machen, indem er Umwege geht oder einen VPN-Tool nutzt. Das Internet beruht aber darauf, dass der Nutzer einen Anspruch darauf hat, Webseiten frei zu besuchen, ohne sich auf rechtswidrige Eingriffe des Webseitenbetreibers einstellen zu müssen.

Das Interesse des Klägers an dem Schutz seiner personenbezogenen Daten überwiegt dem der Beklagten hinsichtlich der Schwere des Eingriffs: Die Speicherung und Übermittlung der IP-Adresse des Klägers an Google Inc. durch den Tracking-Dienst Google Analytics stellt einen schweren Eingriff in das allgemeine Persönlichkeitsrecht des Klägers dar. Google Analytics überwacht Daten und Aktivitäten der Nutzer einer Internetpräsenz, die den Tracking-Dienst eingebunden haben, und übermittelt diese in Echtzeit an Google. Die Übermittlung der Daten verfolgt den Zweck, dass diese im Gesamten ausgewertet werden können. Da dies von Datenschützern als unzulässig eingestuft wurde, hat Google den Quellcode-Zusatz „anonymisiert" eingeführt, mit dem die letzten 8 Bit einer IP-Adresse vor Übermittlung und Speicherung anonymisiert werden.

Die Beklagte verwendete auf ihrer Webseite Google Analytics aber so, dass ohne den wichtigen Zusatz „anonymisiert" gespeichert und an Google Inc. übermittelt wurde. Diese Tatsache stellt einen gravierenden Verstoß gegen die Vorschriften des Datenschutzes dar.

Ein Webdienstleister wie Google kann durch die Sammlung von Daten der Nutzer auf die Identität des Nutzers schließen, denn in diesem Zusammenhang stellt die Übermittlung der IP-Adresse ein weiteres Mosaik-Stück zu dessen Identifizierung dar (vgl. Anmerkung zu LG Berlin, 31.1.2013, Az.: 57 S 87/08, ZD 213, 618).

Auf Seiten der Beklagten ist kein vertretbarer Zweck erkennbar, der die Beeinträchtigung des allgemeinen Persönlichkeitsrechts des Klägers rechtfertigt.

Eine rechtswidrige Verletzung des allgemeinen Persönlichkeitsrechts des Klägers liegt vor. Diese hat die Beklagte auch nach § 31 BGB analog zu vertreten.

Da ein Erstverstoß vorlag, wird die Wiederholungsgefahr identifiziert. Allein die Tatsache, dass die Beklagte nunmehr den Tool nicht mehr verwendet, lässt das Rechtschutzbedürfnis nicht entfalten. Dieses würde nur entfallen, wenn die Beklagte eine strafbewehrte Unterlassungserklärung abgeben würde.

Dem Kläger steht ein Anspruch auf Freistellung von den Rechtsanwaltskosten zu.

Der Anspruch beruft auf § 823 Abs. 1 i. V. m. § 1004 BGB analog, da die Beklagte die Rechte des Klägers verletzt und sie auf die Abmahnung ohne anwaltliche Hilfe nicht reagierte.

Nachdem der Kläger nicht unter Beweis gestellt hat, dass er die Kosten an den Rechtsanwalt bezahlt hat, steht ihm als minus nur ein Freistellungsanspruch zu (vgl. Zöller/Feskorn, ZPO, 32. Auflage 2018, § 308, Rn. 4).

Zur Veröffentlichung eines Lehrerfotos im Schuljahrbuch

(**Verwaltungsgericht Koblenz**, Urteil vom 6. September 2019 – 5 K 101/19. KO –)

1. **Jahrbücher und Klassenfotos sind jedenfalls von lokaler gesellschaftlicher Bedeutung und können als Bildnisse aus dem Bereich der Zeitgeschichte nach § 23 Abs. 1 Nr. 1 KUG ohne Einwilligung des Betroffenen für den Schulbereich veröffentlicht werden.**

2. **Eine Einwilligung eines Lehrers kann zudem darin liegen, dass er sich mit den Schülern auf Veranlassung der Schule abbilden lässt.**

(nicht amtliche Leitsätze)

Sachverhalt:

Die Beteiligten streiten um die Rechtmäßigkeit der Veröffentlichung von Fotos in einem Schuljahrbuch.

Der Kläger steht als Studienrat im Dienst des beklagten Landes. Von September 2005 bis Juli 2016 verrichtete er seinen Dienst am Gymnasium A. in B., bevor er mit Wirkung zum 1. August 2016 an eine andere Schule versetzt wurde. Im Schuljahr 2015/2016 gab das Gymnasium – wie bereits im Jahr zuvor – ein Jahrbuch mit Abbildungen sämtlicher Klassen und Kurse nebst den jeweiligen Lehrern heraus. Beim Fototermin ließ sich der Kläger mit der Klasse 8c und dem Kurs MSS 12 m2 ablichten. Die entsprechenden Bilder sindim Jahrbuch auf den Seiten 64 und 90 mit Namensnennung abgedruckt. Die Schule hatte vor Anfertigung der Jahrbücher das Interesse der Schülerschaft abgefragt und lediglich eine entsprechende Anzahl drucken lassen. Mit Ausnahme eines Restexemplars, das sich im Schularchiv befindet, wurden sämtliche Exemplare des Jahrbuchs verkauft.

Mit Schreiben vom 16. Juni 2017 und vom 22. September 2017 beanstandete der Kläger sowohl gegenüber der Aufsichts- und Dienstleistungsdirektion (im Folgenden: ADD) als auch gegenüber der Schulleitung die Veröffentlichung der beiden Bilder. Da seine vorherige Zustimmung nicht eingeholt worden sei, verletze die Publikation sein Persönlichkeitsrecht.

Mit seiner Klage macht der Kläger geltend, ihm stehe ein Anspruch auf Rückruf der Jahrbücher, Unkenntlichmachung seiner Person auf den beiden Bildern sowie ein Unterlassen der weiteren Verbreitung der Jahrbücher zu, weil er in seinem Namensrecht, seinem Recht am eigenen Bild sowie seinem allgemeinen Persönlichkeitsrecht verletzt sei.

Mit den Klageanträgen zu 1. und 2. verlangt der Kläger die Beseitigung eines von ihm als rechtswidrig eingestuften Zustandes. Als Rechtsgrundlage hierfür kommt allein der – gewohnheitsrechtlich anerkannte – öffentlich-rechtliche Folgenbeseitigungsanspruch in Betracht. Dieser verpflichtet zur Herstellung des früheren Zustandes und setzt voraus, dass durch hoheitlichen Eingriff in ein subjektiv-öffentliches Recht aus einfachgesetzlichen Vorschriften oder Grundrechten ein rechtswidriger Zustand geschaffen wurde, der fortdauert (HessVGH, Beschluss vom 11. Juli 2017 – 8 B 1144/17 –, juris, Rn. 20).

Diese Voraussetzungen sind hier nicht gegeben.

Es fehlt an einem rechtswidrigen Eingriff und infolgedessen auch am Bestehen eines rechtswidrigen Zustandes. Den Ausgangspunkt der rechtlichen Betrachtung bildet hier das Recht am eigenen Bild als spezielle Ausgestaltung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz. Nach der insoweit maßgeblichen Vorschrift des § 22 Satz 1 Kunsturhebergesetz – KUG – dürfen Bildnisse nur mit Einwilligung des Abgebildetenverbreitet oder öffentlich zur Schau gestellt werden. Ein Eingriff setzt somit schon begrifflich voraus, dass eine Einwilligung erforderlich war, aber nicht eingeholt wurde. Hier bedurfte es schon keiner Einwilligung (1.). Selbst wenn man dies anders sehen wollte, liegt nach den Gesamtumständen jedenfalls eine wirksame konkludente Einwilligung des Klägers vor, die eine Verletzung seines Rechts am eigenen Bild ausschließt (2.).

Das Einwilligungserfordernis entfällt jedoch nach § 23 Abs. 1 Nr. 1 KUG, da die vom Kläger beanstandeten Klassenfotos dem Bereich der Zeitgeschichte zuzuordnen sind. Schon die Beurteilung, ob Abbildungen Bildnisse aus dem Bereich der Zeitgeschichte i. S. d. § 23 Abs. 1 Nr. 1 KUG sind, erfordert eine Abwägung zwischen den Rechten der Abgebildeten einerseits und den Rechten der Medien bzw. der Herausgeber andererseits. Der für die Frage, ob es sich um ein Bildnis aus dem Bereich der Zeitgeschichte handelt, maßgebende Begriff des Zeitgeschehens umfasst alle Fragen von allgemeinem gesellschaftlichem Interesse. Dazu können auch Veranstaltungen von nur regionaler oder lokaler Bedeutung gehören. Ein Informationsinteresse besteht allerdings nicht schrankenlos, vielmehr ist der Grundsatz der Verhältnismäßigkeit zu berücksichtigen und es bedarf gerade bei unterhaltenden Inhalten im besonderen Maß einer abwägenden Berücksichtigung der kollidierenden Rechtspositionen (vgl. BGH, Urteil vom 8. April 2014 – VI ZR 197/13 –, juris, Rn. 10).

Nach diesen Maßstäben bedurfte es keiner Einwilligung des Klägers. Jahrbücher mit Klassenfotos sind jedenfalls von lokaler gesellschaftlicher Bedeutung für die Angehörigen der Schule. Die Schule hat zudem ein berechtigtes Interesse daran, den Schülerinnen und Schülern sowie deren Eltern ein Jahrbuch nebst Illustrationen zur Verfügung zu stellen, um sich gegenüber diesem (beschränkten) Personenkreis nach außen darzustellen. Die Beeinträchtigung der Rechte des Klägers ist dagegen gering. Das Foto wurde im dienstlichen Bereich aufgenommen und zeigt den Kläger in einer völlig unverfänglichen, gestellten Situation. Der Kläger ist von daher lediglich in der sog. Sozialsphäre betroffen, die einem geringeren Schutz unterliegt als die Intim- oder Privatsphäre (vgl. zum Schutzniveau in der sog. Sozialsphäre: BGH, Urteil vom 27. September 2016 – VI ZR 250/13 –, juris, Rn. 21). Der Verbreitung der Bilder stehen auch keine besonderen schützenswerten Interessen des Klägers i. S. d. § 23 Abs. 2 KUG entgegen, insbesondere sind die Bilder in keiner Weise unvorteilhaft oder ehrverletzend.

Selbst wenn man eine Einwilligung nach dem KUG für erforderlich halten würde, hat der Kläger diese jedenfalls erteilt. Die Einwilligung nach § 22 KUG bedarf keiner besonderen Form, sondern ist auch konkludent möglich (vgl. etwa BGH, Urteil vom 11. November 2014 – VI ZR 9/14 – juris, Rn. 6). Eine solche konkludente Einwilligung hat der Kläger gegeben, indem er sich beim Fototermin mit den beiden Schülergruppen hat ablichten lassen. Dies, obwohl er wusste oder jedenfalls hätte wissen müssen, dass die Schule derartige Klassenfotos bereits in der Vergangenheit für Jahrbücher verwendet hat. Wer sich angesichts dieser Praxis mit einer Klasse bzw. einem Kurs fotografieren lässt, muss mit einer Verbreitung der Bilder rechnen, zumal schon das gewählte Format der Bilder auf eine Veröffentlichungsabsicht hindeutete. Der Beweggrund für die Teilnahme des Klägers an dem Fototermin spielt insoweit keine Rolle.

Ebenso wenig führt sein Widerspruch gegen die Veröffentlichung von Fotos auf der Homepage der Schule zu einer anderen Einschätzung. Es handelt sich hierbei um einen völlig anderen Sachverhalt: Auf der Homepage veröffentlichte Bilder sind für einen unbegrenzten Personenkreis einsehbar, wohingegen das Jahrbuch von vornherein nur einem begrenzten Personenkreis, nämlich den Schülerinnen und Schülern, zugänglich gemacht werden sollte. Angesichts dessen bestand kein Anlass, vom Widerspruch gegen die Veröffentlichung von Bildern auf der Homepage auf einen Widerspruch gegen die Veröffentlichung von Bildern im Jahrbuch zu schließen. Dies gilt umso mehr, als die hier streitgegenständlichen Fotos nicht

digital verfügbar und die vom Kläger gerügten Missbrauchsmöglichkeiten von daher reduziert sind.

Soweit der Kläger vorträgt, er habe gegenüber der Fotografin einer Veröffentlichung ausdrücklich widersprochen, ist dies ebenfalls unerheblich. Dem Kläger war bekannt, dass allein die Schulleitung die Entscheidung über die Veröffentlichung der von der Fotografin lediglich zur Verfügung gestellten Klassenfotos trifft. Von daher hätte er seinen Widerspruch dem Schulleiter gegenüber erklären müssen. Auf eine allgemeine Abwehrhaltung gegen die „Amerikanisierung" des Schulsystems und die damit einhergehende Jahrbuch-Praxis kann der Kläger sich nicht mit Erfolg berufen. Indem er an den Klassenfotos teilgenommen hat, hat er sich von dieser Haltung gerade distanziert. Es stellt ein widersprüchliches Verhalten dar, die Veröffentlichung von Fotos einerseits strikt abzulehnen und sich andererseits auf Fotos ablichten zu lassen, die offensichtlich dem Zweck der Veröffentlichung dienen.

Überdies ist der Anspruch – und dies ist selbstständig tragend – wegen tatsächlicher und rechtlicher Unmöglichkeit nicht mehr realisierbar.

Die Wiederherstellung des früheren Zustandes ist tatsächlich unmöglich, weil keine Kenntnis über den Verbleib der Jahrbücher besteht. Ob es dem Beklagten zumutbar wäre, sich eine entsprechende Kenntnis zu verschaffen, kann offenbleiben, da der Kläger einen entsprechenden Auskunftsanspruch gegenüber dem Beklagten jedenfalls nicht geltend gemacht hat.

Die Erfüllung des Anspruchs ist auch rechtlich unmöglich. Auf welcher (zivil-)rechtlichen Grundlage der Beklagte von den Käufern eine Herausgabe verlangen könnte, ist nicht ersichtlich.

Zur Wahrung der Vertraulichkeit eines behördlichen Informanten (Ls)

(**Verwaltungsgericht Minden**, Urteil vom 26. August 2019 – 10 K 9520/17 –)

1. **§ 6 Satz 1 lit. a) IFG NRW steht der Offenbarung des Namens einer Person, die eine Behörde auf einen möglichen Verstoß gegen das Tierschutzgesetz hinweist und der Offenbarung ihres Namens nicht zustimmt, grundsätzlich unabhängig vom Wahrheitsgehalt ihrer Angaben entgegen, es sei denn, es liegen ausreichende Anhaltspunkte dafür vor, dass sie die Behörde wider besseres Wissen oder leichtfertig falsch informiert hat.**
2. **Die Offenbarung des Namens von Hinweisgebern ohne ihre Zustimmung ist geeignet, die Tätigkeit von Behörden im Bereich des Tierschutzes spürbar zu beeinträchtigen, weil weniger Personen bereit wären, entsprechende Hinweise zu geben, wenn ihre Anonymität nicht mehr gewährleistet wäre.**
3. **Hinweise an Behörden erfolgen in der Regel in der Annahme, dass die Identität des Hinweisgebers vertraulich behandelt wird. Diese Erwartungshaltung ist als wesentliche Grundlage für das Handeln eines Hinweisgebers schutzwürdig und überwiegt im Rahmen der Abwägung gemäß § 9 Abs. 1 lit. e) IFG NRW grundsätzlich ein geltend gemachtes rechtliches Interesse an der Offenbarung seines Namens, es sei denn, es liegen ausreichende Anhaltspunkte dafür vor, dass der Hinweisgeber die Behörde wider besseres Wissen oder leichtfertig falsch informiert hat.**

Information des Personalrats über die Anordnung gesundheitlicher Untersuchungen nur in anonymisierter Form (Ls)

(**Verwaltungsgericht Darmstadt**, Beschluss vom 30. Juli 2019 – 23 K 2160/18.DA.PV –)

1. **Der Personalrat kann verlangen, über die nach § 3 Abs. 4 Satz 1 TVöD ergehenden gesundheitliche Untersuchungsanordnungen und die ihnen zugrunde liegenden Umstände informiert zu werden; allerdings nur in anonymisierter Form ohne Namensnennung der betroffenen Person, soweit diese der Weiterleitung nicht ausdrücklich zugestimmt hat.**
2. **Die Kenntnis von Name und ldentität der betroffenen Personen ist zur Wahrnehmung der Überwachungsangabe aus §§ 62 Abs. 1 Nr. 2, 61 Abs. 1 HPVG nicht erforderlich.**

DataAgenda.de

IHR PORTAL ZUM DATENSCHUTZ

Expertenwissen in GDD-Qualität

- detaillierte Arbeitspapiere, Checklisten uvm.
- Videos in TV-Qualität zur aktuellen Gesetzeslage mit Handlungsempfehlungen
- aktuelle Nachrichten zum Datenschutz: Urteile, Fallbeispiele, Entwicklungen
- Datenschutz Newsbox - aktuelle Themen monatlich im Überblick

+++ DS-GVO Bußgelder +++ Löschpflichten und Löschkonzepte +++ Stellung des Betriebsrates nach DS-GVO +++ Fotos und die DS-GVO +++ Datenschutz beim E-Mail-Versand +++ EuGH: Facebook Fanpages +++

DATAKONTEXT

Berichte, Informationen, Sonstiges

EuGH: Das Setzen von Cookies erfordert die aktive Einwilligung des Internetnutzers

Ein voreingestelltes Ankreuzkästchen genügt daher nicht.

Der deutsche Bundesverband der Verbraucherverbände wendet sich vor den deutschen Gerichten dagegen, dass die deutsche Planet49 GmbH bei Online-Gewinnspielen zu Werbezwecken ein Ankreuzkästchen mit einem voreingestellten Häkchen verwendet, mit dem Internetnutzer, die an einem solchen Gewinnspiel teilnehmen möchten, ihre Einwilligung in das Speichern von Cookies[1] erklären. Die Cookies dienen zur Sammlung von Informationen zu Werbezwecken für Produkte der Partner der Planet49 GmbH.

Der Bundesgerichtshof (Deutschland) ersucht den Gerichtshof um die Auslegung des Unionsrechts über den Schutz der Privatsphäre in der elektronischen Kommunikation.

Mit Urteil vom 01.10.2019 – C–673/17 entscheidet der Gerichtshof, dass die für die Speicherung und den Abruf von Cookies auf dem Gerät des Besuchers einer Website erforderliche Einwilligung durch ein voreingestelltes Ankreuzkästchen, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss, nicht wirksam erteilt wird.

Es macht insoweit keinen Unterschied, ob es sich bei den im Gerät des Nutzers gespeicherten oder abgerufenen Informationen um personenbezogene Daten handelt oder nicht. Das Unionsrecht soll den Nutzer nämlich vor jedem Eingriff in seine Privatsphäre schützen, insbesondere gegen die Gefahr, dass „Hidden Identifiers" oder ähnliche Instrumente in sein Gerät eindringen.

Der Gerichtshof stellt klar, dass die Einwilligung für den konkreten Fall erteilt werden muss. Die Betätigung der Schaltfläche für die Teilnahme am Gewinnspiel stellt deshalb noch keine wirksame Einwilligung des Nutzers in die Speicherung von Cookies dar.

Der Gerichtshof stellt ferner klar, dass der Diensteanbieter gegenüber dem Nutzer hinsichtlich der Cookies u.a. Angaben zur Funktionsdauer und zur Zugriffsmöglichkeit Dritter machen muss.

(Pressemitteilung des EuGH vom 01.10.2019)

1 Cookies sind Textdateien, die der Anbieter einer Website auf dem Computer des Nutzers der Website speichert und bei ihrem erneuten Aufruf durch den Nutzer wieder abrufen kann, um die Navigation im Internet oder Transaktionen zu erleichtern oder Informationen über das Nutzerverhalten zu erlangen.

DSK positioniert sich zu Personenkennzeichen

Wichtigstes Thema der DSK-Zwischenkonferenz am 12.09.2019 in Mainz war die von der Bundesregierung geplante Modemisierung der Registerlandschaft in Deutschland und der in diesem Zusammenhang diskutierten Einführung von verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren.

In ihrer diesbezüglichen Entschließung weist die DSK darauf hin, dass die Schaffung einer Infrastruktur mit verwaltungsübergreifenden eindeutigen Personenkennzeichen erhebliche datenschutzrechtlichen Risiken und verfassungsrechtliche Bedenken auslösen würde. Sie erinnert dabei daran, dass das Bundesverfassungsgericht schon seit Jahrzehnten der Einführung und Verarbeitung derartiger Personenkennzeichen sehr enge Schranken auferlegt.

Der stellvertretende BfDI, Jürgen H. Müller, erklärte hierzu: Wir stehen einer Registermodemisierung grundsätzlich aufgeschlossen gegenüber. Es ist sicherlich ein Gewinn, wenn Bürgerinnen und Bürger Dienstleistungen der Verwaltung durch die Nutzung einmal hinterlegter Daten leichter in Anspruch nehmen können. Dieser Vorteil und die erwarteten Effizienzsteigerungen für die öffentliche Verwaltung muss aber zwingend mit einem hohen Maß an Datenschutz einhergehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) lehnt daher die von der Bundesregierung in Betracht gezogene Nutzung von einheitlichen, verwaltungsübergreifenden Personenkennzeichen zur direkten Identifizierung von Bürgerinnen und Bürgern ab.

(Pressemitteilung des BfDI vom 16.09.2019)

Bitkom: Das digitale Büro erobert den Mittelstand

Rechnungen werden digitalisiert, Akten elektronisch archiviert, Teams arbeiten an Dokumenten von unterschiedlichen Standorten aus zusammen: Das digitale Büro erobert den Mittelstand. Schon fast jedes zweite Unternehmen (47 Prozent) setzt nicht mehr nur auf Papier, sondern organisiert und verwaltet seine Dokumente digital.

Gegenüber 2017 ist das ein deutlicher Anstieg: Hier setzten noch 33 Prozent auf das sogenannte Enterprise Content Management (ECM), wie eine solche ganzheitliche Strategie, die die Erstellung, Bearbeitung und Speicherung umfasst, genannt wird. Dabei geht es heute nicht mehr nur um klassische Office- oder PDF-Dateien, die jeweils bei 92 Prozent und damit bei so gut wie allen Unternehmen im Mittelstand digital organisiert werden. Sondern etwa auch um Bilder (57 Prozent), Audio-Dateien (25 Prozent) oder Videos (18 Prozent). Das hat die repräsentative Studie „Digital Office im Mittelstand 2019" von Bitkom Research im Auftrag des Digitalverbands

Bitkom unter 613 Unternehmen mit 20 bis 499 Mitarbeitern ergeben.

„ECM-Lösungen" bilden die wichtigste Grundlage für die Digitalisierung von Büro- und Verwaltungsprozessen. Dadurch erhalten Unternehmen etwa Unterstützung beim effizienten Erfassen, Ablegen und Wiederauffinden von Dokumenten, bei der Abwicklung dokumentenbasierter Prozesse sowie bei der Einhaltung rechtlicher Vorgaben. Das digitale Büro kommt dabei zunehmend aus der Cloud. Mehr als jedes zweite Unternehmen (58 Prozent) verwaltet seine digitalen Dokumente mittlerweile dort, das sind 9 Prozentpunkte mehr als im Jahr 2017. Die Zahl der Unternehmen, die ihre ECM-Software im eigenen Unternehmen („on premise") betreiben, ging im gleichen Zeitraum von 59 Prozent auf 44 Prozent zurück. Vor allem für den Mittelstand bietet die Dokumentenverwaltung und -Organisation aus der Cloud großes Potenzial, da IT-Ressourcen hier besonders knapp sind.

(Pressemitteilung vom 14. Oktober 2019)

Literaturhinweise

Katharina Höhne, **Auswirkungen der unionsrechtlichen Öffnungsklausel nach Art. 88 DS-GVO auf den Beschäftigtendatenschutz nach deutschem Recht,** Beiträge zu Datenschutz und Informationsfreiheit, Band 28, Verlag Dr. Kovac, Hamburg 2019, 236 S., 88,90 €

Die Öffnungsklausel nach Art. 88 DS-GVO ermöglicht dem nationalen Gesetzgeber, den Beschäftigtendatenschutz im dem von der DS-GVO vorgegebenen Rahmen nach deutschem Recht zu präzisieren. Dabei könnte auf der durch Gesetzgebung und überwiegend Rechtsprechung gestalteten Lage aufgebaut werden. Demgemäß gibt die Verfasserin einen Überblick über die Entwicklung des Beschäftigtendatenschutzes. Hierbei wird mit einem Abriss über die Entwicklung des Beschäftigtendatenschutzes, der sich in die zwei Zeitabschnitte „bis zur Reform durch die DS-GVO" und „im Lichte der DS-GVO" gliedert, wobei es galt die REichweite des Art. 88 DS-GVO auszuloten. Der Schwerpunkt liegt hierbei auf der Untersuchung der Primärrechtmäßigkeit und der Rechtsnatur des Art. 88 DS-GVO. Hierauf folgt eine Analyse des Regelungsgehalts des Art. 88 DS-GVO. Dem ist zunächst ein Abschnitt zur Methodik vorangestellt, in dem die Spezifika der Auslegung unionsrechtlicher Vorschriften wie dem hier einschlägigen Art. 88 DS-GVO herausgearbeitet werden. Art. 88 DS-GVO wird sodann sowohl auf seine zwingenden Vorgaben als auch auf seine Regelungsspielräume an die Mitgliedstaaten untersucht. Bedeutung kommt hierbei dem persönlichen Anwendungsbereich, konkret der Auslegung des Beschäftigtenbegriffs, und dem Grad der Regelungstiefe des Art. 88 DS-GVO in dem § 26 BDSG-neu als Regelungsergebnis zu. Nachgegangen wird neben der Darstellung des Regelungsgehalts zunächst der Frage, ob § 26 BDSG-neu den von Art. 88 DS-GVO vorgegebenen Rahmen einhält, was nicht in Frage gestellt wird. Besonders praxisrelevant ist sodann die Darstellung der Änderungen in § 26 BDSG-neu gegenüber der bisherigen Rechtslage. In einem weiteren Schritt stellt die Verfasserin das Verhältnis des BDSG-neu zu Rechtsvorschriften und Gesetzen außerhalb des BDSG mit Relevanz für den Beschäftigtendatenschutz dar.

Abschließend beurteilt die Verfasserin die Zukunft von Gesetzgebung und Betriebsvereinbarungen im Beschäftigungskontext nach deutschem Recht. Begonnen wird mit der Analyse des Gestaltungsspielraums, den Art. 88 DS-GVO den Mitgliedstaaten lässt. Das Kapitel zur Zukunft des deutschen Beschäftigtendatenschutzes endet mit einer Untersuchung des Schicksals von Kollektivvereinbarungen, wobei der Schwerpunkt auf Betriebsvereinbarungen aufgrund ihrer praktischen Relevanz gelegt wird.

(Redaktion)

Christina-Maria Leeb, **Digitalisierung, Legal Technology und Innovation** – Der maßgebliche Rechtsrahmen für und die Anforderungen an den Rechtsanwalt in der Informationstechnologiegesellschaft, Internetrecht und Digitale Gesellschaft, Band 19, Duncker & Humblot, Berlin 2019, 431 S., Print: 99,90 €, PrintE-Book: 119,90 €

Die Arbeitsweise von Rechtsanwältinnen und Rechtsanwälten wird aller Voraussicht nach schon in – relativ betrachtet – wenigen Jahren in essentiellen Punkten nicht mehr derjenigen gleichen, die sie heute ist. Auch dem Rechtsmarkt im Gesamten stehen gravierende Umwälzungen bevor. Diesen Entwicklungen steht vor allem das bisweilen von den Berufsträgern selbst als (zu) eng empfundene Korsett des anwaltlichen Berufsrechts gegenüber, das aus Gründen der eigenen Wettbewerbsfähigkeit im digitalen Zeitalter gelockert werden müsse. Nicht erst die aktuellen Diskussionen

um neue Geschäftsmodelle im Bereich „Legal Tech(nology)“ zeigen, dass das Berufsrecht einem über die Jahre hinweg betrachtet enormen Wandlungsprozess unterliegt. Die Arbeit leitet aus einem bewusst breit gewählten Ansatzpunkt heraus ein Anforderungsprofil für die Anwaltschaft in der gegenwärtigen Informationstechnologiegesellschaft her, welches auch und gerade auf grundlegende, rechtstheoretische Überlegungen gestützt wird.

(Redaktion)

Jürgen Taeger (Hrsg.), **Die Macht der Daten und der Algorithmen – Regulierung von IT, IoT und KI**, Tagungsband DSRI-Herbstakademie 2019, Oldenburger Verlag für Wirtschaft, Informatik und Recht, Edewecht 2019, 886 S., 69,80 €

Die Deutsche Stiftung für Recht und Informatik (DSRI) veranstaltete in diesem Jahr ihre 20. Herbstakademie. Zu Referaten eingeladen waren junge Juristinnen und Juristen aus allen Tätigkeitsfeldern (Anwaltschaft, Unternehmen, Universität, Referendariat). Ausgewählt werden konnten ein aktuelles Thema aus dem Informationstechnologierecht (inkl. IT-Vertragsrecht, Immaterialgüterrecht, TK-Recht, Fernabsatzrecht, Datenschutzrecht, Strafrecht, Rechtsinformatik). Das Ergebnis war wiederum bemerkenswert. Die in Bremen stattgefundene Tagung bot 65 Vortrage, bei denen neben dem Datenschutzrecht das Internetrecht und die Künstliche Intelligenz im Mittelpunkt standen. Vornehmlich die letztgenannte Thematik bedingte die Erörterung der mit der Erweiterung des technischen Wissens verbundenen gesellschaftspolitischen Auswirkungen.

Der vorliegende Jahresband gibt auf 886 eng bedruckten Seiten die schriftliche Fassung der 65 Tagungsbeiträge wieder. Das ist nicht auf einmal lesbar. Allein schon die Aufzählung der Autoren und der Titel ihrer Beiträge würde den Rahmen dieses Buchhinweises überschreiten. Insoweit hilft das Internet weiter (Tagungsbände: olwir.de>reihen). Auch die Gliederung des Buches hilft weiter. Hier werden die Beiträge nach folgenden Themengebieten geordnet: Datenschutz, Smart Contracts/Legal Tech, Cyber Physical Systems (CPS), Künstliche Intelligenz, Experten-/Entscheidungssysteme, Internet, World Wide Web, IT-Recht, Datenschutz international, Immaterialgüterrecht/Updates. Wenn in dieser Besprechung einige wenige Einzelthemen herausgegriffen werden, so ist das durch das persönliche Interesse des Verfassers dieses Buchhinweises bestimmt.

Zur Eröffnung der Tagung setzte sich der Medienrechtler Prof. Dr. Dieter Dörr, mit der Digitalisierung der Medienangebote auseinander, die die Gefahr birgt, dass anstelle des seriösen Journalismus Interessengruppen demokratiegefährdenden Einfluss auf die Meinungsbildung in der Gesellschaft nehmen. Mehrere Beiträge widmen sich der die datenschutzrechtlichen Regulierbarkeit und der Transparenz algorythmischer Entscheidungsprozesse u.a. am Beispiel automatisierter Kreditentscheidungen. Daniela Herdes zeigt den beginnenden Einsatz von KI im Bewerbungsprozess und die zu beachtenden Vorgaben auf. Kommentierung von vornehmlich Regelungen der DS-GVO sind Beiträge zum Schadensersatz bei unzulässiger Datenverarbeitung, zur Wirksamkeit von Einwilligungen, zu den Anforderungen an die Erklärung maschinengestützter Entscheidungen, zur Durchsetzung und Vollstreckung der Datenübertragbarkeit oder zu Codes of Conduct zum Datenschutz.

Alles in allem findet man zu einer Vielfalt von Themen interessante und hilfreiche Ausführungen, so dass das Buch für den jeweiligen Bedarfsfall bereit stehen sollte.

(Prof. Peter Gola, Königswinter)

DATENSCHUTZ-PRAXIS

Fortbildungsveranstaltung gemäß
Art. 38 Abs. 2 DS-GVO, §§ 5, 6, 38 BDSG

Datenschutzverletzungen richtig behandeln

Prozesse, Meldefristen, Praxisbeispiele und Haftungsrisiken

5. Februar 2020 in Frankfurt/M.
5. November 2020 in Köln

Referenten: Sascha Kremer, Per Stöcker

Jetzt informieren und anmelden unter **datakontext.com**

DATAKONTEXT GmbH · Postfach 41 28 · 50217 Frechen · Tel.: +49 22 34/989 49-40 · Fax: +49 22 34/989 49-44
Internet: datakontext.com · E-Mail: tagungen@datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Neuerscheinungen

Aufsätze

Die RDV weist regelmäßig auch auf in anderen Zeitschriften erschienene Beiträge zum Recht der Datenverarbeitung hin, um Recherchen zu relevanten Themen zu erleichtern. Einreichungen von Beiträgen zur Aufnahme eines Hinweises werden gerne entgegen genommen.

Bierekoven, Christiane, **Datenschutzkonforme Ausgestaltung von KI,** ITRB 2019, S. 261
Der Beitrag stellt die im Zusammenhang mit KI zu beachtenden wesentlichen Anforderungen der DS-GVO dar und zeigt auf, wie insbesondere durch technische Lösungsansätze eine datenschutzkonforme Nutzung im Rahmen von KI möglich ist.

Brink, Stefan/Joos, Daniel, **Reichweite und Grenzen des Auskunftsanspruchs und des Rechts auf Kopie – Tatbestandlicher Umfang und Einschränkungen des Art. 15 DS-GVO,** ZD 2019, S. 483
Der Beitrag geht dem Anspruch auf Ergänzung einer Auskunft durch Erteilung einer Kopie gespeicherter Daten nach.

Brink, Stefan/Joos, Daniel, **Datenschutzrechtliche Verantwortlichkeiten der betrieblichen und behördlichen Beschäftigtenvertretungen,** NZA 2019, S. 1395
Erörtert wird die Diskussion um die datenschutzrechtliche Rolle der Mitarbeitervertretungen.

Engeler, Malte/Marosi, Johannes, **Planet49: Neues vom EuGH zu Cookies, Tracking und ePrivacy,** CR 2019, S. 707
In seiner Planet49-Entscheidung hat der EuGH zum Einsatz von Cookies durch Webseitenbetreibende Stellung genommen und Anforderungen an die dafür u.U. erforderliche datenschutzrechtliche Einwilligung formuliert. Dieser Beitrag diskutiert die Kernaussagen des Urteils und erörtert den voraussichtlichen Vollzug der Entscheidung durch die deutschen Datenschutzaufsichtsbehörden.

Gola, Peter, **Das Geschäftsgeheimnisgesetz und die Datenschutz-Grnndverordnung,** DuD 2019, S. 569
Der Beitrag zeigt die teilweise parallelen Regelungen des Geschäftsgeheimnisgesetzes und der DS-GVO und die sich hieraus ergebenden neuen Verpflichtungen für Datenschutzbeauftragte auf.

Golland, Alexander, **Reichweite des "Joint Controllership": Neue Fragen der gemeinsamen Verantwortlichkeit,** K&R 2019, S. 533
Die Entscheidung des EuGH in der Rechtssache "Wirtschaftsakademie Schleswig-Holstein"(C-210/16) warf in datenschutzrechtlicher Literatur und Öffentlichkeit zahlreiche Fragen auf: Der EuGH hat sich kürzlich in einem weiteren Urteil zu diesem Fragenkomplex geäußert. Der Beitrag kommentiert diese Rechtsprechung.

Güngör, Volkan, **Kooperation lohnt sich: Ablauf einer Datenschutzüberprüfung durch die Aufsichtsbehörde beim Verantwortlichen,** ITRB 2019, S. 256
An Hand eines Fall eines Versicherungsmaklers zeigt der Beitrag die Hintergründe einer Datenschutz-Begehung sowie mögliche Schutzmaßnahmen, die von seiten des Verantwortlichen bereits präventiv im Unternehmen implementiert werden sollten.

Holthausen, Joachim, **Die arbeitsvertragliche Verschwiegenheit,** NZA 2019, S. 1377
Unter dem Aspekt des neuen Geschäftsgeheimnisgesetzes ist als parallele Grundpflicht die arbeitsvertragliche Verschwiegenheitspflicht Voraussetzung des Geschäftsgeheimnischarakters.

Körner, Marita, **Beschäftigtendatenschutz in Betriebsvereinbarung unter Geltung der DSGVO,** NZA 2019, S. 1389
Art. 88 DS-GVO eröffnet einerseits weiterhin die Möglichkeit, den Datenschutz im Beschäftigungsverhältnis per Kollektivvereinbarungen, womit Tarifverträge und Betriebsvereinbarungen gemeint sind, zu regeln, und gibt grundsätzliche Vorgaben für derartige Regelungen vor.

Lee, Laureen/Cross, Samuel, **(Gemeinsame) Verantwortlichkeit beim Einsatz von Drittinhalten auf Websites,** MMR 2019, S. 559
Der Beitrag erörtert die Anwendung des Art. 26 DS-GVO auf die dargestellte Fallkonstellation.

Reinhard, Andre, **Pflicht zur Arbeitszeiterfassung und Arbeit 4.0,** NZA 2019, S. 1313
Der Beitrag geht auf die Konsequenzen des Urteils des EuGH zur Pflicht der Arbeitszeiterfassung im Rahmen moderner Arbeitszeitgestaltung ein.

Söbbing, Thomas/Sauter, Fabian, **Quo vadis Legal Tech?,** ITRB 2019, S. 259
"Legal Tech" ist in aller Munde, doch wenig Greif- und vor allem Anwendbares lässt sich finden. Legal Tech-Produkte sind von einer echten Usability noch weit entfernt. Der Beitrag beginnt wie jedes strukturierte IT-Projekt mit einem Lastenheft für ein Legal Tech-Produkt.

Kuh und Botanik

Wir wollen auf digitale Technik nicht verzichten. Zu Recht, denn der private und berufliche Alltag wäre ohne sie nicht vorstellbar und will Deutschland international mithalten, braucht die Wirtschaft Nachwuchs. Die wenigsten verstehen aber die Geräte, die sie benutzen. Man weiß von der Funktion des Smartphones so wenig, wie von der einer Mondrakete. Während wir die aus guten Gründen nicht betreiben, nutzen schon Kinder täglich Geräte und Anwendungen, die vermutlich mehr Technik enthalten als eine Apollo11-Rakete. Wenn Technik auf dem Weg zur künstlichen Intelligenz immer wichtiger wird, dann sollten wir und vor allem unsere Kinder lernen, sie zu verstehen und vor allem zu beherrschen. Anderenfalls besteht die Gefahr, dass die Technik sich selbstständig macht und uns beherrscht. Nun kann nicht jeder Informatiker sein. Aber wer ins Ausland reisen will, der ist gut beraten, eine Fremdsprache zu lernen. Warum also nicht eine Programmiersprache ins Pflichtprogramm der Sprachen aufnehmen, die an den Schulen gelehrt werden? Noch jedenfalls beschreibt unseren gesellschaftlichen Kenntnisstand in Sachen Technik ein mahnender Vergleich von Albert Einstein. Er eröffnete die Funkausstellung 1930 als es um die Einführung der Funktechnik ging mit der Bemerkung, dass sich alle schämen sollen, „die gedankenlos sich der Wunder von Wissenschaft und Technik bedienen und nicht mehr davon geistig erfasst haben als die Kuh von der Botanik der Pflanzen, die sie mit Wohlbehagen frisst."

die neue Aufgabe des DSB

» **Der Leitfaden ist für jeden ohne Audithintergrund Gold wert. Endlich jemand, der die neue Rolle des DSB verstanden hat.** «

(Feedback der DAFTA-Teilnehmer)

Ralf Herweg/Thomas Müthlein:
Die Überwachungsaufgabe des Datenschutzbeauftragten nach DS-GVO

88 Seiten/DIN A4, ISBN 978-3-89577-853-7
69,99 € inkl. E-Book

Bestellen Sie direkt unter:
datakontext.com/ueberwachungsaufgabe

DATAKONTEXT

WIR VERSCHAFFEN HANDLUNGSFREIHEIT.

Bereit, um etwas zu bewegen?

CBH
RECHTSANWÄLTE

CBH ist eine der führenden Wirtschaftskanzleien in Deutschland und berät in den strategischen Schwerpunkten Geistiges Eigentum, Medien und IT, Unternehmen und Finanzen, Personal und Sozialwesen, Bau und Immobilien sowie Verwaltung und Wirtschaft.

JUVE 2019 AWARDS
Kanzlei des Jahres für Vergaberecht

Im Fachbereich IT-Recht decken wir das gesamte Spektrum IT-rechtlicher Angelegenheiten ab und konzentrieren uns unter anderem auf datenschutzrechtliche Fragen. Datenschutz-Compliance verstehen wir dabei nicht nur als Pflichtaufgabe unserer Mandaten, sondern auch als Chance.

JUVE TOP 50
Wirtschaftskanzlei Deutschland
2019|2020

Unsere Ansprechpartner für IT- und Datenschutzrecht, Dr. Sascha Vander, LL.M. (s.vander@cbh.de) und Niklas Kinting (n.kinting@cbh.de), unterstützen Sie gerne.

Mehr Infos unter www.cbh.de

KÖLN BERLIN HAMBURG MÜNCHEN STUTTGART COTTBUS