

Zehnter Tätigkeitsbericht

des Datenschutzbeauftragten der Deutschen Welle

(Berichtszeitraum: 01.01.2010 bis 31.12.2011)

Inhaltsverzeichnis

- I. Vorbemerkung
 - 1. Tätigkeitsbericht
 - a) Berichtspflicht
 - b) Berichtszeitraum
 - c) Veröffentlichung
 - 2. Aufgaben

- II. Datenschutz außerhalb der Deutschen Welle
 - 1. Vorratsdatenspeicherung
 - 2. Beschäftigtendatenschutz
 - 3. Gesetz zum elektronischen Entgeltnachweis (ELENA)
 - 4. Zusammenarbeit mit ARD und ZDF

- III. Datenschutz innerhalb der Deutschen Welle
 - 1. Allgemeine Beratung
 - 2. Informationen zum Datenschutz
 - 3. Prüfung Beihilfe-Berechnungs-Zentrum (bbz)
 - 4. Gesetz zum elektronischen Entgeltnachweis (ELENA)
 - 5. Hausinterner Postversand
 - 6. Videoüberwachung
 - 7. Verpflichtung zum Datenschutz/Datengeheimnis
 - 8. Kooperation WDR-Rechenzentrum

9. Auskunftersuchen/Beschwerden/Anfragen

IV. Schlussbemerkungen

I. Vorbemerkung

1. Tätigkeitsbericht

a) Berichtspflicht

Der Beauftragte für den Datenschutz erstattet den Organen der Deutschen Welle gemäß § 42 Abs. 4 des Bundesdatenschutzgesetzes (BDSG) alle 2 Jahre einen Tätigkeitsbericht, der auch dem Bundesbeauftragten für den Datenschutz übermittelt wird.

b) Berichtszeitraum

Der vorliegende Bericht bezieht sich auf den Zeitraum vom 01.01.2010 bis zum 31.12.2011.

c) Veröffentlichung

Nach Auffassung der Europäischen Kommission sind die Datenschutzbeauftragten von ARD und ZDF sowie DLR verpflichtet, nach Art.28 Abs. 5 der Datenschutzrichtlinie - auch wenn insoweit eine Umsetzung in nationales Recht bisher nicht erfolgt ist - ihre Tätigkeitsberichte zu veröffentlichen.

Die Datenschutzbeauftragten haben sich daraufhin mit der Europäischen Kommission auf folgendes Verfahren verständigt: der Veröffentlichungspflicht wird dadurch entsprochen, dass die Tätigkeitsberichte im Internetangebot der jeweiligen Rundfunkanstalt veröffentlicht und auch weiterhin auf konkrete Anfragen Interessenten in schriftlicher Form zur Verfügung gestellt werden.

2. Aufgaben

Gemäß § 42 Abs. 2 BDSG kontrolliert der Datenschutzbeauftragte die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes sowie ergänzender Vorschriften über den Datenschutz innerhalb der Deutschen Welle. Dabei tritt er für die Deutsche Welle an die Stelle des Bundesdatenschutzbeauftragten. Bei der Ausübung des Amtes ist der Datenschutzbeauftragte unabhängig und nur dem Gesetz unterworfen. Daneben untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates der Deutschen Welle.

Aus dieser allgemeinen Gesetzesformulierung lassen sich folgende konkrete Aufgabenfelder ableiten:

- Kontrolle aller Stellen des Hauses auf Einhaltung der datenschutzrechtlichen Bestimmungen,
- Beratung bei Planung und Einführung von Informationssystemen,
- Beratung bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Mitarbeiter,

- Beanstandung von festgestellten Verstößen gegen das Datenschutzrecht, verbunden mit der Aufforderung, diese schnellstmöglich abzustellen,
- Überprüfung von Hinweisen und Beanstandungen im Rahmen der Anrufung durch Betroffene.

Nach der Regelung in § 42 Abs. 3 i.V.m. § 21 Satz 1 BDSG, die ihre Entsprechung in § 20 Deutsche-Welle-Gesetz (DWG) gefunden hat, kann sich jedermann an den Datenschutzbeauftragten wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten innerhalb der Deutschen Welle in seinen Rechten verletzt worden zu sein. Der Datenschutzbeauftragte ist verpflichtet, sämtliche Informationen vertraulich zu behandeln.

Der Verwaltungsrat der Deutschen Welle hat die Einzelheiten der Amtsführung des Datenschutzbeauftragten unter Berücksichtigung der rundfunkspezifischen Besonderheiten selbst näher ausgestaltet und sich dabei inhaltlich an die Vorgaben der gesetzlichen Regelungen über die Rechtsstellung, Kontroll- und Beanstandungsbefugnis des Bundesbeauftragten für den Datenschutz orientiert. Hierbei hat der Verwaltungsrat u.a. folgende Grundsätze aufgestellt:

- Der Datenschutzbeauftragte kann zur Erfüllung seiner Aufgaben die Unterstützung aller Stellen des Hauses beanspruchen. Insbesondere hat er folgende Rechte:
- Auskunftsrecht bezüglich aller Fragen sowie Einsichtsrecht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme.
- Recht auf jederzeitigen Zutritt in alle Diensträume.
- Stellt der Datenschutzbeauftragte Verstöße gegen die Vorschriften des BDSG oder anderer Vorschriften des Datenschutzes oder sonstige Mängel bei der Verarbeitung und Nutzung personenbezogener Daten fest und wird dem nicht abgeholfen, so beanstandet er dies bei dem Intendanten. Hilft dieser dem Verstoß nicht ab, so folgt die Beanstandung gegenüber dem Verwaltungsrat.
- Auf Anforderung des Verwaltungsrates oder des Intendanten hat der Datenschutzbeauftragte Gutachten zu erstellen.
- Der Datenschutzbeauftragte führt ein Register der automatisiert geführten Dateien in denen personenbezogene Daten gespeichert werden. Die Deutsche Welle leitet dem Datenschutzbeauftragten eine Übersicht gemäß § 18 Abs. 2 S. 2 Nr. 1-6 BDSG zu.
- Der Datenschutzbeauftragte berät und schult bei Bedarf alle Mitarbeiter.
- Der Datenschutzbeauftragte ist, auch nach Beendigung seines Amtes, verpflichtet, über die ihm amtlich bekannt gewordene Angelegenheiten Verschwiegenheit zu bewahren.

- Der Datenschutzbeauftragte ist berechtigt, über Personen, die ihm in seiner Eigenschaft als Datenschutzbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Soweit das Zeugnisverweigerungsrecht des Datenschutzbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.

II. Datenschutz außerhalb der Deutschen Welle

1. Vorratsdatenspeicherung

Zur Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung in deutsches Recht war zunächst das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ am 1. Januar 2008 in Kraft getreten. Danach bestand für Telekommunikationsdiensteanbieter eine Verpflichtung, die Verbindungsdaten aller Telefon- und Handygespräche (Ausgangs- und Zielrufnummer, Verbindungsdauer, Datum) und die entsprechenden Daten bei der Internetkommunikation verdachts- und anlassunabhängig zu speichern. E-Mail-Anbieter mussten die IP- und Mailadressen von Absender, Empfänger und Zeitpunkte jedes Zugriffs auf das Postfach aufbewahren. Eine Speicherung der Kommunikationsinhalte war hingegen nicht gestattet. Die Speicherdauer betrug in allen Fällen mindestens sechs Monate (vgl. §§ 113a, 113b TKG). Vor Inkrafttreten des Gesetzes durften solche Daten nur solange gespeichert werden, wie der Nutzer dies erlaubt hatte (bis zu 90 Tage) oder solange sie für Abrechnungszwecke benötigt wurden.

Übermittelt werden sollten die Verbindungsdaten in Deutschland schon bei Verdacht von erheblichen oder „mittels Telekommunikation begangener“ Straftaten, zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit und zur Erfüllung der gesetzlichen Aufgaben der Geheimdienste (BND, MAD, Verfassungsschutzbehörden). Die dem Gesetzespaket zugrundeliegende EU-Richtlinie sieht die Datenspeicherung hingegen nur zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten vor. Damit ging das deutsche Gesetz weit über die EU-Vorgaben hinaus. Bisher benötigten die Strafverfolgungsbehörden einen „strafprozessualen Anfangsverdacht“, um ermitteln zu dürfen. Die Regelung stellte damit einen ganz erheblichen Eingriff in die Freiheits- und Persönlichkeitsrechte dar. Das Grundrecht auf informationelle Selbstbestimmung wurde durch die Vorratsdatenspeicherung beeinträchtigt. Diese Regelungen ermöglichten nicht nur die Erstellung eines umfassenden Bildes der privaten und beruflichen Kommunikation jedes Bürgers, sondern über die Speicherung von IP-Adressen lassen sich die Interessen und Vorlieben von Bürgern nachvollziehen. Dies hatte auch gravierende Auswirkungen auf die journalistische Praxis, denn mithilfe der genannten Daten konnte auch die gesamte berufliche Kommunikation von Journalisten nachvollzogen werden. Insbesondere der Informantenschutz, der unabdingbar für eine freie Presse ist, war so nicht mehr zu gewährleisten. Das

galt umso mehr, wenn man die erweiterten Verwendungsmöglichkeiten bedenkt, die den Strafverfolgungsbehörden nach §§ 97 ff. StPO eingeräumt werden sollten.

Der Arbeitskreis Vorratsdatenspeicherung - ein bundesweiter Zusammenschluss von Bürgerrechtlern, Datenschützern und Internet-Nutzern – hat gegen das Gesetz eine Verfassungsbeschwerde eingereicht. Das Urteil des Bundesverfassungsgerichts zu den Verfassungsbeschwerden wurde am 2. März 2010 verkündet. Das Verfassungsgericht erklärte die Vorschriften zur Vorratsdatenspeicherung für verfassungswidrig und die entsprechenden Vorschriften für nichtig: Das Gesetz in seiner jetzigen Fassung verstößt gegen Artikel 10 Abs. 1 des Grundgesetzes. Zwar sei eine Vorratsdatenspeicherung nicht grundsätzlich mit dem Grundgesetz unvereinbar; im Hinblick auf das Telekommunikationsgeheimnis der betroffenen Bürger sei aber Voraussetzung, dass die Daten nur dezentral gespeichert und mit besonderen Maßnahmen gesichert würden; die Nutzung der Daten durch Behörden müsse auf genau spezifizierte Fälle schwerster Kriminalität und schwerer Gefahren beschränkt bleiben; diesen Anforderungen werde das angegriffene Gesetz nicht gerecht. Seit dem Urteil des Bundesverfassungsgerichts darf in Deutschland nicht mehr ohne Anlass auf Vorrat gespeichert werden.

Das Bundesjustizministerium stellte im Juni 2011 einen erneuten Gesetzesentwurf vor. Entsprechend dem Eckpunktepapier vom Januar 2011 ist darin eine siebentägige Vorratsspeicherung von Daten zu jeder Internetverbindung vorgesehen, um Bestandsdatenauskünfte (insbesondere über die Zuordnung von IP-Adressen zu Personen) zu ermöglichen.

Am 16. Juni 2011 wurde durch die EU-Kommission als erste Stufe eines Vertragsverletzungsverfahrens wegen der nicht erfolgten Umsetzung der Vorratsdatenspeicherung eine Stellungnahme des Bundesjustizministeriums angefordert

2. Beschäftigtendatenschutz

Noch in der vergangenen Legislaturperiode sollte ein eigenes Arbeitnehmerdatenschutzgesetz verabschiedet werden, das sämtliche Regelungen zum Datenschutz in Beschäftigungsverhältnissen beinhaltet. Der aktuelle Gesetzesentwurf dagegen sieht Änderungen bzw. Ergänzungen vor allem im Bundesdatenschutzgesetz (BDSG) vor. An die Stelle des bisherigen § 32 BDSG treten die §§ 32 bis 32f. Der Gesetzesentwurf enthält keine wesentlichen Neuregelungen, hat aber u.a. zum Ziel, die Beschäftigten besser zu schützen. Bisher ergibt sich der rechtliche Rahmen für den Beschäftigtendatenschutz aus verschiedenen allgemeinen Gesetzen wie dem Bundesdatenschutzgesetz und dem Betriebsverfassungsgesetz, vor allem aber aus einer Vielzahl von gerichtlichen Einzelfallentscheidungen der Arbeitsgerichte. Gerade diese für die betroffenen Beschäftigten schwer zu erschließenden Regelungen will der Gesetzesentwurf in klare nachvollziehbare Bestimmungen umsetzen. Als Anlass für die Gesetzesnovelle werden teilweise die zahlreichen Datenskandale bei Lidl u.a. gesehen, allerdings waren diese Vorfälle auch nach der bestehenden Rechtslage unrechtmäßig.

Teilweise werden Eingriffe in die Persönlichkeitsrechte der Beschäftigten befürchtet, insbesondere was das Mitlesen von E-Mails und die Videoüberwachung betrifft. Danach soll es möglich sein, dass

Arbeitgeber künftig die Inhalte von E-Mails ihrer Arbeitnehmer auswerten, wenn sie zuvor die Privatnutzung von E-Mails verboten haben. Ebenso sollen Arbeitgeber unter dem Vorwand der Qualitätssicherung umfassende Verhaltens,- und Leistungskontrollen ihrer Beschäftigten durchführen können.

Allerdings können auch nach der bestehenden Rechtslage Arbeitgeber – so die Rechtsprechung - die Inhalte von E-Mails ihrer Arbeitnehmer auswerten, wenn die Privatnutzung nicht zulässig ist, wenn es sich also nur um dienstliche E-Mails handelt. Aber auch bisher ist die trotzdem vorhandene private E-Mail von der Kenntnisnahme durch den Arbeitgeber ausgenommen. Dies gilt auch nach den Regelungen im Gesetzentwurf. Danach dürfen die dienstlich eingegangenen E-Mails vom Arbeitgeber gemäß den §§ 32c und 32d BDSG erhoben, verarbeitet und genutzt werden. Das bedeutet, dass die Erhebung erforderlich sein muss für die Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses. Dies ist z. B. der Fall, wenn wegen der Abwesenheit des Beschäftigten die dienstlichen E-Mails von dem Vertreter des Beschäftigten oder dem Arbeitgeber selbst weiter bearbeitet werden müssen. Der Arbeitgeber darf die Inhalte allerdings nur erheben, verarbeiten und nutzen, und somit zur Kenntnis nehmen, sofern es sich nicht um erkennbar private Inhalte handelt. Weitere Voraussetzung ist, dass der Arbeitgeber den Beschäftigten hierauf schriftlich hingewiesen hat. Die Kenntnisnahme der Kommunikationsinhalte der Beschäftigten mit ihren Interessenvertretungen ist auch nach dem Gesetzentwurf nicht zulässig. Die amtliche Begründung zum Entwurf des § 32i Abs.4 BDSG regelt dies ausdrücklich.

Arbeitgeber können zwar eine Videoüberwachung unter anderem auch zur Qualitätskontrolle durchführen, dies ist aber nur unter ganz engen Voraussetzungen zulässig. Einerseits muss die Videoüberwachung zur Wahrung wichtiger betrieblicher Interessen erforderlich sein und andererseits dürfen nach Art und Ausmaß der Videoüberwachung keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen am Ausschluss der Datenerhebung überwiegen. Darüber hinaus hat der Arbeitgeber den Umstand der Videoüberwachung durch geeignete Maßnahmen, wie etwa Hinweisschilder, erkennbar zu machen. Außerdem ist eine Videoüberwachung von solchen Teilen von Betriebsstätten, die überwiegend der privaten Lebensgestaltung der Beschäftigten dienen (insbesondere für Sanitär- und Umkleieräume), ohnehin unzulässig. Auch diese Daten sind unverzüglich zu löschen, wenn sie zur Qualitätskontrolle nicht mehr erforderlich sind oder schutzwürdige Interessen der Beschäftigten einer weiteren Speicherung entgegenstehen.

3. Gesetz zum elektronischen Entgeltnachweis (ELENA)

Mit dem ELENA-Verfahren (elektronisches Entgeltnachweis-Verfahren, auch elektronischer Einkommensnachweis; ursprünglicher Begriff JobCard) sollte in Deutschland ursprünglich ab 2012 der Einkommensnachweis elektronisch mithilfe einer Chipkarte und elektronischer Signatur erbracht werden. Das Verfahren umfasste die zentrale Speicherung von Arbeitnehmerdaten und die Nutzung dieser Daten durch die Agenturen für Arbeit und weitere Stellen. Für Abfragen nach dem ELENA-Verfahren sollte jede beliebige, nach einheitlichem Standard funktionierende Signaturkarte mit Chip verwendet werden können. Die Identifizierung sollte durch das Signatur-Zertifikat erfolgen.

Nachdem die Einführung wegen der Sicherheitsmängel zunächst auf 2014 verschoben werden sollte, einigten sich das Bundeswirtschaftsministerium und das Arbeitsministerium im Juli 2011 darauf, ELENA „schnellstmöglich einzustellen“. Die Einstellung wurde damit begründet, dass sich die aus Datenschutzgründen erforderlichen Signaturkarten nicht schnell genug verbreiten.

4 Zusammenarbeit mit ARD und ZDF

Die öffentlich-rechtlichen Rundfunkanstalten Deutschlands haben jeweils einen unabhängigen Datenschutzbeauftragten bestellt, der die Einhaltung der datenschutzrechtlichen Vorschriften kontrolliert. Die dem zugrunde liegenden gesetzlichen Verpflichtungen dienen der Schutzwürdigkeit personenbezogener Daten einerseits und tragen gleichzeitig dem Gebot der Staatsferne des Rundfunks Rechnung, indem sie eine staatliche Kontrolle ausschließen. Die Rundfunk-Datenschutzbeauftragten treten für die öffentlich-rechtlichen Rundfunkanstalten jeweils an die Stelle der Landesdatenschutzbeauftragten bzw. des Bundesdatenschutzbeauftragten.

Die Datenschutzbeauftragten von ARD und ZDF einschließlich DeutschlandRadio haben sich schon seit langem zu einem Arbeitskreis zusammengefunden. Der Erfahrungsaustausch in diesem Arbeitskreis stellt ein wichtiges Hilfsinstrument bei der Aufgabenerfüllung der einzelnen Datenschutzbeauftragten dar und ermöglicht in übergeordneten Angelegenheiten eine koordinierte Wahrnehmung der datenschutzrechtlichen Belange öffentlich-rechtlicher Rundfunkanstalten.

Dieser Erfahrungsaustausch findet sowohl schriftlich und telefonisch als auch zweimal pro Jahr anlässlich einer gemeinsamen Tagung statt. Anlässlich der Tagung am 10. u. 11. November 2011, die bei der Deutschen Welle in Bonn stattfand, hatte ich die Gelegenheit, den Kolleginnen und Kollegen die Besonderheiten und die aktuelle Entwicklung bei der Deutschen Welle nahezubringen.

III. Datenschutz innerhalb der Deutschen Welle

1. Allgemeine Beratung

Der Schwerpunkt der Tätigkeit hinsichtlich des Datenschutzes innerhalb der Deutschen Welle lag wie in den Vorjahren erneut weniger im Bereich der Kontrolle als in der datenschutzrechtlichen Beratung. Ich bin mit den Kollegen von ARD und ZDF der Ansicht, dass allein eine nachträgliche Kontrolle hinsichtlich der Einhaltung der datenschutzrechtlichen Vorschriften nicht zweckmäßig ist. Wesentlich wertvoller und hilfreicher für alle Beteiligten ist eine "präventive Kontrolle", die bereits im Vorfeld bei der Planung neuer Vorhaben mit datenschutzrechtlicher Relevanz ansetzt. Diese Verfahrensweise gewährleistet, dass schon von Anfang an die erforderlichen Maßnahmen geplant und ergriffen werden,

die notwendig sind, um den datenschutzrechtlichen Vorschriften Rechnung zu tragen. Würde lediglich im Nachhinein eine Kontrolle durch den Datenschutzbeauftragten erfolgen, müssten einzelne Maßnahmen möglicherweise völlig neu geplant und geändert ausgeführt werden.

Vor diesem Hintergrund bin ich bei zahlreichen Vorhaben bereits in die Planungsphase mit eingebunden worden und hatte so die Gelegenheit, die datenschutzrechtlichen Aspekte einzubringen.

Daneben haben mich von Kollegen aus den unterschiedlichen Bereichen des Hauses Anfragen und Hinweise erreicht, denen ich jeweils nachgegangen bin.

2. Informationen zum Datenschutz

Ich habe regelmäßig allgemeine Schulungen für Mitarbeiter und Mitarbeiterinnen veranstaltet. Insbesondere die Auszubildenden, die überwiegend im Bereich der Verwaltung tätig sind, erhalten zu Beginn ihrer Tätigkeit eine Einführung in die datenschutzrechtliche Thematik.

Bei diesen Schulungen wurden die Teilnehmer über Sinn und Zweck des Datenschutzes, die Voraussetzungen für eine zulässige Datenverarbeitung und Nutzung einschließlich der Folgen unrichtiger und unzulässiger Datenverarbeitung sowie über die erforderlichen Datensicherungsmaßnahmen informiert. Anhand von praktischen Fällen wurde jeweils das Verständnis für die Themen Datenschutz und Datensicherheit vertieft.

3. Prüfung Beihilfe-Berechnungs-Zentrum (bbz)

Das Beihilfe-Berechnungs-Zentrum in Bad Dürkheim (bbz) dessen alleinige Gesellschafterin die evangelische Kirche ist, erledigt für einen Großteil der öffentlich-rechtlichen Rundfunkanstalten einschließlich der Deutschen Welle die Beihilfeberechnungen. Da es sich um ein Unternehmen der ev. Kirche handelt erfolgt eine Kontrolle nicht nur durch die zuständige Aufsichtsbehörde für gewerbliche Datenverarbeiter in Rheinland-Pfalz, sondern auch durch den kirchlichen Datenschutzbeauftragten. Wegen der besonderen Sensibilität der dort verarbeiteten Daten haben sich die Rundfunkanstalten bei der Beauftragung ebenfalls eine Prüfungsmöglichkeit einräumen lassen.

Diese Prüfung, die jährlich stattfindet, erfolgt „im Auftrag“ durch die Datenschutzbeauftragten von SWR und ZDF. Die bei den bisherigen Prüfungen festgestellten Mängel hat das bbz zwar behoben und sich dabei sehr kooperativ gezeigt. Allerdings haben die bisherigen Prüfungen auch gezeigt, dass eine jährliche Kontrolle auch weiterhin erforderlich ist.

In dem Zusammenhang habe ich auch – einer hausinternen Anregung folgend – die Übermittlung der Beihilfeabrechnungen der Mitarbeiter an das bbz geprüft. Anlass zur Kritik hat sich dabei nicht ergeben.

4. Gesetz zum elektronischen Entgeltnachweis (ELENA)

Schon während der Vorbereitung zur Einführung von ELENA wurde von verschiedenen Seiten Kritik laut, die insbesondere Fragen des Datenschutzes betraf. Ich habe sowohl gemeinsam mit den Datenschutzbeauftragten von ARD und ZDF als auch mit den betroffenen Abteilungen hausintern die Entwicklung begleitet, so dass Risiken minimiert wurden und auf die Beendigung des Verfahrens unmittelbar reagiert werden konnte. So ist eine Datenübermittlung eingestellt worden, sobald die Absicht der Bundesregierung zur Aufhebung des Verfahrens veröffentlicht wurde, auch wenn die gesetzliche Verpflichtung noch bestand.

5. Hausinterner Postversand

Hausinterne Post wird in unverschlossenen und mehrmals verwendeten Hauspostumschlägen versandt. Auf diesen Umschlägen ist lediglich der Empfänger – oft nur die Abteilung, ohne eine Person zu benennen – und nicht der Absender vermerkt. Einer internen Anregung folgend habe ich die von mir seinerzeit eingeführte Verwendung besonderer Aufkleber überprüft. Mit diesen Aufklebern können die Hauspostumschläge verschlossen werden. Gleichzeitig enthält der Aufkleber eine Information darüber, ob der Inhalt persönlich oder vertraulich ist, und wer Absender der Post ist. Meine Überprüfung hat ergeben, dass diese Aufkleber im Hause allgemein bekannt sind und verwendet werden.

6. Videoüberwachung

An der gesamten Fassade des DW-Gebäudes in Bonn sind zu dessen Überwachung Kameras angebracht. Die Kameras sind nicht beweglich und haben keine Zoommöglichkeiten. Sie erfassen die Gebäudefassade und je nach Brennweite ca. 2-3 m des das Gebäude umgebenden Bereichs. Das gesamte Grundstück der DW wird nicht von den Kameras erfasst. Ich habe die Angelegenheit auf bitten der hausintern zuständigen Bereiche begutachtet, mit dem Ergebnis, dass an allen Zugängen zum Bonner Funkhaus durch entsprechende Schilder auf die Videoüberwachung hingewiesen wird. Zwar genügen grundsätzlich auch deutlich sichtbar installierte Kameras den Anforderungen der Erkennbarkeitsregelung des § 6b Abs. 2 BDS, so dass Hinweisschilder nicht in allen Fällen erforderlich sind. Dabei muss jedoch gewährleistet sein, dass die Kameras als solche erkennbar sind, bevor man in ihren Erfassungsbereich gelangt. Dem Einzelnen muss es möglich sein, den Kameras ausweichen, bevor er von ihnen erfasst wird. Wie sich bei einer Begehung des DW-Geländes gezeigt hat, sind einige an der Fassade des DW-Gebäudes befindliche Kameras so deutlich sichtbar installiert, dass es dem Einzelnen möglich ist, die Kameras wahrzunehmen und deren Erfassungsbereich auszuweichen. Es hat sich allerdings auch gezeigt, dass eine Reihe von Kameras nicht so deutlich sichtbar installiert sind, dass der Einzelne vor dem Betreten des videoüberwachten Bereichs gerade dem Erfassungsbereich der Kameras nicht ausweichen kann. Bei weiteren Kameras ist dies jedenfalls zweifelhaft. Dies hat zur Folge, dass auf das

Anbringen von Hinweisschildern nicht gänzlich verzichtet werden kann. Wenn aber an einigen Zugängen Hinweisschilder aufgestellt werden (müssen), so ist es zumindest ratsam auch an den übrigen Zugängen darauf hinzuweisen, nicht zuletzt weil sonst der Eindruck entsteht die Zugänge, an denen keine Schilder stehen, seien nicht videoüberwacht. Gemäß § 6 b Abs. 2 BDSG muss u.a. die für den Umstand der Beobachtung verantwortliche Stelle erkennbar sein. Die Identität dieser Stelle muss feststellbar sein, so dass bei juristischen Personen der Name (Deutsche Welle – gemeinnützige Anstalt des öffentlichen Rechts) sowie die Adresse anzugeben sind. Die Angabe einer genauen Stelle (z.B. Ansprechpartner) ist nicht zwingend, denn dem Betroffenen ist es durch die Angabe des Namens und der Adresse der DW möglich seine Datenschutzrechte insbesondere auf Auskunft oder Löschung geltend zu machen.

Der Hinweis auf die Videoüberwachung kann durch die Anbringung von Schildern mit einem für jedermann verständliche Piktogramm (vgl. DIN 33450.svg) erfolgen. Ein wörtlicher Hinweis (z.B.: „Dieser Bereich wird videoüberwacht.“) ist nicht erforderlich.

7. Verpflichtung zum Datenschutz/Datengeheimnis

Gemäß § 5 BDSG ist den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Deshalb sind diese Personen bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Dies gilt gemäß §5 S.2 BDSG allerdings nur für diejenigen Personen, die bei einer nicht-öffentlichen Stelle beschäftigt sind, so dass die entsprechenden Mitarbeiter der Deutschen Welle als Anstalt des öffentlichen rechts nicht auf das Datengeheimnis zu verpflichten sind. Gleichwohl hatte ich schon vor längerer Zeit mit der Personalabteilung besprochen, dass für neue Mitarbeiter eine Information in der Sache notwendig ist, denn die Pflicht zur Wahrung des Datengeheimnisses besteht und die Mitarbeiter müssen über den Inhalt dieser Pflicht informiert werden, um ihr nachkommen zu können. Ich habe daher in Abstimmung mit der Personalabteilung ein Merkblatt entwickelt, das neuen Mitarbeitern ausgehändigt wird. Es orientiert sich an dem Text der Verpflichtungserklärung des § 5 BDSG und wird regelmäßig aktualisiert. Auf eine konkrete Nachfrage hin habe ich dieses Verfahren nochmals begutachtet und dabei insbesondere festgestellt, dass das Merkblatt den aktuellen Stand wiedergibt.

8. Kooperation WDR-Rechenzentrum

Im Zusammenhang mit einer Rechenzentrums-Kooperation zwischen Deutscher Welle und WDR wurde die Frage an mich herangetragen, ob es sich bei dieser Rechenzentrums-Kooperation um eine Auftragsdatenverarbeitung handelt, die nach § 11 BDSG insbesondere zusätzliche Sicherheitsaspekte birgt.

Die Auftragsdatenverarbeitung nach § 11 BDSG setzt allerdings voraus, dass eine Verarbeitung personenbezogener Daten durch den Auftragnehmer, also durch den WDR, erfolgt. Nach dem Kooperationsvertrag zwischen Deutscher Welle und WDR, und insbesondere nach den Einzelverträgen, die mir

vorgelegen haben, bestehen die Leistungen des WDR in der Überlassung von Software und Hardware, sowie in der Erbringung von Dienstleistungen im Zusammenhang damit. In keiner der vorgenannten Vereinbarungen, insbesondere nicht in den Dienstleistungsverträgen, ist allerdings die Verarbeitung personenbezogener Daten durch den WDR vorgesehen. Die Kooperation beinhaltet daher keine Auftragsdatenverarbeitung durch den WDR.

9. Auskunftersuchen/Beschwerden/Anfragen

In einem Fall wurde ein Auskunftersuchen im Zusammenhang mit einer presserechtlichen Streitigkeit an mich herangetragen. Der Betroffene, der seine Rechte in der Berichterstattung über ihn verletzt sah, beehrte mit seiner Beschwerde Auskunft über die zu seiner Person gespeicherten und durch die Deutsche Welle genutzten Daten. Da es sich insgesamt um eine Datenverarbeitung zu journalistisch-redaktionellen Zwecken handelte, bestand unter Verweis auf das Medienprivileg des § 41 BDSG kein Auskunftsanspruch. Auf einen entsprechenden Bescheid meinerseits hat der Betroffene nicht weiter reagiert.

Im Rahmen einer geschichtlichen Dissertation über die Deutsche Welle habe ich in Abstimmung mit der Personalabteilung Auskünfte über ehemalige, zwischenzeitlich verstorbene Mitarbeiter der Deutschen Welle erteilt. Die Deutsche Welle ist grundsätzlich berechtigt, solche Daten an Dritte zu übermitteln, wenn dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, und wenn dieses wissenschaftliche Interesse dasjenige der Betroffenen überwiegt. Dabei waren Art und Umfang der Auskünfte ebenso zu berücksichtigen, wie eine eventuelle Betroffenheit Hinterbliebener.

Darüber hinaus haben mich zahlreiche Anfragen Beschäftigter der Deutschen Welle erreicht, die sich auf die Frage nach der Zulässigkeit bestimmter Verarbeitungen personenbezogener Daten in dienstlicher Hinsicht bezogen. Diese Anfragen einzelner Betroffener habe ich in Abstimmung mit den jeweils zuständigen Stellen im Hause beantwortet. In keinem Fall boten solche Anfragen Anlass zur Kritik an den bestehenden Verfahren.

IV. Schlussbemerkungen

Nicht nur im elektronischen Geschäftsverkehr und bei der elektronischen Datenverarbeitung, sondern vor allem auch in den neuen Medien gebührt dem Datenschutz nach wie vor besonderes Augenmerk. Die bisherige Zusammenarbeit mit allen Stellen des Hauses hat allerdings gezeigt, dass die notwendige Sensibilität vorhanden ist und interessengerechte Lösungen durchaus gefunden werden können.