Allgemeine datenschutzrechtliche Rechtsgrundlagen sowie technisch-organisatorischer Datenschutz im Bereich des richterlichen Arbeitsplatzes[1]

Franz Josef Kockler

"Die rechtsprechende Gewalt ist den Richtern anvertraut; sie wird durch das Bundesverfassungsgericht, durch die in diesem Grundgesetz vorgesehenen Bundesgerichte und durch die Gerichte der Länder ausgeübt", dies bestimmt in lapidarer Kürze Artikel 92 des Grundgesetzes.
Die "Ausübung" rechtsprechender Gewalt, das "Recht Sprechen", d.h. das Verlautbaren getroffener Entscheidungen ist Rechtsanwendung. Sie vollzieht sich in mehreren Abschnitten: Der Richter ermittelt zunächst unter Beachtung der hierfür vorgesehenen verfahrensrechtlichen Regeln einen bestimmten Lebenssachverhalt. Er prüft sodann in einem mit "Kognition" bezeichneten Arbeitsschritt, welche Rechtsvorschriften auf den (festgestellten oder gedachten) Sachverhalt Anwendung finden können. Danach ordnet er den Sachverhalt im Rahmen der sogenannten Subsumption unter die einschlägigen Normen ein und gelangt schließlich unter Einhaltung einer bestimmten Prüfungsreihenfolge unter Beachtung der anerkannten Methoden der Rechtsfindung zu einer Entscheidung.
Die der Rechtsanwendung dienende richterliche Tätigkeit erfordert eine Befassung mit personenbezogenen Daten des rechtssuchenden Bürgers in einem Umfang, wie dies in anderen Bereichen staatlichen oder privaten Handelns nur selten der Fall ist. Unter den Gegebenheiten heutiger Arbeitsbedingungen – insbesondere angesichts des zunehmenden Einsatzes elektronischer Datenverarbeitung – stellen sich in diesem Zusammenhang zahlreiche datenschutzrechtliche Fragen.

I. Rechtsgrundlagen des den richterlichen Arbeitsplatz betreffenden Datenschutzrechts

Die Zulässigkeit des Umgangs mit personenbezogenen Daten im Bereich des richterlichen Arbeitsplatzes bestimmt sich zunächst nach Maßgabe konkreter (d.h. auf die jeweilige Fragestellung bezogener) bereichsspezifischer, in erster Linie verfahrensrechtlicher[2] oder anderer spezialgesetzlicher[3] Regelungen. Sofern vorrangige bereichsspezifische Regelungen fehlen, ist auf die subsidiär geltenden Normen der allgemeinen Datenschutzgesetze zurückzugreifen.

Das in diesen Gesetzen verankerte allgemeine Datenschutzrecht der Bundesrepublik Deutschland zeigt – föderalistisch und historisch bedingt – eine inhomogene Vielfalt und ist zusätzlich von einer Konkurrenz bundes- und landesrechtlicher Regelungen geprägt.

Dr. Franz Josef Kockler ist Richter am OLG Saarbücken.
E-Mail: rw22mhjk@rz.uni-sb.de

---

1 Eine ausführliche Darstellung der hier behandelten Fragen erfolgt in der von dem Verfasser erstellten Monographie "Richterliches Informationsmanagement und Datenschutz", die Ende 1995/Anfang 1996 in der Schriftenreihe "Computer im Recht" erscheinen wird.

2 So bestimmt beispielsweise die zivilprozessuale Vorschrift des § 130 Nr. 1 ZPO, daß die vorbereitenden Schriftsätze die Bezeichnung der Parteien und ihrer gesetzlichen Vertreter nach Namen, Stand oder Gewerbe enthalten sollen. Aus den Regelungen der §§ 130 Nr. 5, 373, 377 ZPO ergibt sich, daß Zeugen als Beweismittel unter Angabe ihrer ladungsfähigen Anschriften zu bezeichnen sind. Die Erhebung jener Daten ist daher durch die genannten prozessualen Vorschriften, denen datenschutzrechtlich die Funktion bereichsspezifischer Ermächtigungsnormen für den in der Datenerhebung liegenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung zukommt, gedeckt und damit zulässig.

3 De lege lata kann als Beispiel für eine die Übermittlung von gerichtlichen Entscheidungen regelnde bereichsspezifische Vorschrift jedoch § 69k FGG angeführt werden. Diese durch das Betreuungsgesetz (Gesetz zur Reform des Rechts der Vormundschaft und Pflegschaft für Volljährige (Betreuungsgesetz – BtG) vom 12.09.1990, BGBl. I S. 2002) in das FGG eingeführte Vorschrift, welche detaillierte Regelungen über die Mitteilung vormundschaftsgerichtlicher Entscheidungen enthält (vgl. hierzu näher: Zimmermann, FamRZ 1991, 275), bemüht sich ersichtlich, datenschutzrechtlichen Gesichtspunkten Rechnung zu tragen. Nach § 69k Abs. 1 FGG hat das Vormundschaftsgericht Entscheidungen anderen Gerichten, Behörden oder sonstigen öffentlichen Stellen mitzuteilen, soweit dies unter Beachtung berechtigter Interessen des Betroffenen nach den Erkenntnissen im gerichtlichen Verfahren erforderlich ist, um eine erhebliche Gefahr für das Wohl des Betroffenen, für Dritte oder für die öffentliche Sicherheit abzuwenden. § 69k Abs. 3 FGG schreibt die Unterrichtung des Betroffenen, seines Verfahrenspflegers und seines Betreuers über den Inhalt der Mitteilung und deren Empfänger vor und gestattet zugleich unter bestimmten Voraussetzungen (etwa bei Gefährdung der Zwecke des Verfahrens, der Besorgnis von erheblichen Nachteilen für die Gesundheit des Betroffenen oder bei Unfähigkeit des Betroffenen, den Inhalt der Unterrichtung zu verstehen) einstweilen von der Unterrichtung abzusehen (Abs. 3 schreibt nach Wegfall der Voraussetzungen für die Nichtunterrichtung eine Nachunterrichtung vor). § 69k Abs. 4 FGG schreibt schließlich vor, daß der Inhalt der Mitteilung, die Art und Weise ihrer Übermittlung, der Empfänger, die Unterrichtung des Betroffenen oder die Gründe für das Unterbleiben dieser Unterrichtung sowie die Unterrichtung des Pflegers für das Verfahren und des Betreuers aktenkundig zu machen sind.

"Volkszählungsurteil": gewährte Grundrecht auf "informationelle Selbstbestimmung" und brachte die Gesetzgeber in Bewegung

Nach gesetzgeberischer "Pionierarbeit" des hessischen Landesgesetzgebers und nachfolgenden Datenschutzgesetzen der 1. Generation hob das Bundesverfassungsgericht durch die Anerkennung des aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleiteten Grundrechts auf "informationelle Selbstbestimmung" in dem sogenannten "Volkszählungsurteil" vom 15.12.1983 das materielle Datenschutzrecht auf verfassungsrechtliche Ebene.
Das Volkszählungsurteil veranlaßte die Gesetzgeber des Bundes und der – alten – Länder in der Folgezeit, unter Institutionalisierung des Datenschutzes (Stichwort: Datenschutzbeauftragte) eine "2. Generation" von allgemeinen Datenschutzgesetzen sowie von zahlreichen bereichsspezifischen Regelungen zu verabschieden.
Die neueren Datenschutzgesetze und bereichsspezifischen Regelungen – der heutige Stand des Datenschutzrechts läßt sich am deutlichsten an den Datenschutzgesetzen der neuen Bundesländer ablesen – bemühen sich, den verfassungsrechtlichen Vorgaben Rechnung zu tragen.

Vorgaben des BVerfG inhaltlich weitgehend übereinstimmend "umgesetzt" ...

... jedoch formal nicht ganz einheitlich

Im Bereich des allgemeinen, d.h. nicht bereichsspezifischen Datenschutzrechts ist die "Datenschutzlandschaft" der Bundesrepublik Deutschland zwar dadurch gekennzeichnet, daß die in den allgemeinen Datenschutzgesetzen des Bundes und der Länder inhaltlich weitgehend übereinstimmend "umgesetzt" worden sind. Der Teufel steckt jedoch auch hier "im Detail":
Kaum einer der Landesgesetzgeber konnte der Versuchung widerstehen, gesetzgeberische Eigenständigkeit dadurch zu betonen, daß – unbeschadet der Orientierung an dem Aufbau und der Systematik des Bundesdatenschutzgesetzes – oft wortgleich übereinstimmende Regelungen in unterschiedliche Paragraphen oder – sofern es bei übereinstimmender Bezeichnung des Paragraphen blieb, in abweichende Absätze gefaßt wurden , wobei – nota bene – der Freistaat Bayern seine Selbständigkeit dadurch betont, daß die Normen des bayerischen Datenschutzgesetzes nicht in Paragraphen sondern in Artikel gefaßt sind.

Gesetzesgeltung auf Justizverwaltung beschränkt? Auch hier verschiedene Lösungen

Die Wahrnehmung gesetzgeberischer "Eigenständigkeiten" der einzelnen Landesgesetzgeber hat in dem hier untersuchten Bereich der Rechtspflege darüber hinaus zu der Besonderheit geführt, daß ein Teil der Bundesländer die Regelungen ihres jeweiligen Landesgesetzes auf die Justizorgane nur insoweit erstrecken, als Justizverwaltungsaufgaben wahrgenommen werden, während andere Bundesländer – ebenso wie der Gesetzgeber der Bundesdatenschutzgesetzes für den gesamten Bereich der Rechtspflege eine uneingeschränkte Anwendbarkeit der materiellrechtlichen Datenschutzregelungen verankert haben.
Die sich auf die Gerichte beziehenden Regelungen der Datenschutzgesetze des Bundes und der Länder sind in der nachfolgenden tabellarischen Übersicht dargestellt, wobei mit "uneingeschränkter Geltung" stets gemeint ist, daß sowohl die Rechtsprechungstätigkeit der Gerichte, als auch ihre Verwaltungstätigkeit vom Regelungsbereich des jeweiligen Gesetzes erfaßt ist.

Tabellarische Übersicht über die datenschutzrechtlichen Regelungen für Gerichte

Stand: 6. November

Gesetzgeber	Fundstelle	Geltung des Gesetzes für Gerichte
Bund	Bundesdatenschutzgesetz (BDSG) verkündet als Art. I des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20.12.1990 (BGBl. I S. 2954)	§§ 1 Abs. 2 Nr. 1; 2 Abs. 1: uneingeschränkte Geltung
Baden-Württemberg	Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz – LDSG) vom 27.05.1991 (GBl. S. 277)	§ 2 Abs. 1: uneingeschränkte Geltung
Bayern	Bayerisches Datenschutzgesetz vom 23.07.1993 (GVBl. S. 498 ff)	Art. 2 Abs. 1: Geltung auch für Gerichte. Die Bestimmungen über die Durchführung des Datenschutzes bei öffentlichen Stellen (= 4.Abschnitt des Gesetzes) und den Landesbeauftragten für den Datenschutz (= 5. Abschnitt) gelten gemäß Art. 2 Abs. 6 jedoch nur, soweit die Gerichte in Verwaltungsangelegenheiten tätig werden.
Berlin	Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG) i.d.F. der Bekanntmachung vom 17.12.1990 (GVBl.1991, S. 16), ber. S. 54, zuletzt geändert d. Gesetz vom 08.07.1993 (GVBl. S. 313)	§ 2 Abs. 1: uneingeschränkte Geltung
Brandenburg	Gesetz zum Schutz personenbezogener Daten im Land Brandenburg (Brandenburgisches Datenschutzgesetz – BdgDSG) vom 20.01.1992, GVBl, S. 2	§ 2 Abs. 1 S. 2: nur soweit Verwaltungsangelegenheiten wahrgenommen werden

Gesetzgeber	Fundstelle	Geltung des Gesetzes für Gerichte
Bremen:	Bremisches Datenschutzgesetz (BrDSG) i.d.F. der Bekanntmachung vom 06.07.1995 (GBl. S. 343), § 1 Abs. 4: nur soweit Verwaltungsangelegenheiten wahrgenommen werden, mit Hinweis darauf, daß § 1 Abs. 2 Nr. 2 Buchstabe b des Bundesdatenschutzgesetzes "unberührt" bleibt	§ 27 Abs. 1 S. 2: nur soweit Verwaltungsangelegenheiten wahrgenommen werden, Unbeschadet der verfassungsrechtlich gewährleisteten Unabhängigkeit unterliegen Gerichte der Überwachung durch den Landesbeauftragten für den Datenschutz beim Einsatz automatisierter Datenverarbeitung hinsichtlich der organisatorischen und technischen Maßnahmen der Datensicherung.
Hamburg:	Hamburgisches Datenschutzgesetz (HmbDSG) vom 05.07.1990 (GVBl. S. 133), ber. S. 165 , 226, zuletzt geändert d. Gesetz vom 10.03.1992 (GVBl. S. 39). Ein neues Datenschutzgesetz ist in Vorbereitung (vgl. 12. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten 1993, S. 9; 13. Tätigkeitsbericht, S. 10 ff; Stellungnahme des Senats vom 30.03.1993, Drucksache 14/3826 der Bürgerschaft der Freien und Hansestadt Hamburg).	§ 2 Abs. 6: "Auf die Verarbeitung personenbezogener Daten in Akten durch die Gerichte im Rahmen der Rechtspflege...finden § 5, § 6 Absatz 1 Nummern 2 bis 6 sowie die §§ 12 bis 19[T1] keine Anwendung."
Hessen:	Hessisches Datenschutzgesetz (HDSG) vom 11.11.1986 (GVBl. S. 309), geändert durch Gesetz vom 21.12.1988 (GVBl. S. 424)	§ 3 Abs. 3 S. 2: "Insbesondere finden auf die Verarbeitung personenbezogener Daten in Akten durch die Gerichte im Rahmen gerichtlicher Verfahren... § 7, 8 Nr. 1 und 2, §§ 11 bis 14 und 16 bis 19[T2] keine Anwendung."
Mecklenburg-Vorpommern:	Gesetz zum Schutz des Bürgers beim Umgang mit seinen Daten (Landesdatenschutzgesetz von Mecklenburg-Vorpommern – DSG MV) vom 24.07.1992 (GVBl. S. 487)	§ 2 Abs. 3 S. 2: nur soweit Verwaltungsangelegenheiten wahrgenommen werden
Niedersachsen:	Niedersächsisches Datenschutzgesetz (NDSG) vom 17.06.1993 (GVBl. S. 141)	§ 2 Abs. 1 Nr. 1: uneingeschränkte Geltung
Nordrhein-Westfalen:	Gesetz zum Schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen – DSG NW) vom 15.03.1988 (GVBl. S. 160)[T3]	§ 2 Abs. 1 S .2: Nur soweit Verwaltungsangelegenheiten wahrgenommen werden
Rheinland-Pfalz:	Landesdatenschutzgesetz – LDSG – vom 05.07.1994, GVBl. S. 293	§ 2 Abs. 1 Nr. 2: uneingeschränkte Geltung
Saarland:	Saarländisches Gesetz zum Schutz personenbezogener Daten (Saarländisches Datenschutzgesetz – SDSG –) vom 24.03.1993 (ABl. S. 286)	§ 2 Abs. 1 S. 2: nur soweit Verwaltungsangelegenheiten wahrgenommen werden
Sachsen:	Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz – SächsDSG) vom 11.12.1991 (SächsGVBl, S. 401)	§ 2 Abs. 1: uneingeschränkte Geltung
Sachsen-Anhalt:	Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA) vom 12.03.1992 (GVBl. LSA S. 152), geändert durch Art. 3 des Gesetzes zur Regelung des Meldewesens und zur Neuberufung eines Landeswahlleiters vom 18.09.1992 (GVBl. LSA S. 682)	§ 3 Abs. 1: uneingeschränkte Geltung
Schleswig-Holstein:	Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Daten vom 30.10.1991 (GVBl. S. 555)	§ 3 Abs. 1: uneingeschränkte Geltung[T4]
Thüringen:	Thüringer Datenschutzgesetz vom 29.10.1991 (GVBl. S. 516)	§ 2 Abs. 1: uneingeschränkte Geltung

T1 § 5 HmbDSG enthält allgemeine Regelungen zur Zulässigkeit der Datenverarbeitung (Erlaubnis durch Gesetz oder Einwilligung des Betroffenen). § 6 Abs. 1 HmbDSG führt die Rechte des Betroffenen (Sperrung, Auskunft, Löschung pp.) auf. §§ 12–17 HmbDSG regeln die Rechtsgrundlagen der Datenverarbeitung, §§ 18 und 19 HmbDSG enthalten nähere Regelungen zu den in § 6 Abs. 1 HmbDSG genannten Rechten des Betroffenen.

T2 § 7 HDSG enthält allgemeine Regelungen zur Zulässigkeit der Datenverarbeitung (Erlaubnis durch Gesetz oder Einwilligung des Betroffenen). § 8 Nr. 1 und 2 HDSG sehen Auskunftsrechte sowie Ansprüche des Betroffenen auf Berichtigung, Sperrung oder Löschung vor. §§ 11–14, 16–19 HDSG regeln die Rechtsgrundlagen der Datenverarbeitung.

T3 Das Datenschutzgesetz Nordrhein-Westfalen ist als Artikel 1 des Gesetzes zur Fortentwicklung des Datenschutzes (GFD) vom 15.03.1988 (GVBl. S. 160) verkündet worden.

T4 Vgl. 15. Tätigkeitsbericht des schleswig-holsteinischen Landesbeauftragten für den Datenschutz S. 46, 80.


Uneingeschränkte Geltung

In denjenigen Bundesländern, die nach dem eindeutigen Wortlaut des jeweiligen Landesdatenschutzgesetzes eine uneingeschränkte Geltung der landesgesetzlichen Datenschutzbestimmungen für die Gerichte vorsehen (Baden-Württemberg, Bayern, Berlin, Niedersachsen, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt, Schleswig-Holstein und Thüringen), finden die Normen über die Erhebung und Verarbeitung von Daten auch hinsichtlich der mit der Rechtsanwendung zusammenhängenden Tätigkeiten der Gerichte Anwendung.
Die von Prütting[4] unter Hinweis auf den Wortlaut von § 1 Abs. 1 Nr. 2b BDSG vertretene Ansicht, für sämtliche Organe der Rechtspflege des Bundes und der Länder, insbesondere also für die gesamte Gerichtsbarkeit, gelte das BDSG, trägt der in § 1 BDSG zum Ausdruck gebrachten Subsidiarität des Bundesdatenschutzgesetzes gegenüber denjenigen Landesdatenschutzgesetzen, die auch den Bereich der eigentlichen Rechtsprechungstätigkeit erfassen, nicht in gebotenem Maße Rechnung.

Eingeschränkte Geltung

In den übrigen Ländern sehen die Landesdatenschutzgesetze keine uneingeschränkte Geltung für die Tätigkeiten von Gerichten vor. Während Bremen in der gerade verabschiedeten Neufassung seines Landesdatenschutzgesetzes[5] unmittelbar auf die für die "Organe der Rechtspflege" geltenden Bestimmungen des Bundesdatenschutzgesetzes[6] verweist, stellt sich die Frage, ob in den übrigen Ländern, deren Landesdatenschutzgesetze keine uneingeschränkte Geltung für die Tätigkeiten von Gerichten vorsehen – d.h. in Brandenburg, Hamburg, Hessen, Mecklenburg-Vorpommern, Nordrhein-Westfalen und im Saarland – diejenigen gerichtlichen Tätigkeiten, welche nicht in der Wahrnehmung von Verwaltungsaufgaben bestehen, d.h. die der Rechtsanwendung dienenden Gerichtstätigkeiten gänzlich den Regelungen des formellen und materiellen Datenschutzrechts entzogen sind.
Im Anschluß an die in dem Kommentar Ordemann/Schomerus/Gola[7] vertretene Auffassung ist diese Frage aus folgenden Gründen zu verneinen:

"Vorrang der Landesdatenschutzgesetzgebung"

Gemäß §§ 1 Abs. 2 Nr. 2 b; 12 Abs. 2 Nr. 2 BDSG gilt das Bundesdatenschutzgesetz nämlich für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Landesorgane der Rechtspflege (d.h. für die Gerichte in ihrer Funktion als Rechtsprechungsorgane und nicht im Rahmen der Ausübung von Verwaltungstätigkeiten) soweit der Datenschutz nicht durch Landesgesetz geregelt ist. In diesen Normen verankert das Bundesdatenschutzgesetz[8] den "Vorrang der Landesdatenschutzgesetzgebung".[9]

Auswirkung der Subsidiaritätsregelung

Die Subsidiaritätsregelung bewirkt, daß das Bundesdatenschutzgesetz auch für die Landesorgane der Rechtspflege nicht gilt, wenn der Datenschutz durch Landesgesetz geregelt ist. Die Regelungen des BDSG treten indes auch nur zurück, soweit die Regelung des Datenschutzes durch Landesgesetz erfolgt ist, d.h., es kommt jeweils darauf an, inwieweit eine bestimmte Regelung des Bundesdatenschutzgesetzes kongruent auch in dem jeweiligen Landesdatenschutzgesetz vorhanden ist. Fehlt eine entsprechende landesgesetzliche Regelung, gelten insoweit die Bestimmungen des Bundesdatenschutzgesetzes.[10]

Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Nordrhein-Westfalen und Saarland

Da in Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Nordrhein-Westfalen und im Saarland die eigentliche Rechtsprechungstätigkeit nicht von den Landesdatenschutzgesetzen erfaßt wird, gelten in den genannten Ländern für die der Rechtsanwendung dienenden gerichtlichen Tätigkeiten die Vorschriften des Bundesdatenschutzgesetzes über die Datenerhebung (§ 13 BDSG), über die Datenspeicherung, über die Veränderung und Nutzung von personenbezogenen Daten (§ 14 BDSG) sowie die Vorschriften über die Datenübermittlung (§§ 13 ff BDSG) als datenschutzrechtliche "Auffangregelungen". Der sich im Zusammenhang mit der Rechtsprechungstätigkeit ergebende Umgang der Gerichte mit personenbezogenen Daten der an gerichtlichen Verfahren beteiligten Personen würde in verfassungswidriger Art und Weise in deren Grundrecht auf informationelle Selbstbestimmung eingreifen, wenn in den genannten Ländern dieser Kernbereich gerichtlicher Tätigkeit aus dem Geltungsbereich datenschutzrechtlicher Regelungen ausgenommen wäre.[11]

---

4 ZZP 106, 437.

5 § 1 Abs. 4 S. 1, 2. Hs. der Neufassung des Bremischen Datenschutzgesetzes (BrDSG) vom 06.07.1995, (GBl. S. 343).

6 § 1 Abs. 2 Nr. 2, Buchstabe b BDSG.

7 Bundesdatenschutzgesetz (BDSG), 5. Aufl., § 1, Anm. 5.1; zu diesem Ergebnis gelangt für die nordrhein-westfälischen Gerichte auch Liebscher, Datenschutz, S. 47f.

8 Die von dem Bundesgesetzgeber in Anspruch genommene Kompetenz zur Regelung des Datenschutzes ergibt sich im Anwendungsbereich der öffentlichen Verwaltung in Ermangelung ausdrücklicher Bestimmungen im Grundgesetz einerseits als sogenannte "Annexkompetenz" zu den jeweiligen Sachkompetenzen der Art. 73 bis 75. Für die Regelung des Datenschutzes im hier interessierenden Bereich der Rechtspflege wird die Gesetzgebungskompetenz des Bundes im Anschluß an Auernhammer, Bundesdatenschutzgesetz, Einführung, Rz. 31, in der konkurrierenden Gesetzgebungszuständigkeit für die Gerichtsverfassung und das gerichtliche Verfahren sowie der konkurrierenden Zuständigkeit zur Regelung der Gebiete des bürgerlichen Rechts, des Strafrechts, Wirtschafts- und Arbeitsrechts (Art. 74 Nr. 1, 11, 12 GG) gesehen.

9 Auernhammer, Bundesdatenschutzgesetz, § 12, Rz. 10.

10 Vgl. zur Frage der subsidiären Geltung des BDSG: Auernhammer, Bundesdatenschutzgesetz, § 12, Rz.14 m.w.N.; Tinnefeld-Tubies, Datenschutzrecht, S. 17 f; Liebscher, Datenschutz, S. 47.

11 so auch Rüßmann in dem – nichtveröffentlichten – Schlußvortrag auf dem EDV-Gerichtstag 1992.

Nach einer von Auernhammer vertretenen Ansicht[12] soll eine Ausnahme hiervon lediglich für den Fall zu machen sein , daß der Landesgesetzgeber bewußt davon abgesehen hätte, eine bestimmte Regelung des Bundesdatenschutzgesetzes zu übernehmen und dies auch zum Ausdruck gebracht hätte.
Fraglich ist, ob die von Auernhammer genannten Voraussetzungen hinsichtlich der Rechtsprechungstätigkeit der hamburgischen und hessischen Gerichte gegeben sein könnten.
§ 2 Abs. 6 des Hamburgischen Datenschutzgesetzes (HmbDSG) bestimmt, daß auf die Verarbeitung personenbezogener Daten in Akten durch die Gerichte im Rahmen der Rechtspflege die §§ 5, 6 Abs. 1 Nummern 2 bis 6 sowie die §§ 12 bis 19 des HmbDSG[13] keine Anwendung finden. Weitgehend wörtlich übereinstimmend ordnet § 3 Abs. 3 S. 2 des Hessischen Datenschutzgesetzes (HDSG) an, daß auf die Verarbeitung personenbezogener Daten in Akten durch die Gerichte im Rahmen der Rechtspflege die §§ 7, 8 Nr. 1 und 2, §§ 11 bis 14 sowie §§ 16 bis 19 HDSG[14] keine Anwendung finden.
Der Wortlaut beider Landesdatenschutzgesetze könnte jedenfalls dafür sprechen, daß beide Landesgesetzgeber bewußt die materiellrechtlichen Datenschutzregelungen für den Bereich der Rechtspflege hatten ausnehmen wollen.[15]
Während das hessische Landesdatenschutzgesetz noch vor Erlaß des beispielgebenden Bundesdatenschutzgesetzes verabschiedet worden war, waren die materiellrechtlichen Regelungen des BDSG dem Gesetzgeber des hamburgischen Landesdatenschutzgesetzes bekannt, so daß in Anbetracht des § 2 Abs. 6 HmbDSG ein weiteres Argument dafür sprechen könnte, daß jener Gesetzgeber bewußt davon abgesehen hat, die zur Zeit des Erlasses des Landesdatenschutzgesetzes bereits bekannten Regelungen des Bundesdatenschutzgesetzes zu übernehmen.
Es wird abzuwarten sein, ob und inwieweit der von dem hamburgischen Senat angekündigte[16] Gesetzesentwurf diese Fragen neu regelt und ob das für Hamburg zu erwartende neue Landesdatenschutzgesetz – nicht zuletzt auch in Anbetracht der zwischenzeitlich in anderen Bundesländern in Kraft getretenen Gesetze und Novellen – in diesem Punkt dem im übrigen bundeseinheitlichen Standard folgt.

In Hamburg und Hessen richterliche Tätigkeit vom materiellen Datenschutzrecht ausgenommen?

De lege lata bleibt jedenfalls die Frage zu beantworten, ob wegen des vorerwähnten Wortlauts in den beiden Landesdatenschutzgesetzen die rechtsprechende Tätigkeit der Gerichte in Hamburg und Hessen von der Anwendbarkeit jeglicher Bestimmungen des materiellen Datenschutzrechts ausgenommen sein soll. Selbst wenn die beiden Landesgesetzgeber dies gewollt und durch die entsprechenden Formulierungen bewußt zum Ausdruck gebracht hätten, würde die überragende, das gesamte heutige Datenschutzrecht prägende Bedeutung des Grundrechts auf informationelle Selbstbestimmung der subsidiären Geltung des Bundesdatenschutzgesetzes nicht entgegenstehen.

Von zentraler Bedeutung: Der "Zweckbindungsgrundsatz"

Eine zentrale Bedeutung kommt im materiellen Datenschutzrecht dem sogenannten "Zweckbindungsgrundsatz" zu, wonach jeder von dem (ursprünglichen) Zweck nicht gedeckte (weitere) Eingriff in personenbezogene Daten unzulässig ist, sofern hierfür nicht eine ausdrückliche gesetzliche Grundlage besteht. Das Ziel, zu dessen Zweck die Daten erhoben werden, bildet hiernach zugleich auch die Grenze für die Zulässigkeit ihrer späteren Verwertung. Je strenger in diesem Zusammenhang die Zweckbindung ist, desto großzügiger darf mit personenbezogenen Daten umgegangen werden.
Für den hier in Rede stehenden Bereich des richterlichen Arbeitsplatzes und in diesem untergeordneten Arbeitsbereichen (Geschäftsstelle, Kanzlei) bedeutet dies, daß nach Maßgabe der allgemeinen Datenschutzgesetze der Umgang, d.h. die Erhebung und Verarbeitung personenbezogener Daten – sofern er nicht bereits durch bereichsspezifische Vorschriften gestattet ist – unabhängig von den zum Einsatz gelangenden Medien (Printmedien/EDV) regelmäßig durch den mit der Einleitung eines gerichtlichen Verfahrens verfolgten Zweck der Rechtsanwendung gerechtfertigt, zugleich aber auch im Rahmen dieser Zweckbindung begrenzt wird.

---

12 Auernhammer, Bundesdatenschutzgesetz, § 12, Rz. 14.

13 § 5 HmbDSG enthält allgemeine Regelungen zur Zulässigkeit der Datenverarbeitung (Erlaubnis durch Gesetz oder Einwilligung des Betroffenen). § 6 Abs. 1 HmbDSG führt die Rechte des Betroffenen (Sperrung, Auskunft, Löschung pp.) auf. §§ 12–17 HmbDSG regeln die Rechtsgrundlagen der Datenverarbeitung, §§ 18 und 19 HmbDSG enthalten nähere Regelungen zu den in § 6 Abs. 1 HmbDSG genannten Rechten des Betroffenen.

14 § 7 HDSG enthält allgemeine Regelungen zur Zulässigkeit der Datenverarbeitung (Erlaubnis durch Gesetz oder Einwilligung des Betroffenen). § 8 Nr. 1 und 2 HDSG sehen Auskunftsrechte sowie Ansprüche des Betroffenen auf Berichtigung, Sperrung oder Löschung vor. §§ 11–14, §§ 16–19 HDSG regeln die Rechtsgrundlagen der Datenverarbeitung.

15 Vgl. zu den durch § 3 Abs. 3 HDSG aufgeworfenen Rechtsfragen: 18. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, S. 61f.

16 Vgl. zur Novellierung des HmbDSG: 12. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, S. 9; Stellungnahme des Senats vom 30.03.1993, Drucksache 14/3826 der Bürgerschaft der Freien und Hansestadt Hamburg.


Behandlung von personenbezogenen Daten nach Verfahrensabschluß

Nach Abschluß eines gerichtlichen Verfahrens ist daher die Vorhaltung von Texten mit personenbezogenen Daten (gerichtliche Entscheidungen, Namensdateien) im Bereich des richterlichen Arbeitsplatzes und in diesem untergeordneten Arbeitsbereichen (Geschäftsstelle, Kanzlei) in gespeicherter Form daher nur insoweit statthaft, als die entsprechenden Dokumente zukünftig benötigt werden können (etwa zum Zwecke der Erteilung von Ausfertigungen oder im Hinblick auf eventuelle Abänderungs-, Restitutions- und Wiederaufnahmeverfahren). Im übrigen sind die personenbezogene Daten enthaltenden Textdokumente entweder dauerhaft zu anonymisieren oder endgültig zu löschen.

II. Technisch-organisatorischer Datenschutz im Bereich des richterlichen Arbeitsplatz

Datenschutz im Bereich des richterlichen Arbeitsplatzes beginnt mit organisatorischen und technischen Vorkehrungen. In Ermangelung detaillierter bereichsspezifischer Regelungen ergeben sich die insoweit maßgeblichen Rechtsgrundlagen aus den vorerwähnten Datenschutzgesetzen des Bundes und der Länder.

§ 9 BDSG

So ordnet etwa der hier beispielgebend anzuführende § 9 BDSG unter bewußtem Verzicht darauf, die in Betracht kommenden Sicherheitsmaßnahmen in allen Einzelheiten zu beschreiben, in allgemeiner Form an, daß öffentliche und nichtöffentliche Stellen, die personenbezogene Daten verarbeiten, diejenigen technischen und organisatorischen Maßnahmen zu treffen haben, welche erforderlich sind, um die Ausführung der Vorschriften des Gesetzes zu gewährleisten, wobei einschränkend nur solche Maßnahmen als erforderlich angesehen werden, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Äußere Sicherung der Diensträume

Zur Erzielung eines wirksamen Schutzes der personenbezogenen Daten sind geeignete Maßnahmen zu treffen, wobei unter dem Gesichtspunkt der Zugangskontrolle vorrangig die äußere Sicherung der Diensträume, in welchen personenbezogene Daten vorgehalten werden, durch gerichtsinterne Verfügungen auf das jeweilige Gerichtsgebäude bezogen detailliert geregelt werden sollte.

Zugangskontrolle

Der – mit guten Gründen – an erster Stelle in dem Katalog der Kontrollmaßnahmen in Anlage zu § 9 BDSG (bzw. den entsprechenden Vorschriften der Landesdatenschutzgesetze) aufgeführten Zugangskontrolle, welche Unbefugten die Möglichkeit des Zugangs zu den im Bereich des jeweiligen Arbeitsplatzes zugänglichen Daten verwehren soll, kommt auch im Umfeld des richterlichen Arbeitsplatzes als vorrangige Sicherungsmaßnahme eine besondere Bedeutung zu.

Das Zimmer abschließen ...

Dies beginnt zunächst einmal mit einfachsten – mechanischen – Sicherheitsmaßnahmen, die etwa darin bestehen, das Dienstzimmer oder das häusliche Büro, in welchem sich Akten oder der – eingeschaltete – Computer befinden, für die Zeit der Abwesenheit des Richters abgeschlossen wird.

"Typische Mängel"

Instruktiv sind in diesem Zusammenhang einige "typische Mängel", die der hessische Datenschutzbeauftragte bei einer Überprüfung von Staatsanwaltschaften[17] festgestellt hat[18], Mängel, die nach Erfahrungen des Verfassers jedoch auch bei Gerichten hätten festgestellt werden können, wenn diese der Kontrollbefugnis des Datenschutzbeauftragten unterliegen würden:

"Lediglich einfach verglastes Justizgebäude"

Die in dem Bericht des Datenschutzbeauftragten beschriebene Situation bestand darin, daß sich die relevanten Anlagen in einem Gebäude befanden, dessen Zugangstüren und Fenster lediglich einfach verglast waren. Sonstige Sicherungsmaßnahmen (etwa eine Diebstahlmeldeanlage usw.) seien nicht vorhanden. Der Datenschutzbeauftragte führt weiter aus, das Gebäude sei abends bis 19.00 Uhr geöffnet. Zwar sei der Zugang ständig von einem Pförtner besetzt, der jedoch zum Zeitpunkt der Prüfung keine Zugangskontrolle vorgenommen habe, sondern lediglich als Auskunftsstelle zur Verfügung gestanden habe. Die Türen zu den einzelnen Diensträumen, die ohnehin nur mit einfachen Schlüsseln gesichert seien, würden zwar beim Verlassen abgeschlossen, die Schlüssel blieben jedoch auch nach Dienstende und während des Urlaubs von Bediensteten von außen stecken. So sei es ihm ohne weiteres möglich gewesen, nach Dienstschluß unbehelligt die Diensträume zu betreten. Er habe freien Zugang zu den offen aufbewahrten Akten und PCs gehabt.

Orientiert an einzelnen Empfehlungen des hessischen Datenschutzbeauftragten[19] sind insoweit folgende Anregungen angezeigt:

---

[17] Gemäß § 24 Abs. 1 HDSG ist die Tätigkeit von Gerichten – soweit es sich nicht um Verwaltungstätigkeiten der Gerichte handelt – der Prüfungskompetenz des Landesdatenschutzbeauftragten entzogen.

[18] Hessischer Datenschutzbeauftragter, 22. Tätigkeitsbericht, S. 46.

[19] Entsprechende Maßnahmen werden auch von anderen Datenschutzbeauftragten empfohlen, vgl. etwa die Broschüre des Landesbeauftragten für den Datenschutz Brandenburg: Sicherheit am PC und in lokalen Netzen, – Dateienregister –, S. 6–12.