# E. Die „Trennung“ der Datenschutzaufsicht

Bayern ist heute das einzige Bundesland, in dem die Aufsicht über die Verarbeitung bei öffentlichen und nicht-öffentlichen Stellen durch zwei voneinander getrennte Aufsichtsbehörden ausgeübt wird. Gleichwohl war die Trennung der Aufsicht in die Aufsicht über die Verarbeitung bei den öffentlichen Stellen und die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen in der ganz überwiegenden Mehrzahl der ersten Landesdatenschutzgesetze vorzufinden. Diese Trennung der Aufsicht (auch bezeichnet als „Trennungsmodell“) wurde von den Ländern jedoch in den folgenden Jahren und Jahrzehnten, spätestens mit der Entscheidung des EuGH aus dem Jahr 2010 zur „völligen Unabhängigkeit“ der Aufsichtsbehörden, aufgegeben bzw. – nach wohl überwiegender Ansicht – korrigiert.[699]

Nachfolgend soll auf die in den Ländern vorgebrachten Gründe für das Zusammenführen der Aufsichtsbehörden (auch bezeichnet als „Einheitsmodell“) eingegangen werden. Dies da schon das Beispiel der Ausgestaltung der Datenschutzaufsicht in Bayern zeigt, dass das „Einheitsmodell“ nicht die alleinig in Betracht kommende Möglichkeit zur Herstellung rechtskonformer und insbesondere auch „völlig unabhängiger“ Datenschutzaufsicht ist.

Die Entwicklung von der Trennung der Datenschutzaufsicht hin zur ganz überwiegend einheitlichen Wahrnehmung der Aufsicht durch eine Behörde bedarf der Einordnung in die historische Entwicklung der Datenschutzaufsicht. Bevor daher auf die Organisation der Aufsicht in den Ländern eingegangen wird, sollen die Anfänge der Kontrolle der Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen aufgezeigt werden.

---

699 Vgl. nur 30. Tätigkeitsbericht des LfD Baden-Württemberg, S. 11: „Damit wurde endlich ein „Geburtsfehler“ der Datenschutzaufsicht in Baden-Württemberg, der seit dem Inkrafttreten des Landesdatenschutzgesetzes am 1. April 1980 bestand, korrigiert.“; EuGH, Urteil v. 9. März 2010, C-518/07.

## I. Die Anfänge der Datenschutzaufsicht

Die Datenschutzaufsicht über die Verarbeitung von Daten bei öffentlichen und nicht-öffentlichen Stellen setzt datenschutzrechtliche Vorgaben an die Verarbeitung voraus.

Die Frage nach dem „Beginn" der Datenschutzaufsicht ist daher auch eine Frage nach dem Beginn der Datenschutzgesetzgebung bzw. den ersten von den verarbeitenden Stellen zu beachtenden datenschutzrechtlichen Bestimmungen.

### 1. Beginn der Datenschutzgesetzgebung

Die Rechtwissenschaft ist sich in Bezug auf die Anfänge der Datenschutzgesetzgebung zu großen Teilen einig und datiert den Beginn der „Geschichte der Datenschutzgesetzgebung" auf den 30. September 1970, den Tag der Verabschiedung des ersten hessischen Datenschutzgesetzes.[700]

Dabei soll der Datenschutz „durchweg vor dem Hintergrund der automatischen Datenverarbeitung entstanden" sein.[701]

---

700 Simitis/Hornung/Spiecker gen. Döhmann, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht,
1. Aufl., Einleitung, Rn. 1, m.w.N.

701 Vgl. Simitis/Hornung/Spiecker gen. Döhmann, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl., Einl. Rn 1 (Fn. 1); bzw. nach dem Wortlaut des ersten HDSG 1970 der „maschinellen Datenverarbeitung", vgl. § 1: „Der Datenschutz erfasst alle für Zwecke der maschinellen Datenverarbeitung erstellten Unterlagen sowie alle gespeicherten Daten (…)"; das BayDSG 1978 knüpft an die Verarbeitung von Daten in Dateien an, ob die Verarbeitung in „herkömmlichen oder automatisierten" Verfahren erfolgt ist unbeachtlich, vgl. Schweinoch/Geiger, Bayerisches Datenschutzgesetz, S. 33; dabei dürfte der Hessische Gesetzgeber weniger das Aufstellen von „Anforderungen" im Sinne von Eingriffsnormen in die Rechte der betroffenen Personen im Blick gehabt haben, als vielmehr eine „Anweisung an die Verwaltung an den Umgang mit Daten", ergänzt durch eine „spezielle, subsidiär geltende Verschwiegenheitspflicht", vgl. Erster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drs. 7/1495, 29. März 1972, S. 11.

a) Die automatisierte Verarbeitung von Daten

Die automatisierte Verarbeitung von Daten (ADV) in der öffentlichen Verwaltung hatte ihre Anfänge in den 60er Jahren im Bereich der Daseinsvorsorge genommen. Nachdem bereits im Jahr 1912 das sog. „Lochkartenverfahren“ bei der Ruhrknappschaft eingeführt worden war, kann jedenfalls seit der Anwendung der ADV bei der Bundesversicherungsanstalt für Angestellte im Jahr 1956 von einem Einsatz der ADV in der öffentlichen Verwaltung gesprochen werden.[702] Die entscheidende Neuerung, die mit zur Verbreitung der ADV führte, bestand im elektronischen Lesen des Datenträgers, der Lochkarte, worauf der Begriff der elektronischen Datenverarbeitung oder kurz „EDV“ zurückgeht.[703]

In den Anfängen wurde die EDV in der Verwaltung wie auch im Bereich der Privatwirtschaft vor allem bzw. fast ausschließlich im Bereich von Routine- und Massenarbeiten eingesetzt.[704] Dem Einsatz zur Bewältigung komplexerer Aufgaben standen die begrenzten technischen Möglichkeiten entgegen. Der Einsatz der EDV diente daher vor allem der Beschleunigung der Datenverarbeitung. Gleichzeitig, bedingt durch die Verbreitung der EDV aber auch dem Ausbau des Sozialstaates, wuchs die von der Verwaltung zu verarbeitende Datenmenge so rasant an, dass deren Bearbeitung schließlich nur noch unter Einsatz von EDV sichergestellt werden konnte.[705]

---

702 Zum Lochkartenverfahren und dem elektronischen Lesen der Lochkarte, vgl. Sandner/Spengler, Die Entwicklung der Datenverarbeitung von Hollerith Lochkartenmaschinen zu IBM Enterprise-Servern, S. 7 ff.

703 In Abgrenzung zu bspw. pneumatischen oder hydraulischen technischen Möglichkeiten als Verarbeitungsmittel, vgl. Meincke, Integrierte Datenverarbeitung in der öffentlichen Verwaltung unter besonderer Berücksichtigung der Kommunalverwaltung, S. 11.

704 vgl. 1. Bericht der Bundesregierung über die Anwendung der EDV in der Bundesverwaltung, BT-Drs. V/3355, S. 3; van Rienen, Frühformen des Datenschutzes?, S. 221.

705 van Rienen, Frühformen des Datenschutzes?, S. 221, m.w.N.; Erster Tätigkeitsbericht des Hessichen Datenschutzbeauftragten, Drs. 7/1495, 29. März 1972, S. 7; sozialkritisch hierzu im Jahr 1977 Mallmann, O.: „Je mehr der einzelne auf staatliche und privatwirtschaftliche Leistungen angewiesen ist, desto mehr Informationen werden von ihm verlangt und desto geringer sind seine Chancen, diese zu verweigern. Kurz, wieviel Privatsphäre der einzelne genießt, richtet sich nach seiner ökonomischen und gesellschaftlichen Position.“, Zielfunktionen des Datenschutzes, S. 32, m.w.N.

Mit fortschreitender technischer Entwicklung konnte die EDV in der Folge bei immer anspruchsvolleren Tätigkeiten eingesetzt werden. Hiermit ging wiederum ein breiterer Anwendungs- und Einsatzbereich der EDV einher. Damit war der „Siegeszug" der EDV vorgezeichnet.

Wie in anderen Bundesländern war auch in Hessen der Aufbau eines integrierten Informationssystems für die staatliche und kommunale Verwaltung beabsichtigt.[706] Hierzu wurde am 16. Dezember 1969 das Gesetz über die Errichtung der Hessischen Zentrale für Datenverarbeitung (HZD) und Kommunaler Gebietsrechenzentren (KGRZ) verabschiedet.[707] Die der ADV zugesprochene Bedeutung wurde vom damaligen Ministerpräsidenten *Osswald* folgendermaßen umschrieben: „Regieren und Verwalten wird in Zukunft mit der Entwicklung von Informationssystemen und Datenbanken untrennbar verbunden sein. Diese Modernisierung der Verwaltung wird (…) dem wachsenden Informationsbedürfnis von Legislative und Exekutive Rechnung tragen".[708]

Zur Abwehr der Gefahren der ADV entschied sich der hessische Gesetzgeber zum Erlass eines neuen Gesetzes. Dieses neue Gesetz war das erste HDSG von 1970.

Als durch die ADV gefährdet galt insbesondere die Privatsphäre der Bürger, die nicht nur in Hessen Ausgangspunkt der aufkommenden datenschutzrechtlichen Überlegungen war.[709] Das HDSG sollte auch dazu dienen etwaigen Bedenken der Bevölkerung gegenüber der automatisierten Verarbeitung vorzubeugen bzw. entgegenzuwirken. Dies wurde von der hessischen Landesregierung betont und vom Hessischen Ministerpräsidenten *Osswald* prägnant zusammengefasst: „Es darf nicht einmal ein berechtigter Anlaß für die Befürchtung gegeben werden, durch die Datenverarbeitung werde die Privatsphäre des Bürgers beeinträchtigt, oder die Automation schränke den Bereich der demokratischen Mitwirkung des

706 „Integrierte Datenverarbeitung" als „beste Organisationsform" der elektronischen Datenverarbeitung, deren „Ziel" und „höchste Stufe", vgl. Meincke, Integrierte Datenverarbeitung in der öffentlichen Verwaltung, S. 11, 16 ff.

707 GVBl. I, S. 304.

708 Hessischer Ministerpräsident Osswald im Vorwort zu „Hessen `80 – Datenverarbeitung", zitiert nach Erster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drs. 7/1495, 29. März 1972, S. 8.

709 Mallmann, O., Zielfunktionen des Datenschutzes, S. 24; Mallmann, C., Datenschutz in Verwaltungs-Informationssystemen, S. 75 f.

Bürgers in Staat und Gemeinde ein. Die wachsende Technisierung darf die Bürger nicht dem Staat entfremden".[710]

Hervorzuheben ist, dass der hessische Gesetzgeber die Initiative zur Verabschiedung des Datenschutzgesetzes ergriff, ohne dass es hierfür bereits eine Veranlassung in der Form von Datenschutzverletzungen gegeben hatte.[711]

Dabei war die fortschreitende automatisierte Verarbeitung in EDV-Anlagen ein in allen Bundesländern vorzufindender Prozess.[712] Spätestens mit den Planungen zu integrierten Datenverarbeitungsanlagen entstand in den Ländern auch ein Bewusstsein über die hiermit für die Bürger einhergehenden Gefahren (vgl. zu den integrierten Datenverarbeitungsanlagen nachfolgende Ausführungen zum sog. „Bayerischen Informationssystem" (BIS)).[713]

So legte beispielsweise die bayerische Staatsregierung im April 1970 den Entwurf eines Gesetzes über die Organisation der EDV vor, um die „voraussehbare stürmische Weiterentwicklung der Datenverarbeitung in der öffentlichen Verwaltung richtig zu lenken, und um gesicherte organisatorische Grundlagen zu schaffen".[714] In Baden-Württemberg wurde bereits

---

710 Osswald, in IBM-Nachrichten, 1971, S. 379; vgl. auch Mallmann, C., Datenschutz in Verwaltungs-Informationssystem, S. 75.

711 Vgl. v. Lewinski, in: Rüpke/v. Lewinski/Eckhardt, Datenschutzrecht, 1. Aufl., S. 21; dass die Verabschiedung des ersten HDSG auf eine „kritisch gewordene" Öffentlichkeit zurückzuführen ist, dürfte nur eingeschränkt zutreffen, so aber Mitrou, Die Entwicklung der institutionellen Kontrolle des Datenschutzes, S. 46; anders wohl hingegen die Entwicklung, die in Frankreich zum ersten franz. Datenschutzgesetz vom 6. Januar 1978 geführt hatte, vgl. Gerhold, 40 Jahre CNIL – Ein Blick auf den französischen Gendarmen des Privatlebens, DuD 2018,
S. 368.

712 Vgl. Seidel, Datenbanken und Persönlichkeitsrecht, S. 45 f.

713 Neben den Gefahren für die Bürger wurde auch eine Gefahr für die „Gewaltenbalance" diskutiert, in der Form, dass sich die Regierung gegenüber dem Parlament mit Hilfe von integrierten Informationssystemen einen „Informationsvorsprung" verschaffen könnte – Datenschutz „im weiteren Sinne" müsse daher auch die Ausgewogenheit der Informationshaushalte der Träger staatlicher oder gesellschaftlicher Macht sicherstellen, so auch mit Hinweis auf § 10 Abs. 2 des HDSG 1970, Löchner, in: Löchner/Steinmüller, Datenschutz u. Datensicherung, Vorträge auf der Tagung vom 26 und 27. Oktober 1974, Datenschutz und Datensicherung erläutert am Bundeszentralregister, S. 3.

714 Entwurf eines Gesetzes über die Organisation der elektronischen Datenverarbeitung im Freistaat Bayern,
Drs. 3248, 22. April 1970, Begründung, S. 3.

1969 der Entwurf des Gesetzes über die Datenzentrale Baden-Württemberg diskutiert.[715]

Vorreiter war allerdings das Land Schleswig-Holstein, in dem die Datenzentrale Schleswig-Holstein als Anstalt des öffentlichen Rechts mit dem Gesetz über die Datenzentrale Schleswig-Holstein vom 2. April 1968 errichtet wurde.[716]

### b) Das Bayerische Informationssystem (BIS)

In den Ländern, aber auch auf Bundesebene, war man der Überzeugung, dass sich die Datenverarbeitung wirtschaftlicher betreiben lasse, je größer die eingesetzten Maschinensysteme seien. So seien „mittelgroße und große Anlagen" nicht nur leistungsfähiger, sondern würden auch die „Vorteile einer integrierten Datenverarbeitung mit der Möglichkeit der Verknüpfung aller Daten eines organisatorisch zusammenhängenden Bereichs eröffnen".[717]

Kurz dargestellt werden soll das in Bayern im Jahr 1970 geplante System der automatisierten Verarbeitung unter Anwendung des Prinzips der integrierten Datenverarbeitung. Die Darstellung des geplanten BIS liegt nicht nur aufgrund des Bezugs dieser Arbeit zu Bayern nahe, sondern auch, da es sich beim BIS um das „umfassendste System dieser Art" unter den von den in den Ländern geplanten integrierten Informationssystem handelte.[718]

Das BIS sollte in einer Kooperation der Bayerischen Staatskanzlei mit der SIEMENS AG entstehen. Es war als System auf drei „Ebenen" angelegt oder wie *Steinmüller* es im Hinblick auf den dahinterstehenden Grundgedanken bezeichnet: „von archaischer Einfachheit".[719] Diese Ebenen lassen sich differenzieren in eine Ebene der staatlichen Verwaltungsstellen („staatliche Gebietsrechenstellen") und eine Ebene der Verwaltung auf kommunaler Ebene („kommunale Gebietsrechenzentren"). Übergeordnet war diesen eine Ebene, die sich aus „Regionalen Speicherzentren" zusammensetzen sollte. In diesen Regionalen Speicherzentren sollten die bislang

715 Drs. 5/1180, 10. Juli 1969.
716 GVOBl. S. 92.
717 Vgl. nur Entwurf eines Gesetzes über die Organisation der elektronischen Datenverarbeitung im Freistaat Bayern, Drs. 3248, 22. April 1970, Begründung, S. 3.
718 So Podlech, Datenschutz im Bereich der öffentlichen Verwaltung, S. 36.
719 Steinmüller, Strukturen der Datenzeit, in: v. Greiff, Das Orwellsche Jahrzehnt und die Zukunft der Wissenschaft, Hochschultage der FU Berlin 1980, S. 29.

organisatorisch getrennten Bereiche der staatlichen und der kommunalen EDV zusammengeführt werden. Über die Regionalen Speicherzentren sollten danach beispielsweise der staatlichen Verwaltung die durch die Kommunalverwaltung erhobenen Daten zur Verfügung stehen (und umgekehrt).[720]

Die Regionalen Speicherzentren sollten wiederum mit der als „Bayerische Informationszentrale" bezeichneten EDV verbunden werden. In der Bayerischen Informationszentrale sollten identifizierende Informationen gespeichert werden, die eine Rückverfolgung von der identifizierenden Information bis zu dem in der staatlichen oder kommunalen EDV gespeicherten Datum ermöglichen sollten. Die Bayerische Informationszentrale ist damit einem Inhaltsverzeichnis aller im BIS gespeicherten Daten vergleichbar und sollte einen „mittelbaren oder unmittelbaren" Zugriff „auf sämtliche im Netz der Datenverarbeitungsanlagen gespeicherten Daten der öffentlichen Verwaltung Bayerns" ermöglichen.[721] Oder wie dies von den Entwicklern beschrieben wurde: „mit totaler horizontaler und vertikaler Durchlässigkeit der Daten und Programme".[722]

Das bayerische integrierte Informationssystem hat nach *Podlech* exemplarischen Charakter für den Einsatz von integrierten Systemen auf Länderebene.[723] Das „Prinzip der Einmal-Beschaffung" von Daten gilt demnach auch vergleichbar für andere integrierte Informationssysteme. Die „Einmal-Beschaffung" auf Länderebene ist Merkmal und „Herzstück" der integrierten Informationssysteme und wird mittels Vorschriften zur Organisation, die die Zusammenarbeit zwischen der (EDV-) Verwaltung auf staatlicher und kommunaler Ebene regeln, sichergestellt. Für Bayern wird dies beispielsweise durch § 10 des bayerischen EDVG und einem Koope-

720 Vgl. Mallmann, C., Datenschutz in Verwaltungs-Informationssystemen, S. 15, m.w.N.

721 Mallmann, C., Datenschutz in Verwaltungs-Informationssystemen, S. 15, m.w.N.

722 Vgl. Steinmüller, Strukturen der Datenzeit, in: v. Greiff, Das Orwellsche Jahrzehnt und die Zukunft der Wissenschaft, Hochschultage der FU Berlin 1980, S. 29.

723 Vgl. auch Beschreibung des BIS durch Podlech im Interview mit Rost und Krasemann (Mitarbeiter des ULD Schleswig-Holstein), unter Min.: 16:37 -0 https://www.maroki.de/pub/video/podlech/interview_podlech_pub_v3_transkription_v1.pdf, abgerufen am 3. Januar 2021.

rationszwang von staatlicher und kommunaler EDV gewährleistet, die technisch in „Regionalen Speicherzentren" zusammengeführt wird.[724]

Auf die mit der Einführung des BIS bzw. allgemein der integrierten Informationssysteme einhergehenden verfassungsrechtlichen Implikationen soll an dieser Stelle nicht eingegangen werden. Schlussendlich trug jedoch insbesondere der technologische Fortschritt dazu bei, dass das BIS – basierend auf dem „überholten Großrechnerprinzip" – nicht umgesetzt wurde.[725]

### c) Das erste Hessische Datenschutzgesetz

Das erste HDSG bezieht sich allein auf die Verarbeitung durch öffentliche Stellen – die öffentlichen Stellen des Landes Hessen, also auf die Verarbeitung durch den Staat. Dabei dürfte außer Frage stehen, dass die Verarbeitung von Daten durch den Staat nicht erst mit den Möglichkeiten der automatischen Verarbeitung beginnt.

Soll die Geschichte der Datenschutzgesetzgebung mit dem ersten HDSG begonnen haben, so stellt sich die Frage nach dem Schutz der von einer Verarbeitung von Daten betroffenen Personen vor dem ersten HDSG bzw. vor der automatischen Verarbeitung von Daten.[726]

Zwar beschränkt sich die Auffassung des BVerfG, wonach es kein belangloses Datum gebe, auf die Verarbeitung unter den Bedingungen der automatischen Datenverarbeitung, jedoch erstreckt beispielsweise die DSGVO ihren Anwendungsbereich auch auf die nicht-automatisierte Verarbeitung von personenbezogenen Daten, jedenfalls sofern diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen.[727] Deutlich

724 Vgl. Mallmann, C., Datenschutz in Verwaltungs-Informationssystemen, S. 16, dort Fn. 35.

725 Steinmüller, Strukturen der Datenzeit, in: v. Greiff, Das Orwellsche Jahrzehnt und die Zukunft der Wissenschaft, Hochschultage der FU Berlin 1980, S. 29; zur technischen Entwicklung und den Auswirkungen auf datenschutzrechtliche Bestimmungen vgl. auch Sechster Tätigkeitsbericht des LfD Bayern, Drs. 10/4383, 2. August 1984, S. 15.

726 Zum Begriff der personenbezogenen Daten, vgl. Klar/Kühling, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl., Art. 4, Nr. 1, Rn. 3 ff.

727 Vgl. BVerfGE 65, 1 Rn. 45, vgl. hierzu auch: Geminn/Roßnagel, „Privatheit" und „Privatsphäre" aus der Perspektive des Rechts – ein Überblick, JZ 2015, S. 703, 706; vgl. Art. 2 Abs. 1 DSGVO, zur jedoch gebotenen restriktiven Auslegung vgl. Rüpke, in: Rüpke/v. Lewinski/Eckhardt, Datenschutzrecht, 1. Aufl., S. 122.

wird, dass die DSGVO anerkennt, dass nicht nur die automatisierte Verarbeitung von Daten Risiken birgt, sondern unter bestimmten Umständen auch die nicht-automatisierte Verarbeitung. Dass der Staat bereits vor den Möglichkeiten der automatischen Verarbeitung Daten in Dateisystemen bzw. auf strukturierte Art und Weise gespeichert und verarbeitet hat, dürfte außer Frage stehen.

Die Intention des hessischen Gesetzgebers beim Erlass des ersten HDSG war die Beschränkung der staatlichen Datenmacht. So habe „bisher die arbeitsteilige Aufgliederung in selbstständige Ressorts eine Barriere gegen die „Allwissenheit“ des Staates“ gebildet, die durch das integrierte Informationssystem aufgehoben werde.[728]

Staatliche Datenmacht dürfte kein Privileg des modernen Staates, sondern vielmehr Element eines Staates sein.[729] Wenn bei der Erzählung der Geschichte des Datenschutzes auf erste Volkszählungen Bezug genommen wird, so darf hierbei nicht vergessen werden, welche „Macht“ der Staat aus diesen Informationen gewinnen konnte.[730] Neben der Ermittlung der militärischen Stärke dürften die zu Grunde liegenden Informationen auch weitere staatliche Planung ermöglicht haben. Nicht zuletzt dürfte seit jeher das Wissen um das Einkommen der Staatsbürger zur Einziehung von Steuern Ausdruck staatlicher Datenmacht sein. Dabei kann nicht genug betont werden, dass neben der grundsätzlich bestehenden Gefahr staatlicher Datenmacht, die häufig mit dem Begriff des „gläsernen Bürgers“ umschrieben wird, auch unmittelbar ein Missbrauch dieser Macht in anderer Form, wie beispielsweise in der nationalsozialistischen Diktatur oder dem DDR-Regime, zu befürchten ist.[731]

---

728 Vgl. Erster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drs. 7/1495, 29. März 1972, S. 8.

729 Nach v. Lewinski verwandelte sich die „informationelle Blindheit“ des „jungen modernen Staates“ „punktuell und allmählich“ vgl. Datenmacht, Geschichte des Datenschutzrechts von 1600 bis 1977, in: Arndt u.a., Freiheit – Sicherheit – Öffentlichkeit, S. 204, ders. geht auf Datenmacht in der Antike und Mittelalter ein, erklärt allerdings, „wie weit zu diesen Zeiten auch Herrschaft durch Datenmacht ausgeübt wurde, darüber ist wenig bekannt“, a.a.O. S. 202.

730 Die Beschreibung als „konstitutiver Prozeß der Umwandlung einer formlosen Masse in ein Volk“, dürfte dies nicht abschließend erfassen, so aber Mitrou, Die Entwicklung der institutionellen Kontrolle des Datenschutzes, S. 31.

731 Vgl. Masing, Herausforderungen des Datenschutzes, NJW 2012, S. 2305; Geminn/Roßnagel, „Privatheit“ und „Privatsphäre“ aus der Perspektive des Rechts – ein Überblick, JZ 2015, S. 703 zum Schutz der Privatsphäre in der DDR.

In dieser Arbeit wird die Entwicklung der Geschichte des Datenschutzes nicht weiter verfolgt, da der Fokus dieser Arbeit auf die Entwicklung des Datenschutzrechts in den 1970er Jahren – und damit einhergehend der Entwicklung der Datenschutzaufsicht – gelegt werden soll.

Gleichwohl soll deutlich zum Ausdruck gebracht werden, dass nach hier vertretener Auffassung mit dem ersten HDSG „lediglich" auf die mit der Entwicklung der automatisierten Verarbeitung einhergehenden Gefahren reagiert wurde.[732] Das Bedürfnis eines Schutzes von Informationen, die der Bürger dem Staat anvertraut hat, und zwar auch vor Missbrauch durch den Staat, bestand jedoch bereits zuvor. Die Geschichte des Datenschutzes ist daher, jedenfalls soweit diese nicht als auf den Datenschutz in Bezug auf die Gefahren der automatisierten Verarbeitung beschränkt verstanden wird, keine „kurze".[733] Dass grundsätzlich ein Bewusstsein für den Schutz der Informationen von und über Menschen bestand, zeigt sich beispielsweise im seit wohl ab 1215 geschützten Beichtgeheimnis der römisch-katholischen Kirche.[734]

Dadurch wird nach hier vertretener Auffassung deutlich, dass die Geschichte des Datenschutzes, auch wenn der Begriff des Datenschutzes nicht weiter zurückverfolgt werden kann als bis zum Gesetzgebungsprozess zum ersten HDSG, weiter als bis ins Jahr 1970 zurückgeht.[735] Dies gilt jedenfalls

---

732 So wohl grds. 1971 auch noch Simitis: „Sämtliche zur Zeit existierende Schutzmaßnahmen sind auf eine ganz andere Informationsstruktur zugeschnitten. Sie stellen Reaktionen auf ein Instrumentarium dar, das mit der elektronischen Datenverarbeitung überhaupt nicht verglichen werden kann. Gerade weil elektronische Anlagen eine neue Informationsqualität garantieren, bedarf es auch neuer, an den spezifischen Eigenschaften der elektronischen Datenverarbeitung ausgerichteter Regeln. Kurzum, noch so erprobte Abwehrstrategien sind nur solange akzeptabel, wie sich auch an den Gefahrenquellen nichts ändert.", Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673, 677.

733 So aber Simitis, Zur Datenschutzgesetzgebung: Vorgaben und Perspektiven, CR 1987, S. 602.

734 IV Laterankonzils, Canon 21; vgl. zum Beichtgeheimnis auch Interview Podlech mit Rost und Krasemann (Mitarbeiter des ULD Schleswig-Holstein), unter Min.: 12:54–0 https://www.maroki.de/pub/video/podlech/interview_podlech_pub_v3_transkription_v1.pdf, abgerufen am 3. Januar 2021.

735 Vgl. Bull, Datenschutz oder die Angst vor dem Computer, S. 84: „es scheint, als sei der hessische Gesetzgeber von 1970 „schuld" an dieser Wortschöpfung", der den Begriff „Datenschutz" als „eigentlich ganz unpassend" bezeichnet, a.a.O., S. 83; v. Lewinski, Geschichte des Datenschutzrechts von 1600 bis 1977, in: Arndt u.a., Freiheit – Sicherheit – Öffentlichkeit, S. 197 m.w.N.

dann, wenn man Datenschutz wie in den Anfängen der Datenschutzgesetzgebung als Regelung bzw. objektiv-rechtliche Beschränkung der staatlichen Datenmacht versteht.[736]

Gleichwohl sind grundsätzlich „einheitlich“ Anwendung findende Datenschutzgesetze, losgelöst von bestimmten Bereichen und an die Verarbeitung von Daten anknüpfend – wie sich diese als Landesdatenschutzgesetze und Bundesdatenschutzgesetz ab den 1970er Jahren entwickelten – zu begrüßen.[737]

Wenn nachfolgend vom Beginn der Datenschutzgesetzgebung gesprochen wird, so wird dabei auf die Entwicklung in den 1970er Jahren in Reaktion auf die Verbreitung findende automatische Verarbeitung von Daten – also dem Datenschutz ab 1970 – Bezug genommen.

## 2. Das Gesetz über die Organisation der elektronischen Datenverarbeitung im Freistaat Bayern (EDVG)

Wie bereits ausgeführt, war man sich in den Ländern der Gefahren der ADV und auch über die Notwendigkeit diesen entgegenzuwirken bewusst.

Allerdings bestand in den Ländern eine „fast elementare Unsicherheit im Umgang mit dem „Datenschutz““.[738]

Die von den Ländern zur Abwehr dieser Gefahren getroffenen Maßnahmen wurden als „mehr oder weniger impulsive Reaktionen, keineswegs also durchdachte, in den Details ausgewogene und die Probleme exakt regelnde Normenkomplexe“ beschrieben.[739] Es würde an „genauen Vorstellungen über Voraussetzungen und Implikationen der angestrebten Regelungen“ fehlen und daher die „Ergebnisse“ in den Ländern unterschiedlich ausfallen, was eine „extreme partikular-rechtliche Zersplitterung“ zur Folge habe.[740]

---

736 Vgl. v. Lewinski, Geschichte des Datenschutzrechts von 1600 bis 1977, in: Arndt u.a., Freiheit – Sicherheit – Öffentlichkeit, S. 220.

737 So wohl schon Kerkau, Automatische Datenverarbeitung, S. 52 f.; gleichwohl bestehen bis heute bereichsspezifische Regelungen, etwa im Sozialdatenschutz.

738 Simitis, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673, 677.

739 Simitis, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673, 677.

740 Simitis, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673, 677.

Wie bereits dargestellt, entschied man sich in Hessen für ein „eigenes" Datenschutzgesetz.[741] Hiermit beschritt Hessen jedenfalls im Jahr 1970 und bis zur Verabschiedung des Datenschutzgesetzes in Rheinland-Pfalz im Jahr 1974 einen Sonderweg.[742]

Andere Länder entschieden sich Regelungen mit Bezug zu den Gefahren der automatisierten Verarbeitung in die Gesetze zur Organisation der EDV aufzunehmen oder versuchten, die erkannten Risiken auf andere Weise zu beschränken. So erklärte beispielsweise der erste niedersächsische LfD *Tebarth*, dass die „erste datenschutzrechtliche Regelung" in Niedersachen bereits 1970 mit dem „Erlaß zur vorläufigen Regelung des Datenschutzes in den Rechenzentren des Landes" getroffen worden sei.[743]

Das erste Land, das ein Gesetz zur Errichtung einer Datenzentrale verabschiedet hatte, Schleswig-Holstein, reagierte ebenfalls bereits 1970 auf die (zwischenzeitlich) erkannten Gefahren und erließ eine Dienstanweisung über den Schutz der Daten und ihre Geheimhaltung (Datengeheimnis) in der Datenzentrale Schleswig-Holstein noch vor dem ersten HDSG.[744]

Bevor exemplarisch die in das bayerische EDVG von 1970 aufgenommenen Regelungen dargestellt werden, soll kurz auf den Gesetzgeber auf Bundesebene eingegangen werden. Dies ist geboten, um aufzuzeigen, dass die gesetzgeberischen Bemühungen der Länder bei aller berechtigter Kritik im Vergleich zur Entwicklung auf Bundesebene durchaus positiv zu bewerten sind.

Auf Bundesebene wurde unter anderem an einem Informationsbankensystem, einer Personaldatenbank des Bundes, einer Sozialdatenbank und einer Arbeitsdatenbank gearbeitet, die auf Grundlage eines einzuführenden Personenkennzeichens aufgebaut werden sollten.[745]

---

741 Angelehnt an Simits, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673, 677, wonach Hessen „einem eigenen „Datenschutzgesetz" den Vorzug" gegeben habe.

742 Vgl. Hondius, Emerging data protection in Europe, S. 35: "The Hessian Act is unique in that rules on data protection have been laid down there in a separate instrument and not just as a part of the law by which the data centre was created.".

743 Erster Bericht über die Tätigkeit des Nds. Datenschutzbeauftragten, Drs. 9/1300, 27. Dezember 1979 S. 4.

744 Dienstanweisung über den Schutz der Daten und ihre Geheimhaltung (Datengeheimnis) in der Datenzentrale Schleswig-Holstein vom 3. Februar 1970.

745 Podlech, Datenschutz im Bereich der öffentlichen Verwaltung, S. 36 f. m.w.N; vgl. auch Seidel, Datenbanken und Persönlichkeitsrecht, S. 47 f.; zum Personenkennzeichen vgl. auch van Rienen, Frühformen des Datenschutzes?, S. 232 f.

Gleichwohl hielt man die „bisherigen Schutzvorkehrungen" für ausreichend und bezog sich hierbei auf die bestehenden „Amts- und Verschwiegenheitspflichten".[746]

So führte der Bundesminister des Innern *Genscher* im Jahr 1970 aus: „Eine denkbare Beeinträchtigung der Privatsphäre des Einzelnen würde folglich nicht durch die Einführung eines Personenkennzeichens, sondern durch missbräuchliche Ausnutzung der Rationalisierungsmöglichkeiten der elektronischen Datenverarbeitung veranlaßt. Derartige Mißbräuche können durch herkömmliche Sicherungen und automationsgerechte Schutzvorkehrungen weitgehend verhindert werden."[747]

Nachfolgend soll dargestellt werden, wie der bayerische Gesetzgeber reagierte, um den erkannten Gefahren der automatisierten Verarbeitung zu begegnen. Nachdem aus der vorangehenden Darstellung der Entwicklung der Datenschutzaufsicht in Bayern bereits hervorgeht, dass der bayerische Gesetzgeber trotz eines gerne vertretenen „bayerischen Wegs" im Datenschutzrecht regelmäßig die Entwicklung auf Bundesebene „abwartete", dürfte es wenig überraschen, dass auch in den Jahren um 1970 die „Aktivitäten" auf Bundesebene abgewartet werden sollten.[748]

Zum Schutz vor den Gefahren der automatisierten Verarbeitung wurden zwei Regelungen ins bayerische EDVG aufgenommen. Zum einen Art. 15 „Geheimhaltung" zur Regelung von Amtsverschwiegenheit und Geheimhaltungspflicht und zum anderen Art. 16 „Strafbestimmungen" bei Verstößen gegen dieselben. Diese sollen nachfolgend zitiert werden:

> *Art. 15*
> *(1) Jede mit Datenverarbeitung im Sinne dieses Gesetzes befaßte Stelle hat dafür zu sorgen, daß die Pflicht zur Amtsverschwiegenheit oder besondere Geheimhaltungspflichten gewahrt werden, auch wenn sie die Daten durch andere Stellen ermitteln, erfassen, speichern oder verarbeiten läßt.*
> *(2) Daten, die der Pflicht zur Amtsverschwiegenheit oder besonderen Geheimhaltungspflichten unterliegen, dürfen Dritten nur nach Maßgabe der hierfür geltenden Regelungen zugänglich gemacht werden. Die Staatsregierung kann durch Rechtsverordnung bestimmen, in welcher Form solche*

746 Van Rienen, Frühformen des Datenschutzes?, S. 225, m.w.N; Simitis, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673, 677.

747 BT-Drs. VI/598, 1. April 1970, für den Bereich des Meldewesens sollten von der Bundesregierung weitere Regelungen vorgeschlagen werden.

748 Vgl. Mallmann, C., Datenschutz in Verwaltungs-Informationssystemen, S. 77, m.w.N.

*Daten weitergegeben und welchen Stellen sie zugänglich gemacht werden dürfen.*

*Art. 16*
*(1) Mit Freiheitsstrafe bis zu einem Jahr und mit Geldstrafe oder mit einer dieser Strafen wird bestraft, wer*
*1. ein fremdes Geheimnis, insbesondere ein Geschäfts- oder Betriebsgeheimnis, das ihm im Zusammenhang mit der Datenverarbeitung im Sinne dieses Gesetzes bekannt geworden ist, unbefugt offenbart oder verwertet.*
*2. ein Geheimnis der in Nr. 1 genannten Art sich unbefugt verschafft oder ein solches, unbefugt erlangtes Geheimnis offenbart oder verwertet.*
*(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einem anderen einen Vermögensvorteil zu verschaffen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren. Daneben kann auf Geldstrafe erkannt werden.*
*(3) Diese Vorschriften gelten nur, soweit die Tat nicht in anderen Bestimmungen mit Strafe bedroht ist.*
*(4) Die Tat wird nur auf Antrag des Verletzten verfolgt. Der Strafantrag kann zurückgenommen werden.*

Aus der Begründung zu Art. 15 EDVG (im Gesetzesentwurf noch Art. 14 EDVG) geht hervor, dass mit Art. 15 EDVG grundsätzlich keine „neuen" Geheimhaltungsverpflichtungen geschaffen werden sollten. Vielmehr wurde in der Begründung auf die bereits bestehenden allgemeinen Vorschriften über die Amtsverschwiegenheit sowie auch die „zahlenreichen" Einzelvorschriften in Bundes- und Landesrecht zum Schutz von „Geheimnissen" der Bürger verwiesen.[749]

Die Regelung des Art. 15 Abs. 1 EDVG sollte sicherstellen, dass die bereits bestehenden Geheimhaltungspflichten auch bei der ADV gewährleistet sind. Darüber hinaus sollten die mit der Verarbeitung von Daten befassten Stellen die Geheimhaltung auch dann sicherstellen, wenn sie die Verarbeitung durch eine andere Stelle vornehmen lassen sollten. Schließlich sollte Art. 15 EDVG „Auffangcharakter" haben. So sollte sichergestellt werden, dass nicht dadurch, dass einzelne Gesetze den zur Geheimhaltung

749 Von den allgemeinen Vorschriften über die Amtsverschwiegenheit wurden Art. 69 bis 72 BayBG, § 9 BAT, Art. 40 bis 42 des Gesetzes über kommunale Wahlbeamte und Art. 20 Abs. 2 und 3 der Gemeindeordnung aufgezählt; für die Einzelvorschriften § 22 Abgabenordnung, § 12 Bundesstatistikgesetz, § 44 Abs. 4 Außenwirtschaftsgesetz, § 9 Kreditwesengesetz, § 9 Lebensmittelgesetz, vgl. Begründung des Gesetzesentwurfs, Beilage 3248, 22. April 1970, S. 6.

verpflichteten Personenkreis unterschiedlich bestimmen, Schutzlücken entstehen.[750]

Auch Art. 15 Abs. 2 EDVG nimmt Bezug auf bereits bestehende Vorschriften („nach Maßgabe der hierfür geltenden Regelungen"). Wie schon mit Art. 15 Abs. 1 EDVG sollte sicher- und klargestellt werden, dass die bislang geltenden Vorschriften, hier für die Weitergabe von Daten an andere Stellen und Dritte, auch für die in EDV-Anlagen gespeicherten Daten gelten.[751]

Entsprechend Art. 15 EDVG sollte auch Art. 16 EDVG die bestehenden Strafvorschriften nach Bundes- und Landesrecht ergänzen. Über die Regelung des Art. 16 EDVG sollte ein „lückenloser Schutz der Geheimhaltung" gewährleistet werden.[752]

Die ins bayerische EDVG aufgenommen Normen zum „Datenschutz" stießen dann auch eher auf verhaltene Resonanz bis hin zu offener Kritik. So würden sich diese Regelungen „zwangsläufig recht summarisch" mit den Gefahren der ADV befassen.[753] Der bayerische Gesetzgeber sei sich der Gefahren, die die ADV für die Privatsphäre mit sich bringe, nicht bewusst geworden. Nach „traditioneller Juristenart" sei eine Änderung der „legislativen Situation" erst im Nachhinein zu erwarten, also nach bereits eingetretenen Verletzungen der Privatsphäre. Das Abwarten des bayerischen Gesetzgebers würde von diesem mit Verweis auf bestehenden Vorschriften zur „Geheimhaltung" gerechtfertigt, um Zeit zu gewinnen.[754]

### 3. Datenschutz als „originär hessische Erfindung"

An dieser Stelle soll ein Vergleich des Wortlauts von Art. 15 Abs. 1 EDVG mit § 3 Abs. 1 HDSG 1970 und Art. 15 Abs. 2 EDVG mit § 5 Abs. 2 des hessischen Gesetzes über die Errichtung der Hessischen Zentrale für Datenverarbeitung (HZD) und Kommunaler Gebietsrechenzentren (KGRZ)

750 Vgl. Begründung des Gesetzesentwurfs, Beilage 3248, 22. April 1970, S. 6.
751 Vgl. Begründung des Gesetzesentwurfs, Beilage 3248, 22. April 1970, S. 6; vgl. auch Mallmann C., Datenschutz in Verwaltungs-Informationssystemen, S. 76.
752 Vgl. Begründung des Gesetzesentwurfs, Beilage 3248, 22. April 1970, S. 6.
753 Simitis, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673, 677.
754 Mallmann, C., Datenschutz in Verwaltungs-Informationssystemen, S. 77.

vorgenommen werden.[755] Da der Datenschutz nach dem hessischen LfD *Ronellenfitsch* eine „originär hessische Erfindung" ist, bietet sich ein solcher Vergleich an.[756]

| § 3 HDSG 1970 „Datengeheimnis" | Art. 15 EDVG 1970 „Geheimhaltung" |
|---|---|
| *(1) Den mit der Datenerfassung, dem Datentransport, der Datenspeicherung oder der maschinellen Datenverarbeitung betrauten Personen ist untersagt, die dabei erlangten Kenntnisse über Unterlagen, Daten und Ergebnisse anderen mitzuteilen oder anderen zu gestatten oder andere dabei zu fördern, derartige Kenntnisse zu erlangen, soweit sich nicht eine Befugnis aus Rechtsvorschriften oder aus der Zustimmung derjenigen ergibt, die über Unterlagen, Daten und Ergebnisse verfügungsberechtigt sind.*<br>*(2) Das Verbot des Abs. 1 gilt nicht, wenn die dort bezeichneten Handlungen zur verwaltungsmäßigen oder technischen Durchführung der Datenverarbeitung erforderlich sind.*<br>*(3) Die Pflicht zur Geheimhaltung besteht auch nach der Beendigung der in Abs. 1 bezeichneten Tätigkeiten.*<br>*(4) Gesetzliche Auskunftspflichten bleiben unberührt.* | *(1) Jede mit Datenverarbeitung im Sinne dieses Gesetzes befaßte Stelle hat dafür zu sorgen, daß die Pflicht zur Amtsverschwiegenheit oder besondere Geheimhaltungspflichten gewahrt werden, auch wenn sie die Daten durch andere Stellen ermitteln, erfassen, speichern oder verarbeiten läßt.*<br>*(2) Daten, die der Pflicht zur Amtsverschwiegenheit oder besonderen Geheimhaltungspflichten unterliegen, dürfen Dritten nur nach Maßgabe der hierfür geltenden Regelungen zugänglich gemacht werden. Die Staatsregierung kann durch Rechtsverordnung bestimmen, in welcher Form solche Daten weitergegeben und welchen Stellen sie zugänglich gemacht werden dürfen.* |
| § 5 Gesetz über die Errichung der HZD und KGRZ „Zugriff auf Datenbestände" | |
| *(2) Durch die Erledigung von Verwaltungsarbeiten und anderen Aufgaben unter Einsatz von Datenverarbeitungsanlagen werden die Vorschriften über die Geheimhaltung nicht berührt.* | |

Ausgehend hiervon wird deutlich, dass auch der hessische Gesetzgeber davon ausging, dass eine Regelung zur Geheimhaltungsverpflichtung von

755 Gesetz über die Errichtung der Hessischen Zentrale für Datenverarbeitung (HZD) und Kommunaler Gebietsrechenzentren (KGRZ) vom 16. Dezember 1969, GVBl. II 300–8.

756 Hessischer LfD Ronellenfitsch im Jahr 2018, vgl. https://www.deutschlandfunkkultur.de/pionier-beim-datenschutzgesetz-eine-originaer-hessische.976.de.html?dram:article_id=409621, abgerufen am 26. Mai 2020.

ihrer Art her ausreiche, um den Gefahren der ADV zu begegnen. In Abgrenzung zu Art. 15 EDVG „erweiterte" man jedoch nicht den Anwendungsbereich der bestehenden Regelungen zur Amtsverschwiegenheit auf die ADV, sondern begründete eine „eigene" Geheimhaltungsverpflichtung für die mit der „Datenerfassung, dem Datentransport, der Datenspeicherung oder der maschinellen Datenverarbeitung" betrauten Personen.[757] Auffällig ist aber die Anknüpfung an die mit der Verarbeitung betrauten Personen und damit einhergehend die Annahme, dass die Verarbeitung vollständig durch betraute Personen erfolge, während das EDVG hier schon an die verarbeitende Stelle anknüpfte.[758]

Grundsätzlich ist jedoch festzustellen, dass sowohl das HDSG 1970 als auch das EDVG „lediglich" an bereits etablierte „Schranken" zum Schutz der Bürger anknüpften. Dies könnte unter anderem darin begründet liegen, dass vor allem an die von den in die EDV eingebundenen Personen ausgehenden Gefahren angeknüpft wurde und weniger an die EDV selbst. So beginnt auch die Begründung zu § 3 HDSG 1970 mit den Worten: „Um einer unzulässigen Verbreitung vor allem von Daten aus der Intimsphäre der Bürger entgegenzuwirken, ist die Einführung eines Datengeheimnisses erforderlich (…)." Gesehen wurde vor allem das Risiko, dass die in die Verarbeitung eingebundenen Personen die verarbeiteten Daten „verbreiten" könnten.

Entsprechend ist auch die Regelung zur Geheimhaltung nach dem bayerischen EDVG zu lesen. Die Vorgabe zur Geheimhaltung nach Art. 15 EDVG steht in Zusammenhang mit den „Einzelvorschriften, die die Behörden verpflichten, die Geheimnisse der Staatsbürger, (…), zu wahren, die ihnen bei der Erfüllung ihrer Aufgaben zur Kenntnis gelangen."[759] Die Regelung des EDVG sollte sicherstellen, dass diese Einzelvorschriften zur Sicherstellung der Geheimhaltung nicht dadurch beeinträchtigt werden, dass „die zur Geheimhaltung verpflichtete Behörde" sich zur Erfüllung ihrer Aufgaben der Mittel der automatischen Datenverarbeitung bedient. Dabei stand im Vordergrund, dass die Geheimhaltung der einer verarbeitenden Stelle zur Kenntnis gelangten Daten – auch bei Einbindung weiterer Stellen – gewahrt bleibt. Im Vergleich zur Regelung des § 3 HDSG

757 Vgl. van Rienen, Frühformen des Datenschutzes?, S. 257; Steinmüller, Gutachten: Grundfragen des Datenschutzes, BT Drs. VI/3826, 7. September 1972, S. 120; vom ersten Hessischen Datenschutzbeauftragten bezeichnet als: „spezielle, subsidiär geltende Verschwiegenheitspflicht", vgl. Erster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drs. 7/1495, 29. März 1972, S. 11.

758 Hierzu auch van Rienen, Frühformen des Datenschutzes?, S. 257 f.

759 Drs. 6/3248, 22. April 1970, S. 6.

1970 ist bei Art. 15 EDVG hervorzuheben, dass sich die Pflicht zur Sicherstellung der Geheimhaltung auch auf die Einbindung von anderen Stellen bereits im Vorfeld der Datenverarbeitung, also bei der „Ermittlung/Erfassung", erstreckte. Auch die Regelungen zur Weitergabe von Daten dürften als ausdifferenzierter bezeichnet werden. Durch die Möglichkeit zum Erlass von Rechtsverordnungen sollten die Voraussetzungen geschaffen werden, Daten nach „dem Grad ihrer Schutzbedürftigkeit" einzuteilen. Ein Ansatz, der, wie die Differenzierung in der DSGVO in Bezug auf sensible Daten zeigt, durchaus zukunftsweisend war.[760]

Die Beschränkung der Gefahr eines für den Staat „gläsernen Bürgers" und damit verbunden der Gefahr des Missbrauchs staatlicher Datenmacht blieb jedoch sowohl im bayerischen EDVG als auch im HDSG 1970 außen vor.

Die Bewertung der oben genannten Normen soll mit Verweis auf die Ausführungen des ersten Hessischen Datenschutzbeauftragten *Birkelbach* in dessen zweiten Tätigkeitsbericht aus dem Jahr 1973 geschlossen werden. Dieser erklärte, dass bei der Untersuchung des Ablaufs der maschinellen Datenverarbeitung unter dem „Blickpunkt möglicher Gefährdungen" deutlich werde, dass es, um dem Bürger ein vergleichbares oder höheres Schutzniveau wie das durch Amtsgeheimnis und Verschwiegenheitspflicht vermittelte zu gewährleisten, „anderer als der herkömmlichen Mittel der öffentlichen Verwaltung bedarf".[761] Denn der Vergleich der herkömmlichen Verwaltungstätigkeit mit der automatisierten Verwaltung zeige, „daß der Mensch hier als Träger der Verschwiegenheitspflicht weitgehend ausgeschaltet ist".[762] Die „Zusammenführung von Informationen aus verschiedenen Lebensbereichen" könne „Konflikte mit der Verpflichtung der staatlichen Gewalt, die Würde des Menschen zu achten" herbeiführen, was in „außerordentlich verstärktem Maße" für die EDV gelte.[763] Umso mehr „individualisierende Daten in den Verarbeitungsvorgang" eingebracht werden würden und „je weiter die Verbindung von Dateien verschiedener Lebensbereiche zu einer Datenbank oder zu einem Informationssystem fortschreite", müsse im Hinblick auf den Schutz des Persönlichkeitsrechts „eine sorgfältige Auswahl der personenbezogenen Daten schon

760 Drs. 6/3248, 22. April 1970, S. 7.
761 Zweiter Tätigkeitsbericht des Hessischen Landesbeauftragten, Drs. 7/3137, 29. März 1973, S. 18.
762 Zweiter Tätigkeitsbericht des Hessischen Landesbeauftragten, Drs. 7/3137, 29. März 1973, S. 19.
763 Zweiter Tätigkeitsbericht des Hessischen Landesbeauftragten, Drs. 7/3137, 29. März 1973, S. 19.

bei der Datenermittlung“ erfolgen.[764] Damit trat neben die Gefahr des Missbrauchs von Datenwissen durch Amtsträger die erkannte Gefahr des Missbrauchs der Datenmacht durch den Staat, zu deren Einschränkung, wie der Hessische Datenschutzbeauftragt ausführte, beispielsweise schon an die „Datenermittlung“ anzuknüpfen war. Hiermit beschrieb er die Entwicklung hin zu den ersten Datenschutzgesetzen, bei denen sich Titel und Inhalt deckten.

Mögliche weitere Kritikpunkte sowohl an der Regelung des § 3 HDSG 1978 als auch des Art. 15 EDVG von 1970 sollen an dieser Stelle jedoch nicht aufgegriffen werden, um den Fokus auf den „Fortschritt“, den das HDSG 1970 mit sich brachte, legen zu können.

Dieser Fortschritt ist insbesondere die Entscheidung für die Fremdkontrolle der Verarbeitung und die Einführung eines Datenschutzbeauftragten als für die Aufsicht zuständige Stelle.

### 4. Ergebnis

Ob das erste HDSG 1970 ein „Zufallsprodukt“ ist, nachdem mit dem Gesetz über die Errichtung der Hessischen Zentrale für Datenverarbeitung (HZD) und Kommunaler Gebietsrechenzentren (KGRZ) von 1969 vergleichsweise früh die Errichtung entsprechender Rechenzentren geregelt, aber mit § 5 Abs. 2 und Abs. 3 dieses Gesetzes den Risiken der Verarbeitung wenig Aufmerksamkeit geschenkt wurde, bleibt vorliegend offen. Gleichwohl fallen die Verabschiedung des bayerischen EDVG von 1970 und des ersten HDSG im Jahr 1970 nur um wenige Tage auseinander.[765] Nachdem der Entwurf der bayerischen Staatsregierung für das EDVG am 22. April 1970 an den bayerischen Landtag übermittelt worden war und damit dem Entwurf für das HDSG, der auf den 25. Juni 1970 datiert, vorausging, war der hessische Gesetzgeber schließlich „schneller“.

Wie gesehen stand bei beiden Gesetzen der Schutz der Bürger vor den sich aus der automatisierten Verarbeitung ergebenden Gefahren im Vordergrund, der über Regelungen zur Amtsverschwiegenheit gewährleistet werden sollte. Wenn etwa der § 3 HDSG 1970 als die wohl zentrale Vorschrift des ersten HDSG den Beginn der Datenschutzgesetzgebung

764 Zweiter Tätigkeitsbericht des Hessischen Landesbeauftragten, Drs. 7/3137, 29. März 1973, S. 20.

765 HDSG 1970 vom 7. Oktober, GVBl. S. 625 und EDVG vom 12. Oktober 1970, GVBl. S. 457.

markieren soll, so lässt sich dem Art. 15 des EDVG die Eigenschaft als „datenschutzrechtliche Bestimmung“ nur schwerlich abstreiten. Anderenfalls müsste dies gegebenenfalls beiden Normen abgesprochen werden und der Beginn der „Datenschutzgesetzgebung“ an anderer Stelle gesucht werden.[766]

Festhalten lässt sich, dass in einer Vielzahl von Ländern die Notwendigkeit des gesetzgeberischen Tätigwerdens gesehen wurde. Jedoch war es allein der hessische Gesetzgeber, der von der Regelung des „Datenschutzes“ mittels Einzelbestimmungen in Gesetzen absah und sich für die Verabschiedung eines eigenen „Datenschutzgesetzes“ entschied, dessen Anwendungsbereich sich auf die Verarbeitung bei grundsätzlich allen öffentlichen Stellen des Landes erstreckte.[767] Das HDSG 1970 bereitete damit auch den Weg für den Datenschutz im Hinblick auf die Abkehr vom Prinzip der integrierten Verarbeitung mittels großer EDV-Anlagen hin zur durch den technologischen Fortschritt ermöglichten dezentralen Verarbeitung.

Auch wenn der These „Datenschutz ist eine originär hessische Erfindung“ daher unter Bezugnahme auf die vorhergehenden Ausführungen nur eingeschränkt gefolgt werden kann, soll jedoch die Bedeutung des HDSG nicht geschmälert und jedenfalls der Landesbeauftragte für den Datenschutz bzw. nach dem ersten HDSG der Datenschutzbeauftragte als originär hessische Erfindung gewürdigt werden.[768] Denn unabhängig von einer Diskussion über den Beginn der Datenschutzgesetzgebung, hat der hessische Gesetzgeber mit Einrichtung des Datenschutzbeauftragten – auch wenn dessen Rolle und Kompetenzen kritisiert worden sind – nicht nur die Ausgestaltung der Kontrolle der Einhaltung des Datenschutzes bis

766 Vgl. v. Lewinski, Geschichte des Datenschutzrechts von 1600 bis 1977, in: Arndt u.a., Freiheit – Sicherheit – Öffentlichkeit, S. 211: „die Amtsverschwiegenheit füllte in diesen „Datenschutzgesetzen der ersten Generation“ die inhaltliche Lücke, als sie schon so hießen, aber noch keine waren“.

767 Angelehnt an Simits, NJW 1971, S. 673, 677, wonach Hessen „einem eigenen „Datenschutzgesetz“ den Vorzug“ gegeben habe

768 Zum Datenschutz als originär hessische Erfindung vgl. der Hessische Datenschutzbeauftragte Ronellenfitsch im Jahr 2018, vgl. https://www.deutschlandfunkkultur.de/pionier-beim-datenschutzgesetz-eine-originaer-hessische.976.de.html?dram:article_id=409621, abgerufen am 26. Mai 2020; vgl. v. Lewinski, Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive, in: Schmidt/Weichert, Datenschutz, S. 29: „eine bis heute für das deutsche Datenschutzrecht strukturprägende Institution“.

heute geprägt, sondern auch besonderes Bewusstsein für die Gefahren der automatisierten Verarbeitung bewiesen.[769]

## II. Die Datenschutzaufsicht als „gemeinsame Entwicklung" in Bund und Ländern

Auf die 1970 in Hessen getroffene Entscheidung für die Einrichtung eines Datenschutzbeauftragten wurde, wie auch auf die Diskussion in Rheinland-Pfalz und auf Bundesebene, die zur Einrichtung des BfD führte, bereits unter Kapitel D., II. eingegangen.

Die Darstellung unter Kapitel D., II. ist auf die zur Entscheidung für die Fremdkontrolle in den Datenschutzgesetzen von Hessen, Rheinland-Pfalz und dem BDSG 1977 führenden Gründe beschränkt – da diese vor dem ersten BayDSG verabschiedet worden waren und der bayerische Gesetzgeber sich hieran orientierte.

An dieser Stelle soll auf die allgemein in den Ländern getroffene Entscheidung für die Fremdkontrolle der Verarbeitung bei den öffentlichen Stellen eingegangen werden. Die Notwendigkeit einer solchen Kontrolle wurde grundsätzlich in allen Ländern gesehen. Eine prägnante Begründung hierfür gibt der erste LfD von Nordrhein-Westfalen *Weyer* in seinem ersten Tätigkeitsbericht.

Der erste Tätigkeitsbericht des LfD NRW *Weyer* datiert auf den 31. März 1980 und fällt damit noch in eine Zeit, in der mit der um sich greifenden ADV viele Hoffnungen verknüpft worden waren. Der LfD NRW beschreibt, wie der Einsatz der ADV geprägt war von der „Zielvorstellung der Rationalisierung, der Wirtschaftlichkeit, einer gegenüber herkömmlichen Verfahren größeren Schnelligkeit und Effektivität unter gemeinsamer Nutzung und Verknüpfung der Datenbestände". Dieser Zielvorstellung würden die Erfordernisse des Datenschutzes „oft diametral" entgegenstehen. Dies habe einen Interessenkonflikt zur Folge, aufgrund dessen die

769 Simitis bezeichnet die Einrichtung des Datenschutzbeauftragten gar als die „wohl wichtigste Neuerung" die mit dem ersten HDSG eingeführt wurde, vgl. Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673, 678, erklärt diesen aber auch mangels Interventionsmöglichkeiten als „zum schlichten Postamt" degradiert, a.a.O. S. 681; vgl. auch Hondius zum ersten HDSG: „The importance of the Hessian Act is perhaps not so much its specific contents which are in conformity with the main trends in data protection in Europe, but above all the fact that Hesse was the first country to translate ideas into practice.", in: Emerging data protection in Europe, S. 36.

Selbstkontrolle der Verwaltung keine ausreichende Gewähr dafür biete, dass „der Datenschutz stets in dem erforderlichen Umfang berücksichtigt“ werde.[770]

Dabei sei die „Persönlichkeitssphäre der Bürger“ wie aus „zahlreichen Eingaben an den Landesbeauftragten“ hervorgehe im Bereich der nicht-automatisierten Verarbeitung in gleichem Maße bedroht wie im Bereich der ADV. Die vom LfD NRW ausgeübte Kontrolle diene der Gewährleistung der Rechte der Bürger und diene dem Rechtsschutz des Einzelnen. Daher sei im Bereich der nicht-automatisierten Verarbeitung eine Kontrollstelle „im Interesse der Bürger ebenso notwendig“.[771]

Der LfD NRW nimmt dabei aufgrund seiner Zuständigkeit nur Bezug auf die Kontrolle der Verarbeitung bei öffentlichen Stellen. Zwar galt im Jahr 1980, dem Jahr seines ersten Tätigkeitsberichts, bereits das BDSG 1977, jedoch waren die ersten Jahre der Datenschutzgesetzgebung ab 1970 geprägt von den Landesdatenschutzgesetzen, die allein die Verarbeitung bei den öffentlichen Stellen regelten.

So war auch der Einrichtung des Datenschutzbeauftragten in Hessen mit den weiteren Regelungen des ersten HDSG und beispielsweise den Regelungen im bayerischen EDVG von 1970 gemeinsam, dass diese bzw. die Aufgabe des Datenschutzbeauftragten sich auf die Datenverarbeitung durch öffentliche Stellen beschränkten und „nirgends (…) sich auch nur der bescheidenste Ansatz, private Initiativen mit einzubeziehen“ finden lässt.[772]

Dies wurde als verständlich, wenn auch „auf den ersten Blick recht verwunderlich“ bezeichnet, da die Länder mit den angestoßenen gesetzlichen Regelungen nur in die Bereiche eingreifen würden, für die „kaum Zweifel an ihrer Kompetenz“ bestünde.[773] Auch wenn die „Parallelität der Probleme“ bei der Verarbeitung im nicht-öffentlichen Bereich „auf der Hand“ liege, so könnten weitere Regelungen eben nur „im Rahmen der von der Verfassung selbst gezogenen Grenzen“ vollzogen werden.[774]

---

770 Erster Tätigkeitsbericht des Landesbeauftragten NRW, 31. März 1980, S. 1 f.

771 Erster Tätigkeitsbericht des Landesbeauftragten NRW, 31. März 1980, S. 1 f.

772 So Simitis, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673, 677.

773 Vgl. Simitis, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673, 677.

774 Simitis, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673, 677; vgl. auch Erster Tätigkeitsbericht des Ausschusses für Datenschutz RLP Drs. 7/3342, 17. Oktober 1974: „Der Landtag hat damit von

Die bereits 1971 kritisierte „Zurückhaltung" des Bundes in diesem Bereich sollte aber bis ins Jahr 1977 und der Verabschiedung des ersten BDSG 1977 andauern.[775] Grundsätzlich kann festgehalten werden, dass dem Bereich der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen in den Anfängen der Datenschutzgesetzgebung – trotz der sich abzeichnenden Entstehung von „privater Datenmacht" – wenig Aufmerksamkeit geschenkt wurde.[776]

Mit Blick auf das 1977 verabschiedete BDSG, aber auch alle dem HDSG und dem LDatG RLP nachfolgenden Datenschutzgesetze, muss wohl sowohl für die Entwicklung der Aufsicht über die Verarbeitung bei den öffentlichen Stellen als auch der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen die „Rolle" des Föderalismus bei der Entwicklung des Datenschutzrechts hervorgehoben werden.

So sahen die ersten Datenschutzgesetze in Hessen und Rheinland-Pfalz, wenn auch unterschiedlich ausgestaltet, die Aufsicht über die Verarbeitung bei den öffentlichen Stellen vor. Hinter diesen hierdurch vermittelten Schutz für die betroffenen Personen konnte dann auch der Bundesgesetzgeber bei der Ausgestaltung der Kontrolle über die Verarbeitung bei den öffentlichen Stellen des Bundes kaum zurück. Aber auch auf die Frage der Aufsicht über die nicht-öffentlichen Stellen dürfte sich die Einrichtung externer Kontrollstellen im Bereich der Verarbeitung durch öffentliche Stellen ausgewirkt haben.

So war bei der Beratung im Innenausschuss auf Bundesebene in Abweichung vom Entwurf der Bundesregierung für ein Bundesdatenschutzgesetz entschieden worden, dass auch die Verarbeitung bei den nicht-öffentlichen Stellen durch eine externe Stelle kontrolliert werden sollte und zwar sowohl für die Verarbeitung zu fremden als auch eigenen Zwecken.[777]

Die für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen für eigene Zwecke zuständige Aufsichtsbehörde war nach § 30 Abs. 1 BDSG 1977 nach Landesrecht zu bestimmen; dies galt nach § 40

---

seiner Gesetzgebungskompetenz, soweit sie eindeutig gegeben war, Gebrauch gemacht.".

775 Simitis, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673, 677.

776 Kerkau kritisierte bereits 1970 zu Recht, dass diesem Bereich gar keine Aufmerksamkeit geschenkt wurde, und merkte an, dass das „Problem einer Aufsicht und damit verbunden das Problem des Datenschutzes (..) daher in der Praxis für die Privatwirtschaft zumindest ebenso dringend wie für die öffentliche Verwaltung" erscheine, vgl. Automatische Datenverarbeitung (ADV), S. 49.

777 Bericht des Innenausschusses, Drs. 7/5277, 2. Juni 1976, S. 5.

Abs. 1 BDSG 1977 auch für die Bestimmung der für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen für fremde Zwecke zuständigen Aufsichtsbehörde. Der Bundesgesetzgeber machte darüber hinaus, schon aus verfassungsrechtlichen Gründen, keine weiteren Vorgaben, wie die Datenschutzaufsicht zu organisieren war. Dies betraf auch die Frage, ob die Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen durch allein eine Aufsichtsbehörde erfolgen sollte, die damit den Ländern überlassen war.[778]

Führt man sich vor Augen, dass zum Zeitpunkt der Verabschiedung des ersten BDSG 1977 lediglich Hessen und Rheinland-Pfalz ein Landesdatenschutzgesetz verabschiedet hatten, stellt sich die Frage, weshalb die Länder die Datenschutzaufsicht über die öffentlichen und nicht-öffentlichen Stellen zum größten Teil nicht durch eine Institution wahrnehmen ließen. Dabei handelte es sich um eine allein von den Ländern getroffene Entscheidung, die im „Wissen“ um die durch das BDSG vorgegebene Fremdkontrolle der Verarbeitung durch die nicht-öffentlichen Stellen und der von den Ländern gesehenen Notwendigkeit der Fremdkontrolle der Verarbeitung durch die öffentlichen Stellen auf Landesebene getroffen wurde. Hierauf soll nachfolgend eingegangen werden.

### 1. Die Datenschutzaufsicht nach den ersten Landesdatenschutzgesetzen

In den ersten Jahren der Datenschutzaufsicht wurde, mit Ausnahme von Hamburg, Bremen und im Jahr 1991 nachziehend Niedersachen, in allen Ländern die Aufsicht über die Verarbeitung bei öffentlichen und nicht-öffentlichen Stellen durch unterschiedliche Institutionen wahrgenommen.[779]

Zu berücksichtigten ist dabei allerdings, dass die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen in den Ländern Saarland und Schleswig-Holstein ursprünglich zwar den Innenministern zugewie-

778 Vgl. BT-Drs. 7/1027, S. 16 unter Bezugnahme auf Art. 83, 84 GG.

779 Vgl. hierzu auch Kapitel E., III., 4. zu Bremen und Kapitel E., III., 5. zu Hamburg.; in Niedersachsen wurde die Aufgabe der Aufsicht vom Innenministerium auf den LfD übertragen, allerdings nahm das Innenministerium die im BDSG nicht vorgesehene Funktion einer „Obersten Aufsichtsbehörde“ wahr, vgl. Bericht des Berliner Datenschutzbeauftragten, Drs. 13/303, 31. Dezember 1995, S. 62 dort Fn. 170a.

sen worden war, diese die Wahrnehmung der Aufsicht dann jedoch an den LfD des Saarlandes bzw. Schleswig-Holsteins delegiert hatten.[780]

Da die genannten Länder mit dieser Entscheidung die „Minderheit“ in der Bundesrepublik Deutschland stellten, soll am Beispiel Hamburgs darauf eingegangen werden, wie die Bündelung der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen und der Aufsicht über die Verarbeitung bei den öffentlichen-Stellen begründet wurde. Am Beispiel der Regelung im Saarland wird wiedergegeben, wie die Aufgabe der bis zum Jahr 1993 bestehenden Delegation der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen vom Innenminister an den LfD mit der Novelle 1993 begründet wurde.

### a) Hamburg

In Hamburg wurde das erste Landesdatenschutzgesetz im Jahr 1981 verabschiedet, womit man „Schlusslicht“ der Länder war (HmbDSG 1981).[781] Da die Vorschriften des BDSG 1977 bereits zum größten Teil ab 1978 Anwendung fanden, war das BDSG nach § 7 Abs. 2 BDSG 1977 mangels landesgesetzlicher Regelungen des Datenschutzes von den Behörden und sonstigen öffentlichen Stellen in Hamburg bis zum Inkrafttreten des HmbDSG 1981 bei der Ausführung von Bundesrecht zu beachten.

Da nach §§ 30, 40 BDSG 1977 die für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen zuständigen Aufsichtsbehörde von den Ländern bestimmt werden musste, musste auch in Hamburg die für die Aufsicht zuständige Behörde bestimmt werden. Die Entscheidung fiel dabei auf die Behörde für Wirtschaft, Verkehr und Landwirtschaft als Aufsichtsbehörde im Sinne von §§ 30, 40 BDSG 1977.[782]

Dabei stand Hamburg, wie auch die Länder Hessen und Rheinland-Pfalz in den Jahren 1970 bzw. 1974, vor der Entscheidung, eine Aufsichtsbehörde für einen Bereich der Verarbeitung (nicht-öffentliche Verarbeitung) zu bestimmen, ohne dass für den Bereich der Verarbeitung bei den öffentlichen Stellen des Landes bereits ein Landesdatenschutzgesetz

780 Neben Kapitel E., III., 11. zum Saarland und Kapitel E., III., 14. zu Schleswig-Holstein, vgl auch. Wind, Die Kontrolle des Datenschutzes im nicht-öffentlichen Bereich, S. 32 f.

781 HmbDSG vom 31. März 1981, GVBl. 1981, S. 71.

782 Anordnung zur Durchführung des Bundesdatenschutzgesetzes vom 20. September 1977, Amtl. Anz. vom 26. September 1977, S. 1433.

– mit entsprechenden Regelungen zur Aufsicht der Verarbeitung – verabschiedet worden war. Dies gleichwohl unter umgekehrten Vorzeichen, als dass Hessen und Rheinland-Pfalz Kontrollorgane für die Aufsicht über die Verarbeitung bei den öffentlichen Stellen zu einem Zeitpunkt bestimmten als es noch an Regelungen über die Verarbeitung und Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen fehlte.

Im Unterschied zu Hessen und Rheinland-Pfalz entschied sich der Hamburger Senat dann aber zeitnah zur Verabschiedung des HmbDSG 1981 dazu, die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen anstatt der Behörde für Wirtschaft, Verkehr und Landwirtschaft dem mit dem HmbDSG 1981 eingeführten Datenschutzbeauftragten zuzuweisen.[783]

Auf die Gründe für das Zusammenführen der Aufsicht geht der hamburgerische Datenschutzbeauftragte *Schapper* in seinem ersten Tätigkeitsbericht ein.[784] So solle durch das Zusammenführen der Aufsicht nicht nur „Doppelarbeit“ vermieden, sondern auch die „einheitliche Handhabung“ der „– bis auf wenige Abweichungen – identischen Bestimmungen des Bundes- und Landesdatenschutzgesetzes“ sichergestellt werden.[785]

Die Aufsicht durch eine Stelle würde dazu führen, dass die Bürger nicht länger durch die Unterscheidung von Datenschutz im „öffentlichen und privaten Bereich“ überfordert werden – selbst „Kenner“ würden sich schwertun, „bestimmte Vorgänge“ dem Bereich der öffentlichen bzw. nicht-öffentlichen Verarbeitung zuzuordnen.[786] Schließlich sei es häufig von zufälligen Voraussetzungen abhängig, ob das BDSG oder das HmbDSG Anwendung finden würde.[787]

783 Anordnung über Zuständigkeiten auf dem Gebiet des Datenschutzes vom 25. Mai 1982, Amtl. Anz. 1982, S. 969.

784 Erster Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, Drs. 11/50, 5. Januar 1983, S. 12.

785 Erster Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, Drs. 11/50, 5. Januar 1983, S. 12.

786 Erster Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, Drs. 11/50, 5. Januar 1983, S. 12.

787 Erster Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, Drs. 11/50, 5. Januar 1983, S. 12.

b) Saarland

Mit der Novellierung des Saarländischen Datenschutzgesetzes im Jahr 1993 wurde der LfD dem Landtag angegliedert.[788] Hierdurch sollte dessen Unabhängigkeit, insbesondere im Verhältnis zur Exekutive, gestärkt werden.[789] Zuvor war der LfD dem saarländischen Ministerium des Innern angegliedert. Dieses war auch zur Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen zuständig erklärt worden.[790] Allerdings wurde die Wahrnehmung der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen durch verwaltungsinterne Anordnung an den LfD delegiert.[791] Die Aufsicht über die Verarbeitung, sowohl bei den öffentlichen als auch nicht-öffentlichen Stellen, war damit beim LfD „zusammengefasst".

Im Zusammenhang mit der geplanten Angliederung des LfD an den saarländischen Landtag ging der LfD *Schneider* in seinem 13. Tätigkeitsbericht darauf ein, ob er, angegliedert an den Landtag, weiterhin die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen ausüben könne.[792] Dabei vertrat er die Position, dass die Wahrnehmung der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen keinen Verstoß gegen den Grundsatz der Gewaltenteilung darstellen würde. Der LfD würde durch die Zuordnung zum Landtag nicht zu einem Organ der Legislative oder gar zum „verlängerten Arm" des Parlaments werden, die Unabhängigkeit in Sach- und Rechtsfragen bliebe unangetastet und die Dienststelle organisatorisch verselbstständigt. Da das Parlament keine Exekutivbefugnisse erhalte, sei die Gewaltenteilung nicht gefährdet.[793]

Der LfD *Schneider* ging dabei auch auf die seiner Einschätzung nach drohenden Gefahren der „Aufteilung" der Aufsicht ein. So könne die auch für den „Fachmann" nicht immer einfache Unterscheidung zwischen

788 § 25 Abs. 3 SDSG 1993, Amtsbl. S. 286.

789 Dies geht auf die Beratung in den Ausschüssen zurück, vgl. Abgeordneter Rischar (SPD), Plenarprotokoll 10/47, 24. März 1993, S. 2604 f.

790 Verordnung über die zuständige Aufsichtsbehörde für die Überwachung der Durchführung des Datenschutzes in nicht-öffentlichen Stellen vom 20. Januar 1978, Amtsbl. S. 91.

791 Fünfzehnter Bericht über die Tätigkeit des LfD Saarland, Drs. 11/59, 23. Januar 1995, S. 7.

792 Dreizehnter Bericht über die Tätigkeit des LfD Saarland, Drs. 10/941, 6. März 1992, S. 5.

793 Dreizehnter Bericht über die Tätigkeit des LfD Saarland, Drs. 10/941, 6. März 1992, S. 5.

öffentlicher Verwaltung und privatem Bereich für den Bürger zur Kompetenzfalle werden – diesem könne nicht die Notwendigkeit vermittelt werden, dass die bisherige Organisation der Aufsicht aufgegeben werden müsse. Schließlich würden Verzögerungen in der Interessenwahrnehmung für die Bürger drohen.[794]

Trotz der vorgebrachten Argumente wurde dem LfD nach der Angliederung an den saarländischen Landtag nicht länger die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen übertragen.

Dass sich seine im 13. Tätigkeitsbericht vorgebrachten Befürchtungen teilweise bestätigt hätten, trug der LfD *Schneider* dann in seinem 15. Tätigkeitsbericht vor. So habe er „in Einzelfällen“ immer wieder seine Unzuständigkeit erläutern müssen, bevor er Vorgänge an das zuständige Innenresort abgegeben habe. Dies sei nachteilig und zeitraubend für den Bürger, insbesondere in den Fällen, bei denen es sich um „einheitliche Lebenssachverhalte“ handele, die „in beide Kompetenzbereiche fallen“. Beispiele für solche Konstellationen trug er allerdings nicht vor.[795]

Naheliegend ist aber auch, dass das Innenministerium im Saarland sich trotz der Delegation der Aufsicht an den LfD bis ins Jahr 1993 stets der Möglichkeiten der Einflussnahme gewiss war und von Seiten der Landesregierung die „Hoheit“ der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen keinesfalls abgegeben werden sollte. Dies dürfte wiederum die eigenständige Wahrnehmung der Aufsicht durch das Innenministerium nach der Novelle und Zuordnung des LfD zum Landtag im Jahr 1993 bedingt haben. So wenig wie von der Landesregierung im Jahr 1993 die Bestimmung des LfD als die im Sinne des BDSG zur Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen zuständige Behörde ins Auge gefasst wurde, so wenig kann wohl für die Zeit vor 1993 – in Abgrenzung zu Organisation der Aufsicht in den Ländern Hamburg und Bremen – von einer „Zusammenfassung“ der Aufsicht beim LfD gesprochen werden.[796]

---

794 Dreizehnter Bericht über die Tätigkeit des LfD Saarland, Drs. 10/941, 6. März 1992, S. 4.

795 Fünfzehnter Bericht über die Tätigkeit des LfD Saarland, Drs. 11/59, 23. Januar 1995, S. 7.

796 So aber der LfD, vgl. Dreizehnter Bericht über die Tätigkeit des LfD Saarland, Drs. 10/941, 6. März 1992,
S. 4 und Fünfzehnter Bericht, Drs. 11/59, 23. Januar 1995, S. 6.

## 2. Die Diskussion um die Organisation der Datenschutzaufsicht

Die Zuweisung der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen zur Aufsichtsbehörde für die Verarbeitung bei den öffentlichen Stellen, wie beispielsweise in Hamburg, wurde auch in den anderen Ländern bzw. allgemein in der Rechtswissenschaft diskutiert.

Gegen die einheitliche Wahrnehmung der Aufsicht wurde vor allem die Unabhängigkeit der Aufsicht über die Verarbeitung bei den öffentlichen Stellen angeführt. Auch wenn die LfD in den Ländern zu großen Teilen der Dienst- und/oder Rechtsaufsicht unterlagen, so war die Unabhängigkeit der LfD in den Landesdatenschutzgesetzen normiert. Die Aufsichtsbehörden für den nicht-öffentlichen Bereich waren hingegen in den hierarchischen Verwaltungsaufbau eingegliedert und unterlagen damit der Fachaufsicht. Bei den Aufsichtsbehörden, eingerichtet bei den obersten Landesbehörden, war die behördeninterne Hierarchie und damit Weisungsgebundenheit der Mitarbeiter der Aufsichtsbehörde vergleichbar gegeben.[797]

Würde die Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen zusammengeführt werden, so wären weisungsgebundene und unabhängige Kontrolltätigkeit nicht deutlich voneinander getrennt. Dies sollte jedoch gerade vor dem Hintergrund der gesetzlich geforderten Unabhängigkeit der Aufsicht über die Verarbeitung bei den öffentlichen Stellen vermieden werden.[798]

Diese für die Trennung der Aufsicht angeführte Argumentation konnte naheliegender Weise nur Bestand haben, solange für die Aufsicht über die öffentlichen und nicht-öffentlichen Stellen unterschiedliche Vorgaben galten und die Aufsicht über die nicht-öffentlichen Stellen anders strukturiert war.

Bereits 1987 wurde von *Simitis* festgestellt, dass die Ausgestaltung der Aufsicht über die Verarbeitung im nicht-öffentlichen Bereich einen „Konstruktionsfehler“ enthalte.[799] Neben der personellen und sachlichen Aus-

---

797 Vgl. Wind, Die Kontrolle des Datenschutzes im nicht-öffentlichen Bereich, S. 40.

798 In den Ländern Hamburg und Hessen waren die LfD, soweit sie die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen ausübten, ebenfalls weisungsgebunden – hierbei fielen also unabhängige und weisungsgebundene Ausübung der Aufsicht zusammen, vgl. Wind, Die Kontrolle des Datenschutzes im nicht-öffentlichen Bereich, S. 40, m.w.N.

799 Simitis, Zur Datenschutzgesetzgebung: Vorgaben und Perspektiven, CR 1987, S. 602, 608.

stattung der Aufsichtsbehörden für den nicht-öffentlichen Bereich kritisierte dieser, dass die Aufsichtsbehörden als weisungsgebundene Behörden die in eine wirksame Kontrolle gesetzten Erwartungen nicht erfüllen könnten.[800] Bezug nahm er dabei auf das Volkszählungsurteil des BVerfG, in dem die Bedeutung der unabhängigen Kontrolle für den Schutz der Bürger in Form des Schutzes des Rechts auf informationelle Selbstbestimmung hervorgehoben wurde.[801]

Diese Auffassung und Kritik an der fehlenden Unabhängigkeit der Aufsichtsbehörden konnte sich jedoch vorerst nicht durchsetzen. Entgegengehalten wurde dieser Ansicht unter anderem, dass unter Anlegen dieser Maßstäbe jede weisungsgebundene behördliche Aufsichtstätigkeit keine wirksame Kontrolle darstellen würde, was dazu führen würde, dass auch beispielsweise die Gewerbeaufsicht als nicht wirksame Kontrolle eingestuft werden müsste.[802]

Die Diskussion um das Zusammenführen der Aufsicht erhielt dann mit der RL 95/46/EG nicht nur neuen Auftrieb, sondern gewann im Hinblick auf die Umsetzung der Vorgaben der Richtlinie auch an Bedeutung. Wie bereits unter Kapitel D., X., 1. ausgeführt, ging das Urteil des EuGH

---

800 Simitis, Zur Datenschutzgesetzgebung: Vorgaben und Perspektiven, CR 1987, S. 602, 610.

801 Simitis, Zur Datenschutzgesetzgebung: Vorgaben und Perspektiven, CR 1987, S. 602, 610; hierbei bezog sich das BVerfG allerdings auf den Datenschutzbeauftragten und damit auf die Aufsicht über die öffentlichen Stellen, da im Jahr 1983 die LfD grds. allein die Aufsicht über die öffentlichen Stellen ausübten und auch das Volkszählungsurteil nur die Verarbeitung durch öffentliche Stellen zum Gegenstand hatte – „Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatisierten Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung.“, BVerfG – 1 BvR 209/83, Rn. 155; vgl. hierzu auch Mitrou, Die Entwicklung der institutionellen Kontrolle des Datenschutzes, S. 32.

802 Vgl. Masing, Herausforderungen des Datenschutzes, NJW 2012, S. 2305, 2311, „warum sollte auch die Aufsicht über die Datenverarbeitung unabhängiger sein müssen als die Gewerbeaufsicht sonst oder die Aufsicht über die Beachtung von Umweltrechtsvorschriften?“; v. Lewinski, in: Auernhammer, DSGVO BDSG, 7. Aufl., Art. 52, Rn. 9, „ist die Weisungsfreiheit bei der Aufsicht im nicht-öffentlichen Bereich nicht unmittelbar einsichtig; schließlich sind selbst Behörden aus deutlich grundrechtssensibleren Bereichen (Lebensmittelaufsicht, Gesundheitsamt, Jugendhilfe) gerade nicht unabhängig – ders. vermutet die „Herauslösung der Datenschutzaufsicht aus dem mitgliedstaatlichen Verwaltungskontext“ als tieferen Grund für die Anforderung der Weisungsfreiheit, a.a.O.

im Jahr 2010 auf die Auslegung der in Art. 28 Abs. 1 S. 2 RL 95/46/EG geregelten „völligen Unabhängigkeit" zurück.[803] Dabei war bereits vor der Entscheidung des EuGH ein großer Teil der deutschen Rechtswissenschaft zu der Überzeugung gekommen, dass die Datenschutzaufsicht „völlig unabhängig" sein müsse, und da dies (gerade) auch für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen gelten müsse, ein Zusammenführen der Aufsicht beim LfD naheliegend sei.[804]

So wurde die RL 95/EG/EG teilweise dahingehend ausgelegt, dass eine „Bündelung der Kräfte", also das Zusammenführen der Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen, dem „Willen" bzw. „Geist" der Richtlinie entspreche.[805] Zum einen werde aufgrund der RL 95/46/EG die das BDSG „bisher beherrschende Trennung" von Regelungen über die Verarbeitung durch öffentliche und nicht-öffentliche Stellen zurückgedrängt und wichtige Grundsätze an die Rechtmäßigkeit der Verarbeitung würden daher einheitlich gelten.[806] Zum anderen liefere die Richtlinie deutliche Anhaltspunkte dafür, dass die Aufsicht „möglichst konzentriert" von einer Kontrollstelle ausgeübt werden solle. Soweit die RL 95/46/EG nach Art. 28 auch die Beauftragung mehrerer Stellen mit der Aufsicht ermögliche, geschehe dies mit Blick auf föderal konstituierte Mitgliedstaaten.[807] Aber auch in diesen solle die Datenschutzaufsicht „in jedem föderalen Teilbereich auf eine Kontrollstelle beschränkt bleiben".[808] Dies dürfte jedenfalls der Wortlaut der Richtlinie aber nicht erkennen lassen.

---

803 Art. 28 Abs. 1 S. 2 RL 95/46/EG, „Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.".

804 Vgl. nur Ronellenfitsch, Rechtsgutachten zur Neugestaltung der Datenschutzkontrolle, Drs. 18/375, S. 30 f., 39, m.w.N.

805 Gola/Schomerus, Die Organisation der staatlichen Datenschutzkontrolle der Privatwirtschaft, ZRP 2000, S. 183, 185.

806 Gola/Schomerus, Die Organisation der staatlichen Datenschutzkontrolle der Privatwirtschaft, ZRP 2000, S. 183; zur Unterscheidung im dt. Datenschutzrecht zwischen Datenschutz im öffentlichen und privaten Bereich und der „entsprechenden" Trennung der Aufsicht vgl. auch Bericht des Berliner Datenschutzbeauftragten, Drs. 13/303, 31. Dezember 1995, S. 62.

807 Art. 28 Abs. 1 S. 1 RL 95/46/EG, „Die Mitgliedstaaten sehen vor, daß eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen.".

808 Vgl. Gola/Schomerus, Die Organisation der staatlichen Datenschutzkontrolle der Privatwirtschaft, ZRP 2000, S. 183.

Auch wurde auf die Herausforderung hingewiesen, dass nach Art. 29 Abs. 2 der RL 95/46/EG die nach Art. 29 Abs. 1 RL 95/46/EG einzurichtende Datenschutzgruppe sich aus je einem Vertreter der von den einzelnen Mitgliedstaaten bestimmten Kontrollstellen zusammensetzt, was bei einer Vielzahl von Aufsichtsbehörden, wie in Deutschland, zwingend zu einem gewissen Abstimmungsbedarf führen würde.[809] Ob sich hieraus schließen lässt, dass die Richtlinie eine „weitgehende Konzentration der Datenschutzkontrolle" anstrebte, erscheint jedoch fraglich.[810] Denn wie beispielsweise aus Art. 29 Abs. 2 S. 3 RL 95/46/EG hervorgeht, sah die Richtlinie für den Fall, dass im Mitgliedstaat mehrere Kontrollstellen bestimmt worden sind, die Möglichkeit vor, dass diese einen gemeinsamen Vertreter benennen. Die Möglichkeit der Errichtung mehrerer Aufsichtsbehörden wurde damit ausdrücklich anerkannt. Die Notwendigkeit der Repräsentation eines Mitgliedstaates mit mehreren Kontrollstellen durch einen gemeinsamen Vertreter ergibt sich schon aus dem Bedürfnis nach Stimmengleichheit der Mitgliedstaaten – die Datenschutzgruppe wäre mithin auch nicht funktionsfähiger gewesen, wenn Vertreter „aller" Aufsichtsbehörden aufgenommen werden würden, sondern nur „vergrößert".[811] Da der gemeinsame Vertreter nach Art. 29 Abs. 2 S. 3 RL 95/46/EG auch von den Aufsichtsbehörden mitbestimmt wurde und auch „mit deren Stimme" sprechen sollte, bestand hierfür schon auch kein Bedürfnis. Ein solches Bedürfnis wäre nur dann naheliegend, wenn die Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen bzw. die legislatorischen Anforderungen so wesensverschieden wären, dass ein gemeinsamer Vertreter mithin nicht beide Bereiche repräsentieren könnte – dies würde aber in Widerspruch zur aus der Richtlinie herausgelesenen angestrebten Konzentration der Datenschutzkontrolle stehen.[812]

---

809 Die Datenschutzgruppe sei „primäre Reflexions- und Konsultationsinstanz für alle supranationalen Überlegungen zum Stand und zur Zukunft des Datenschutzes", vgl. Simitis: Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz, NJW 1997, S. 281, 287; dabei erfolgte die Abstimmung ohne institutionalisierte Verfahrensregelungen wie etwa § 18 BDSG 2018, vgl. Wilhelm, in: Sydow, BDSG, 1. Aufl., § 18, Rn. 6.

810 So aber Gola/Schomerus, Die Organisation der staatlichen Datenschutzkontrolle der Privatwirtschaft,
ZRP 2000, S. 183.

811 Vgl. aber Gola/Schomerus, Die Organisation der staatlichen Datenschutzkontrolle der Privatwirtschaft,
ZRP 2000, S. 183.

812 Wobei zu berücksichtigen ist, dass die RL 95/46/EG grundsätzlich keine Differenzierung zwischen dem öffentlichen und nicht-öffentlichen Bereich vornahm.

Ob die Richtlinie eine Konzentration der Datenschutzkontrolle im Sinne eines Zusammenführens der Aufsicht über den öffentlichen und nicht-öffentlichen Bereich anstrebte, erscheint jedoch auch vor dem Hintergrund der Entstehungsgeschichte der Richtlinie fraglich. So war die Regelung des freien Datenverkehrs zwischen den Mitgliedstaaten immer wieder Bezugspunkt der Bemühungen für eine Datenschutz-Richtlinie. Der freie Datenverkehr sollte durch die Herstellung eines einheitlichen Schutzniveaus gewährleistet werden. Ein unterschiedliches Schutzniveau wurde als ein Hemmnis für die Ausübung von Wirtschaftstätigkeiten verstanden, das den Wettbewerb verfälsche und auch der Erfüllung der Aufgaben der im Anwendungsbereich des Gemeinschaftsrechts tätigen Behörden entgegenstehe.[813]

Allerdings wurden der Europäischen Union, geprägt vom Verständnis, Garant für den freien Warenverkehr zu sein, mit dem Vertrag von Maastricht und der Maßgabe, die Grundrechte in der Europäischen Union zu gewährleisten, nicht nur neue Aufgaben zugewiesen, sondern diese in bestimmten Maße neu ausgerichtet.[814] Ausdruck dieser Entwicklung ist Art. 1 Abs. 2 der RL 95/46/EG, wonach die Mitgliedstaaten den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten nicht aus Gründen des Schutzes der Grundrechte und Grundfreiheiten sowie insbesondere dem Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten beschränken oder untersagen sollen. Dies ist jedoch nicht dahingehend zu verstehen, dass dem freien Datenverkehr der Vorrang vor dem Schutz der betroffenen Personen eingeräumt wird oder die Richtlinie einen „Abwägungsprozess" vorsieht.[815] Vielmehr soll die Richtlinie „den Datenaustausch vereinfachen, nicht aber um den Preis eines verminderten Datenschutzes".[816]

Dies mit einbeziehend lässt sich jedoch festhalten, dass die Richtlinie sich „von Anfang an, schon aus Kompetenzgründen, ganz am nicht-öffentlichen Sektor" orientiert hatte.[817] So sollten die Anforderungen an die Verarbeitung bei den nicht-öffentlichen Stellen auf das Niveau des

813 Vgl. Erwägungsgrund 7 der Richtlinie 95/46/EG.
814 Vgl. Simitis, Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz?, NJW 1997, S. 281.
815 Vgl. Simitis, Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz?, NJW 1997, S. 281, 282.
816 Vgl. Simitis, Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz?, NJW 1997, S. 281, 282.
817 Vgl. Simitis, Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz?, NJW 1997, S. 281, 287.

Schutzstandards für die Betroffenen bei der Verarbeitung durch öffentliche Stellen angehoben werden.[818] Hierzu sollte auch die Aufsicht über die Verarbeitung durch nicht-öffentliche Stellen beitragen.

Diese sollte nicht länger durch weisungsgebundene Aufsichtsbehörden, sondern durch in „völliger Unabhängigkeit" tätige Kontrollinstanzen wahrgenommen werden.[819] Dass aber Konsequenz hiervon nur sein kann, dass die Aufteilung der Datenschutzaufsicht aufgegeben wird und die Aufsicht „uneingeschränkt" den für die Aufsicht der Verarbeitung im öffentlichen Bereich zuständigen Landesbeauftragten übertragen wird, erscheint jedoch nicht als die allein mögliche Schlussfolgerung.[820] So zeigt allein schon das Beispiel Bayerns, dass die „völlige Unabhängigkeit" der Aufsichtsbehörde für die Verarbeitung im nicht-öffentlichen Bereich auch anderweitig hergestellt werden kann.

## *III. Die Datenschutzaufsicht in den Ländern*

Vereinzelt hatten die Länder sowohl die Zuständigkeit für die Aufsicht über die Verarbeitung bei den öffentlichen Stellen als auch die Zuständigkeit für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen bereits mit dem ersten Landesdatenschutzgesetz auf allein eine Aufsichtsbehörde übertragen, vgl. Kapitel E., II., 1. Bei der Mehrzahl der Länder erfolgte dies jedoch erst in Reaktion auf die RL 95/46/EG bzw. auf das Urteil des EuGH im Jahr 2010 zur „völligen Unabhängigkeit" der Aufsichtsbehörden.[821]

Wie voranstehend gezeigt, war das Zusammenführen der Datenschutzaufsicht nicht von der Richtlinie 95/46/EG vorgegeben und auch der EuGH hatte nur über die Anforderungen an die „völlige Unabhängigkeit" der Datenschutzaufsicht entschieden.

Nachfolgend soll daher wiedergegeben werden, wie die Länder das Zusammenführen der Datenschutzaufsicht in Reaktion auf das Urteil des EuGH im Jahr 2010 – oder falls diese bereits zuvor erfolgt war – begründeten. Aufgrund der Darstellung der Entwicklung der Datenschutzaufsicht

---

818 Vgl. Simitis, Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz?, NJW 1997, S. 281, 287.

819 Vgl. Simitis, Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz?, NJW 1997, S. 281, 287.

820 So aber Simitis, Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz?, NJW 1997, S. 281, 287.

821 EuGH Urt. v. 9. März 2010, C-518/07.

in Bayern soll an dieser Stelle auch die Organisation der Aufsicht in den Ländern nach dem jeweiligen „ersten" Datenschutzgesetz aufgezeigt werden. Mit Blick auf die im nachfolgenden Kapitel behandelte Frage der weiteren Harmonisierung der Datenschutzaufsicht mit der DSGVO wird darüber hinaus auch die im Jahr 2020 bestehende Organisation der Aufsicht in den Ländern aufgenommen.

## 1. Baden-Württemberg

In Baden-Württemberg wurde ab 1978 die Aufsicht im nicht-öffentlichen Bereich durch die beim Innenministerium angesiedelte Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich wahrgenommen.[822] Für die Aufsicht im öffentlichen Bereich war der Landesbeauftragte für den Datenschutz zuständig.[823]

Bereits vor dem Urteil des EuGH zur Unabhängigkeit der Datenschutzaufsicht war die Organisation der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen diskutiert worden. Allerdings wurde von der baden-württembergischen Landesregierung um den Ministerpräsidenten *Oettinger* trotz des bereits eröffneten Vertragsverletzungsverfahrens noch im Jahr 2008 kein „Anlass" gesehen, das Landesdatenschutzgesetz zu ändern.[824] Anders hingegen die SPD-Fraktion, die im Landtag bereits einen Antrag mit dem Ziel der Zusammenlegung der Aufsicht gestellt hatte. Die SPD führte aus, dass das Zusammenführen der Aufsicht notwendig bzw. „notwendiger denn je" sei, da „nur so" Synergieeffekte erzielte werden könnten, „um den ohnehin in Baden-Württemberg personell zu schwach ausgestatteten Datenschutz zu stärken".[825]

---

822 Verordnung der Landesregierung über die zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich vom 10. Januar 1978, GBl. 1978, S. 78.

823 Vgl. Erster Tätigkeitsbericht des LfD BW, Drs. 8/830, 30. Dezember 1980, S. 9.

824 Stellungnahme des Innenministeriums auf Antrag der Abgeordneten Rülke u.a. (FDP/DVP), Drs. 14/3487, 5. November 2008, S. 4.

825 Antrag der Fraktion der SPD, Drs. 14/3495, 5. November 2008 – der Antrag der SPD fiel damit mit der Stellungnahme des Innenministeriums zusammen, vgl. vorangehende Fn.

Im Oktober 2009 erklärte die CDU-Landtagsfraktion dann, dass sie beschlossen habe, die Datenschutzaufsicht beim LfD zu bündeln.[826] Auch die Landesregierung erklärte auf Antrag der SPD-Fraktion, dass beabsichtigt sei, die Aufsicht „baldmöglichst" beim LfD zu bündeln.[827] Einen entsprechenden Gesetzesentwurf legten die Fraktionen von CDU und FDP/DVP schließlich Ende 2010 vor. Dieser sah vor, dass die Zuständigkeit für die Aufsicht beim Landesbeauftragten gebündelt wird.[828] Der Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Einrichtung eines unabhängigen Datenschutzzentrums unter Leitung des LfD wurde nicht aufgegriffen.[829]

Aus dem Gesetzesentwurf von CDU und FDP/DVP geht hervor, dass als Alternative zur Bündelung der Aufsicht beim LfD die Beibehaltung der Trennung der Aufsicht durchaus gesehen wurde.[830] Allerdings war man der Auffassung, dass durch die Bündelung der Aufsicht deren „Schlagkraft" erhöht werde. So könne eine „einheitliche und größere Datenschutzbehörde" die Mitarbeiter „flexibler und damit effizienter" einsetzen. Es könnten wechselnde Arbeitsschwerpunkte gesetzt und „datenschutzrechtliche Großverfahren", die umfangreicher, komplexer sowie zeit- und personalaufwendiger werden würden, schneller bewältigt werden. Auch hätten Bürger, Behörden, nicht-öffentliche Stellen und behördliche bzw. betriebliche Datenschutzbeauftragte für ihre Anliegen einen einheitlichen Ansprechpartner – aus welchen Gründen dies einen Vorteil darstellen soll wurde jedoch nicht erörtert.[831]

Abgeordnete aller Fraktionen befürworteten in der ersten Beratung zum Gesetzesentwurf die Bündelung der Aufsicht. Effektiver Datenschutz könne nur dann stattfinden, wenn die Aufsicht über die Verarbeitung bei öffentlichen und nicht-öffentlichen Stellen beim LfD zusammengefasst werde.[832]

Nach der Änderung des baden-württembergischen Datenschutzgesetzes im Jahr 2011 ist der LfD sowohl für die Aufsicht über den öffentlichen als

826 Presseerklärung vom 22. Oktober 2009, Vgl. Drs. 14/5333, 23. Oktober 2009 S. 2.
827 Stellungnahme des Innenministeriums auf Antrag der Abgeordneten Stoch u.a. (SPD), Drs. 14/5333, 23. Oktober 2009, S. 2.
828 Drs. 14/7313, 8. Dezember 2010.
829 Drs. 14/7104, 27. Oktober 2010.
830 Vgl. Drs. 14/7313, 8. Dezember 2010, S. 2.
831 Zu diesem Abschnitt, vgl. Drs. 14/7313, 8. Dezember 2010, S. 15.
832 Vgl. Abgeordneter Stoch (SPD), Plenarprotokoll Nr. 107, 16. Dezember 2010, S. 7657 f.

auch über den nicht-öffentlichen Bereich zuständig, vgl. § 31 Abs. 1 LDSG BW 2011. Der damalige LfD *Klingbeil* begrüßte die Zusammenführung der Aufsichtsbehörden. Hierdurch sei endlich ein seit dem Inkrafttreten des ersten LDSG in Baden-Württemberg am 1. April 1980 bestehender „Geburtsfehler" der Datenschutzaufsicht korrigiert worden.[833]

Nach Anpassung des LDSG BW an die DSGVO ist der LfD gemäß § 25 Abs. 1 LDSG BW 2018 zuständige Aufsichtsbehörde im Sinne des Art. 51 Abs. 1 DSGVO und Aufsichtsbehörde für die Verarbeitung von Daten bei nicht-öffentlichen Stellen gemäß § 40 BDSG.[834]

### 2. Berlin

Die Kontrolle der Verarbeitung im öffentlichen Bereich wurde nach dem ersten Berliner Datenschutzgesetz von 1990 durch den Berliner Datenschutzbeauftragten ausgeübt.[835] Die Zuständigkeit für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen war der Senatsverwaltung für Inneres zugewiesen worden.[836]

Bereits 1990 war von den Fraktionen SPD und AL ein Gesetzesentwurf für eine Novellierung des BlnDSG vorgelegt worden, wonach unter anderem dem Datenschutzbeauftragten die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen übertragen werden sollte.[837] Hierdurch sollte bei Privatunternehmen der „gleiche Kontrollstandard" wie bei öffentlichen Stellen gewährleistet werden. Dabei wurde auch auf die Ausgestaltung der Aufsicht in Hamburg, Bremen und im Saarland Bezug genommen.[838] Im Laufe des Gesetzgebungsverfahrens entfiel diese Regelung jedoch.[839] Vom Datenschutzbeauftragten wurde dies kritisiert, da dem

833 Vgl. 30. Tätigkeitsbericht des LfD BW, Drs. 15/955, 1. Dezember 2011, S. 11.
834 LDSG BW vom 12. Juni 2018, GBl. 2018, S. 173; nach § 12 Abs. 1 des Gesetzes zur Regelung der Informationen in Baden-Württemberg (LIFG BW) nimmt der LfD auch die Aufgabe des Landesbeauftragten für die Informationsfreiheit wahr.
835 Bericht des Berliner Datenschutzbeauftragten, Drs. 9/277, 22. Januar 1980, S. 2.
836 Vgl. Bericht des Berliner LfD, Drs. 9/248, 29. Dezember 1981, S. 18 und Bericht des Berliner LfD, Drs. 12/76, 31. Dezember 1990, S. 5.
837 Antrag der Fraktion SPD und der Fraktion AL, Drs. 11/717, 28. März 1990, dort § 32.
838 Vgl. Begründung zu § 32 des Gesetzesentwurfs, Antrag der Fraktion SPD und der Fraktion AL, Drs. 11/717, dort § 32.
839 Bericht des Berliner Datenschutzbeauftragten, Drs. 12/76, 31. Dezember 1990, S. 4 f.

Bürger „nach wie vor“ nur schwer zu vermitteln sei, wann er sich an den Datenschutzbeauftragten wenden könne und wann dieser nicht zuständig sei.[840]

Im Jahr 1995 wurde dann schließlich das BlnDSG entsprechend geändert und dem Datenschutzbeauftragten die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen übertragen.[841] Dieser wurde gemäß § 33 Abs. 1 S. 2 BlnDSG 1995 der Rechtsaufsicht des Senats unterstellt. Der Datenschutzbeauftragte war der Ansicht, dass den Bürgern hierdurch eine „einheitliche, möglichst effektive Datenschutzkontrollinstanz zur Verfügung“ gestellt werde.[842] Die bisherige Aufteilung der Aufsicht „stelle eine unnötige Zersplitterung von Aufgaben zu Lasten der Bürger dar“ und sei, wie die Beschwerdepraxis gezeigt habe, „von niemandem nachvollziehbar“.[843]

Nach der Anpassung an die DSGVO ist der Berliner Datenschutzbeauftragte gemäß § 8 Abs. 2 BlnDSG 2018 Aufsichtsbehörde für die Verarbeitung bei den nicht-öffentlichen Stellen und den öffentlichen Stellen, soweit diese am Wettbewerb teilnehmen und nach § 8 Abs. 1 BlnDSG 2018 auch Aufsichtsbehörde für die öffentlichen Stellen des Landes Berlin.[844]

### 3. Brandenburg

Zur Aufsichtsbehörde für die Verarbeitung bei nicht-öffentlichen Stellen war 1992 das Ministerium des Innern bestimmt worden.[845] Die Aufsicht über die Verarbeitung bei den öffentlichen Stellen wurde vom LfD ausgeübt.[846]

---

840 Bericht des Berliner Datenschutzbeauftragten, Drs. 12/76, 31. Dezember 1990, S. 5.

841 § 33 Abs. 1 BlnDSG 1995, GVBl. 1995, S. 404.

842 Bericht des Berliner Datenschutzbeauftragten, Drs. 13/303, 31. Dezember 1995, S. 4.

843 Bericht des Berliner Datenschutzbeauftragten, Drs. 13/303, 31. Dezember 1995, S. 62.

844 BlnDSG vom 13. Juni 2018, GVBl. 2018, S. 418; nach § 18 Abs. 1 S. 2 des Gesetzes zur Förderung der Informationsfreiheit im Land Berlin (IFG) wird die Aufgabe des Beauftragten für das Recht auf Informationsfreiheit vom Beauftragten für Datenschutz wahrgenommen.

845 § 1 Verordnung über die Regelung von Zuständigkeiten im Datenschutz DS-ZustV vom 10. August 1992, GVBl. II/92, S. 503.

846 §§ 22 – 27 Bbg DSG vom 20. Januar 1992, GVBl. 1992 I, S. 2.

Mit Gesetz vom 6. Mai 2010 wurde die Aufsicht über die nicht-öffentlichen Stellen mit der Aufsicht über die öffentlichen Stellen beim LfD zusammengeführt.[847]

Dem ging ein langwieriger Gesetzgebungsprozess voraus. So war bereits im Oktober 2008 ein Antrag von der Fraktion DIE LINKE auf Zusammenführung der Aufsicht gestellt worden – dem wiederum ein „zehnjährigen Diskussionsprozess" zu dieser Frage zu Grunde lag.[848] Die Zusammenführung sollte beim LfD erfolgen, da dieser hierfür prädestiniert sei. So würden sich zunehmend Überschneidungen zwischen dem öffentlichen und privaten Bereich ergeben, etwa bei Krankenkassen, Banken oder Sicherheitsdiensten. Durch die Zusammenführung der Aufsicht könnten personelle Ressourcen und die „verschiedenen Erfahrungen" im Datenschutz gebündelt werden. Auch hätten Bürger einen zentralen Ansprechpartner „für ihre Probleme".[849] Die Landesregierung sprach sich allerdings dafür aus, das Verfahren vor dem EuGH zur Anforderung der „völligen Unabhängigkeit" abzuwarten – insbesondere sei die Zusammenlegung der Aufsicht aufgrund der „notwendigen Rechtsaufsicht" auch eine verfassungsrechtliche Frage.[850]

Anfang 2010 legten die SPD-Fraktion und die Fraktion der LINKEN dann gemeinsam einen Gesetzesentwurf vor, der die Zusammenführung der Aufsicht beim LfD vorsah.[851] Aufgrund der „rasanten technischen Entwicklungen" und der „stark wachsenden Überschneidungen der Aufsichtsbereiche" sei eine effektive Datenschutzkontrolle nur zu gewährleisten, wenn die bei den Datenschutzkontrollbehörden vorhandenen Ressourcen gebündelt würden.[852] Hierdurch werde auch der Aufwand für Bürger und Unternehmen „bei der Suche der richtigen Aufsichtsbehörde" reduziert.[853] Daneben falle der Abstimmungsbedarf zwischen den Aufsichtsbehörden weg, was „unnötigen Bürokratieaufwand" einspare.[854] Hinzukomme, dass die Zusammenlegung der Aufsichtsbereiche geeignet sei, den gestiegenen technischen Anforderungen bei der Realisierung von Datenschutz im

847 Viertes Gesetz zur Änderung des Brandenburgischen Datenschutzgesetzes und anderer Rechtsvorschriften vom 25. Mai 2010 (GVBl. I Nr. 21).
848 Drs. 4/6804, 7. Oktober 2008.
849 Drs. 4/6804, 7. Oktober 2008.
850 Abgeordneter (u. Minister des Innern) Schönbohm (CSU), Plenarprotokoll 4/74, 16. Oktober 2008, S. 5535.
851 Drs. 5/293, 12. Januar 2010.
852 Drs. 5/293, 12. Januar 2010, S. 1.
853 Drs. 5/293, 12. Januar 2010, S. 2.
854 Drs. 5/293, 12. Januar 2010, S. 1 der Begründung des Gesetzesentwurfs.

privaten Bereich besser Rechnung zu tragen – auf welche technischen Anforderungen hierbei Bezug genommen wird wurde jedoch nicht weiter ausgeführt.[855]

Eine untergeordnete Rolle schien die von Art. 28 Abs. 1 S. 1 der RL 95/46/EG geforderte „völlige Unabhängigkeit" gespielt zu haben. So heißt es hierzu in der Begründung des Gesetzesentwurfs: „Die Übertragung der Kontrolle (…) ist darüber hinaus geeignet, stärker als bisher dem (…) Erfordernis" der in der Richtlinie geforderten „völligen Unabhängigkeit" Rechnung zu tragen.[856] Die Beschreibung „stärker als bisher" ist dabei durchaus zutreffend gewählt worden, da im Gesetzesentwurf noch die Rechtsaufsicht durch den Innenminister vorgesehen war.[857]

Das dem Gesetzesentwurf um circa zwei Monate nachfolgende Urteil des EuGH führte dazu, dass die Rechtsaufsicht im Gesetzesentwurf gestrichen wurde.[858]

Festhalten lässt sich, dass die Frage der Zusammenführung der Aufsicht in Brandenburg bereits einige Jahre vor dem Urteil des EuGH diskutiert worden war, die entsprechende Änderung des Landesdatenschutzgesetzes dann aber erst im Jahr 2010, nach dem Urteil des EuGH, erfolgte.

Nunmehr ist nach § 18 Abs. 1 BbgDSG 2018 der LfD zuständige Aufsichtsbehörde für die Verarbeitung bei den öffentlichen Stellen und nach § 18 Abs. 3 BbgDSG 2018 auch Aufsichtsbehörde im Sinne von § 40 BDSG für die Verarbeitung bei den nicht-öffentlichen Stellen.[859]

### 4. Bremen

In Bremen wurde die Zuständigkeit für die Aufsicht über die Verarbeitung im öffentlichen und nicht-öffentlichen Bereich bereits mit dem ersten Bremischen Datenschutzgesetz (BremDSG) von 1978 beim LfD vereint.[860] Allerdings wurde dennoch von einer „Zweigleisigkeit der Kontrolle" ge-

855 Drs. 5/293, 12. Januar 2010, S. 1 der Begründung des Gesetzesentwurfs.
856 Drs. 5/293, 12. Januar 2010, S. 1 der Begründung des Gesetzesentwurfs.
857 Drs. 5/293, 12. Januar 2010, Art. 1 Nr. 8 b).
858 Vgl. Änderungsantrag der Fraktionen SPD und DIE LINKE, Drs. 5/923, 14. April 2010, S. 2.
859 Nach § 11 Abs. 1 S. 2 des Akteneinsichts- und Informationszugangsgesetzes (AIG Brandenburg) nimmt der LfD die Aufgabe des Landesbeauftragten für das Recht auf Akteneinsicht wahr.
860 Durch Verordnung des Bremer Senats vom 29. Mai 1978, vgl. Erster Jahresbericht des LfD vom 31. März 1979, Drs. 9/1028, S. 3, dennoch wurde von einer

sprochen, da neben dem LfD ein parlamentarischer Datenschutzausschuss bestellt wurde – zu dessen Tätigkeit das BremDSG jedoch keine weiteren Bestimmungen traf.[861] Der LfD führte dazu aus, dass der Ausschuss nach „parlamentarischen Verfahrensweisen“ und der „Datenschutzbeauftragte“ weisungsfrei mit speziellen Überwachungskompetenzen arbeiten würden.[862] Die Zusammenlegung der Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen sei aus wirtschaftlichen Gesichtspunkten „besonders in einem Stadtstaat“ geboten. Auch würde die Zusammenlegung der Aufsicht garantieren, dass Wirtschaft und Verwaltung mit gleichen Maßstäben gemessen werden würden.[863]

In Reaktion auf das Urteil des EuGH wurde die Unabhängigkeit des LfD mit dem Gesetz zur Änderung des BremDSG von 2010 in § 25 BremDSG, insbesondere bei der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen, festgelegt.[864]

Die Zuständigkeit des LfD ist im Bremischen Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG) in § 21 Abs. 1 für die Aufsicht über die öffentlichen Stellen und in § 21 Abs. 2 für die nicht-öffentlichen Stellen geregelt.[865]

### 5. Hamburg

Auf die Gründe, die in Hamburg bereits 1981 zum Zusammenführen der Aufsicht geführt haben, wurde bereits unter E., II., 1., a) eingegangen.

Aufgrund des Urteils des EuGH im Jahr 2010 wurde die Unabhängigkeit des Hamburgischen Beauftragten für Datenschutz hervorgehoben, vgl. § 22 Abs. 1 S. 2 HmbDSG 2011.

---

„Zweigleisigkeit der Kontrolle“ gesprochen, jedoch aufgrund der Kombination des LfD mit einem parlamentarischen Datenschutzausschuss, vgl. a.a.O., S. 6.

861 Erster Jahresbericht des LfD Bremen vom 31. März 1979, Drs. 9/1028, S. 6.

862 Erster Jahresbericht des LfD Bremen vom 31. März 1979, Drs. 9/1028, S. 6.

863 Erster Jahresbericht des LfD Bremen vom 31. März 1979, Drs. 9/1028, S. 18.

864 Zu Grunde liegender Gesetzesentwurf vgl. Drs. 17/1491, 26. Oktober 2010, Brem.GBl. 2010, S. 573.

865 Brem. GBL. S. 131; nach § 13 Abs. 2 des Gesetzes über die Freiheit des Zugangs zu Informationen für das Land Bremen (BremIFG) nimmt der LfD auch die Aufgabe des Landesbeauftragten für die Informationsfreiheit wahr.

Die Zuständigkeit des Hamburgischen Beauftragten für Datenschutz für die Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen ist in § 19 Abs. 2 HmbDSG 2018 geregelt.[866]

## 6. Hessen

Wie bereits ausgeführt, wies Hessen mit der Errichtung der Institution des Datenschutzbeauftragten bereits 1970 den Weg in der Datenschutzaufsicht. Die Aufgaben des Datenschutzbeauftragten waren in § 23 des HDSG 1970 geregelt.

Die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen wurde den Regierungspräsidien Darmstadt, Kassel und Gießen übertragen.[867] Mit der Verordnung zur Regelung der Zuständigkeiten nach dem BDSG und anderen Gesetzen zum Datenschutz wurde die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen zum 1. März 2005 dem Regierungspräsidium Darmstadt übertragen.[868]

In Reaktion auf das Urteil des EuGH zur Unabhängigkeit der Aufsichtsbehörden für den nicht-öffentlichen Bereich und anlässlich des 40. Jahrestags des ersten HDSG verabschiedeten die Fraktionen von CDU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN gemeinsam die sog. „Wiesbadener Erklärung" vom 8. Oktober 2010.[869] Danach sollte die Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen „unter dem Dach" des Datenschutzbeauftragten zusammengeführt werden.[870]

---

866 HmbGVBl. S. 145; nach § 14 Abs. 2 des Hamburgischen Transparenzgesetzes (HmbTG) überwacht der Beauftragte für den Datenschutz auch die Einhaltung der Vorschriften des HmbTG.

867 Anordnung über die zuständige Aufsichtsbehörde nach den §§ 30 und 40 des Bundesdatenschutzgesetzes BDSG vom 10. Januar 1978, GVBl. 1978, S. 49.

868 GVBl. I S. 90; Achtzehnter Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden vom 5. Dezember 2005, Drs. 16/4752, S. 4.

869 Wiesbadener Erklärung zur Neuordnung des Datenschutzes in Hessen der Fraktionen der CDU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN, abgedruckt in: Kartmann/Ronellenfitsch, 40 Jahre Datenschutz in Hessen, S. 81; vgl. auch 39. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drs. 18/3847, 18. März 2011, S. 12 – dort allerdings auf den 8. Oktober 2011 datiert und im 40. Tätigkeitsbericht auf den 7. Oktober 2010, vgl. Drs. 18/5409, 20. März 2012, S. 24.

870 Vgl. 39. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drs. 18/3847, 18. März 2011, S. 15.

Ein bereits 2009 von der Fraktion der SPD eingebrachter Gesetzesentwurf mit dem Ziel der Zusammenlegung der Aufsicht wurde mit einem Änderungsantrag, den die Wiesbadener Erklärung unterzeichnenden Fraktionen gemeinsam einbrachten, verabschiedet und die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen im Jahr 2011 dem Datenschutzbeauftragten übertragen.[871] Der Hessische Datenschutzbeauftragte *Ronellenfitsch* betonte, dass es nun darauf ankomme, die mit der Zusammenlegung der Aufsicht verknüpfte Hoffnung auf eine Verbesserung des Datenschutzes zu erfüllen.[872] Ausführlich wies er dabei jedoch auch auf die Unterschiede zwischen dem öffentlichen und privaten Bereich hin, um „die rechtlichen Schwierigkeiten, vor die sich der Datenschutz aus einer Hand gestellt sieht", aufzuzeigen.[873]

Mit Blick auf die in Bayern bestehende räumliche Trennung zwischen dem Landesamt in Ansbach und dem LfD in München soll an dieser Stelle noch auf die auch in Hessen vor der Zusammenlegung der Aufsicht bestehende räumliche Trennung zwischen dem Regierungspräsidium in Darmstadt als Aufsichtsbehörde für die Verarbeitung bei den nicht-öffentlichen Stellen und dem Datenschutzbeauftragten mit Sitz in Wiesbaden eingegangen werden.

Der Hessische Datenschutzbeauftragte *Ronellenfitsch* ging auf die mit der Zusammenlegung einhergehenden Herausforderungen im 40. Tätigkeitsbericht ein. So wurden die im Dezernat Datenschutz beim Regierungspräsidium eingesetzten Mitarbeiter zur Dienststelle des Datenschutzbeauftragten abgeordnet. Auch mangels geeigneter Räumlichkeiten in Wiesbaden richtete der Datenschutzbeauftragten allerdings übergangsweise eine Außenstelle in Darmstadt ein. Dies ging mit verschiedenen Herausforderungen, wie beispielsweise der IT-Einbindung, einher. Von den im Dezernat Datenschutz tätigen Beschäftigten entschieden sich lediglich drei Mitarbeiter für einen Wechsel nach Wiesbaden, was zur Folge hatte, dass neues Per-

871 Drs. 18/375, 29. April 2009, Änderungsantrag mit Drs. 18/3869, 22. März 2011, GVBl. I S. 208.

872 40. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drs. 18/5409, 20. März 2012, S. 23.

873 40. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drs. 18/5409, 20. März 2012, S. 23; gleichwohl hatte der Datenschutzbeauftragte Ronellenfitsch bereits 2010 das Zusammenführen der Aufsicht beim Datenschutzbeauftragten empfohlen, vgl. Rechtsgutachten zur Neugestaltung der Datenschutzkontrolle,
Drs. 18/375, S. 39.

sonal gefunden werden musste.[874] Die Zusammenlegung ging mit „hohen Anforderungen" einher und stellte, so der Datenschutzbeauftragten, eine „– wenn auch gerne übernommene – Verpflichtung und Last" dar und war nicht die „Erfüllung eines fachimperialistischen Wunschtraums".[875]

Die Zuständigkeiten und Aufgaben des Hessischen Beauftragten für Datenschutz wurden 2018 im Gesetz zur Anpassung an die DSGVO in § 13 Abs. 1 HDSIG geregelt.[876] An dessen Zuständigkeit für die Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen wurde festgehalten.[877]

## 7. Mecklenburg-Vorpommern

In Mecklenburg-Vorpommern trat im Jahr 1992 das erste Landesdatenschutzgesetz (DSG M-V) in Kraft. Die Aufsicht über die Verarbeitung bei den öffentlichen Stellen wurde danach dem LfD zugewiesen. Für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen wurde das Innenministerium für zuständig erklärt.[878]

Mit der Änderung des DSG M-V im Jahr 2004 wurde der LfD auch zur Aufsichtsbehörde für die Verarbeitung bei den nicht-öffentlichen Stellen bestimmt.[879] Das Zusammenführen der Aufsicht erfolgte zwar nicht vor dem Hintergrund des Urteils des EuGH zur „völligen Unabhängigkeit" der Aufsicht, aber doch aufgrund der Vorgaben der RL 95/46/EG.[880] Auch sollten hierdurch Ressourcen gebündelt und eine „Vereinfachung" für die Bürger erreicht werden.[881]

Die Bündelung der Aufsicht wurde vom LfD begrüßt, der die Aufteilung der Aufsicht als für den Bürger „verwirrende Angelegenheit" bezeich-

874 40. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drs. 18/5409, 20. März 2012, S. 26 ff.
875 41. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drs. 18/7202, 4. April 2013, S. 25.
876 HDSIG vom 3. Mai 2018, GVBl. 2018, S. 82.
877 Nach § 89 HDSIG nimmt der Hessische Datenschutzbeauftragte auch die Aufgabe des Hessischen Informationsfreiheitsbeauftragten war.
878 Erster Tätigkeitsbericht des LfD M-V, Drs. 1/3950, 6. Januar 1994, S. 10.
879 GVOBl. M-V, S. 505.
880 Vgl. Begründung des Gesetzesentwurfs, Drs. 4/1168, 29. April 2004, S. 6 – allerdings war man der Auffassung, die Unabhängigkeit des LfD sei dadurch sichergestellt, dass die Staatsaufsicht auf eine Rechtsaufsicht durch die Landesregierung beschränkt bleibe, vgl. a.a.O.
881 Begründung des Gesetzesentwurfs, Drs. 4/1168, 29. April 2004, S. 8.

nete.[882] Der Bürger könne mit der Zusammenlegung der Aufsicht unbürokratisch und bürgerfreundlich „Datenschutz aus einer Hand" erhalten.[883] Der LfD erklärte, dass durch die Zuweisung der Aufsicht die „Chance" bestanden habe, durch „Nutzung des vorhandenen personellen und fachlichen Potentials Synergieeffekte für den Datenschutz im nicht-öffentlichen Bereich zu erzielen".[884]

Diese „Chance" des Wissenstransfers aus den Erfahrungen über die Aufsicht im nicht-öffentlichen Bereich wurde jedoch nicht genutzt – so wurde zwar ein Mitarbeiter des höheren Dienstes aus dem Innenministerium zur Dienststelle des LfD versetzt, dieser musste sich jedoch, da es sich nicht um den „bisherigen Amtsinhaber" handelte, erst in das Aufgabengebiet einarbeiten.[885]

In Reaktion auf das Urteil des EuGH im Jahr 2010 wurde dann die Unabhängigkeit des LfD durch Aufhebung der Rechtsaufsicht hervorgehoben.[886] Mit dieser Gesetzesänderung wurde auch der Datenschutzbeirat beim LfD eingeführt.[887]

Mit der Änderung des DSG M-V im Jahr 2018 wurden die Aufgaben des LfD in § 19 DSG M-V geregelt.[888] Der LfD ist nach § 19 Abs. 1 DSG M-V Aufsichtsbehörde für die Verarbeitung bei den öffentlichen Stellen und nach § 19 Abs. 2 DSG M-V Aufsichtsbehörde für die Verarbeitung bei den nicht-öffentlichen Stellen.

### 8. Niedersachsen

In dem im Jahr 1978 verabschiedeten ersten niedersächsischen Datenschutzgesetz (NDSG) wurde die Aufsicht über die Verarbeitung bei den öffentlichen Stellen dem LfD übertragen.[889] Mit Runderlass des Ministers des Innern waren 1977 die Bezirksregierungen zu den Aufsichtsbehörden

882 Vgl. Sechster Tätigkeitsbericht des LfD M-V, Drs. 4/1137, 27. April 2004, S. 9.
883 Vgl. Sechster Tätigkeitsbericht des LfD M-V, Drs. 4/1137, 27. April 2004, S. 9.
884 Vgl. Siebter Tätigkeitsbericht des LfD M-V, Drs. 4/2078, 23. Januar 2006, S. 7.
885 Vgl. Siebter Tätigkeitsbericht des LfD M-V, Drs. 4/2078, 23. Januar 2006, S. 7.
886 § 33a S. 2 DSG M-V 2004, wurde gestrichen, vgl. GVOBl. M-V, S. 277.
887 Vgl. § 33b DSG M-V 2011, GVOBl. M-V, S. 277; vgl. hierzu auch unter Kapitel D., XIII.
888 GVOBl. M-V, S. 193; nach § 14 Abs. 1 S. 2 des Gesetzes zur Regelung des Zugangs zu Informationen für das Land Mecklenburg-Vorpommern (IFG M-V) ist der LfD zugleich auch Landesbeauftragter für die Informationsfreiheit.
889 Niedersächsisches Datenschutzgesetz vom 26. Mai 1978, GVBl. S. 421.

für die Verarbeitung bei den nicht-öffentlichen Stellen bestimmt worden.[890]

Bereits im Jahr 1991 wurden dann dem LfD die Aufgaben der Aufsichtsbehörde für die Verarbeitung im nicht-öffentlichen Bereich, unter der Fachaufsicht der niedersächsischen Landesregierung, übertragen.[891]

Hintergrund der Übertragung der Aufsicht an den LfD war unter anderem die bisherige Wahrnehmung der Aufsichtstätigkeit durch die Bezirksregierungen. Diese wurde als „sicherlich ehrenhaft", allerdings nicht den Anforderungen an eine „vernünftige Kontrolle" gerecht werdend bezeichnet.[892]

Der LfD *Dronsch* erklärte die „Abkehr von der Zersplitterung auf die vier niedersächsischen Bezirksregierungen" als für dringend erforderlich. Gleichwohl sprach er sich dafür aus, dass „nach einiger Zeit praktischer Erfahrung" geprüft werden sollte, ob die Bündelung der Aufsicht beim LfD die beste Lösung sei.[893]

Nach einjähriger Aufsichtstätigkeit über die Verarbeitung bei den nicht-öffentlichen Stellen erklärte er, dass die Erfahrungen „fast ausnahmslos positiv" seien. So hätten die unterschiedlichen Arbeitsweisen der Bezirksregierungen bei der Datenschutzkontrolle vereinheitlicht und die Erfahrungen aus dem öffentlichen Bereich fruchtbar eingebracht werden können.[894]

Eine ausführliche Bewertung der Erfahrungen nach der Zusammenlegung der Aufsicht erfolgte dann im zwölften Tätigkeitsbericht des LfD.[895]

So seien vor der Gesetzesänderung Eingaben aus dem privaten Bereich beim LfD eingegangen – nun könnten Fälle einheitlich bearbeitet werden. Dies gelte nicht nur für materiell-rechtliche, sondern insbesondere auch für technisch-organisatorische Fragen, bei denen das Anlegen eines einheitlichen Maßstabes sowie umfassende EDV-Kenntnisse erforderlich

---

890 Runderlass vom 29. November 1977, Nds. MBl. S. 1488.

891 Beschluss vom 17. Dezember 1991, Nds. MBl. 1992, S. 230, in Kraft getreten am 1. Januar 1992; die gesetzliche Grundlage hierfür wurde mit § 18 Abs. 6 des NDSG 1991 geschaffen.

892 Abgeordneter Kempmann (DIE GRÜNEN), Plenarprotokoll 12/12, 11. Dezember 1990, S. 945.

893 Elfter Bericht über die Tätigkeit des Nds. LfD, Drs. 12/4400, 7. Januar 1993, S. 17.

894 Elfter Bericht über die Tätigkeit des Nds. LfD, Drs. 12/4400, 7. Januar 1993, S. 196.

895 Zwölfter Bericht über die Tätigkeit des Nds. LfD, Drs. 13/610, 30. Dezember 1994, S. 251.

seien. In der Dienststelle sei nun derselbe Mitarbeiter oft sowohl für den privaten als auch den öffentlichen Datenschutz zuständig, was eine Schwerpunktsetzung mit sich bringe und damit eine spürbare Verstärkung der Kontrolltätigkeit im privaten Bereich.[896]

Die Bündelung der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen beim LfD sei gerade auch im Vergleich zur Aufsicht durch die Bezirksregierungen vorzugswürdig, da sich die datenverarbeitenden Stellen weder an Landes- noch an Bezirksgrenzen orientieren würden. So müssten aufgrund der Zentralisierung die „immer wieder (…) gleichen Fragestellungen“ nur einmal bearbeitet werden. Auch in Bezug auf die Kommunikation mit den Aufsichtsbehörden der anderen Länder, unter anderem über den Düsseldorfer Kreis – an deren Beratungen dem LfD durch das niedersächsische Innenministerium die Möglichkeit der Teilnahme „zugestanden“ worden war –, sei die Kommunikation durch eine zentrale Landesbehörde von Vorteil.[897]

Er erklärte weiter, dass die Kontrolle über die öffentlichen Stellen, die am Wettbewerb teilnehmen, nun nicht länger durch den (nur) für den öffentlichen Bereich zuständigen LfD ausgeübt werde – was die Gefahr der unterschiedlichen Auslegung des BDSG mit sich gebracht hätte.[898] Auch sei die gebündelte Zuständigkeit des LfD im Hinblick auf die zunehmenden informationellen Beziehungen zwischen privaten und öffentlichen Stellen von Vorteil.[899]

Dass der LfD, soweit dieser als Aufsichtsbehörde über die Verarbeitung bei den öffentlichen-Stellen tätig werde, der Fachaufsicht unterliege, sei „sicher nicht unproblematisch“, habe in Niedersachsen aber bisher nicht zu Konflikten geführt. Auch sei das Ministerium als oberste Aufsichtsbehörde nicht in der Lage und habe auch nicht die Aufgabe, die Vielzahl der auflaufenden Fälle aufzuarbeiten. Bei Grundsatzfragen sei „ohnehin zumeist eine bundesweite Abstimmung nötig“, so dass die „Einschaltung der obersten Aufsichtsbehörde durch den LfD zum Zweck der Thematisierung im „Düsseldorfer Kreis“ selbstverständlich“ sei.[900]

In Reaktion auf das Urteil des EuGH erklärte das niedersächsische Ministerium für Inneres und Sport, dass es keinerlei fachaufsichtsrechtliche

---

896 Zwölfter Bericht über die Tätigkeit des Nds. LfD, Drs. 13/610, 30. Dezember 1994, S. 252.
897 Zwölfter Bericht über die Tätigkeit des Nds. LfD, Drs. 13/610, 30. Dezember 1994, S. 252.
898 Dies war in §§ 15, 18 NDSG 1978 geregelt.
899 Zwölfter Bericht über die Tätigkeit des Nds. LfD, Drs. 13/610, S. 252.
900 Vgl. Zwölfter Bericht über die Tätigkeit des Nds. LfD, Drs. 13/610, S. 253.

Weisungen mehr erteilen werde und sich auch aus dem Düsseldorfer Kreis zurückziehen werde.[901]

Mit dem „Gesetz zur Neuregelung der Rechtsstellung der oder des Landesbeauftragten für den Datenschutz“ wurde der LfD dann 2011 zur Aufsichtsbehörde für die Verarbeitung bei den nicht-öffentlichen Stellen erklärt.[902] Darüber hinaus wurde auch die niedersächsische Verfassung geändert. So wurde in Art. 62 Abs. 4 S. 3 der Niedersächsichen Verfassung geregelt, dass dem LfD durch Gesetz die Aufgabe übertragen werden kann, „die Durchführung des Datenschutzes bei der Datenverarbeitung nicht öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen zu kontrollieren“.[903] Hierdurch sollte auch die Zuständigkeit für den nicht-öffentlichen Bereich in den Verfassungsrang erhoben werden.[904]

Bei der 2018 verabschiedeten Novellierung des NDSG wurde die Organisation der Datenschutzaufsicht in Niedersachsen beibehalten. Danach leitet der LfD gemäß § 18 Abs. 1 S. 1, 2 NDSG 2018 sowie § 22 S. 1 NDSG 2018 eine von der niedersächsischen Landesregierung unabhängige oberste Landesbehörde, die Aufsichtsbehörde sowohl für die Verarbeitung bei den öffentlichen als auch nicht-öffentlichen Stellen ist.

### 9. Nordrhein-Westfalen

Die Aufsicht über die Verarbeitung bei den öffentlichen Stellen wurde in Nordrhein-Westfalen durch einen Landesbeauftragten für den Datenschutz ausgeübt.[905]

Der Regierungspräsident Arnsberg wurde für die nicht-öffentlichen Stellen in den Regierungsbezirken Arnsberg, Detmold und Münster und der Regierungspräsident Köln für die nicht-öffentlichen Stellen in den Regierungsbezirken Düsseldorf und Köln zur zuständigen Aufsichtsbehörde erklärt. Oberste Aufsichtsbehörde war das Innenministerium.[906]

---

901 Vgl. 20. Tätigkeitsbericht des Nds. LfD, Drs. 16/4240, 8. Dezember 2011, S. 9.
902 Vgl. § 22 Abs. 6 NDSG 2011, GVBl. S. 210.
903 Vgl. Art. 1 des Gesetzes zur Neuregelung der Rechtsstellung der oder des Landesbeauftragten für den Datenschutz vom 30. Juni 2011, Nds. GVBl. S. 210.
904 Vgl. Begründung des Gesetzesentwurfs der Fraktionen CDU und FDP, Drs. 16/3417, 8. März 2011, S. 5.
905 Vgl. Erster Tätigkeitsbericht des LfD NRW vom 31. März 1980, S. 11.
906 Erster Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden, MMV 10/2589,

Diese Zuständigkeitsverteilung war nach dem ersten Tätigkeitsbericht der Landesregierung für die Bürger wohl „zuweilen überraschend". Sie füge sich aber, so die Landesregierung, in die Unkenntnis über die vom Bürger häufig vermutete, gerade nicht gegebene Zuständigkeit des LfD bzw. BfD für die Verarbeitung bei den nicht-öffentlichen Stellen in Nordrhein-Westfalen ein.[907]

Allerdings wurde bereits im Jahr 2000 die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen auf den LfD übertragen, der insoweit der Aufsicht des nordrhein-westfälischen Innenministeriums unterstand.[908]

Die Präsidenten der Regierungspräsidien Arnsberg und Köln hatten sich im Gesetzgebungsverfahren deutlich gegen die Zusammenführung der Aufsichtsbehörden ausgesprochen und wurden dabei vom nordrhein-westfälischen Innenminister unterstützt.[909] Sie brachten vor, dass die Bezirksregierungen über mehr als 20 Jahre Erfahrung und Wissen aus der Datenschutzaufsicht über den nicht-öffentlichen Bereich verfügen würden. Durch die Aufteilung der Aufsicht zwischen Arnsberg und Köln sei eine größere räumliche Nähe zu den Unternehmen gegeben, als dies bei einer zentralisierten Aufsicht durch den LfD der Fall wäre. So könnten Zeitverluste durch eine weitere Anreise, die eine Verringerung der Effektivität und Anzahl der Prüfungen zur Folge hätte, vermieden werden.[910]

Auch wenn Synergieeffekte durch die Bündelung der Aufsicht beim LfD nicht bestritten wurden, so wurde argumentiert, dass Synergieeffekte auch bei der Ausübung der Aufsicht durch die Bezirksregierungen bestehen würden. Dort würde durch die Nähe zum Gewerberecht sowie zum Medizinal- und Pharmaziebereich Erfahrungswissen aus anderen Sachgebieten eingebracht, das datenschutzrechtlichen Prüfungen in diesen Bereichen zugutekommen würde.[911]

---

Dezember 1989, S. 3; § 1 der Verordnung über die Zuständigkeiten nach dem BDSG vom 29. September 1992, GV NRW. 1992, S. 369.

907 1. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden, MMV 10/2589, Dezember 1989, S. 25.

908 § 22 Abs. 6 S. 3 DSG NRW 2000.

909 Vorlage 12/3154 des Innenministeriums vom 24. Januar 2000; Zuschrift 12/3689, 31. Januar 2000 und Zuschrift 12/3693, 2. Februar 2000.

910 Vgl. Vorlage 12/3154 des Innenministeriums vom 24. Januar 2000, Schreiben der Regierungspräsidenten der Bezirksregierungen Arnsberg und Köln.

911 Vgl. Vorlage 12/3154 des Innenministeriums vom 24. Januar 2000, Schreiben der Regierungspräsidenten der Bezirksregierungen Arnsberg und Köln.

Aus den eingeholten Stellungnahmen zum Gesetzesentwurf für die Änderung des Datenschutzgesetzes aus dem Jahr 1999, der noch keine Zusammenführung der Aufsicht vorgesehen hatte, sticht die Stellungnahme des LfD Schleswig-Holstein *Bäumler* hervor.[912] Dessen Stellungnahme datiert auf den 12. Januar 2000 und erfolgte damit nur kurze Zeit nachdem der LfD Schleswig-Holstein durch Gesetz vom 25. November 1999 durch den Landtag zur Aufsichtsbehörde für die Verarbeitung bei den nicht-öffentlichen Stellen bestimmt wurde.[913] Der LfD Schleswig-Holstein *Bäumler* bezeichnete die im Gesetzesentwurf vorgesehene „Beibehaltung des Dualismus" als „nicht nur rückwärtsgerichtet, sondern geradezu anachronistisch".[914]

Er begründete dies mit der „Konvergenz" der Verarbeitung durch öffentliche und nicht-öffentliche Stellen durch Outsourcing, Privatisierung öffentlicher Aufgaben und Nutzung gemeinsamer Medien. Auch würden allein die LfD in der Öffentlichkeit als kompetente und vertrauenswürdige Interessenvertreter der Datenschutzbelange wahrgenommen.[915]

Die „Zersplitterung" der Aufsicht in vier Behörden sei eine „nicht zu verantwortende Vergeudung öffentlicher Ressourcen" – ein rationalerer Mitteleinsatz könne dazu führen, dass das insbesondere im nicht-öffentlichen Bereich bestehende „massive Vollzugsdefizit" gemildert werden könne. Schließlich wirke sich die Zweiteilung der Aufsicht auch dahingehend auf die „datenverarbeitende Wirtschaft" aus, dass diese bei einem datenschutzrechtlich relevanten Vorgang unter Umständen mit mehreren Datenschutzbehörden und deren nicht abgestimmten Positionen konfrontiert werde.[916]

Die Entscheidung für das Zusammenführen der Aufsicht wurde in Nordrhein-Westfalen dann jedoch vor allem damit begründet, dass hierdurch ein (zentraler) Ansprechpartner für die Bürgerinnen und Bürger

912 Drs. 12/4476, 2. Dezember 1999.
913 Vgl. Gesetz zur Errichtung des Unabhängigen Landeszentrums für Datenschutz, GVBl. SH 1999, S. 414 ff.
914 Stellungnahme des LfD Schleswig-Holstein vom 12. Januar 2000, Zuschrift 12/3641, S. 2 f.
915 Stellungnahme des LfD Schleswig-Holstein vom 12. Januar 2000, Zuschrift 12/3641, S. 2 f.
916 Vgl. zu diesem Absatz: Stellungnahme des LfD Schleswig-Holstein vom 12. Januar 2000, Zuschrift 12/3641, S. 2 f.

geschaffen werde.[917] So begrüßte dies auch die LfD NRW *Sokol* als „bürgerfreundliche Bündelung" bzw. als serviceorientiert „aus einer Hand".[918]

Die Aufsicht über die Tätigkeit des LfD im nicht-öffentlichen Bereich durch das Innenministerium wurde mit Hinweis auf das Rechtsstaatsprinzip begründet.[919]

Aufgrund der Entscheidung des EuGH im Jahr 2010 zur Unabhängigkeit der Aufsicht wurden die Regelungen zur Aufsicht durch das Innenministerium und dessen Weisungsbefugnisse aufgehoben.[920]

Die Zuständigkeit des LfD wurde 2018 in § 26 DSG NRW geregelt.[921] Dessen Zuständigkeit für die Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen wurde beibehalten.[922]

## 10. Rheinland-Pfalz

Rheinland-Pfalz hatte sich 1974 entgegen dem hessischen „Vorbild" nicht für einen Landesbeauftragten für den Datenschutz, sondern für einen Ausschuss für Datenschutz entschieden.[923] Diesem wurde die Aufsicht über die Verarbeitung bei den öffentlichen Stellen übertragen. An die Stelle des Ausschusses trat im Jahr 1991 eine Datenschutzkommission.[924]

---

917 Beschlussempfehlung und Bericht des Ausschusses für Innere Verwaltung, Drs. 12/4780, 10. April 2000, S. 62.

918 15. Datenschutzbericht der LfD NRW, Vorlage 13/0479, 20. Februar 2001, S. 2, 4.

919 Beschlussempfehlung und Bericht des Ausschusses für Innere Verwaltung, Drs. 12/4780, 10. April 2000, S. 62.

920 Vgl. § 22 Abs. 5 DSG NRW 2011, GV. NRW, S. 338, vgl. 21. Datenschutzbericht des LfD NRW, S. 6 f.

921 Nach § 13 Abs. 1 des Gesetzes über die Freiheit des Zugangs zu Informationen für das Land Nordrhein-Westfalen (IFG NRW) ist der LfD auch Beauftragter für das Recht auf Informationen.

922 DSG NRW vom 25. Mai 2018, GV. NRW, S. 244, ber. 278 und S. 404.

923 § 6 LDatG 1974, GVBL, S. 31, vgl. Erster Tätigkeitsbericht des Ausschusses für Datenschutz nach § 9 des Gesetzes gegen missbräuchliche Datennutzung (Landesdatenschutzgesetz), Drs. 7/3342, 17. Oktober 1974, S. 3.

924 Vgl. Sechster Tätigkeitsbericht nach § 21 des Landesgesetzes zum Schutz des Bürgers bei der Verarbeitung personenbezogener Daten (Landesdatenschutzgesetz) Rheinland-Pfalz, S. 1.

Die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen wurde durch die Bezirksregierungen ausgeübt.[925] Oberste Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich war das Ministerium des Innern und Sport. Im Jahr 2000 kam es zur Reform und Neuorganisation der Landesverwaltung, aus der die Aufsichts- und Dienstleistungsdirektion (ADD) in Trier hervorging. Diese wurde zur landesweit zuständigen Aufsichtsbehörde für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen erklärt.[926] Das Ministerium des Innern und für Sport blieb oberste Aufsichtsbehörde.

Die Zuständigkeit des LfD für die Aufsicht über die Verarbeitung bei den öffentlichen Stellen ist nunmehr in § 15 Abs. 1 LDSG RLP 2018 geregelt.[927] Nach § 15 Abs. 2 LDSG RLP 2018 ist der LfD auch Aufsichtsbehörde im Sinne von § 40 BDSG und für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen zuständig.[928] Der LfD wird nach § 18 LDSG RLP 2018 durch eine aus acht Mitgliedern bestehende Datenschutzkommission unterstützt.

## 11. Saarland

Zur Aufsichtsbehörde für die Verarbeitung bei den nicht-öffentlichen Stellen war in Saarland das Ministerium für Inneres und Sport bestimmt worden.[929] Die Aufsicht war allerdings bis 1993 an den Landesbeauftragten für Datenschutz, der die Aufsicht über die Verarbeitung bei den öffentlichen Stellen ausübte, übertragen und dann diesem 1993 trotz dessen offenen Widerspruchs entzogen worden.[930] In der Folge war die Datenschutzkon-

925 Landesverordnung über Zuständigkeiten nach dem Bundesdatenschutzgesetz vom 29. September 1992, GVBl. 1992, S. 369; Vgl. Drs. 11/1665, 10. Oktober 1988.

926 Erster Tätigkeitsbericht der ADD über den Datenschutz im nicht-öffentlichen Bereich, S. 8.

927 Nach § 19 Abs. 1 S. 2 des Landestransparenzgesetzes (LTranspG) RLP ist der LfD auch Landesbeauftragter für die Informationsfreiheit.

928 Landesdatenschutzgesetz Rheinland-Pfalz vom 8. Mai 2018, GVBl. 2018, S. 93.

929 Verordnung über die zuständige Aufsichtsbehörde für die Überwachung der Durchführung des Datenschutzes in nicht-öffentlichen Stellen vom 20. Januar 1978, Amtsbl. S. 91; Erster Tätigkeitsbericht der Aufsichtsbehörde für Datenschutz im nicht-öffentlichen Bereich Saarland, September 2003, S. 9.

930 Vgl. Dreizehnter Bericht über die Tätigkeit des LfD Saarland, Drs. 10/941, 6. März 1992, S. 4, Fünfzehnter Bericht Drs. 11/59, 23. Januar 1995, S. 7.

trolle aufgeteilt und wurde durch das Innenministerium ausgeübt.[931] Auf die Entwicklung der Aufsicht wurde bereits unter E., II., 1., b) eingegangen.

Im Jahr 2009 wurde dann von der saarländischen Landesregierung die Zusammenlegung der Datenschutzaufsicht für den öffentlichen und nicht-öffentlichen Bereich beschlossen.[932] Dies zog sich allerdings noch bis in das Jahr 2011 hin. Damit einhergehend wurde das Unabhängige Datenschutzzentrum Saarland gegründet.[933]

Die Zusammenlegung wurde damit begründet, dass zwischen öffentlichen und nicht-öffentlichen Stellen zunehmend elektronischer Datenaustausch stattfinden würde – dies erfordere immer öfter eine einheitliche Beratung im öffentlichen und nicht-öffentlichen Bereich.[934]

Auch würde den rat- und hilfesuchenden Bürgerinnen und Bürgern „erspart bleiben", zwischen öffentlich-rechtlichen und privatrechtlichen Datenschutzbelangen zu unterscheiden und verschiedene Datenschutzkontrollstellen aufsuchen zu müssen. Schließlich würden sich aus der Zusammenlegung Synergieeffekte ergeben und die Effizienz verbessert werden.[935]

Der LfD ist nach der Anpassung des SaarlDSG an die DSGVO nach § 16 Abs. 1 S. 1 Nr. 1 SaarlDSG 2018 Aufsichtsbehörde für die Verarbeitung bei den öffentlichen Stellen und gemäß § 16 Abs. 1 S. 1 Nr. 2 SaarlDSG 2018 Aufsichtsbehörde für die Verarbeitung bei den nicht-öffentlichen Stellen. An der Institution des Unabhängigen Datenschutzzentrums wurde festgehalten. Dieses wird nach § 16 Abs. 1 S. 3 SaarlDSG vom LfD geleitet.[936]

---

931 Durch Verordnung vom 24. Januar 2006 Amtsbl. S. 174, Ministerium für Inneres und Europaangelegenheiten.

932 23. Tätigkeitsbericht des LfDI Saarland, Drs. 14/425, 13. April 2011, S. 11, diese war bis dahin beim Ministerium für Inneres und Europaangelegenheiten angesiedelt, vgl. 24. Tätigkeitsbericht Unabhängiges Datenschutzzentrum Saarland vom 26. Juni 2013, S. 3.

933 24. Tätigkeitsbericht Unabhängiges Datenschutzzentrum Saarland vom 26. Juni 2013, S. 12; diesem stand der Landesbeauftragte vor, vgl. § 25 Abs. 1 SDSG 2011, Amtsbl. I S. 184.

934 Vgl. Gesetzesentwurf der Regierung des Saarlandes zur Änderung des Saarl. Datenschutzgesetzes, Drs. 14/443, 5. April 2011, S. 1.

935 Vgl. Gesetzesentwurf der Regierung des Saarlandes zur Änderung des Saarl. Datenschutzgesetzes, Drs. 14/443, 5. April 2011, S. 1, S. 5. wg.

936 Der LfD ist nach § 4 Abs. 2 des Saarländischen Informationsfreiheitsgesetzes (SIFG) auch Landesbeauftragter für Informationsfreiheit.

## 12. Sachsen

In Sachsen waren die Regierungspräsidien für die Aufsicht über die nicht-öffentlichen Stellen zuständig.[937] Diese unterlagen der Fachaufsicht durch das Staatsministerium des Innern als oberster Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich.[938]

Mit Wirkung zum Januar 2007 wurde die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich dem Datenschutzbeauftragten übertragen.[939] Hierdurch sollten Kompetenzstreitigkeiten vorgebeugt und durch die Nutzung von Synergieeffekten eine Verbesserung des Datenschutzniveaus erreicht werden.[940] So ging man davon aus, dass technische Fragen im Datenschutz an Bedeutung gewinnen würden und qualifiziertes Personal mit der Bündelung der Aufsicht sowohl für die technischen Fragen im öffentlichen als auch nicht-öffentlichen Bereich eingesetzt werden könnte. Auch sollten hierdurch Kosteneinspareffekte erzielt werden.[941]

Nach § 30a S. 2 SächsDSG 2007 unterlag der Datenschutzbeauftragte, insoweit er die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen ausübte, der Aufsicht der Sächsischen Staatsregierung. Durch das in Reaktion auf das Urteil des EuGH verabschiedete Zweite Gesetz zur Änderung des SächsDSG wurde die Rechtsaufsicht nach § 30a S. 2 SächsDSG aufgehoben. Der Datenschutzbeauftragte forderte darüber hinaus allerdings auch die Streichung der Regelung zur Dienstaufsicht nach § 25 Abs. 4 SächsDSG, konnte sich hiermit jedoch nicht durchsetzen.[942]

Mit dem sächsischen Datenschutzdurchführungsgesetz vom April 2018 wurde die Zuständigkeit des sächsischen Datenschutzbeauftragten in § 14

---

937 Vgl. § 1 Verordnung der Sächsischen Staatsregierung über die Regelung der Zuständigkeit der Aufsichtsbehörden nach § 38 Abs. 6 des BDSG vom 27. August 1991 (SächsGVBl. S. 324); Regierungspräsidien Chemnitz, Dresden und Leipzig, vgl. Dritter Tätigkeitsbericht für den Datenschutz im nicht-öffentlichen Bereich Sachsen, S. 6.

938 Verordnung vom 27. August 1991, GVBl. S. 324; Dritter Tätigkeitsbericht für den Datenschutz im nicht-öffentlichen Bereich Sachsen, S. 6.

939 SächsGVBL 2006, S. 530 f., vgl. Dritter Tätigkeitsbericht für den Datenschutz im nicht-öffentlichen Bereich, S. 56.

940 Gesetzesentwurf zur Änderung des SächsDSG, Drs. 4/5121, 2. Mai 2006, Vorblatt.

941 Gesetzesentwurf zur Änderung des SächsDSG, Drs. 4/5121, 2. Mai 2006, Begründung Ziff. 9 zu Art. 1 Nr. 9.

942 5. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten (Schutz des Persönlichkeitsrechts im nicht-öffentlichen Bereich), Drs. 5/7447, 16. Dezember 2011, S. 17.

SächsDSDG geregelt.[943] Nach § 14 Abs. 1 SächsDSDG ist der Datenschutzbeauftragte Aufsichtsbehörde für die Verarbeitung bei den öffentlichen Stellen und nach § 14 Abs. 2 SächsDSDG Aufsichtsbehörde für die Verarbeitung bei den nicht-öffentlichen Stellen.

### 13. Sachsen-Anhalt

In Sachsen-Anhalt nahm der spätere LfD noch als abgeordneter niedersächsischer Beamter im Ministerium des Innern bis zum 31. März 1992 die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen wahr.[944] Damit einhergehend wurde ihm durch Kabinettsbeschluss vom 4. Dezember 1990 der Auftrag erteilt, die „rechtlichen und tatsächlichen Voraussetzungen“ für einen wirksamen Datenschutz in Sachsen-Anhalt zu schaffen.[945] Mangels eines Landesdatenschutzgesetzes fand das BDSG bis zum 31. Dezember 1991 auch Anwendung auf die Verarbeitung durch die öffentlichen Stellen des Landes, soweit diese Bundesrecht ausführten. Für die Aufsicht über die Verarbeitung durch die öffentlichen Stellen war insoweit der BfD zuständig.[946]

Mit dem Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA) im Jahr 1992, wurde dem LfD die Aufsicht über die Verarbeitung bei den öffentlichen Stellen übertragen.[947] Für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen wurden die Bezirksregierungen Halle, Dessau und Magdeburg für zuständig erklärt und im Jahr 2002 die Zuständigkeit beim Regierungspräsidium Halle als alleinige Aufsichtsbehörde für den nicht-öffentlichen Bereich in Sachsen-Anhalt konzentriert.[948]

---

943 SächsGVBl. S. 198, 199.

944 Die spätere LfD (Sachsen-Anhalt) Kalk nahm diese Aufgaben noch als abgeordneter niedersächsischer Beamter im Ministerium des Innern des Landes Sachsen-Anhalt wahr, Erster Tätigkeitsbericht des LfD LSA, Drs. 1/2500, 2. April 1993, S. 4 f.

945 Erster Tätigkeitsbericht des LfD Sachsen-Anhalt, Drs. 1/2500, 2. April 1993, S. 4 f.

946 Erster Tätigkeitsbericht des LfD Sachsen-Anhalt, Drs. 1/2500, 2. April 1993, S. 4 f.

947 § 3 Abs. 1 DSG-LSA 1992, GVBl. LSA S. 682.

948 Vgl. zu diesem Absatz: Erster Tätigkeitsbericht des Regierungspräsidiums Halle als Aufsichtsbehörde des Landes Sachsen-Anhalt, S. 4.

Im Jahr 2004 entstand aus den Regierungspräsidien Halle, Dessau und Magdeburg und 22 weiteren Einzelbehörden das Landesverwaltungsamt Sachsen-Anhalt. Auf dieses ging auch die Zuständigkeit für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen über.[949]

Die Entscheidung des EuGH aus dem Jahr 2010 führte in Sachsen-Anhalt dazu, dass die Aufsicht über die öffentlichen und nicht-öffentlichen Stellen beim LfD zusammengeführt wurde.[950]

Die Zuständigkeit des LfD für die Aufsicht über die Verarbeitung bei den öffentlichen als auch nicht-öffentlichen Stellen besteht weiterhin fort.[951] Dessen Zuständigkeit für die Aufsicht über die Verarbeitung bei den öffentlichen Stellen ist in § 23 Abs. 1 DSAG LSA und für die Verarbeitung bei den nicht-öffentlichen Stellen in § 23 Abs. 4 DSAG LSA geregelt.[952]

## 14. Schleswig-Holstein

Die Erfahrungen der Aufsichtsbehörde zuständig für die Verarbeitung bei den nicht-öffentlichen Stellen in Schleswig-Holstein ist vergleichsweise gut dokumentiert, da der schleswig-holsteinische Landtag die Landesregierung bereits 1983 dazu aufgefordert hatte, einen Bericht über die Datenschutzkontrolle in der Wirtschaft vorzulegen.[953]

Die Landesregierung Schleswig-Holstein hatte Ende 1977 den Innenminister zur Aufsichtsbehörde für die Verarbeitung bei den nicht-öffentlichen Stellen bestimmt.[954] Dieser betraute dann im Jahr 1978 den LfD mit der Wahrnehmung der Aufsicht über die nicht-öffentlichen Stellen. Der LfD übte damit die Aufsicht über die Verarbeitung bei den öffentlichen

---

949 Zweiter Tätigkeitsbericht der Aufsichtsbehörde im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt, S. 7.

950 Vgl. § 22 Abs. 1 und Abs. 2 DSG LSA, GVBl. LSA S. 648.

951 Nach § 12 Abs. 2 des Informationszugangsgesetzes Sachsen-Anhalt (IZG LSA) wird die Aufgabe des Landesbeauftragten für die Informationsfreiheit vom LfD wahrgenommen.

952 DSAG LSA vom 18. Februar 2020, GVBl. LSA S. 25.

953 Bericht der Landesregierung Schlewig-Holstein über den Datenschutz in der Wirtschaft, Drs. 10/791, 20. Dezember 1984.

954 Vgl. Bericht der Landesregierung Schlewig-Holstein über den Datenschutz in der Wirtschaft, Drs. 10/791, 20. Dezember 1984, S. 10.

und nicht-öffentlichen Stellen aus.[955] Dies wurde von der Landesregierung mit den „Möglichkeiten des effektiven und damit kostengünstigen Personal- und Sachmitteleinsatzes“ begründet.[956] So habe die Praxis gezeigt, dass eine Vielzahl „spezieller Datenschutzfragen“ sowohl für den öffentlichen als auch den privaten Bereich von Bedeutung seien, eine Bündelung der Aufsicht bringe daher nicht nur eine „Verringerung des Verwaltungsaufwands“ mit sich, sondern diene auch der Rechtssicherheit.[957]

Mit dem im Jahr 2000 verabschiedeten LDSG wurde die Aufsicht über die nicht-öffentlichen Stellen dann vom Innenministerium auf das neu errichtete Unabhängige Landeszentrum für Datenschutz übertragen.[958] Aber auch die dem LfD obliegende Aufgabe der Aufsicht über die Verarbeitung bei den öffentlichen Stellen ging auf das Unabhängige Landeszentrum für Datenschutz über.[959] Das Unabhängige Landeszentrum für Datenschutz übte daher nach § 39 Abs. 1, 2 LDSG 2000 sowohl die Aufsicht über die Verarbeitung bei den öffentlichen als auch nicht-öffentlichen Stellen aus. Organ des Landeszentrums als Anstalt war der Vorstand, der aus dem Leiter der Anstalt bestand. Der Leiter der Anstalt führte die Bezeichnung „Landesbeauftragter für Datenschutz“.[960]

In Reaktion auf das Urteil des EuGH zur völligen Unabhängigkeit der Aufsichtsbehörden wurde die Unabhängigkeit des Landeszentrums hervorgehoben.[961]

Der LfD wurde mit dem LDSG 2018 zur Aufsichtsbehörde für die Verarbeitung bei den öffentlichen Stellen und nicht-öffentlichen Stellen bestimmt.[962] Die Einrichtung des Unabhängigen Landeszentrums für Da-

---

955 Vgl. Bericht der Landesregierung Schlewig-Holstein über den Datenschutz in der Wirtschaft, Drs. 10/791, 20. Dezember 1984, S. 10.

956 Vgl. Bericht der Landesregierung Schlewig-Holstein über den Datenschutz in der Wirtschaft, Drs. 10/791, 20. Dezember 1984, S. 10.

957 Vgl. Bericht der Landesregierung Schlewig-Holstein über den Datenschutz in der Wirtschaft, Drs. 10/791, 20. Dezember 1984, S. 96.

958 GVOBl. 2000, S. 169 ff.

959 Vgl. § 45 Abs. 1 LDSG 2000.

960 Vgl. § 34 Abs. 2 LDSG 2000, der Vorstand kann nach § 38 LDSG einen Beirat berufen, der den Vorstand der Anstalt berät.

961 Vgl. § 39 Abs. 1 S. 1 LDSG 2011: „Das Unabhängige Landeszentrum für Datenschutz nimmt die ihm zugewiesenen Aufgaben in Unabhängigkeit wahr und ist nur dem Gesetz unterworfen.“

962 Vgl. § 17 Abs. 1 LDSG 2018, GVOBl. 2018, S. 162 ff.

tenschutz wurde beibehalten und ist im Gesetz zur Errichtung eines Unabhängigen Landeszentrums für Datenschutz (Errichtungsgesetz ULD) geregelt.[963] Der LfD ist nach § 3 Abs. 2 des Errichtungsgesetzes ULD Leiter des Unabhängigen Landeszentrums für Datenschutz.

## 15. Thüringen

In Thüringen wurde das Thüringer Landesverwaltungsamt zur zuständigen Aufsichtsbehörde für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen bestimmt.[964] Die Aufsicht über die Verarbeitung bei den öffentlichen Stellen wurde dem LfD übertragen.[965] Dieser wurde durch den Beirat beim LfD in seiner Arbeit unterstützt, vgl. hierzu unter Kapitel D., XIII., 3.

Mit dem ThürDSG von 2011 wurde die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen dem LfD übertragen.[966] Dies wurde vom Thüringer Landesverwaltungsamt in dessen letztem Tätigkeitsbericht begrüßt. So würden durch das Zusammenführen der Aufsicht die „bisherigen Unsicherheiten" der Bürger bei der Suche nach dem „richtigen Ansprechpartner" beseitigt. Auch werde die datenschutzrechtliche Fachkompetenz mit allen Befugnissen der Datenschutzaufsicht bei einer Stelle gebündelt – Problemlösungen „im Umgang" mit Daten würden zukünftig aus einer Hand erfolgen. Die bislang „zweigleisige Bearbeitung" je nach öffentlichem oder privatem Ausgangspunkt mit allen „sich daraus ergebenden Abgrenzungsfragen" entfalle. Dies würde auch dazu führen, dass der Informationsaustausch der Aufsichtsbehörden länderübergreifend optimiert und die Abstellung und Ahndung datenschutzrechtlicher Verstöße beschleunigt werde.[967]

---

963 GVOBl. 2018, S. 162; die Einrichtung des Unabhängigen Landeszentrums als Anstalt des öffentlichen Rechts anstatt als oberste Landesbehörde wurde als „mindestens irritierend" bezeichnet, so Schwartmann/Jacquemain, Die DS-GVO und ihre Auswirkung auf die Bundesländer, RDV 2018, S. 65, 67.

964 § 6 der Zweiten Verordnung zur Bestimmung von Zuständigkeiten im Geschäftsbereich des Thüringer Innenministeriums vom 12. Februar 1992, vgl. Erster Tätigkeitsbericht nach § 38 Abs. 1 BDSG vom 18. Mai 2001 der für die Überwachung des Datenschutzes bei den nicht-öffentlichen Stellen zuständigen Aufsichtsbehörde im Thüringer Landesverwaltungsamt Weimar, S. 3.

965 Vgl. § 37 ThürDSG 1991.

966 § 42 Abs. 1 ThürDSG 2011.

967 5. Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich, S. 7 f.

Auch der LfD *Hasse* begrüßte das Zusammenführen der Aufsicht. So habe die Wahrnehmung der Aufsicht durch das Landesverwaltungsamt, und dort durch sog. 0,85 Vollbeschäftigten-Einheiten, dazu geführt, dass der Datenschutz im unternehmerischen Bereich in den letzten 20 Jahren „am Boden“ gelegen habe.[968]

Auch nach der Änderung des ThürDSG im Jahr 2018 wurde die Bündelung der Aufsicht beim LfD beibehalten. Dieser übt nach § 6 Abs. 1 ThürDSG 2018 die Aufsicht über die Verarbeitung bei den öffentlichen Stellen in Thüringen aus und ist gemäß § 11 Abs. 1 ThürDSG 2018 auch die für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen zuständige Behörde.[969]

## *IV. Trennung der Datenschutzaufsicht in Bayern*

Sowohl aus den Ausführungen in diesem Kapitel als auch den Ausführungen zur Entscheidung des bayerischen Gesetzgebers für die Beibehaltung der Trennung der Datenschutzaufsicht in Bayern gehen Argumente für und gegen das Zusammenführen der Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen hervor.

Auf diese und weitere Argumente soll nachfolgend eingegangen werden und eine abschließende Bewertung der Trennung („Trennungsmodell“) bzw. des Zusammenführens der Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen („Einheitsmodell“) getroffen werden.

Geprüft wird dabei auch, ob aufgrund der DSGVO die Aufsicht in Bayern zusammengeführt werden sollte. Hierzu wird insbesondere darauf eingegangen, ob noch zwischen der Verarbeitung durch öffentliche und nicht-öffentliche Stellen differenziert werden sollte.

### 1. Synergieeffekte

In keinem der Länder kam die Debatte um das Zusammenführen der Aufsicht ohne das Argument der Synergieeffekte aus.

---

968 10. Tätigkeitsbericht zum Datenschutz: Öffentlicher Bereich, S. 15.

969 Nach § 18 Abs. 6 S. 1 des Thüringer Transparenzsgesetzes (ThürTG) wird die Aufgabe des Landesbeauftragten für die Informationsfreiheit vom LfD übernommen.

So soll nach *Ronellenfitsch* die Aufteilung der Aufsicht zu einem höheren Mittelbedarf „sowohl für die Verwaltungsaufgaben als auch für das Vorhalten von spezifischem Sachverstand – nicht nur im technischen Bereich –" führen.[970]

Dies ist sowohl in Bezug auf die Verwaltungsaufgaben als auch auf das Vorhalten von spezifischem Sachverstand, insbesondere im technischen Bereich, durchaus zutreffend. Unabhängig von der Aufgabenwahrnehmung erfordert jede Behörde einen gewissen organisatorischen Unterbau, der bei der Unterhaltung von zwei Behörden doppelt anfällt.

Speziell im technischen Bereich des Datenschutzes ist ein Sachverstand erforderlich, der sowohl bei der Aufsicht über die Verarbeitung bei den öffentlichen als auch nicht-öffentlichen Stellen notwendig ist.[971] Öffentliche und nicht-öffentliche Stellen greifen nicht nur regelmäßig auf eine ähnliche Infrastruktur zurück, auch sind bestimmte technische Fragen, etwa aus dem Bereich der IT-Sicherheit, deckungsgleich.

Allerdings kann nach hier vertretener Auffassung das Argument der Synergieeffekte nur eingeschränkt herangezogen werden und ist auch weitaus weniger „allgemeingültig", als dies auf den ersten Blick scheint.

Bevor auf mögliche Synergieeffekte am Beispiel der Aufgabenverteilung in einer Aufsichtsbehörde eingegangen wird, soll eine, nach hier vertretener Auffassung „negative" Begleiterscheinung der Suche nach Synergieeffekten aufgezeigt werden. So haben das Zusammenführen der Aufsicht und die weitere regulatorische Entwicklung dazu geführt, dass die Landesbeauftragten heute in den Ländern in der Regel drei „Zuständigkeiten" bei sich vereinen.

Neben der Wahrnehmung der Aufsicht über die Verarbeitung bei den öffentlichen Stellen sind diese auch Aufsichtsbehörde für die Verarbeitung bei den nicht-öffentlichen Stellen und Beauftragte für die Informationsfreiheit.[972] Die „Vereinigung" des Beauftragten für den Datenschutz als Aufsichtsbehörde für die Verarbeitung bei den öffentlichen Stellen und dem

---

970 Ronellenfitsch, Rechtsgutachten zur Neugestaltung der Datenschutzkontrolle, Drs. 18/375, S. 27.

971 Wird die Aufsicht zusammengeführt, so würde sich, so Gola/Schomerus „das Problem bzw. die Notwendigkeit der Heranziehung „privaten" Sachverstands erledigen", vgl. Gola/Schomerus, Die Organisation der staatlichen Datenschutzkontrolle der Privatwirtschaft, ZRP 2000, S. 183, 185, dabei auf die Mitwirkung des TÜV e.V. in Bayern Bezug nehmend.

972 Vgl. bspw. § 12 Abs. 1 des Landesinformationsfreiheitsgesetzes (LIFG) BW vom 17. Dezember 2015; in Bayern existiert bislang kein vergleichbares Gesetz. Vgl. vorangehend auch unter Kapitel E., III., 1. – 15.

Beauftragtem für die Informationsfreiheit in einer Person ist nach hier vertretener Auffassung aufgrund der Unvereinbarkeit der Aufgaben abzulehnen. Allerdings kann – wenn auch mit Mühe – ein gewisser „verbindender" Bezug zur „Verarbeitung von Daten" bei öffentlichen Stellen bzw. zwischen dem Tätigwerden des LfD in seiner Rolle als Aufsichtsbehörde über die Verarbeitung bei den öffentlichen Stellen und als Beauftragter für die Informationsfreiheit „gegenüber" öffentlichen Stellen hergestellt werden.

Ein Zusammenhang zwischen der Aufgabe des LfD, die Verarbeitung bei den nicht-öffentlichen Stellen zu beaufsichtigen und beispielsweise Anrufungen nach dem jeweiligen Landesinformationsfreiheitsgesetz (IFG) in Zusammenhang mit Begehren, die allein gegenüber öffentlichen Stellen geltend gemacht werden können, dürfte jedoch abzulehnen sein.[973] Eine „Entzerrung" dieser Zuständigkeiten, insbesondere zwischen der Rolle als Aufsichtsbehörde für den nicht-öffentlichen Bereich und als Landesbeauftragter für die Informationsfreiheit, ist daher geboten. Allerdings sollte nach hier vertretener Auffassung, wie bereits ausgeführt, jedoch auch eine Trennung zwischen der Person des Landesbeauftragten für den Datenschutz (auch soweit dies die Wahrnehmung der Aufsicht über die Verarbeitung bei den öffentlichen-Stellen betrifft) und dem Landesbeauftragten für die Informationsfreiheit aufgrund der Wesensverschiedenheit der Aufgaben erfolgen.[974]

Mit anderen Worten geht die Suche nach möglichen Synergieeffekten mit einer Kumulation von Aufgaben, Befugnissen und auch Zuständigkeiten einher, die nach hier vertretener Auffassung wesensverschieden sind. Synergieeffekte lassen sich daher daher mit der Zusammenlegung von Zuständigkeiten nur begrenzt erzielen. Dies gilt insbesondere auch, da wie nachfolgend aufgezeigt wird, zwischen der Verarbeitung durch öffentliche und der Verarbeitung durch nicht-öffentliche Stellen zu differenzieren ist.

Das „Zusammenführen der Aufsicht" bei einer Behörde unter dem Gesichtspunkt von Synergieeffekten kommt, nach hier vertretener Auffassung, nur für Teilbereiche wie beispielsweise den technischen Datenschutz in Betracht. Wird die Aufsicht zusammengeführt, um darüber hinaus

---

973 Vgl. bswp. § 2 LIFG BW, dort auch § 1 Abs. 1 LIFG BW: „Zweck dieses Gesetzes ist es, (…) durch ein umfassendes Informationsrecht den freien Zugang zu amtlichen Informationen (…) zu gewährleisten, um die Transparenz der Verwaltung zu vergrößern (…).".

974 Vgl. auch v. Lewinski, Unabhängigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, ZG 2015, S. 229, 238 u. 241 ff.

Synergieeffekte zu erzielen, so muss beachtet werden, dass innerhalb der Aufsichtsbehörde grundsätzlich eine Trennung zwischen dem öffentlichen und nicht-öffentlichen Bereich erfolgen muss und daneben auch eine Trennung nach Sektoren, mit dem Ziel einer möglichst effektiven, spezialisierten Aufsicht, empfehlenswert ist. Das Argument der Synergieeffekte verliert vor diesem Hintergrund allerdings deutlich an Gewicht.

Beispielhaft soll der Aufbau der Aufsichtsbehörde von Nordrhein-Westfalen untersucht werden, um mögliche Synergieeffekte beziehungsweise eine Trennung in den öffentlichen und nicht-öffentlichen Bereich aufzuzeigen.[975] Im Jahr 2001 erklärte die LfD NRW *Sokol*, dass beim Zusammenführen der Aufsicht beim LfD organisatorisch die Umsetzung eines „Lebenssachverhaltskonzepts" angestrebt werde, um die „frühere Zersplitterung" der Aufsicht für den öffentlichen und den nicht-öffentlichen Bereich „tatsächlich vollständig" zu beseitigen.[976] Als Beispiele hierfür führte sie an, dass in dem für die Polizei zuständigen Referat auch die privaten Sicherheitsdienste angesiedelt werden; dass das für die öffentlichen Sparkassen zuständige Referat auch für private Banken oder auch dass das für die öffentlichen Krankenhäuser zuständige Referat für die Kontrolle der „Gesundheitsdatenflüsse" zu den niedergelassenen Ärztinnen und Ärzten zuständig sein soll.[977]

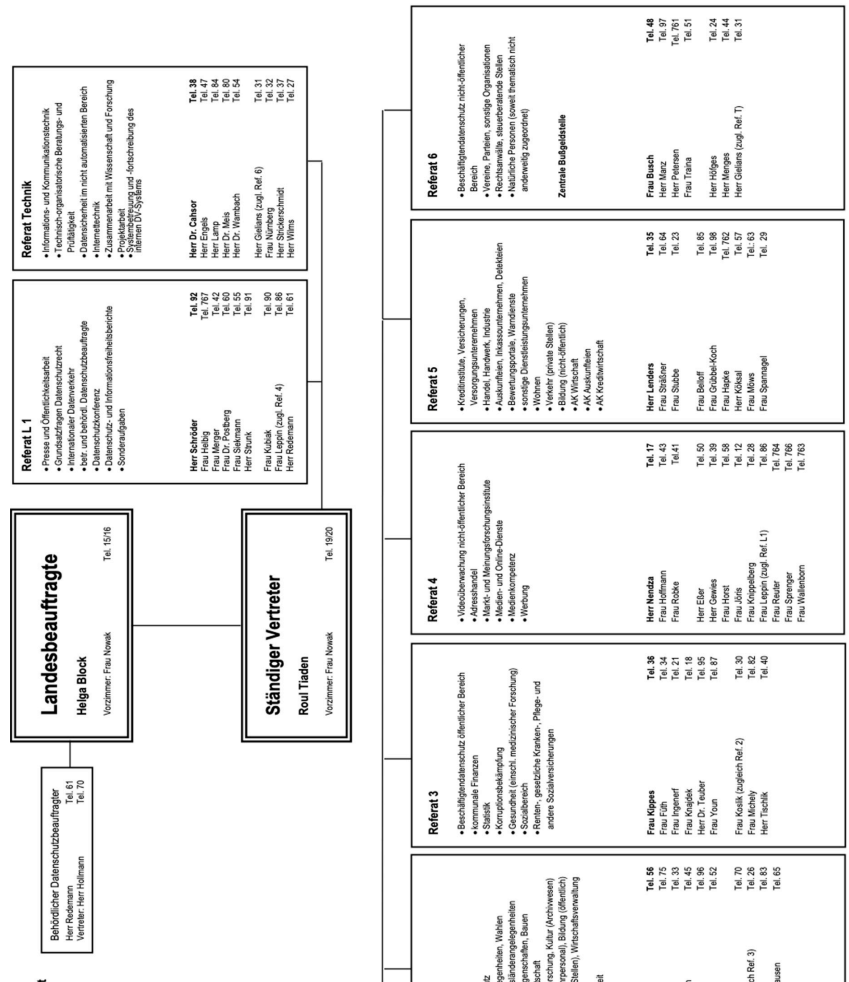
Die Dienststelle der LfD NRW und Nachfolgerin von Frau *Sokol*, Frau *Block,* ist im Jahr 2020 wie folgt aufgebaut:[978]

975 Die Aufsichtsbehörden haben keinen einheitlichen organisatorischen Aufbau, wie auch das Zusammenführen der Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen nicht einheitlich organisatorisch umgesetzt wurde, gleichwohl wird hier vertreten, dass sich eine gewisse Trennung in einen öffentlichen und nicht-öffentlichen Bereich in der Organisation aller Aufsichtsbehörden (mal mehr mal weniger offen) erkennen lässt.

976 15. Datenschutzbericht der LfD NRW, S. 4.

977 15. Datenschutzbericht der LfD NRW, S. 5.

978 https://www.ldi.nrw.de/mainmenu_Ueberuns/Inhalt/Ueberuns/organigramm.pdf Stand vom 1. Juli 2020, abgerufen am 19. August 2020.



Die Geschäftsstelle der LfD NRW ist in 8 Referate gegliedert. Hiervon sind zwei Referate, das Referat L 1 und das Referat Technik beim Ständigen Vertreter der LfD angesiedelt.

Das Referat L 1 übernimmt unter anderem die Presse und Öffentlichkeitsarbeit, Grundsatzfragen des Datenschutzrechts und die Datenschutz- und Informationsfreiheitsberichte. Im Referat L 1 ist auch der Bereich des internationalen Datenverkehrs angesiedelt, was zwar zu großen Teilen die Verarbeitung durch nicht-öffentliche Stellen betreffen dürfte, jedoch nicht allein dem nicht-öffentlichen Bereich zuzurechnen ist. Im Referat L 1 kann damit keine Trennung zwischen dem öffentlichen und nicht-öffentlichen Bereich festgestellt werden. Selbiges gilt für das Referat Technik. Wie bereits ausgeführt, können im Bereich des technischen Datenschutzes unbestritten Synergieeffekte zwischen der Aufsicht über die Verarbeitung bei öffentlichen und nicht-öffentlichen Stellen erzielt werden.

Neben dem Referat L 1 und dem Referat Technik ist auch das Referat 1 nicht in einen öffentlichen und nicht-öffentlichen Bereich getrennt. Das Referat 1 befasst sich unter anderem mit der Organisation der Geschäftsstelle des LfD, so beispielsweise Personalangelegenheiten. Wie bereits ausgeführt, sind im Hinblick auf Verwaltungsaufgaben Effizienzgewinne bzw. ein „Einsparpotential" möglich, da diese anstelle von bei zwei nun lediglich bei einer Behörde anfallen. Dies gilt entsprechend für die beim Referat L1 angesiedelte Presse- und Öffentlichkeitsarbeit.

Schon das Referat 2 befasst sich jedoch zum allergrößten Teil mit der Aufsicht über die Verarbeitung bei den öffentlichen Stellen; so beispielsweise der Aufsicht über die Verarbeitung bei der Polizei, Justiz und dem Verfassungsschutz. Nicht ersichtlich ist, dass dort auch die Aufsicht über die privaten Sicherheitsdienste, wie von der LfD *Sokol* im Jahr 2001 angedacht, angesiedelt wurde. Der Bereich Vermessung, Liegenschaften, Bauen dürfte in Abgrenzung zu dem im Referat 5 angesiedelten Bereich des Handwerks vor allem die Aufsicht über die Verarbeitung unter anderem in den Baubehörden betreffen. Wissenschaft, Forschung und Kultur sind nicht auf öffentliche Stellen beschränkt, aber dort wohl doch größtenteils zu verorten – bzw. der öffentliche Bereich jedenfalls durch „Public Private Partnerships" häufig involviert sein. Daneben gelten in diesen Bereichen aber auch grundsätzlich verschiedene datenschutzrechtliche Sonderregelungen, die eine gewisse Abgrenzung zum nicht-öffentlichen Bereich rechtfertigen.[979]

979 Bspw. § 27 BDSG, vgl. auch ErwG 159 DSGVO.

Ausdrücklich von Referat 2 nur insoweit beaufsichtigt, als es sich um die Verarbeitung durch öffentliche Stellen handelt, sind die Bereiche der Bildung und des Verkehrs. Damit wird deutlich, dass Referat 2 vor allem die Aufsicht über die Verarbeitung bei den öffentlichen Stellen wahrnimmt.

Dies gilt entsprechend auch für das Referat 3. Dieses ist ausdrücklich für den Beschäftigtendatenschutz im öffentlichen Bereich zuständig. Auch die Aufsicht über die kommunalen Finanzen ist dem öffentlichen Bereich zuzuordnen. Die Bereiche der Gesundheit und Rentenversicherung sowie der Sozialbereich sind zwar nicht auf den öffentlichen Bereich beschränkt, allerdings ist das Referat 3 „nur" für die Aufsicht über die gesetzlichen Kranken-, Pflege- und andere Sozialversicherungen zuständig, was erkennen lässt, dass auch im Referat 3 der Schwerpunkt der Aufsicht im öffentlichen Bereich liegt.

Anders hingegen die Referate 4, 5 und 6; ausdrücklich für den nicht-öffentlichen Bereich zuständig sind diese bei Videoüberwachung, Verkehr, Bildung und dem Beschäftigtendatenschutz. Aber auch in den anderen dort verorteten Sektoren, wie dem der Markt- und Meinungsforschungsinstitute oder der Werbung, sind zu großen Teilen allein nicht-öffentliche Stellen tätig.

Für die Medien- und Onlinedienste sind die für diese geltenden Besonderheiten zu beachten. So haben die öffentlich-rechtlichen Rundfunkanstalten auf Grundlage von Art. 85 Abs. 2 DSGVO, dem Medienstaatsvertrag und Landesrecht eigene Rundfunkdatenschutzbeauftragte eingerichtet. Aber auch für privaten Rundfunkveranstalter ist beispielsweise in Nordrhein-Westfalen auf dieser Grundlage nach § 49 Landesmediengesetz NRW (LMG NRW) der von der Medienkommission ernannte Datenschutzbeauftragte zuständig, soweit Daten im Sinne von § 46 Abs. 1 LMG NRW zu journalistischen Zwecken verarbeitet werden.

Die von Referat 5 zu überwachenden Kreditinstitute, Versicherungen, Handel, Handwerk und Industrie sind regelmäßig dem nicht-öffentlichen Bereich zuzuordnen.[980] Ebenfalls von Referat 5 beaufsichtigte Versorgungsunternehmen, wenn auch in öffentlicher Hand, nehmen regelmäßig

980 In Bayern gelten öffentlich-rechtliche Finanzdienstleitungsunternehmen sowie deren Zusammenschlüsse und Verbände nach Art. 1 Abs. 2 S. 2 BayDSG als nicht-öffentliche Stellen und unterliegen, wie bspw. die Sparkassen, der Datenschutzaufsicht durch das BayLDA.

am Wettbewerb im Sinne des § 2 Abs. 5 S. 1 bzw. S. 2 BDSG teil und gelten daher als nicht-öffentliche Stellen.[981]

Das Referat 6 wird als „Sammelbecken" tätig und ist, wie bereits ausgeführt, unter anderem zuständig für die Aufsicht über die Einhaltung des Beschäftigtendatenschutzes, der durch die auf Art. 88 Abs. 1 DSGVO gestützte Regelung des § 26 BDSG geprägt ist. Die Aufsicht über Rechtsanwälte und steuerberatende Stellen ist dort ebenfalls verortet und wird gesondert erwähnt, was auf eine besondere Grundrechtssensibilität der Aufsichtsbehörde in diesen Bereichen hoffen lässt, jedenfalls bis die Diskussion um die sektorielle Aufsicht Früchte trägt.[982]

Die bei Referat 6 angegliederte „Zentrale Bußgeldstelle" lässt schon begrifflich erwarten, dass diese sowohl für Bußgelder im öffentlichen als auch nicht-öffentlichen Bereich zuständig ist. Jedoch ist die Verhängung von Bußgeldern in Deutschland sowohl auf Bundes- als auch Landesebene gegen öffentliche Stellen grundsätzlich ausgeschlossen worden – jedenfalls, soweit diese nicht als Unternehmen am Wettbewerb teilnehmen.[983] Entsprechende Regelungen für am Wettbewerb teilnehmende öffentliche Stellen finden sich in § 43 Abs. 3 BDSG oder beispielsweise in Art. 22 BayDSG und § 32 DSG NRW.

Die zentrale Bußgeldstelle ist damit eine Bußgeldstelle, zuständig allein für die Verhängung von Bußgeldern gegen nicht-öffentliche Stellen.

Voranstehende Ausführungen zur Organisation der Geschäftsstelle der LfD in Nordrhein-Westfalen lassen erkennen, dass die von der früheren LfD *Sokol* angestrebte „vollständige" Beseitigung der „Zersplitterung der Aufsicht" in den öffentlichen und nicht-öffentlichen Bereich nicht umgesetzt werden konnte. Unstrittig lassen sich gewisse Effizienzgewinne

---

981 Allerdings wurde in Bayern die Aufsicht über am Wettbewerb teilnehmende öffentliche Stellen nach Art. 1 Abs. 3 S. 2 BayDSG der Zuständigkeit des LfD übertragen, was nicht überzeugen kann.

982 Zu dieser vgl. Ehmann, in: Ehmann/Selmayr, DS-GVO, 2. Aufl., Art. 90, Rn. 2; Ziebarth, in: Sydow, DSGVO, 2. Aufl., Art. 51, Rn. 17; König, Zur Möglichkeit einer sektoralen Datenschutzkontrolle nach dem Entwurf der EU-Datenschutzgrundverordnung, DuD 2013, S. 101, 103; in Bayern ist die Kontrollkompetenz auch auf dem Berufsgeheimnis unterliegende Daten erstreckt, vgl. Drs. 17/19628, 12. Dezember 2017, S. 39 und Wilde u.a., Datenschutz in Bayern, 29. AL, Art. 15, Rn. 28 f.

983 Bergt, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl., Art. 83, Rn. 26 f.; Frenzel, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl., Art. 83, Rn. 27 f.; der vollständige Ausschluss von Bußgeldern im öffentlichen-Bereich erfolgt nach Nemitz allerdings entgegen Art. 83 Abs. 7 DSGVO, vgl. Nemitz in: Ehmann/Selmayr, DS-GVO, 2. Aufl., Art. 83, Rn. 47.

erzielen, dies gilt aber vor allem für den organisatorischen „Verwaltungsaufbau“ der Aufsichtsbehörde selbst. Synergieeffekte in der Aufsicht sind hingegen beschränkt. Dies zeigt sich schon darin, dass beispielsweise die Aufsicht über die Bildung (öffentlich) und Bildung (nicht-öffentlich) nicht in Personalunion wahrgenommen wird. Dies dürfte nicht allein im Arbeitsaufwand begründet liegen, dem durch Arbeitsbewältigung im „Team“ entgegengetreten werden könnte, sondern eben gerade in den unterschiedlichen rechtlichen Anforderungen im öffentlichen und nicht-öffentlichen Bereich, beispielsweise für die Lehrkörper als Beamte (Beamtenrecht). Die unterschiedlichen Anforderungen im öffentlichen und nicht-öffentlichen Bereich spiegeln sich, wenn auch nicht vergleichbar ausdrücklich im Organigramm vermerkt, grundsätzlich in dem Aufbau der Referate und deren Aufgabenwahrnehmung wieder.

Dies bestätigt nach hier vertretener Auffassung, dass sich die Synergieeffekte im Bereich der Aufsicht vor allem auf den Bereich des technischen Datenschutzes beschränken. Die daneben durch Zusammenführen der Aufsichtsbehörden erreichte Struktur der Geschäftsstelle ist hingegen nicht durch Synergieeffekte geprägt, sondern zeigt vielmehr das „Einsparpotential“ bei dem Zusammenführen der Aufsichtsbehörden für den öffentlichen und nicht-öffentlichen Bereich auf.

Nach vorliegend vertretener Auffassung sollten bzw. sind Synergieeffekte eher im Bereich der Abstimmung und Kooperation mit anderen Aufsichtsbehörden für den öffentlichen bzw. nicht-öffentlichen Bereich zu finden. So wurde auch von den Aufsichtsbehörden selbst bereits in den 1970er Jahren die Abstimmung im Düsseldorfer Kreis bzw. der DSK gesucht. Die sich jeweils im öffentlichen bzw. nicht-öffentlichen Bereich stellenden Fragen sind „länderübergreifend näher“, als dies im öffentlichen bzw. nicht-öffentlichen Bereich „innerhalb eines Landes“ der Fall ist.

### 2. Bürgerfreundlichkeit

Das Zusammenführen der Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen wurde von den Landesgesetzgebern häufig mit einer damit einhergehend erhöhten Bürgerfreundlichkeit begründet. Dabei sollte statt von Bürgerfreundlichkeit vielmehr von einer „Freundlichkeit“ gegenüber den von der Verarbeitung betroffenen Personen gesprochen werden, da das Datenschutzrecht sich nicht auf den Schutz von Bürgern beschränkt. Nachfolgend wird zwar grundsätzlich

der Begriff der Bürgerfreundlichkeit übernommen, hiervon sollen aber allgemein die von der Verarbeitung betroffenen Personen umfasst sein.

Von den Befürwortern der Zusammenführung der Aufsicht wurde erklärt, dass eine aufgeteilte Zuständigkeit den Bürgern kaum vermittelbar sei.[984] So sei die Abgrenzung des öffentlichen und nicht-öffentlichen Bereichs „selbst für fachlich vorgebildete Juristen" kaum zu bewältigen.[985]

Dabei wurde von den Befürwortern der Zusammenführung insbesondere auf die Privatisierung von Staatskonzernen und den damit einhergehenden Zuständigkeitsfragen in der Datenschutzaufsicht Bezug genommen.[986] Allerdings ist in diesen Fällen (wie z.B. bei der Privatisierung der Deutschen Bundespost) regelmäßig die Zuständigkeit des BfDI gegeben.[987] Damit kann die Privatisierung nur beschränkt als Argument für das Zusammenführen der Aufsicht auf Landesebene herangeführt werden. Daneben dürfte die Zuständigkeit des BfDI nicht zur Bürgerfreundlichkeit, nach dem Verständnis der Befürworter des Zusammenführens der Aufsicht, beitragen.

Hier wird vertreten, dass den Bürgern die Differenzierung zwischen einer Aufsichtsbehörde für den öffentlichen und nicht-öffentlichen Bereich vor allem dann schwerfallen dürfte, wenn es an der Kenntnis über die Existenz der jeweils anderen Behörde fehlt. So dürfte auch von den Aufsichtsbehörden in Bayern kaum bestritten werden, dass es beispielweise zu Beschwerden bei der „falschen" Behörde kommt. Fraglich ist jedoch, ob dies darin begründet liegt, dass die Bürger nicht zwischen der Datenverarbeitung durch den Staat (beispielsweise in der Verwaltung) und einem Unternehmen differenzieren können, oder ob schlicht das Bewusstsein von zwei getrennt existierenden Aufsichtsbehörden mit unterschiedlichen Zuständigkeiten fehlt. Soweit kritisiert wird, dass die Aufteilung der Datenschutzaufsicht auf verschiedene Behörden nicht zur Transparenz beitrage, so ist die Ursache für die mangelnde Transparenz gegebenenfalls nicht

984 Ronellenfitsch, Rechtsgutachten zur Neugestaltung der Datenschutzkontrolle, Drs. 18/375, S. 27.

985 Ronellenfitsch, Rechtsgutachten zur Neugestaltung der Datenschutzkontrolle, Drs. 18/375, S. 27.

986 Ronellenfitsch, Rechtsgutachten zur Neugestaltung der Datenschutzkontrolle, Drs. 18/375, S. 27.

987 Vgl. § 42 Abs. 3 PostG und § 115 Abs. 4 TKG, hierzu auch unter Kapitel C., II., 1.

in der Trennung der Aufsicht, sondern in der unzureichenden Kommunikation und dem fehlenden Dialog mit den Bürgern zu suchen.[988]

Die „Bürgerfreundlichkeit" dürfte in den Ländern aber auch vor Zusammenführung der Aufsichtsbehörden gewährleistet gewesen sein, da die Aufsichtsbehörden die an die unzuständige Stelle adressierten Begehren an die zuständige Aufsichtsbehörde weitergeleitet haben dürften. So wie dies heute noch in Bayern der Fall und auch ausdrücklich in Art. 34 Abs. 3 BayDSG 2018 geregelt ist.[989] Ein „Mehraufwand" für die betroffenen Personen ist, da „falsch" adressierte Begehren nach vorliegendem Kenntnisstand von keiner Aufsichtsbehörde an den Bürger zurückgewiesen wurden, nicht ersichtlich. Wenn überhaupt, kann von einem Mehraufwand für die Aufsichtsbehörden gesprochen werden.

Die Bedeutung des Arguments der Bürgerfreundlichkeit soll vorliegend jedoch nicht geschmälert werden. So kommen den betroffenen Personen durch die DSGVO weitreichende Rechte zu, deren Gewährleistung auch von den Aufsichtsbehörden sicherzustellen ist. Dies wird grundsätzlich erschwert, wenn die betroffene Person in der Wahrnehmung ihrer Rechte eingeschränkt oder „gehemmt" ist, da sie die zuständige Stelle, an die sie sich wenden möchte, nicht ermitteln kann. Gleichwohl wird hier vertreten, dass die „Bürgerfreundlichkeit" durch das Zusammenführen der Aufsicht nicht erhöht wird, da sich die betroffene Person auch bei der zweigeteilten Aufsicht stets an die Aufsichtsbehörde wendet, die nach ihrer Einschätzung zuständig ist. Das Bewusstsein für die Unzuständigkeit dürfte schon nicht gegeben sein. Die betroffene Person wird sich grundsätzlich „weniger Gedanken" über die Trennung zwischen dem öffentlichen und nicht-öffentlichen Bereich machen, als dies beim „fachlich vorgebildeten Juristen" der Fall ist, und seine Anfrage an die ihm zuständig erscheinende

988 Zum Argument der Transparenz, vgl. Ronellenfitsch, Rechtsgutachten zur Neugestaltung der Datenschutzkontrolle, Drs. 18/375, S. 27.

989 Art. 34 Abs. 3 BayDSG: „(1) Wird eine Beschwerde bei einer sachlich unzuständigen Aufsichtsbehörde eingereicht, gibt diese die Beschwerde unverzüglich an die sachlich zuständige Aufsichtsbehörde ab und unterrichtet die beschwerdeführende Person. (2) In diesem Fall hat die abgebende Stelle die betroffene Person über die Weiterleitung zu unterrichten und ihr auf Ersuchen weitere Unterstützung zu leisten."; inwieweit die Weiterleitung an die zuständige Stelle „aufwändig" sein soll, erscheint vorliegend nicht nachvollziehbar, da jede Eingabe, auch im Einheitsmodell, zu prüfen und der zuständigen Stelle zuzuleiten ist und die ganz große Mehrheit aller Eingaben heute auf elektronischem Weg erfolgen dürfte, was deren Weiterleitung erleichtert, anders aber zur „aufwändigen Abgabe", vgl. Taeger, Kommentar zu EuGH C-518/07, K&R 2010, S. 326, 330, 331.

oder eben überhaupt bekannte Behörde richten. „Bürgerfreundlichkeit" kann auch bei der Zweiteilung der Aufsicht hergestellt werden, indem Anfragen unmittelbar an die zuständige Stelle weitergeleitet werden, wie auch heute weiterhin die Aufsichtsbehörden für den öffentlichen und nicht-öffentlichen Bereich in den Ländern stets prüfen müssen, ob ihre Zuständigkeit, etwa im Verhältnis zur Zuständigkeit des BfDI, gegeben und welche Abteilung oder welcher Mitarbeiter behördenintern zuständig ist.

### 3. Verflechtung von öffentlichen und nicht-öffentlichen Stellen

Kritisiert wird, dass es bei der getrennten Aufsicht zu „Vermischungen" bei der Zuständigkeit der Aufsichtsbehörden für eine zu beaufsichtigenden Stelle kommen könne, bzw. öffentliche und nicht-öffentliche Stellen so eng zusammenarbeiten, dass es zu „Überschneidungen und Wechselwirkungen" komme.[990]. Hierdurch könnten „Zuständigkeitsnischen" entstehen, die wiederum zu „Datenschutzskandalen" führen könnten.[991]

Bei der Zusammenarbeit und Verflechtung von öffentlichen und nicht-öffentlichen Stellen handelt es sich um eine Herausforderung für die nach dem Trennungsmodell organisierte Datenschutzaufsicht, die jedoch auch in gewissem Maß bei der zusammengeführten Aufsicht besteht. Auch dort ist abzugrenzen, ob der öffentliche oder der nicht-öffentliche Bereich betroffen ist, um beispielsweise die Anwendung findenden datenschutzrechtlichen Regelungen zu bestimmen.

Aufgrund der im deutschen Datenschutzrecht grundsätzlich eindeutig angelegten Zuordnung zu entweder dem öffentlichen oder nicht-öffentlichen Bereich kann das Argument, dass sich der „öffentliche und nicht-öffentliche Bereich kaum noch klar trennen lassen", was für eine für beide Bereiche zuständige Aufsichtsbehörde spreche, nach hier vertretener Auffassung nicht überzeugen.[992] Vielmehr ist die Trennung zwischen öffentlichem und nicht-öffentlichem Bereich aufrechtzuerhalten und klare

990 Beisenherz/Tinnefeld, Sozialdatenschutz – eine Frage des Beschäftigtendatenschutzes?, DuD 2010, S. 221, 224 für den Bereich des Sozialdatenschutzes.

991 Vgl. Ronellenfitsch, Rechtsgutachten zur Neugestaltung der Datenschutzkontrolle, Drs. 18/375, S. 31 unter Bezugnahme auf: ders., Datenschutz bei der Bahn, DVBl. 2010, S. 401 ff.

992 So aber Ronellenfitsch, Rechtsgutachten zur Neugestaltung der Datenschutzkontrolle, Drs. 18/375, S. 31; vgl. hierzu auch Buchner, in: Tinnefeld u.a., Einführung in das Datenschutzrecht, 7. Aufl., S. 220 ff. u. 403 ff.

Zuständigkeiten sind zu definieren. Sollten hier Schutzlücken erkannt werden, so ist der Gesetzgeber gefordert, diese durch Zuständigkeitszuweisungen zu schließen.

### 4. Öffentliche Stellen als Adressaten von Grundrechten – Auslegungsmaßstab

Verarbeitet die öffentliche Verwaltung, sei es auf Bundes- oder Landesebene, personenbezogene Daten, so handelt der Staat (der Bund bzw. die Länder). Staatliches Handeln in Form der Verarbeitung von personenbezogenen Daten erfordert eine Rechtsgrundlage, auf die dieses Handeln gestützt werden kann, da die Verarbeitung einen Eingriff in die Grundrechte der betroffenen Personen darstellt.[993] Ein solcher Eingriff muss für die Bürger so wenig einschneidend wie möglich, also verhältnismäßig sein.[994] Allerdings sind nur die öffentlichen Stellen unmittelbare Adressaten der Grundrechte.[995]

In Abgrenzung hierzu werden nicht-öffentliche Stellen bei der Verarbeitung in Ausübung ihrer grundrechtlich gewährleisteten Freiheit tätig.[996]

Die Datenschutzgesetze sind in Bezug auf die Verarbeitung durch nicht-öffentliche Stellen „Ermächtigungsgrundlage" für Eingriffe in die grundsätzliche Datenverarbeitungsfreiheit Privater, die sich untereinander in „Freiheit und Gleichheit" gegenüberstehen.[997] Im Verhältnis zwischen den nicht-öffentlichen Stellen und den betroffenen Personen, deren Daten von den nicht-öffentlichen Stellen verarbeitet werden, kommen die Grundrechte durch die bei der Verarbeitung zu beachtenden datenschutzrechtlichen Bestimmungen (nur) mittelbar zur Geltung (sog. mittelbare Drittwirkung).[998]

---

993 Vgl. v. Lewinski, in: Auernhammer, DSGVO BDSG, 7. Aufl., Einf., Rn. 59; Stentzel, Der datenschutzrechtliche Präventionsstaat, PinG 2016, S. 45 f.

994 Vgl. Masing, Herausforderungen des Datenschutzes, NJW 2012, S. 2305, 2306.

995 Buchner, in: Tinnefeld u.a., Einführung in das Datenschutzrecht, 7. Aufl., S. 221.

996 Insb. der Berufsfreiheit und Unternehmerfreiheit (Art. 16 GRCh; Art. 12. Abs. 1 GG) und der Allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG), vgl. v. Lewinski, in: Auernhammer, DSGVO BDSG, 7. Aufl., Einf., Rn. 62.

997 Vgl. Masing, Herausforderungen des Datenschutzes, NJW 2012, S. 2305, 2306; v. Lewinski, in: Auernhammer, DSGVO BDSG, 7. Aufl., Einf., Rn. 62;

998 Vgl. Buchner, in: Tinnefeld u.a., Einführung in das Datenschutzrecht, S. 221; Masing, Herausforderungen des Datenschutzes, NJW 2012, S. 2305, 2306 ff.

Vertreten wird, dass die sich gegenüber stehenden Grundrechte von datenverarbeitenden Stellen und betroffenen Personen, dazu führen würden, dass der Gesetzgeber bei der Normierung datenschutzrechtlicher Bestimmungen nicht nur seine grundrechtliche Schutzpflicht gegenüber den betroffenen Personen, sondern auch die Grundrechte der datenverarbeitenden Stellen beachten müsse, was zu regelmäßig großzügigeren Regelungen des Datenschutzes im nicht-öffentlichen Bereich führen würde.[999] Aufgrund der „Datenmacht" großer Konzerne und auch der Zugriffsmöglichkeiten des Staates auf deren „Datenbestände" würden jedoch gute Gründe für einen einheitlichen Regelungsansatz und eine ganzheitliche Betrachtungsweise sprechen.[1000]

Dieser Ansicht wird vorliegend nicht gefolgt. Vielmehr wird vertreten, dass gerade kein einheitlicher Reglungsansatz, sondern eine weitest mögliche (regulatorische) Trennung des öffentlichen und nicht-öffentlichen Bereiches erfolgen sollte.[1001] Gleichwohl sollten beispielsweise die die Datenverarbeitung in den Mittelpunkt ihres wirtschaftlichen Handelns stellenden Technologiekonzerne strengen rechtlichen Anforderungen unterworfen werden.[1002]

Wie bereits ausgeführt wirken die Grundrechte zwischen den nicht-öffentlichen Stellen und den betroffenen Personen, deren Daten sie verarbeiten, nicht unmittelbar, sondern nur mittelbar. Auch die nicht-öffentlichen Stellen sind Träger von Grundrechten, insbesondere dem Recht der wirtschaftlichen Betätigung, die mit den Rechten der betroffenen Personen in Abwägung gebracht werden müssen.

Dieser unterschiedliche Auslegungsmaßstab lässt sich auch der DSGVO entnehmen. Nach Art. 6 Abs. 1 UAbs. 2 DSGVO kann die Rechtsgrundlage des Art. 6 Abs. 1 lit. f) DSGVO nicht von den Behörden für die in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung herangezogen werden. Bei Art. 6 Abs. 1 lit. f) DSGVO handelt es sich um eine für die nicht-öffentlichen Stellen wichtige und von diesen häufig herangezogene Rechtsgrundlage.[1003] Bei Art. 6 Abs. 1 lit. f) DSGVO sind die berechtigten Inter-

---

999 Vgl. Buchner, in: Tinnefeld u.a., Einführung in das Datenschutzrecht, S. 221.

1000 Vgl. Buchner, in: Tinnefeld u.a., Einführung in das Datenschutzrecht, S. 221.

1001 So auch Stentzel, Der datenschutzrechtliche Präventionsstaat, PinG 2016, S. 45, 49.

1002 Vgl. Masing, Herausforderungen des Datenschutzes, NJW 2012, S. 2305, 2308 mit Verweis auf die Fraport Entscheidung des BVerfG und zur Reichweite der mittelbaren Schutzwirkung der Grundrechte.

1003 Reimer, Verwaltungsdatenschutzrecht, DÖV 2018, S. 881, 886: „die vielleicht wichtigste und vermutlich umstrittenste Klausel für die Privatwirtschaft".

essen des Verantwortlichen oder eines Dritten mit den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person abzuwägen. Behörden sollen Daten jedoch nicht aus berechtigtem Interesse, sondern zur Erfüllung ihrer Aufgaben verarbeiten. Für die insoweit erforderliche Verarbeitung muss aber der Gesetzgeber – und nicht die Behörden selbst durch Abwägung von Interessen – die Rechtsgrundlage schaffen.[1004]

Wer hierin bzw. allgemein in der DSGVO eine „großzügigere Regelung" des Datenschutzes im nicht-öffentlichen Bereich erkennt, lässt die unterschiedlichen Möglichkeiten von öffentlichen und nicht-öffentlichen Stellen Daten zu erheben außer Betracht. So kann der Staat grundsätzlich den Bürger zur Preisgabe von Daten bei Vorliegen entsprechender Rechtsgrundlagen, beispielsweise mittels Verwaltungsaktes, „zwingen". Im nicht-öffentlichen Bereich sind die verarbeitenden Stellen hingegen darauf angewiesen, dass die betroffenen Personen „freiwillig" agieren. Die „großzügigeren" Regelungen des Datenschutzes für den nicht-öffentlichen Bereich, etwa Art. 6 Abs. 1 lit. f) DSGVO oder die Möglichkeit gemäß Art. 6 Abs. 1 lit. a) DSGVO die Verarbeitung auf eine Einwilligung der betroffenen Person zu stützen, sind nicht nur Ausdruck der Anerkennung der Grundrechte der verarbeitenden Stellen, sondern eben gerade auch der Privatautonomie der betroffenen Personen, die im öffentlichen Bereich beschränkt ist.[1005]

Berechtigt und zutreffend ist daher die Frage, inwieweit es überzeugend ist, wenn für nicht-öffentliche Stellen und den Staat ein „scheinbar gleichartiges Verbot mit scheinbar allgemeinen Rechtfertigungsgründen geschaffen wird, dann aber zentrale Elemente (die Einwilligung und die Wahrnehmung berechtigter Interessen) für Behörden sogleich wieder zurückgenommen werden müssen – weil eben Verbot und Rechtfertigung der Datenverarbeitung für Private und den Staat nicht gleich sind".[1006] Dies soll vorliegend allerdings nicht weiter behandelt werden.

---

1004 Vgl. ErwG 47 S. 5 DSGVO.

1005 Vgl. Masing, Herausforderungen des Datenschutzes, NJW 2012, 2305, S. 2308: „Im Zentrum des privaten Datenschutzes steht die Selbstbestimmung des Betroffenen"; zu der „unterschiedlichen Bedeutung" der Rechtsgrundlagen im öffentlichen und nicht-öffentlichen Bereich, vgl. Buchner, in: Tinnefeld u.a., Einführung in das Datenschutzrecht, 7. Aufl., S. 405 und Reimer, Verwaltungsdatenschutzrecht, DÖV 2018, S. 881, 886 ff.; vgl. zur Einwilligung auch ErwG 43 S. 1 DSGVO; zur Einwilligung vgl. auch Ingold, in: Sydow, DSGVO, 2. Aufl., Art. 7 Rn. 11, wonach auch öffentliche Stellen grds. uneingeschränkt auf die Einwilligung zugreifen können sollen.

1006 Vgl. Masing, Herausforderungen des Datenschutzes, NJW 2012, 2305, S. 2310.

Wie aufgezeigt wurde, ist der Datenschutz im öffentlichen und nicht-öffentlichen Bereich keineswegs „einheitlich". Die Aufsichtsbehörden sollten diese Differenzierung und den unterschiedlichen Auslegungsmaßstab stets ihrem Handeln zu Grunde legen und keinesfalls die ihnen gegenüber nicht-öffentlichen Stellen zustehenden Befugnisse missbrauchen.[1007]

### 5. Harmonisierung des Datenschutzrechts

Neben einem einheitlich anzuwendenden Auslegungsmaßstab (s. vorangehende Ausführungen) wird vertreten, dass nach der DSGVO ein einheitliches Datenschutzrecht sowohl für den öffentlichen als auch den nicht-öffentlichen Bereich gelten soll.[1008] Insbesondere die Vielzahl an Öffnungsklauseln für den öffentlichen Bereich wird daher kritisch gesehen.[1009] Dies würde zumindest „potentiell" dazu führen, dass der „Harmonierungseffekt der DSGVO" geschwächt wird.[1010] So würden Öffnungsklauseln mit sich bringen, dass eine „Vereinheitlichung des Datenschutzes in der Union noch lange auf sich warten lassen wird".[1011]

Gerade aber die öffentliche Verwaltung sei schon „seit jeher ein wichtiger Nachfrager nach Daten und ein intensiv agierender Datenverarbeiter".[1012] Dass die Mitgliedsstaaten bereichsspezifische Verarbeitungsgrundlagen im Sinne von Art. 6 Abs. 2 und Abs. 3 DSGVO verabschieden kön-

1007 Ausführlich hierzu Stentzel, Der datenschutzrechtliche Präventionsstaat, PinG 2016, S. 45, 49.

1008 Hornung/Spiecker gen. Döhmann, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl., Einleitung, Rn. 232 f.

1009 Hornung/Spiecker gen. Döhmann, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl., Einleitung, Rn. 232 f.; Buchner, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl., Art. 1, Rn. 7; die Öffnungsklauseln im nicht-öffentlichen Bereich würden dazu führen, dass sich auch mit der DSGVO an „dem Nebeneinander von allgemeinen und bereichsspezifischem Datenschutzrecht nicht viel ändern wird", so Buchner, in: Tinnefeld u.a., Einführung in das Datenschutzrecht, 7. Aufl., S. 223 f.

1010 Hornung/Spiecker gen. Döhmann, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl., Einleitung, Rn. 231.

1011 Vgl. Buchner, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl., Art. 1, Rn. 7.

1012 Hornung/Spiecker gen. Döhmann, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl., Einleitung, Rn. 232.

nen, sei daher für die „Wahrung einheitlicher und effektiver Datenschutzvorstellungen problematisch".[1013]

Vielmehr dürfte jedoch gelten, dass sowohl in der DSGVO als auch dem BDSG zwar der öffentliche und nicht-öffentliche Bereich in „einer Verordnung" bzw. „einem Gesetz" geregelt werden, diese Bereiche jedoch grundsätzlich getrennt werden und auch zu trennen sind.[1014]

Die Öffnungsklauseln der DSGVO für den öffentlichen Bereich führen nicht zu einem unterschiedlichen Datenschutzniveau in den Mitgliedstaaten, sondern sind vielmehr Ausdruck des Subsidiaritätsprinzips nach Art. 5 Abs. 3 EUV.

Auch werden die Ziele der DSGVO durch die Öffnungsklauseln für den öffentlichen Bereich nicht gefährdet.

So sind die Ziele der DSGVO nach Art. 1 Abs. 1 und 2 DSGVO, der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und der Schutz deren personenbezogener Daten, auch im öffentlichen Bereich gewährleistet. Es gelten beispielsweise zum einen grundsätzlich dieselben „Schutzinstrumente", wie etwa die Art. 12 ff. DSGVO, zum anderen sehen Art. 6 Abs. 2 und Abs. 3 DSGVO lediglich die Möglichkeit spezifischerer Bestimmungen vor. Die von den Mitgliedstaaten getroffenen spezifischeren Bestimmungen müssen sich daher an das generelle Schutzniveau der DSGVO anpassen. Soweit Daten zwischen öffentlichen Stellen in der Union übermittelt werden, so darf das von der DSGVO vorgegebene Schutzniveau in keinem Mitgliedstaat unterschritten werden.[1015]

Aber auch das Ziel des freien Verkehrs personenbezogener Daten nach Art. 1 Abs. 1 und Abs. 3 DSGVO wird nicht gefährdet. Dieses Ziel bezieht sich auf den freien Verkehr von Daten in der Union zur Förderung des Binnenmarkts und der Wirtschaft.[1016] Die Harmonisierung des Datenschutzrechts und auch der Datenschutzaufsicht ist geeignet, hierzu einen Beitrag zu leisten. Eine Harmonisierung des für die öffentlichen Stellen

---

1013 Hornung/Spiecker gen. Döhmann, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl., Einleitung, Rn. 232.

1014 Vgl. v. Lewinski, in: Auernhammer, DSGVO BDSG, 7. Aufl., Einf., Rn. 57.

1015 Geteilt wird die Kritik an bestimmten Öffnungsklauseln wie bspw. der des Art. 8 Abs. 1 S. 3 DSGVO, wonach die Mitgliedstaaten unterschiedliche Regelungen für die Einwilligungsfähigkeit Minderjähriger bei einem Dienst i.S. von Art. 8 Abs. 1 S. 1 DSGVO treffen können – hier ist allerdings auch grds. allein der nicht-öffentliche Bereich betroffen.

1016 Sydow, in: Sydow, DSGVO, 2. Aufl., Art. 1, Rn. 18; einschränkend Hornung/Spiecker gen. Döhmann, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl., Art. 1, Rn. 42.

geltenden Datenschutzrechts ist für den Binnenmarkt allerdings nur eingeschränkt von Relevanz. Die Öffnungsklauseln der DSGVO betreffen daher auch nicht den „Kern des gemeinsamen (digitalen) Binnenmarkts, sondern Regelungsmaterien, in denen es aus Sicht des gemeinsamen Marktes vertretbar erscheint, dass in den Mitgliedstaaten unterschiedliche Regelungen gelten".[1017]

Nach hier vertretener Auffassung ist die DSGVO primär auf die Harmonisierung des Datenschutzrechts und der Datenschutzaufsicht bei der Verarbeitung durch nicht-öffentliche Stellen gerichtet und kann daher als „Wirtschaftsdatenschutzrecht" bezeichnet werden.[1018] Eine „vollständige" Harmonisierung des Datenschutzrechts in der Europäischen Union, die Öffnungsklauseln ausschließen würde, ist nicht nur nicht erforderlich, sondern aufgrund des Subsidiaritätsprinzips auch abzulehnen.

### 6. Gefährdungspotenzial

In Bezug auf das Verhältnis von öffentlichen und nicht-öffentlichen Stellen ist auch dahingehend zu differenzieren, dass die öffentlichen Stellen gegenüber betroffenen Personen verbindliche Anordnungen treffen und durchsetzen können (bezeichnet als „Gefährdungspotential").[1019]

Der Staat kann natürliche Personen zur Preisgabe von personenbezogenen Daten (bei Vorhandensein entsprechender Rechtsgrundlagen) verpflichten. Eine solche Verpflichtung, beispielsweise mittels eines Verwaltungsaktes, ermöglicht ihm die Verarbeitung von Daten. Rechtshistorische Beispiele hierfür sind etwa die Diskussion um die Einführung eines Per-

---

1017 Vgl. Roßnagel, Zusätzlicher Arbeitsaufwand für die Aufsichtsbehörden durch die DSGVO, S. 140.

1018 Vgl. v. Lewinski, in: Auernhammer, DSGVO BDSG, Einf., Rn. 61, m.w.N.; gleichwohl soll nicht verkannt werden, dass die Bürger der Union in Ausübung bspw. ihrer Freizügigkeit (Art. 45 AEUV), der Niederlassungs- (Art. 49 AEUV) und Dienstleistungsfreiheit (Art. 56 AEUV) sowie des freien Kapital- und Zahlungsverkehrs
(Art. 63) auch mit der Verwaltungstätigkeit der Behörden verschiedener Mitgliedstaaten in Berührung kommen und die DSGVO daher mit Blick auf das Ziel des Schutzes der betroffenen Personen (und grds. nicht des freien Verkehrs personenbezogener Daten) auch im Bereich der Verarbeitung durch öffentliche Stellen grds. eine Harmonisierung herbeiführt, vgl. Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 1. Aufl., S. 46, Rn. 24.

1019 Vgl. Bull, Die „völlig unabhängige" Aufsichtsbehörde, EuZW 2010, S. 488, 493.

sonenkennzeichens oder die „Volkszählung“, die jeweils entsprechende Reaktionen hervorgerufen haben.[1020] Dabei ist diese Thematik weiterhin aktuell, wie beispielsweise die Diskussion um die Einführung einer „Warn-App“ in Zeiten der COVID-19-Pandemie im Jahr 2020 und eine verpflichtende Nutzung dieser App gezeigt hat.[1021]

Auch wenn Technologiekonzerne wie Google oder Facebook heute quasi-monopolistische Marktstellungen erlangt haben, so können sie doch nicht zur Nutzung ihrer Dienste „verpflichten“.

Da dem Staat theoretisch besondere „Machtmittel“ zur Verfügung stehen, ist im Bereich der Aufsicht nicht nur die Unabhängigkeit der Aufsichtsbehörde von Bedeutung, sondern auch das dort vorhandene Bewusstsein um das Gefährdungspotential in Bezug auf die Verarbeitung durch öffentliche Stellen.

## 7. Harmonisierung der Datenschutzaufsicht

Wie unter anderem bereits in Bezug auf die einheitliche Anwendung der DSGVO auf öffentliche und nicht-öffentliche Stellen ausgeführt, zielt die DSGVO neben der Sicherstellung des Schutzes der betroffenen Personen auf die Harmonisierung des für die Verarbeitung bei den nicht-öffentlichen Stellen geltenden Datenschutzrechts sowie dessen einheitliche Anwendung und Durchsetzung ab.[1022]

Die Aufsichtsbehörden sollen, wie bereits ausgeführt, an der Harmonisierung des Datenschutzrechts in der Union mitwirken. Hierzu sollen insbesondere auch die Regelungen der DSGVO zur Zusammenarbeit und Kohärenz in den Art. 60–76 DSGVO beitragen. Die Vorschriften der Art. 60 ff. DSGVO, insbesondere das sog. Kohärenzverfahren und das

---

1020 Vgl. nur Mallmann C., Datenschutz in Verwaltungs-Informationssystemen, S. 15, m.w.N.; Stollreither, Der gläserne Mensch – noch Zukunft oder schon Gegenwart, in: Vollkommer, Datenverarbeitung und Persönlichkeitsschutz, S. 15 ff.; im Jahr 2020 wurde mit dem Gesetzesentwurf zum Registermodernisierungsgesetz ein neuer Anlauf in diese Richtung unternommen, vgl. BT-Drs. 19/24226 vom 11. November 2020.

1021 SWR Aktuell „Weiter Vorbehalte gegen Corona-Warn-App – Forderung nach verpflichtender Nutzung“,

1022 So wohl auch v. Lewinski, in: Auernhammer, DSGVO BDSG, 7. Aufl., Einf., Rn. 61: „Die DSGVO als Binnenmarktregelung (vgl. Art. 1 Abs. 3 DSGVO) ist damit – nach bisheriger deutscher Konzeption – sogar primär auf den „nicht-öffentlichen Bereich“ gerichtet.“.

„One-Stop-Shop"-Verfahren nach Art. 56 DSGVO, sollen dazu dienen, die Wettbewerbsnachteile von nicht-öffentlichen Stellen mit (mehreren) Niederlassungen in der Union zu beseitigen und diesen allein eine Aufsichtsbehörde als Ansprechpartner gegenüber zu stellen.[1023]

Dabei differenzieren die Art. 60–76 DSGVO grundsätzlich nicht zwischen der Aufsicht über die Verabeitung bei den öffentlichen und der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen.

Gleichwohl werden die Vorschriften zur Zusammenarbeit und Kohärenz vor allem im nicht-öffentlichen Bereich relevant. Hiervon geht auch die DSGVO aus, die beispielsweise in Art. 60 Abs. 7 S. 1 DSGVO bzw. ErwG 124 S. 1 von den Niederlassungen bzw. der Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters spricht und sich dabei auf Unternehmen bezieht. Deutlich zielt Art. 60 DSGVO damit auf den nicht-öffentlichen Bereich ab.[1024]

Dies gilt nach hier vertretener Auffassung auch für das „One-Stop-Shop"-Verfahren nach Art. 56 DSGVO. So finden nach Art. 55 Abs. 2 S. 2 DSGVO die Vorschriften über die Zuständigkeit der federführenden Behörde keine Anwendung, wenn die Verarbeitung durch Behörden oder nicht-öffentliche Stellen gestützt auf Art. 6 Abs. 1 lit. c) oder e) DSGVO erfolgt. In diesen Fällen ist nach Art. 55 Abs. 2 S. 1 DSGVO die Aufsichtsbehörde des betroffenen Mitgliedstaates zuständig. Auch dadurch wird nach hier vertretener Auffassung deutlich, dass die DSGVO trotz der grundsätzlich bestehenden Forderung nach einer einheitlichen Rechtsanwendung und Durchsetzung die Souveränität der Mitgliedstaaten respektiert und, da Art. 6 Abs. 1 lit. c) oder e) DSGVO vor allem auf die Verarbeitung durch öffentliche Stellen Anwendung finden dürften, insoweit auch zwischen der Verarbeitung durch öffentliche und nicht-öffentliche Stellen differenziert.

Die DSGVO legt damit den Schwerpunkt bei der Harmonisierung der Aufsicht auf die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen.

### 8. Unabhängigkeit der Aufsichtsbehörden

Wie bereits aus den vorangehenden Ausführungen ersichtlich, erfolgte das Zusammenführen der Aufsicht über die Verarbeitung bei den öffentlichen und nicht-öffentlichen Stellen in den meisten Ländern in Zusammenhang

1023 Klabunde, in: Ehmann/Selmayr, DS-GVO, 2. Aufl., Art. 60, Rn. 2.
1024 Lachmayer, in: Auernhammer, DSGVO BDSG, 7. Aufl., Art. 60, Rn. 1.

mit der Entscheidung des EuGH zur nach der RL 95/46/EG geforderten völligen Unabhängigkeit.[1025]

Die Unabhängigkeit der Aufsichtsbehörden ist auch nach der DSGVO eine „völlige Unabhängigkeit", die neben der institutionellen Eigenständigkeit nach Art. 52 Abs. 1 DSGVO auch die materielle Unabhängigkeit, vermittelt durch Art. 52 Abs. 4 und Abs. 6 DSGVO sowie die Weisungsfreiheit, das Verbot von nicht mit dem Amt zu vereinbarenden Tätigkeiten und die eigene Personalauswahl umfasst, Art. 52 Abs. 2, 3 und 5 DSGVO.[1026]

Die Anforderungen an die Unabhängigkeit der Aufsichtsbehörden sind in der Rechtswissenschaft ausführlich behandelt worden und sollen daher hier nicht weiter dargestellt werden.[1027]

Erwähnt werden soll jedoch, dass mit der Unabhängigkeit der Aufsichtsbehörden einhergeht, dass die vorzeitige Beendigung der Amtszeit eines LfD bzw. des Präsidenten des BayLDA nur unter sehr eingeschränkten Voraussetzungen möglich ist.

So hatte der EuGH in der Rechtssache Kommission vs. Ungarn, die eine vorzeitige Beendigung der Amtszeit des Präsidenten der ungarischen Datenschutzaufsichtsbehörde zum Gegenstand hatte, verdeutlicht, dass eine vorzeitige Beendigung des Mandates der Aufsichtsbehörde bzw. deren Leitung grundsätzlich ausgeschlossen ist.[1028] Andernfalls könnte der Behördenleitung mit einer vorzeitigen Beendigung des Mandats gedroht werden, womit die Gefahr der Einflussnahme bestehe.[1029] Eine Beendigung komme daher nur bei schwerwiegenden und objektiv nachprüfbaren Gründen in Betracht.[1030]

Aufgrund der bei allen Aufsichtsbehörden in der Bundesrepublik Deutschland bestehenden monokratischen Behördenstruktur führt dies zu einer „Abhängigkeit" der unabhängigen Datenschutzaufsicht von der Behördenleitung.[1031] Es besteht das Risiko, dass die „Güte der Aufsicht" mit

1025 EuGH v. 9. März 2010, C – 518/07.
1026 Vgl. Boehm, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl., Art. 52, Rn. 7 ff.
1027 Vgl. Thomé, Reform der Datenschutzaufsicht.
1028 EuGH Urt. v. 8.4.2014 – C-288/12, Rn. 54.
1029 EuGH Urt. v. 8.4.2014 – C-288/12, Rn. 52.
1030 Boehm, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl., Art. 52, Rn. 15; EuGH Urt. v. 8.4.2014 – C-288/12, Rn. 52.
1031 Zum monokratischen Modell vgl. Mitrou, Die Entwicklung der institutionellen Kontrolle des Datenschutzes, S. 85 ff.

der Leitung der Aufsichtsbehörde „steht und fällt".[1032] Wie das Beispiel des BayLfD *Oberhauser* zeigt, ist die Gefahr einer Ernennung einer möglichst opportunen Behördenleitung nicht von der Hand zu weisen.[1033]

Nachfolgend soll jedoch nicht diese Gefahr in den Vordergrund gestellt werden, sondern die „völlige Unabhängigkeit" der Aufsichtsbehörden für die Verarbeitung bei den nicht-öffentlichen Stellen diskutiert werden.

Die unabhängige Aufsichtsbehörde kann vereinfacht gesagt „tun und lassen, was sie will". Dies wird kaum je als Problem angesehen, da die Aufsichtsbehörde „bestimmungsgemäß auf der Seite der Betroffenen, also der Schwachen und damit auf der Seite des Guten" stehe.[1034] Dies dürfte zwar für die Datenschutzaufsicht der letzten Jahrzehnte grundsätzlich zutreffen, aber gleichwohl nicht für die Zukunft gesichert sein. Dies gilt insbesondere aufgrund der Abhängigkeit der Aufsichtsbehörde von ihrer Leitung. Aufsichtsbehörden könnten aus eigenem Antrieb, nach Besetzung durch politische opportune Leitungspersonen oder aufgrund wie auch immer gearteter Interessen das Datenschutzrecht instrumentalisieren. So könnte eine im „demokratischen Sinne" schützenswerte Datenverarbeitung, etwa die Verbreitung von Informationen über Korruption in der Politik, verhindert werden oder, unter Rückgriff auf die Möglichkeit der Verhängung immenser Geldbußen, entsprechende Verarbeitung sanktioniert bzw. durch die Androhung von Geldbußen von Vornherein beschränkt werden. Nicht ausgeschlossen ist, dass Aufsichtsbehörden die ihnen zustehenden weitreichenden Befugnisse missbrauchen und beispielsweise den demokratischen Willensbildungsprozess beschränken.[1035]

Ein Hinweis auf die demokratische Legitimation der Leitung einer Aufsichtsbehörde scheint vor diesem Hintergrund zu kurz zu greifen.[1036] Daher sollte die Diskussion um die Aufsichtsbehörden als Ordnungsbehörden ohne quasi jede politisch-parlamentarische oder ministerielle Kontrolle neu aufgegriffen werden.[1037]

---

1032 So etwa v. Lewinski, Brauchen wir einen Informationsbeauftragten, in: Dix u.a., Jahrbuch Informationsfreiheit und Informationsrecht 2011, S. 265, 282.

1033 Vgl. hierzu unter Kapitel D., III., 9.

1034 Vgl. v. Lewinski, Unabhängigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, ZG 2015, S. 228, 244.

1035 Vgl. ausführlich hierzu Stentzel, Der datenschutzrechtliche Präventionsstaat?, PinG 2016, S. 46, 49.

1036 Petri/Tinnefeld, Völlige Unabhängigkeit der Datenschutzkontrolle, MMR 2010, S. 157, 161.

1037 Vgl. Masing, Herausforderungen des Datenschutzes, NJW 2012, S. 2305, 2311; Stenzel, Der datenschutzrechtliche Präventionsstaat, PinG 2016, S. 47, 49.

Dies muss für den nicht-öffentlichen Bereich unter anderem daher in ganz besonderem Maße gelten, als dass dieser noch weiter als der öffentliche Bereich durch Generalklauseln und ausfüllungsbedürftige Rechtsbegriffe geprägt und für den nationalen Gesetzgeber nur eingeschränkt die Möglichkeit der Verabschiedung weitergehender Regelungen eröffnet ist.[1038]

Eine ausführliche Behandlung dieser Frage würde über den Rahmen dieser Arbeit hinausgehen. In Bezug auf die Trennung der Aufsicht ist jedoch nach hier vertretener Auffassung festzuhalten, dass die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen dringend stärker demokratisch legitimiert werden sollte.

Durch die Trennung der Aufsicht sind diesbezüglich weitergehende Lösungsmöglichkeiten eröffnet und die demokratische Legitimation kann an die Aufsichtsbehörde für den nicht-öffentlichen Bereich anknüpfen und muss nicht „innerhalb“ der Aufsichtsbehörde trennen.

## *V. Ergebnis*

Wurde schon die Darstellung der Entwicklung der Datenschutzaufsicht in Bayern mit der Frage abgeschlossen, „was wäre, wenn das Landesamt für Datenschutzaufsicht nicht in Ansbach hätte gehalten werden sollen?“, so drängt sich nach vorstehender Prüfung auch hier eine Überlegung der Art „was wäre, wenn“ auf. Wenig überraschend lautet diese: „Wie würde die Datenschutzaufsicht in den Ländern ohne die von der Richtlinie 95/46/EG geforderte „völlige Unabhängigkeit“ der Aufsichtsbehörden und das Urteil des EuGH zur „völligen Unabhängigkeit“ aussehen?“.

Dabei ist zu berücksichtigen, dass die Anforderung der „völligen Unabhängigkeit“ zwar den finalen Anstoß gegeben haben dürfte, aber bereits zuvor die meisten Länder zu einem Zusammenführen der Aufsicht tendiert haben dürften.

Für das Zusammenführen der Aufsicht in den Ländern ausschlaggebend gewesen sein dürfte das bereits als Fazit zur Aufsicht in Bayern Festgehaltene: Eine Behörde ist „günstiger“ als zwei Behörden.

---

1038 Vgl. v. Lewinski, Unabhängigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, ZG 2015, S. 228, 242; Stentzel, Der Datenschutzrechtliche Präventionsstaat, PinG 2016, S. 45, 47, dort auch zu weiteren Unterscheidungen zwischen öffentlichem und nicht-öffentlichem Bereich.

Die Ausstattung von zwei Behörden ist insbesondere im Hinblick auf den Behördenaufbau, aber auch in Bezug auf einzelne Bereiche der Aufsicht, wie etwa dem technischen Datenschutz, eine Frage des „Haushalts". Weitere Einsparungen lassen sich jedoch nach hier vertretener Auffassung aufgrund der vorzuhaltenden „behördeninternen" Trennung in einen öffentlichen und nicht-öffentlichen Bereich und der allgemein erforderlichen Ressourcen kaum erzielen. Daher sind Einheits- und Trennungsmodell weitaus weniger „unterschiedlich", als dies noch nach deren Bezeichnung nahe liegen mag.

Gleichwohl besteht nach hier vertretener Auffassung ein ganz erheblicher Unterschied in den Auswirkungen der „völligen Unabhängigkeit" der Aufsicht über die Verarbeitung bei den öffentlichen Stellen und der „völligen Unabhängigkeit" der Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen. Für die Aufsicht über die Verarbeitung bei den nicht-öffentlichen Stellen sollten dringend Lösungen zur Verbesserung der demokratischen Legitimation, insbesondere vor dem Hintergrund der weitreichenden Befugnisse der Aufsichtsbehörden und der zwischen dem öffentlichen und nicht-öffentlichen Bereich bestehenden Unterschiede gefunden werden. Dies dürfte jedoch bei einer Trennung der Aufsicht einfacher auszugestalten sein.

Festhalten lässt sich, dass die für das Zusammenführen der Aufsicht angeführten Gründe nach hier vertretener Auffassung nicht dazu führen, dass die vereinheitlichte Aufsicht der allein „richtige Weg" ist. Von einem „Geburtsfehler" der Datenschutzaufsicht kann daher nicht gesprochen werden.[1039]

Vielmehr ist nach hier vertretener Auffassung, aufgrund der Unterschiede im öffentlichen und nicht-öffentlichen Bereich, eine Trennung der Aufsicht zu befürworten. So sollen auch nachfolgende Überlegungen zur Frage der Zentralisierung der Aufsicht im nicht-öffentlichen Bereich zeigen, dass eine Trennung der Aufsicht, gerade mit Blick auf die Zukunft der Datenschutzaufsicht, vorzugswürdig ist.

---

1039 So aber der LfD BW, vgl. 30. Tätigkeitsbericht des LfD BW, Drs. 15/955, 1. Dezember 2011, S. 11.