Ausarbeitung

Videoüberwachung von Abgeordnetenbüros

Datenschutzrechtliche Anforderungen und Verwertbarkeit im Strafverfahren

Videoüberwachung von Abgeordnetenbüros
Datenschutzrechtliche Anforderungen und Verwertbarkeit im Strafverfahren

Aktenzeichen: WD 3 - 3000 - 001/19
Abschluss der Arbeit: 28. Januar 2019
Fachbereich: WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Einleitung

Die Ausarbeitung gibt einen Überblick über die für die Videoüberwachung von Abgeordnetenbüros und ggf. angrenzenden Straßenbereichen geltenden datenschutzrechtlichen Regelungen. Ferner werden die Grundsätze zur Verwertbarkeit solcher Aufnahmen im Strafverfahren dargestellt.

2. Datenschutzrechtliche Anforderungen

Mit der Datenschutz-Grundverordnung[1] (**DSGVO**) sowie der EU-Richtlinie für die Datenverarbeitung bei Polizei und Justiz[2] (**DSRL-JI**) gelten seit 2018 neue unionsrechtliche Vorgaben für den Datenschutz. Die Regelungen der DSGVO sind für öffentliche Stellen des Bundes im parlamentarischen Bereich gemäß **§ 1 Abs. 8 (Bundesdatenschutzgesetz) BDSG** entsprechend anzuwenden.[3]

DSGVO und DSRL-JI werden von den Regelungen der Datenschutzgesetze des Bundes sowie der Länder flankiert, welche zum einen die unionsrechtlichen Vorgaben soweit erforderlich und zulässig näher konkretisieren und zum anderen datenschutzrechtliche Anforderungen für Sachverhalte formulieren, die nicht dem Unionsrecht unterfallen. Das **BDSG** beinhaltet mit § 4 eine spezifische Rechtsgrundlage für die Videobeobachtung im öffentlich zugänglichen Raum. Darüber hinaus sind die Regelungen des Beschäftigtendatenschutzes in § 26 BDSG, die Zulässigkeit der Datenverarbeitung durch öffentliche Stellen nach § 3 BDSG sowie ggf. das Vorliegen von Einwilligungen relevant. Zudem kommen in den Bereichen der Gefahrenabwehr und der Strafverfolgung auch gegenüber dem BDSG vorrangige spezialgesetzliche Rechtsgrundlagen für die dafür zuständigen öffentlichen Stellen in Betracht.

Bezüglich der Zulässigkeit der Videoüberwachung bestanden schon nach früherer Rechtslage zahlreiche Auslegungs- und Abwägungsfragen. Diese müssen nun insbesondere vor dem Hintergrund des Inkrafttretens der DSGVO und der entsprechenden Anpassung des BDSG neu reflektiert werden. Die nachfolgenden Ausführungen zeichnen den **derzeitigen Stand der (bislang nur vereinzelten) Rechtsprechung und der noch in Entwicklung befindlichen Diskussion in der Fachliteratur** nach.

2.1. Videoüberwachung öffentlich zugänglicher Bereiche nach § 4 BDSG

Konkrete Vorgaben für die Videoüberwachung öffentlich zugänglicher Räume enthält **§ 4 BDSG**, der dem früheren § 6b BDSG a. F. weitestgehend entspricht. **Abs. 1** regelt die Voraussetzungen für die Zulässigkeit der **Erhebung** personenbezogener Daten durch Videobeobachtung. Die **Speicherung und weitere Verwendung** der Daten soll als **2. Stufe** nach **Abs. 3** nur möglich sein, wenn dies zur Erreichung des damit verfolgten Zweckes erforderlich ist. In beiden Stadien ist die

---

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4. Mai 2016, S. 1.

2 Richtlinie (EU) 2016/680 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 4.5.2016,S. 89.

3 Vgl. Bundesbeauftragte für den Datenschutz und die Informationssicherheit (BfDI), Datenschutz-Grundverordnung für Abgeordnete – Handreichung für die Mitglieder des Deutschen Bundestages, Dezember 2018, S. 3.

Datenverarbeitung zudem lediglich dann zulässig, wenn keine Anhaltspunkte für das Überwiegen schutzwürdiger Belange der Betroffenen bestehen (vgl. § 4 Abs.1 und Abs. 3 S. 1 BDSG). Die **Änderung des Verarbeitungszweckes** ist gemäß § 4 Abs. 3 S. 3 BDSG nur erlaubt, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

2.1.1. Anwendungsbereich und Reichweite von § 4 BDSG

2.1.1.1. Öffentliche Stellen

§ 4 BDSG ist gemäß § 1 Abs. 1 S. 1 Nr. 1 BDSG insbesondere für öffentliche Stellen des Bundes anwendbar. **Abgeordnete** des Deutschen Bundestages sind bezüglich des gesamten Umfanges der Mandatsausübung als **öffentliche Stellen des Bundes** zu qualifizieren.[4]

2.1.1.2. Nichtöffentliche Stellen

§ 4 Abs. 1 Nr. 1 BDSG ist schon dem Wortlaut nach nur auf öffentliche Stellen im Sinne von § 1 S. 1 BDSG anwendbar. **Nichtöffentliche Stellen im Sinne von § 1 S. 2 BDSG** (beispielsweise Hauseigentümer) können sich bezüglich der Durchführung von Videoüberwachungsmaßnahmen von öffentlich zugänglichen Bereichen nach überwiegender Ansicht in der Literatur wegen des Anwendungsvorrangs der DSGVO aber auch **nicht auf § 4 Abs. 1 Nr. 2 bzw. 3 BDSG stützen**.[5] Begründet wird dies damit, dass der in diesen Fällen maßgebliche Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO bezüglich der Wahrnehmung berechtigter Interessen nichtöffentlicher Stellen **keine Öffnungsklausel für nationale Regelungen** vorsieht und die Mitgliedsstaaten auch das in der DSGVO enthaltene Normwiederholungsverbot beachten müssten.[6] Die Videoüberwachung durch nichtöffentliche Stellen richte sich mithin im öffentlichen Raum nicht nach § 4 BDSG, sondern direkt nach **Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO.** Sofern die Videoüberwachung Beschäftigte betrifft, gilt allerdings auch für nichtöffentliche Stellen § 26 BDSG (dazu näher unter 2.2., S. 11 ff.).

2.1.1.3. Offene Videoüberwachung

Der **Begriff der Videoüberwachung** ist gemäß § 4 Abs. 1 BDSG als „**Beobachtung mit optisch-elektronischen Einrichtungen“** legaldefiniert. Auf eine bestimmte Art der Speicherung oder gar eine automatisierte Weiterverarbeitung der Videoaufnahmen kommt es nach dem Wortlaut der Norm nicht an. Daher sind sowohl analoge und digitale Videoaufnahmen als auch die Überwachung

---

4 Vgl. BfDI, Datenschutz-Grundverordnung für Abgeordnete – Handreichung für die Mitglieder des Deutschen Bundestages, Dezember 2018, S. 3; Wissenschaftliche Dienste des Deutschen Bundestages, „Datenschutzbeauftragte im Abgeordnetenbüro“, WD 3 - 3000 - 387/18, S. 3.

5 Vgl. Buchner in: Kühling/Buchner, 2. Auflage 2018, BDSG § 4 Rn. 12; Frenzel in: Paal/Pauly, 2. Auflage 2018, BDSG § 4 Rn. 5; Jandt, ZRP 2018, 16 (18); Kühling NJW 2018, 1985 (1987); Lachenmann, ZD 2017, 407 (410); Schindler/Wentland, ZD-Aktuell 2018, 06057; Scholz in: Simitis, DSGVO, Anhang 1 zu Art. 6 Rn. 23 f.; Ziebarth, ZD 2017, 467 (469).

6 Vgl. Scholz in: Simitis, DSGVO, Anhang 1 zu Art. 6 Rn. 23 f. m. w. N.

mittels Videoaufnahmen in Echtzeit erfasst.[7] Die in Abs. 4 geregelte Kennzeichnungspflicht stellt klar, dass § 4 BDSG nicht zu einer verdeckten, sondern nur zu einer **offenen Videoüberwachung** ermächtigt.

2.1.1.4. Öffentlich zugängliche Räume

Von der Formulierung der **öffentlich zugänglichen Räume** in § 4 BDSG sind nicht nur überdachte, baulich abgeschlossene Zimmer bzw. Teile von Bauten, sondern nach Sinn und Zweck der Norm auch alle öffentlich zugänglichen Bereiche erfasst.[8] Diese sind unabhängig von den jeweiligen Eigentumsverhältnissen öffentlich zugänglich, wenn sie entweder dem allgemeinen Verkehr gewidmet sind oder nach dem erkennbaren Willen des Berechtigten jedenfalls von einem offenen, d.h. unbestimmten oder nur nach allgemeinen, von jedermann erfüllbaren Merkmalen bestimmten Personenkreis genutzt oder betreten werden dürfen.[9] Dies trifft nach Rechtsprechung[10] und überwiegender Meinung in der Literatur[11] jedenfalls während der Geschäftszeiten auch auf Geschäfts- und sonstige Räume zu, die generell oder auch nur nach Voranmeldung für den Publikumsverkehr geöffnet sind. Unter diesen Voraussetzungen können auch (Teile von) Abgeordnetenbüros öffentlich zugängliche Räume im Sinne von § 4 BDSG darstellen.

Umstritten ist allerdings, ob § 4 BDSG auch dann anzuwenden ist, wenn sich die Videoüberwachung nicht öffentlich zugänglicher Räume **nur teilweise auch auf öffentlich zugängliche Bereiche** (z. B. frei zugängliche Eingangsbereiche, Straßenabschnitte) erstreckt.[12] Die Frage ist in der Rechtsprechung nicht geklärt. Der Europäische Gerichtshof (EuGH) urteilte zur Anwendbarkeit der früheren Datenschutzrichtlinie (DSRL)[13] im Jahr 2014 allerdings, dass eine Videoüberwachung des Eingangsbereichs eines Einfamilienhauses durch eine nichtöffentliche Stelle, bei der teilweise auch der öffentliche Straßenraum erfasst wird, jedenfalls keinen ausschließlich persönlichen oder familiären

---

7 Vgl. BT-Drs. 14/4329 S. 38 sowie für die h. M. in der Literatur Onstein in: Auernhammer, 6. Auflage 2018, BDSG § 4 Rn. 19 m.w.N.

8 Vgl. Wolff/Brink in: BeckOK DatenschutzR, 26. Auflage Stand 1. August 2018, § 4 BDSG Rn. 8 m.w.N.

9 Vgl. Wolff/Brink in: BeckOK DatenschutzR, 26. Auflage Stand 1. August 2018, § 4 BDSG Rn. 9 m.w.N.

10 Vgl. BAG, Urteil vom 22. September 2016, Az.: 2 AZR 848/15, NZA 2017, 112 (115 Rz. 32; Verkaufsräume); OVG Lüneburg, Urteil vom 29. September 2014, Az.: 11 LC 114/13, juris (Eingangsbereich Bürogebäude); OVG Berlin-Brandenburg, Urteil vom 06. April 2017, Az.: OVG 12 B 7.16, juris (Eingangsbereich Arztpraxis) unter Bestätigung von VG Potsdam, Urteil vom 20. November 2015, Az.: 9 K 725/13, juris; VG Saarlouis, Urteil vom 29. Januar 2016, Az.: 1 K 1122/14, juris (Eingangs- und Verkaufsbereich Apotheke); VG Oldenburg, Urteil vom 12. März 2013, Az.: A 3850/12, juris (Treppenhaus Praxis- und Bürogebäude).

11 Vgl. Duhr/Naujok/Peter/Seiffert, DuD 2002, 27; Scholz in: Simitis/Scholz, 8. Auflage 2014, BDSG (a. F.) § 6b Rn. 49; Wolff/Brink in: BeckOK DatenschutzR, 26. Auflage Stand 1. August 2018, § 4 BDSG Rn. 9.

12 Für die Anwendbarkeit von § 4 BDSG n. F. Wolff/Brink in: BeckOK DatenschutzR, 26. Auflage Stand 1. August 2018, § 4 BDSG Rn. 10; zu § 6b BDSG a. F.: Klar, NJW 2015, S. 464 (465); a.A. Gola in: Gola/Schomerus, BDSG (a. F.), 12. Auflage 2015, § 6b Rn. 9.

13 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. Nr. L 281 S. 31, ber. 2017 Nr. L 40 S. 78), zuletzt geändert durch Art. 94 ÄndEU-DSGVO vom 27. April 2016 (ABl. Nr. L 119 S. 1).

Charakter im Sinne von Art. 3 Abs. 2 DSRL aufweise.[14] Ob aber in der Rechtsprechung daraus gefolgert werden wird, dass jede Mitbetroffenheit des öffentlichen Raums von einer Videoüberwachung durch öffentliche Stellen zur Anwendbarkeit von § 4 BDSG führt, bleibt abzuwarten.

2.1.1.5. Verhältnis zu § 26 BDSG (Beschäftigtendatenschutz)

§ 4 BDSG bezieht sich wie schon § 6b BDSG a. F. nur auf die offene Videoüberwachung in öffentlich zugänglichen Räumen und beinhaltet keine spezifischen Regelungen für die Überwachung Beschäftigter. **§ 26 BDSG als zentrale Norm für den Beschäftigtendatenschutz** enthält generelle Regelungen zur Erhebung und Verarbeitung von personenbezogenen Daten von Beschäftigten und schließt nach dem Wortlaut auch eine verdeckte Überwachung nicht aus. Das Bundesarbeitsgericht (BAG) hat 2018 entschieden, dass die Regelungen zur Verarbeitung von Beschäftigtendaten in § 32 BDSG a. F. sowie § 26 BDSG n. F. gegenüber § 6b BDSG a. F. bzw. § 4 BDSG n. F. **unabhängige Rechtsgrundlagen** für die Videoüberwachung von Beschäftigten darstellen.[15] Diese Bewertung teilt auch die überwiegende Literatur.[16] Mithin kann die offene Videoüberwachung von Beschäftigten in öffentlich zugänglichen Räumen sowohl nach § 4 BDSG als auch nach § 26 BDSG gerechtfertigt sein. Wie schon nach der Rechtsprechung des BAG[17] zu § 6b und 32 BDSG a. F. komme es bei Vorliegen der Voraussetzungen des § 26 BDSG für die Videoüberwachung in öffentlich zugänglichen Räumen aber nicht etwa zusätzlich auch auf die Einhaltung der Anforderungen des § 4 BDSG (insb. der Kennzeichnungspflicht nach § 4 Abs. 2 BDSG) an.[18] Soweit die Videoüberwachung **zur Aufdeckung von Straftaten von Beschäftigten** dient, wird § 26 Abs. 1 S. 2 BDSG von *Riesenhuber* sogar als gegenüber § 4 BDSG vorrangige Spezialnorm bezeichnet.[19]

2.1.1.6. Verhältnis zur Einwilligung

§ 4 BDSG schließt unter der Geltung der DSGVO die Erhebung und Verarbeitung von personenbezogenen Daten mittels Videoüberwachung im öffentlich zugänglichen Raum auf Grundlage einer **Einwilligung** von Beschäftigten nach § 26 Abs. 2 BDSG (sh. dazu unter 2.2.2., S. 15) bzw. Dritter nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO (sh. dazu unter 2.4., S. 16) nicht aus.[20] Vielfach wird die öffentliche Zugänglichkeit von Bereichen jedoch die Einholung von wirksamen Einwilligungen erschweren.

---

14 EuGH, Urteil vom 11. Dezember 2014, Az.: C-212/13 (Rynes), NJW 2015, 463 (Rn. 33).

15 Vgl. BAG, Urteil vom 23. August 2018, Az.: 2 AZR 133/18, juris Rz. 23 (zu BDSG a. F.) und Rz. 46 (zu BDSG n. F.) = NZA 2018, 1329 (1331 bzw. 1335).

16 Vgl. Riesenhuber in: BeckOK DatenschutzR, 26. Auflage Stand 1. November 2018, § 26 BDSG Rn. 147 ff; Kort, NZA 2018, 1097 (1100); Lachenmann, ZD 2017, 407 (410 f.); Thüsing/Rombey, NZA 2018, 1105.

17 Vgl. Urteil vom 22. September 2016, Az.: 2 AZR 848/15, NZA 2017, 112 (115 Rz. 34).

18 Vgl. Riesenhuber in: BeckOK DatenschutzR, 26. Auflage Stand 1. November 2018, § 26 BDSG Rn. 147.

19 Vgl. Riesenhuber, ebenda.

20 Vgl. Frenzel in: Paal/Pauly, 2. Auflage 2018, BDSG § 4 Rn. 10.

2.1.1.7. Besondere Kategorien von Daten, Art. 9 Abs. 1 DSGVO

§ 4 BDSG genügt mangels hinreichender Konkretisierung erheblicher öffentlicher Interessen wohl nicht den Anforderungen von **Art. 9 Abs. 1 lit. g DSGVO** für die Erhebung und Verarbeitung **besonderer Kategorien von Daten**.[21] Besondere Schwierigkeiten bereitet in dieser Hinsicht die Frage, ob mittels Videoaufnahmen erhobene Daten wie insbesondere **Gesichtsbilder** stets „biometrische Daten" im Sinne von Art. 4 Nr. 14, Art. 9 Abs. 1 Var. 8 DSGVO sind.[22] In der Literatur ist die Tendenz erkennbar, jedenfalls die Livebeobachtung einfacher Videoaufnahmen ohne weitere Speicherung und Auswertung nicht darunter zu fassen.[23] Nicht abschließend geklärt ist auch, ob öffentliche Stellen die Erhebung und Verarbeitung sensibler Daten im Rahmen der Videoüberwachung anstelle von § 4 BDSG auf § 22 Abs. 1 Nr. 1 BDSG stützen können.[24]

2.1.2. Rechtfertigende Zwecke der Videoüberwachung

Öffentliche Stellen können sich der Videoüberwachung gemäß § 4 Abs. 1 BDSG zur **Erfüllung ihrer Aufgaben** (Nr. 1) oder zur **Wahrnehmung des Hausrechts** (Nr. 2) bedienen, soweit dies erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die „Wahrnehmung berechtigter Interessen" (**§ 4 Abs. 1 Nr. 3 BDSG)** scheidet nach überwiegender Ansicht in der Literatur als Erlaubnisnorm für die Videoüberwachung durch öffentliche Stellen bei **europarechtskonformer Auslegung** der Norm aus.[25] Art. 6 Abs. 1 UAbs. 2 DSGVO verbietet öffentlichen Stellen ausnahmslos, sich bei der Datenverarbeitung auf die Wahrnehmung berechtigter Interessen (Art. 6 Abs. 1 UAbs. 1 lit f DSGVO) zu berufen.

2.1.2.1. Aufgabenerfüllung öffentlicher Stellen, § 4 Abs. 1 S. 1 Nr. 1 BDSG

Durch die Schaffung von **§ 4 Abs. 1 S. 1 Nr. 1 BDSG** als nationale Erlaubnisnorm für die Verarbeitung personenbezogener Daten zur **Aufgabenerfüllung öffentlicher Stellen** hat der Bundesgesetzgeber von der entsprechenden **Öffnungsklausel** des **Art. 6 Abs. 1 UAbs. 1 lit. e, Abs. 2, Abs. 3 UAbs. 1 lit. b DSGVO** Gebrauch gemacht.[26] Die Videoüberwachung sei nach § 4 Abs. 1 Nr. 1 BDSG

---

21 Vgl. den Überblick bei Reuter, ZD 2018, 564.

22 Vgl. Jandt, ZRP 2018, 16; Reuter, ZD 2018, 564; Wolff/Brink in: BeckOK DatenschutzR, 26. Auflage Stand 1. August 2018, § 4 BDSG Rn. 15 ff.

23 Vgl. Jandt, ZRP 2018, 16 (18); Wolff/Brink in: BeckOK DatenschutzR, 26. Auflage Stand 1. August 2018, § 4 BDSG Rn. 16.

24 Vgl. Reuter, ZD 2018, 564 (567).

25 Vgl. Onstein in: Auernhammer, 6. Auflage 2018, BDSG § 4 Rn. 29; Frenzel in: Paal/Pauly, 2. Auflage 2018, BDSG § 4 Rn. 13.

26 Vgl. Wolff/Brink in: BeckOK DatenschutzR, 26. Auflage Stand 1. August 2018, § 4 BDSG Rn. 18; Buchner in: Kühling/Buchner, 2. Auflage 2018, BDSG § 4 Rn. 2.

nur für vor der Datenerhebung konkret festgelegte Aufgaben der verantwortlichen Stelle zulässig.[27] Sie müsse zwar nicht für die Aufgabenerfüllung unerlässlich sein, diese aber jedenfalls unterstützen oder absichern.[28] Dies sei insbesondere bei der **Eigensicherung öffentlicher Stellen durch Zugangskontrollen oder Objektsicherungsmaßnahmen** der Fall.[29] Insofern können sich Überschneidungen zur Wahrnehmung des Hausrechts nach § 4 Abs. 1 Nr. 2 BDSG ergeben. Zur Mandatsausübung als öffentlicher Aufgabe von Abgeordneten gehört auch die Unterhaltung von Abgeordnetenbüros.

2.1.2.2. Wahrnehmung des Hausrechts, § 3 Abs. 1 S. 1 Nr. 2 BDSG

Auch die Wahrnehmung des Hausrechts durch öffentliche Stellen nach § 4 Abs. 1 S. 1 Nr. 2 BDSG stellt nach überwiegender Ansicht in der Kommentierung eine unter die Öffnungsklausel des **Art. 6 Abs. 1 UAbs. 1 lit. e, Abs. 2, Abs. 3 UAbs. 1 lit. b DSGVO** fallende Regelung dar.[30]

Inhaber des Hausrechts im Sinne von **§ 4 Abs. 1 S. 1 Nr. 2 BDSG** ist der Besitzer des öffentlich zugänglichen Raumes, der nicht notwendig auch dessen Eigentümer sein muss. Mithin obliegt Abgeordneten auch dann das Hausrecht, wenn sie Büroräume und zugehörige Bereiche lediglich anmieten oder durch die Bundestagsverwaltung zur Nutzung überlassen bekommen. Das Hausrecht ende nach der Rechtsprechung des Bundesgerichtshofes (BGH) jedoch grundsätzlich an der **Grundstücksgrenze**.[31] Die Wahrnehmung des Hausrechts könne **im Einzelfall** aber auch eine darüberhinausgehende Beobachtung des öffentlich zugänglichen Raumes rechtfertigen, wenn dies nach Abwägung aller betroffenen Interessen zur Abwehr **schwerwiegender Beeinträchtigungen**, denen nicht in anderer Weise zumutbar begegnet werden kann, erforderlich ist. Diese Schwelle sei bei Beeinträchtigungen durch Unrat nicht erreicht.[32] Der BGH nennt als Beispiele aber etwa Angriffe auf die Person des Hausrechtsinhabers oder dessen unmittelbare Wohnsphäre.[33] Denkbar erscheint dies ebenfalls in Fällen, in denen die verfassungsrechtlich durch **Art. 38 Abs. 1 S. 2 Grundgesetz** besonders geschützte **Freiheit der Mandatsausübung** durch Angriffe auf Abgeordnetenbüros gefährdet sein sollte. Eine entsprechende Rechtsprechung ist bislang nicht ersichtlich.

---

27 Vgl. Wolff/Brink in: BeckOK DatenschutzR, 26. Auflage Stand 1. August 2018, § 4 BDSG Rn. 24 sowie zur alten Rechtslage Gola/Klug/Körffer in: Gola/Schomerus, 12. Auflage 2015, BDSG (a. F.) § 6b Rn. 15; Wohlfarth RDV 2000, 186.

28 Vgl. Onstein in: Auernhammer, 6. Auflage 2018, BDSG § 4 Rn. 25; Wolff/Brink in: BeckOK DatenschutzR, 26. Auflage Stand 1. August 2018, § 4 BDSG Rn. 24 sowie zur alten Rechtslage Scholz in: Simitis/Scholz, 8. Auflage 2014, BDSG (a. F.) § 6b Rn. 71.

29 Ebenda.

30 Dafür Wolff/Brink in: BeckOK DatenschutzR, 26. Auflage Stand 1. August 2018, § 4 BDSG Rn. 28; wohl auch Frenzel in: Paal/Pauly, 2. Auflage 2018, BDSG § 4 Rn. 11; Buchner in: Kühling/Buchner, 2. Auflage 2018, BDSG § 4 Rn. 11; a. A. Nebel in: Roßnagel, Das neue Datenschutzrecht, 1. Auflage 2018, § 3 Rn. 119.

31 Vgl. BGH, Urteil vom 25. April 1995, Az.: VI ZR 272/94, NJW 1995, 1955 (1957); Urteil vom 16. März 2010, Az.: VI ZR 176/09, NJW 2010, 1533 (1534).

32 Vgl. BGH, Urteil vom 25. April 1995, Az.: VI ZR 272/94, NJW 1995, 1955 (1955, 1957).

33 Vgl. BGH, Urteil vom 25. April 1995, Az.: VI ZR 272/94, NJW 1995, 1955 (1957).

2.1.3. Erforderlichkeit

Die Videoüberwachung bzw. die Speicherung und weitere Verwendung der Daten muss zu den in § 4 Abs. 1 S. 1 Nr. 1 bzw. Nr. 2 BDSG genannten Zwecken **erforderlich** sein (§ 4 Abs. 1 bzw. Abs. 3 S. 1 BDSG), d.h. es dürfen **keine gleich geeigneten, milderen Mittel** zur Verfügung stehen. Die Prüfung hängt von den konkreten Umständen des Einzelfalls ab. In Betracht kommen insbesondere **andere Arten** der Überwachung und Sicherung von Abgeordnetenbüros bspw. durch Alarmanlagen, Zugangskontrollsysteme, Wachpersonal, Umzäunungen, Tür- und Fensterverriegelungen, bessere Beleuchtung und Schutzversiegelungen von Schaufenstern und anderen Oberflächen gegen Graffiti und Verschmutzungen. Hierbei ist auch die **wirtschaftliche Zumutbarkeit** zu berücksichtigen.[34] Aber auch eine **zeitliche oder räumliche Beschränkung** der Videoüberwachung kann ein milderes Mittel darstellen. Insbesondere ist es technisch möglich, den Bildausschnitt durch Position und Winkel der Kamera sowie durch digitales Ausblenden bestimmter Bereiche individuell auf das jeweils erforderliche Maß anzupassen.

2.1.4. Interessenabwägung

Personenbezogene Daten dürfen gemäß § 4 Abs.1 BDSG durch Videoüberwachung nur erhoben und als weitere Stufe gemäß § 4 Abs. 3 S. 1 BDSG gespeichert bzw. weiterverwendet werden, wenn **keine Anhaltspunkte für das Überwiegen schutzwürdiger Belange der Betroffenen bestehen** bzw. solche jedenfalls nicht ausgeräumt werden können.[35] Maßgeblich für Art und Intensität von Eingriffen in die Interessen von durch die Videoüberwachung Betroffenen sind insbesondere

- die Anzahl der betroffenen Personen und ob diese selbst Anlass für die Videoüberwachung gegeben haben bzw. ob auch unbeteiligte Dritte miterfasst werden,
- die Identifizierbarkeit der Personen unter Berücksichtigung der Auflösung der Kameraaufnahmen sowie etwaiger Möglichkeiten zur Vergrößerung von Bildausschnitten und der biometrischen[36] Gesichtserkennung,
- die zeitliche Ausgestaltung und Dauer der Videoüberwachung,
- Art und Größe des beobachteten Bereichs sowie das Vorhandensein von Ausweichmöglichkeiten.

Je intensiver die möglichen Eingriffe in die Interessen Betroffener sind, desto größer werden die Anforderungen an das Gewicht des mit der Videoüberwachung verfolgten Zweckes. Im Rahmen der Abwägung ist auch zu berücksichtigen, ob und in welcher Weise ggf. die **Freiheit der Mandatsausübung** etwa durch zu befürchtende schwerwiegende Angriffe auf das Abgeordnetenbüro

---

34 Vgl. Onstein in: Auernhammer, 6. Auflage 2018, BDSG § 4 Rn. 29; Frenzel in: Paal/Pauly, 2. Auflage 2018, BDSG § 4 Rn. 35.

35 Vgl. Wolff/Brink in: BeckOK DatenschutzR, 26. Auflage Stand 1. August 2018, § 4 BDSG Rn. 34 mit Verweis auf OVG Nordrhein-Westfalen, Urteil vom 8. Mai 2009, Az.: 16 A 3375/07, juris zu § 6b BDSG a. F.; dieser Rspr. zustimmend Gola in: Gola/Schomerus, 12. Auflage 2015, BDSG (a. F.), § 6b Rn. 19.

36 Ausführliche datenschutzrechtliche Bewertung bei Jandt, ZRP 2018, 16 und Reuter, ZD 2018, 564.

betroffen ist. Sofern sich die Videoüberwachung auch auf Beschäftigte bezieht, sind zudem die zum **Beschäftigtendatenschutz** durch die Rechtsprechung entwickelten Grundsätze zu berücksichtigen, soweit diese auch nach Inkrafttreten der DSGVO fortgelten (sh. dazu unter 2.2., S. 11 ff.).

2.1.5. Kennzeichnungs-, Informations- und Löschpflichten sowie Datenschutzfolgeabschätzung

Der **Umstand der Beobachtung** und der **Name** und die **Kontaktdaten des Verantwortlichen** sind durch geeignete Maßnahmen (insb. durch eine gut sichtbare Beschilderung) **zum frühestmöglichen Zeitpunkt erkennbar zu machen**, § 4 Abs. 2 BDSG.

Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, so besteht gemäß § 4 Abs. 4 Satz 1 BDSG die **Pflicht zur Information der betroffenen Person** über die Verarbeitung nach Art. 13 und 14 der DSGVO, sofern keine abweichenden Regelungen des gemäß § 4 Abs. 4 Satz 2 BDSG entsprechend anzuwendenden § 32 BDSG eingreifen, die aber bezüglich der Überwachung von Abgeordnetenbüros durch Abgeordnete regelmäßig nicht vorliegen.

Die Daten sind **unverzüglich zu löschen**, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen (§ 4 Abs. 5 BDSG).

Gemäß Art. 35 Abs. 3 lit. c DSGVO sowie Erwägungsgrund 91 zur DSGVO erfordert eine systematische umfangreiche Videoüberwachung öffentlich zugänglicher Bereiche zudem eine **Datenschutzfolgeabschätzung**.[37]

2.2. Videoüberwachung Beschäftigter nach § 26 BDSG

§ 26 BDSG regelt die Zulässigkeit der Verarbeitung von **Beschäftigtendaten**. Anders als § 4 BDSG erfasst § 26 BDSG **auch** eine Datenerhebung mittels Videoüberwachung **in nicht öffentlich zugänglichen Räumen**.

2.2.1. § 26 Abs. 1 BDSG

§ 26 Abs. 1 enthält gesetzliche Erlaubnistatbestände für die Verarbeitung von Beschäftigtendaten. Die Informations- und Mitteilungspflichten von Arbeitgebern richten sich auch bei der Datenverarbeitung nach § 26 Abs. 1 BDSG nach den allgemeinen Bestimmungen in Art. 12 ff. DSGVO und die Betroffenenrechte nach Art. 15 f. DSGVO.

Inhaltlich hat der Gesetzgeber in § 26 Abs. 1 BDSG die Regelungen des § 32 BDSG a. F. übernommen und wollte dadurch auch die dazu ergangene Rechtsprechung absichern.[38]

---

37 Vgl. auch Onstein in: Auernhammer, 6. Auflage 2018, § 4 BDSG Rn. 4.

38 Vgl. BT-Drs. 16/13657, 35.

2.2.1.1. Aufdecken von Straftaten, § 26 Abs. 1 S. 2 BDSG

Erfolgt die Videoüberwachung von Beschäftigten zur **Aufdeckung von Straftaten,** kommt **§ 26 Abs. 1 S. 2 BDSG** als Rechtsgrundlage in Betracht. Danach ist die Verarbeitung von Beschäftigtendaten zulässig, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die beschäftigte Person eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Bei **§ 32 Abs. 1 S. 2 BDSG a. F.** ließ das BAG schon einen einfachen Anfangsverdacht einer Straftat genügen. Dieser musste jedoch auf konkreten Tatsachen basieren und sich gegen einen abgrenzbaren Kreis von Beschäftigten richten.[39] Diese Anforderungen gelten nach der Literatur auch für die insoweit vergleichbare neue Regelung in § 26 Abs. 1 S. 2 BDSG fort.

2.2.1.2. Aufdecken schwerwiegender Pflichtverletzungen, § 26 Abs. 1 S. 1 BDSG

Die Videoüberwachung zur Aufdeckung **sonstiger schwerwiegender Pflichtverstöße** konnte nach der Rechtsprechung des BAG mangels entgegenstehender Sperrwirkung des § 32 Abs. 1 S. 2 BDSG auf den – inhaltlich mit **§ 26 Abs. 1 S. 1 BDSG n. F.** übereinstimmenden – § 32 Abs. 1 S. 1 BDSG a. F. gestützt werden, wenn dies für die **Durchführung oder Beendigung des Arbeitsverhältnisses** erforderlich ist.[40] Zur Durchführung des Arbeitsverhältnisses gehöre auch die Kontrolle, ob Arbeitnehmer ihren Pflichten nachkommen. Gleichsam könne die Aufdeckung tatsächlicher Pflichtverletzungen als Kündigungsvorbereitung zur Beendigung des Beschäftigungsverhältnisses erforderlich sein.[41] Der Arbeitgeber dürfe bei Vorliegen konkreter Anhaltspunkte für eine schwerwiegende Pflichtverletzung „grundsätzlich alle Daten speichern und verwenden, die er benötigt, um die ihm obliegende Darlegungs- und Beweislast in einem potenziellen Rechtsstreit um die Wirksamkeit einer Kündigung und/oder das Bestehen von Schadensersatzansprüchen zu erfüllen“[42]. Dagegen sei eine verdeckte Ermittlung „ins Blaue hinein“, ob ein Arbeitnehmer sich pflichtwidrig verhält, stets unzulässig.[43]

2.2.1.3. Verhältnismäßigkeit bei § 26 Abs. 1 S.1 und S. 2 BDSG

Die Datenverarbeitung muss sowohl zur Aufdeckung von Straftaten gemäß § 26 Abs. 1 S. 2 BDSG als auch von schwerwiegenden Pflichtverletzungen gemäß § 26 Abs. 1 S. 1 BDSG erforderlich sein. Dabei ist nach der Rechtsprechung des BAG zu § 32 BDSG a. F. eine **vollumfängliche Verhältnismäßigkeitsprüfung** durchzuführen.[44] Art, Dauer und Intensität der Videoüberwachung muss also

---

39 Vgl. BAG, Urteil vom 20. Oktober 2016, Az.: 2 AZR 395/15 = NZA 2017, 443.

40 Vgl. BAG, Urteil vom 29. Juni 2017, Az.: 2 AZR 597/16, NZA 2017, 1179 (1182 Rz. 28).

41 Vgl. BAG, Urteil vom 29. Juni 2017, Az.: 2 AZR 597/16, NZA 2017, 1179 (1181 Rz. 26).

42 BAG, Urteil vom 29. Juni 2017, Az.: 2 AZR 597/16, NZA 2017, 1179 (1181 Rz. 22).

43 Vgl. BAG, Urteil vom 29. Juni 2017, Az.: 2 AZR 597/16, NZA 2017, 1179 (1183 Rz. 32); Urteil vom 27. Juli 2017, Az.: 2 AZR 681/16, NZA 2017, 1327 (1330 Rz. 30).

44 Vgl. BAG, Urteil vom 23. August 2018, Az.: 2 AZR 133/18, NZA 2018, 1329 (1332 Rz. 24).

zur Zweckerreichung geeignet sein und das mildeste der gleich geeigneten Mittel bilden. Darüber hinaus ist die Angemessenheit der Datenverarbeitung unter Berücksichtigung der Interessen der Betroffenen festzustellen.

Das Kriterium der Erforderlichkeit bezieht sich nicht nur auf die Erhebung, sondern auch auf die **Speicherung** von Videoaufnahmen. Der Arbeitgeber sei in dem von gegenseitigem Vertrauen geprägten Beschäftigungsverhältnis nicht gehalten, Videoaufnahmen laufend auf Pflichtverletzungen zu überprüfen.[45] Die Speicherung und anlassbezogene, stichprobenartige Durchsicht von Daten kann gegenüber der ständigen Überprüfung ein milderes Mittel darstellen, soweit eine missbräuchliche Verwendung durch den Arbeitgeber oder Dritte ausgeschlossen ist.[46] Das BAG sah die Speicherung unter diesen Voraussetzungen auch gegenüber miterfassten Dritten als erlaubt an.[47]

Eine Videoüberwachung „von Personen, die sich in (…) einem gegen Einblick besonders geschützten Bereich befinden", also etwa in Umkleide-, Dusch- oder Sanitärräumen, ist bereits gemäß **§ 201a Strafgesetzbuch** verboten. „Das allgemeine Persönlichkeitsrecht gewährleistet [aber] nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des **Rechts auf informationelle Selbstbestimmung** auch den informationellen Schutzinteressen desjenigen Rechnung, der sich in die **(Betriebs-)Öffentlichkeit** begibt."[48]

So ist eine Datenerhebung und -verarbeitung nach Ansicht des BAG auch unter Berücksichtigung des Rechts des Arbeitgebers zur Leistungskontrolle unzulässig, wenn diese lücken- und anlasslos erfolgt und mithin einen **ständigen Überwachungs- und daran anknüpfenden Anpassungs- und Leistungsdruck** begründet.[49] Dies sei auch nach einhelliger Auffassung in der Literatur sowohl bei einer **offenen** als auch einer **heimlichen Totalüberwachung** von Beschäftigten insbesondere mittels Videoüberwachung der Fall.[50] Wegen der hohen Eingriffsintensität und der Unveräußerlichkeit des Kernbereichs des allgemeinen Persönlichkeitsrechts sei eine Totalüberwachung nach Ansicht von *Kort* auch nicht durch eine Einwilligung der Betroffenen zu rechtfertigen.[51]

Ferner ist hinsichtlich der Frage der Zulässigkeit **verdeckter Überwachungsmaßnahmen** unter der Geltung der DSGVO grundsätzlich fraglich, ob § 26 BDSG eine wirksame Ausnahme von der vorherigen Erfüllung der Informationspflichten nach Art. 13, 14 DSGVO sowie dem **Transparenzgebot**

45 Vgl. BAG, Urteil vom 23. August 2018, Az.: 2 AZR 133/18, NZA 2018, 1329 (1332 Rz. 29 ff.).

46 Vgl. BAG, Urteil vom 23. August 2018, Az.: 2 AZR 133/18, NZA 2018, 1329 (1332 Rz. 29 ff.).

47 Vgl. BAG, Urteil vom 23. August 2018, Az.: 2 AZR 133/18, NZA 2018, 1329 (1333 Rz. 32); zustimmend Riesenhuber in: BeckOK DatenschutzR, 26. Auflage Stand 1. November 2018, § 26 BDSG Rn. 153a.

48 Vgl. BAG, Urteil vom 27. Juli 2017, Az.: 2 AZR 681/16, NZA 2017, 1327 (1329 Rz. 25 m. w. N.).

49 St. Rspr. vgl. zuletzt BAG, Urteil vom 27. Juli 2017, Az.: 2 AZR 681/16, NZA 2017, 1327 (1334 Rz. 43 m. w. N.) sowie Urteil vom 27. März 2003, Az.: 2 AZR 51/02, juris (Rz. 25 m. w. N.).

50 Vgl. Kort, RdA 2018, 242 (244 m. w. N. zu § 32 BDSG a. F. in Fn. 33 und 34).

51 Vgl. Kort, RdA 2018, 242 (245).

des Art. 5 Abs. 1a DSGVO darstellt, auf dessen Wahrung in Art. 88 Abs. 2 DSGVO für den Beschäftigtendatenschutz besonders hingewiesen wird.[52] Sofern die in Art. 88 Abs. 1 DSGVO enthaltene Öffnungsklausel überhaupt die Schaffung von Ausnahmen vom Transparenzgebot durch den nationalen Gesetzgeber rechtfertigt, sind zusätzlich die Anforderungen von Art. 23 DSGVO zu wahren. Erwägungsgrund 41 zur DSGVO konkretisiert diese dahingehend, dass eine beschränkende Regelung klar und präzise gefasst sein soll. § 26 BDSG enthält jedoch keine konkreten Vorgaben für die Zulässigkeit verdeckter (Video-)überwachungsmaßnahmen und der damit verbundenen Ausnahme von der Pflicht, Betroffene vorab zu informieren. In der Literatur wird auch eine analoge Anwendung von Art. 14 Abs. 5 lit. b DSGVO diskutiert, der für die Datenerhebung bei Dritten eine Ausnahme von der vorherigen Erfüllung der Informationspflichten zulässt, wenn diese die Verwirklichung der Ziele dieser Verarbeitung voraussichtlich unmöglich macht oder ernsthaft beeinträchtigt.[53]

Ferner ist auch die neuere Rechtsprechung des **Europäischen Gerichtshofes für Menschenrechte (EGMR**) zu berücksichtigen.[54] Dieser hat in einigen jüngeren Entscheidungen mit Blick auf die Wahrung des in Art. 8 EMRK verbürgten Rechts auf Schutz des Privatlebens insbesondere das Erfordernis der vorherigen Information der Beschäftigten vor Überwachung ihrer Tätigkeit betont.[55] In der Literatur wird daraus vielfach gefolgert, dass verdeckte Überwachungsmaßnahmen jedenfalls nicht ohne konkreten Anlass erfolgen dürfen.[56]

2.2.2. Einwilligungen Beschäftigter, § 26 Abs. 2, Abs. 3 S. 2 BDSG

§ 26 BDSG schließt dem Wortlaut nach eine Videoüberwachung von Beschäftigten auf Grundlage von Einwilligungen nicht grundsätzlich aus. Allerdings sind die **Anforderungen an deren Wirksamkeit** gemäß **§ 26 Abs. 2 BDSG** deutlich erhöht: Sie bedarf gemäß S. 3 der **Schriftform**, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Für die Beurteilung der Freiwilligkeit der Einwilligung ist gemäß § 26 Abs. 2 S. 1 BDSG insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. In einer Entscheidung aus dem Jahr 2018 zum BDSG a. F. hatte das BAG erneut bekräftigt, dass das **bloße Unterlassen eines Protestes** eines Beschäftigten gegenüber einer ihm mitgeteilten Maßnahme nicht als Einverständniserklärung in die Informationserhebung gewertet werden kann.[57] Auch das bloße Betreten eines videoüberwachten

---

52 Vgl. dazu Byers, NZA 2017, 1086; Maschmann, NZA-Beilage 2018, 115 (118); derselbe in: Kühling/Buchner, DSGVO, 2. Auflage 2018, Art. 88 Rn. 47.

53 Vgl. Byers NZA 2017, 1086 (1090).

54 Vgl. den Überblick über die Rspr. des EuGH sowie die alte und neue deutsche Rechtslage bei Maschmann, NZA-Beilage 2018, 115 (121).

55 Vgl. zur Videoüberwachung: EGMR, Urteil vom 9. Januar 2018, Az.: 1874/13 u. 8567/13 (López Ribalda/Spain), juris; zur PC-Überwachung: Urteil vom 5. September 2017, Az.: 61496/08 (Bărbulescu/Rumänien), juris = EuZW 2018, 169 sowie Urteil vom 22. Februar 2018, Az.: 588/13 (Libert/France), juris = ZD 2018, 263.

56 Anmerkung von Hembach zu EGMR, Urteil vom 22. Februar 2018, Az.: 588/13 (Libert/France), ZD 2018, 263 (266); Anmerkung von Sörup zu EGMR, Urteil vom 5. September 2017, Az.: 61496/08 (Bărbulescu/Rumänien), ZD 2017, 573 (574); wohl für eine vollständige Unzulässigkeit verdeckter Maßnahmen Matschmann, NZA-Beilage 2018, 115 (121).

57 Vgl. BAG, Urteil vom 27. Juli 2017, Az.: 2 AZR 681/16, NZA 2017, 1327 (1329 Rz. 20).

Bereiches kann wohl grundsätzlich nicht als Einwilligung gewertet werden (vgl. dazu die Ausführungen unter 2.4, S. 16).

Gemäß § 26 Abs. 3 S. 2 BDSG kann die Einwilligung auch die Verarbeitung von **sensiblen Beschäftigtendaten** durch den Arbeitgeber rechtfertigen, soweit sie sich **ausdrücklich** auch auf die in Art. 9 Abs. 1 DSGVO bezeichneten besonderen Kategorien von Daten bezieht.

Der Arbeitgeber hat die beschäftigte Person zudem über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Abs. 3 DSGVO in Textform aufzuklären, § 26 Abs. 2 S. 4 BDSG. Zusätzlich gelten die allgemeinen Informations- und Mitteilungspflichten für verantwortliche Stellen nach Art. 12 ff. DSGVO sowie die Betroffenenrechte nach Art. 15 f. DSGVO.

2.3. Videoüberwachung nicht öffentlich zugänglicher Bereiche durch öffentliche Stellen nach § 3 BDSG

Die Verarbeitung personenbezogener Daten Dritter mittels Videoüberwachung in nicht öffentlich zugänglichen Bereichen ist im BDSG nicht näher geregelt.[58] Nach § 3 Var. 1 BDSG ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen aber grundsätzlich zulässig, wenn dies zur Erfüllung ihrer öffentlichen Aufgaben erforderlich ist. Nach Ansicht der BfDI[59] erfasst die Norm grundsätzlich auch die Datenverarbeitung durch Abgeordnete, sofern diese zur Mandatsausübung erforderlich ist. Allerdings sind jeweils vorrangige Spezialregelungen zu beachten. Bei der Videoüberwachung von Abgeordnetenbüros dürften praktisch in der Regel entweder öffentlich zugängliche Räume oder aber Beschäftigte betroffen sein. Im ersten Fall bildet § 4 BDSG im letzteren Fall § 26 BDSG eine gegenüber § 3 BDSG speziellere Rechtsgrundlage.

2.4. Videoüberwachung auf Grundlage von Einwilligungen Dritter

Weder § 3 noch § 4 bzw. 26 BDSG schließen ihrem Wortlaut nach eine Videoüberwachung Dritter auf Grundlage von Einwilligungen aus. Nach Art. 6 Abs. 1 UAbs. lit. a DSGVO muss diese sich auf einen oder mehrere bestimmte Zwecke beziehen und freiwillig erteilt werden. Eine Einwilligung ist nach Art. 4 Nr. 11 DSGVO „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“. Nach Ansicht der Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) sei „insbesondere […] das [bloße] Betreten des gekennzeichneten Erfassungsbereichs einer Videokamera nicht als ‚eindeutig bestätigende Handlung‘ und auch nicht als informierte Einwilligung i. S. d. Art. 4 Nr. 11 DSGVO zu werten“[60].

Weitere Anforderungen an die Wirksamkeit von Einwilligungen der verantwortlichen Stelle sind in Art. 7 DSGVO geregelt. Einwilligungen sind zudem grundsätzlich jederzeit mit Wirkung für

---

58 Vgl. DSK, Kurpapier Nr. 15, Videoüberwachung nach der Datenschutz-Grundverordnung, S. 1.

59 Vgl. BfDI, Datenschutz-Grundverordnung für Abgeordnete – Handreichung für die Mitglieder des Deutschen Bundestages, Dezember 2018, S. 3.

60 DSK, Kurzpapier Nr. 15, Videoüberwachung nach der Datenschutz-Grundverordnung, S. 1.

die Zukunft frei widerruflich (Art. 7 Abs. 3 S. 1 und S. 2 DSGVO). Hierüber ist die betroffene Person vor Abgabe der Einwilligung in Kenntnis zu setzen, Art. 7 Abs. 3 S. 1 DSGVO.

Eine Einwilligung in die Verarbeitung von **sensiblen Daten** muss gemäß Art. 9 Abs. 2 lit. a DSGVO **ausdrücklich** erteilt werden.

Mangels Eingreifens von im BDSG geregelter Ausnahmen obliegt Abgeordneten als verantwortlichen öffentlichen Stellen die Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO gegenüber den von der Videoüberwachung betroffenen Dritten. Diesen stehen auch das Auskunftsrecht nach Art. 15 DSGVO sowie das Recht auf Berichtigung (Art. 16 DSGVO) und Löschung (Art. 17 DSGVO) zu.

2.5. Videoüberwachung zum Zwecke der Gefahrenabwehr und Strafverfolgung

Maßnahmen zur Gefahrenabwehr und Strafverfolgung fallen gemäß Art. 2 Abs. 2 lit. d DSGVO und Art. 1 Abs. 1 DSRL grundsätzlich nicht in den Anwendungsbereich der DSGVO sondern der DSRL, wenngleich die Einzelheiten der Abgrenzung insbesondere im Bereich der Gefahrenabwehr umstritten sind.[61]

Die Zulässigkeit der Videoüberwachung durch die zuständigen **Ermittlungsbehörden zum Zwecke der Strafverfolgung** richtet sich nicht nach § 4 BDSG, sondern nach den entsprechenden **bereichsspezifischen Vorschriften** insbesondere der Strafprozessordnung (StPO)**.**

Nicht allgemein zugängliche Bereiche von Arbeits- und Geschäftsräumen und mithin auch von Abgeordnetenbüros fallen nach der Rechtsprechung des Bundesverfassungsgerichts unter den in Art. 13 GG verbürgten Schutz der „räumlichen Privatsphäre“.[62] Mithin ist der Begriff der „Wohnung“ nicht nur im Rahmen von Art. 13 GG, sondern auch im Rahmen von **§ 100c StPO** entsprechend weit auszulegen.[63] Aus dem Umstand, dass § 100c StPO lediglich eine akustische Überwachung der vom Wohnungsbegriff umfassten Räume vorsieht, wird gefolgert, dass deren **Überwachung durch Ermittlungsbehörden mittels Videotechnik unzulässig** ist.[64]

Die Zulässigkeit Ermittlungsmaßnahmen in Gestalt von Bildaufnahmen **außerhalb von nach Art. 13 GG geschützten Räumen** richtet sich nach **§ 100h Abs. 1 Nr. 1 StPO**.

Ermittlungsmaßnahmen gegen Abgeordnete durch die voraussichtlich Erkenntnisse gewonnen werden würden, über die diese das Zeugnis verweigern dürften sind gemäß **§ 160a StPO** jedoch generell unzulässig. Insoweit besteht ein **absolutes Beweiserhebungsverbot.** Ermittlungshandlungen,

---

61 Vgl. dazu Wolff in: BeckOK DatenschutzR BDSG § 45 Rn. 17; Schwichtenberg in: Kühling/Buchner, BDSG, 2. Auflage 2018, § 45 Rn. 2.

62 Vgl. BVerfG, Beschluss vom 13. Oktober 1971, Az.: 1 BvR 280/66, BVerfGE 32, 54 ff. = NJW 1971, 2299.

63 Vgl. Günther in: MüKoStPO, 1. Auflage 2014, StPO § 100c Rn. 11.

64 Vgl. Günther in: MüKoStPO, 1. Auflage 2014, StPO § 100c Rn. 11 f.; Singelnstein, NStZ 2014, 305 (309); Schmitt in: Meyer/Goßner, StPO, 81. Auflage 2018, § 100h Rn. 1.

die sich gegen andere Personen richten sind aber grundsätzlich selbst dann zulässig, wenn nicht ausgeschlossen werden kann, dass dadurch nach § 160a StPO geschützte Informationen von Abgeordneten offengelegt werden.[65]

Wird die Videoüberwachung durch Landespolizeibehörden zum Zwecke der Gefahrenabwehr durchgeführt, sind die jeweiligen **Landespolizei- und -datenschutzgesetze** maßgeblich.

3. Verwertbarkeit im Strafverfahren

Die DSGVO ist gemäß Art. 2 Abs. 2 lit. d nicht auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Ermittlung, Aufdeckung und Verfolgung von Straftaten anwendbar. Auch die jedenfalls für öffentliche Stellen insoweit grundsätzlich maßgebliche DSRL-JI enthält keine Bestimmungen zu Beweisverwertungsverboten. Ob solche bestehen richtet sich daher nach den nationalen Bestimmungen.

3.1. Allgemeine Grundsätze

Rechtmäßig erhobene Informationen können regelmäßig auch als Beweismittel im Rahmen von Strafverfahren verwertet werden. Beweisverwertungsverbote können aber ausnahmsweise bestehen, sofern dies gesetzlich angeordnet ist oder die Verwertung als solche Grundrechte verletzt. Sofern nicht gesetzlich anders angeordnet, können grundsätzlich **auch rechtswidrig erhobene Informationen** im Strafverfahren verwertet werden. Denn nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) gehört zu den wesentlichen Prinzipien des deutschen Strafverfahrensrechts, „dass das Gericht die Wahrheit zu erforschen hat und dazu die Beweisaufnahme von Amts wegen auf alle Tatsachen und Beweismittel zu erstrecken hat, die von Bedeutung sind.“[66] Insbesondere folgt nach der durch das Bundesverfassungsgericht (BVerfG) bestätigten ständigen Rechtsprechung des BGH „kein Rechtssatz des Inhalts, dass im Fall einer rechtsfehlerhaften Beweiserhebung die Verwertung der gewonnenen Beweise stets unzulässig wäre“[67]. Die Strafprozessordnung ist jedoch nicht auf die Wahrheitserforschung um jeden Preis gerichtet. Der **Verstoß gegen ein Beweiserhebungsverbot** führt **ausnahmsweise** dann zu einem **Beweisverwertungsverbot**, wenn dies entweder gesetzlich angeordnet ist oder „aus übergeordneten wichtigen Gründen im Einzelfall“ unter Abwägung der widerstreitenden Interessen des Betroffenen einerseits sowie des Interesses der Allgemeinheit an einer wirksamen Strafverfolgung andererseits geboten ist.[68] Dabei spielen Art und

65 Vgl. BT-Drs. 16/5846 S. 35; Sackreuther in: BeckOK StPO, 31. Auflage Stand 15. Oktober 2018, StPO § 160a Rn. 5.

66 Vgl. BVerfG, Kammerbeschluss vom 20. Mai 2011, Az.: 2 BvR 2072/10, NJW 2011, 2783 (2784 Rn. 13) unter Bezug auf BGH, Urteil vom 11. November 1998, Az.: 3 StR 181/98, BGHSt 44, 243, 249; Urteil vom 18. April 2007, Az.: 5 StR 546/06, BGHSt 51, 285 Rn. 20.

67 Vgl. BVerfG, Kammerbeschluss vom 20. Mai 2011, Az.: 2 BvR 2072/10, NJW 2011, 2783 (2784 Rn. 12).

68 Vgl. BVerfG, Kammerbeschluss vom 20. Mai 2011, Az.: 2 BvR 2072/10, NJW 2011, 2783 (2784 Rn. 13).

Gewicht des Verstoßes gegen das Beweiserhebungsverbot sowie Art und Schwere der Beeinträchtigung des Betroffenen eine maßgebliche Rolle.[69] So hat das BVerfG bei „schwerwiegenden, bewussten oder willkürlichen Verfahrensverstößen, bei denen die grundrechtlichen Sicherungen planmäßig oder systematisch außer Acht gelassen worden sind“ und in Fällen, in denen der absolute Kernbereich privater Lebensgestaltung berührt ist, Beweisverwertungsverbote angenommen.[70]

3.2. Videoüberwachung von Abgeordnetenbüros durch Strafverfolgungsbehörden

§ 160a Abs. 1 S. 2 StPO normiert ausdrücklich ein **absolutes Beweisverwertungsverbot** bezüglich Informationen, über die Abgeordnete das Zeugnis verweigern dürften. Dieses besteht gemäß **§ 160a Abs. 1 S. 5 StPO** auch dann, wenn sich die Videoüberwachung nicht gegen den Abgeordneten selbst, sondern gegen Dritte richtet.

Im Hinblick auf sonstige Informationen ist zu beachten, dass die Videoüberwachung **nicht öffentlich zugänglicher Bereiche von Arbeits- und Geschäftsräumen** durch Strafverfolgungsbehörden unzulässig ist (siehe oben bei 2.5). Die Frage, ob und ggf. in welchem Umfang gleichwohl gewonnenes Bildmaterial aus nicht öffentlich zugänglichen Arbeits- und Geschäftsräumen verwertet werden darf, richtet sich somit nach den bei 3.1. dargestellten Grundsätzen. Die Annahme eines Verwertungsverbots wäre hiernach also etwa dann anzunehmen, wenn der Kernbereich privater Lebensgestaltung betroffen oder von einem schwerwiegenden, bewussten oder willkürlichen Verfahrensverstoß bzw. einer planmäßigen oder systematischen Außerachtlassung grundrechtlicher Sicherungen auszugehen ist.

3.3. Videoüberwachung durch sonstige öffentliche bzw. nichtöffentliche Stellen

Die Frage wie sich datenschutzrechtliche Verstöße bei der Beweiserhebung auf die gerichtliche Verwertbarkeit von Informationen im Straf- und Zivilverfahren auswirken, wird in der rechtswissenschaftlichen Literatur seit langem diskutiert.[71] Auch wenn Bestimmungen des Datenschutzes gerade dem Schutz der informationellen Selbstbestimmung dienen, ist in der **Rechtsprechung** bislang **kein allgemeiner Grundsatz** anerkannt worden, **wonach eine datenschutzrechtswidrige Beweiserhebung zwingend zu einem Beweisverwertungsverbot im Strafverfahren führen würde**. So entschied das **OLG Hamburg** in einem Beschluss aus dem Jahr 2017, der einen Verstoß gegen die Hinweispflicht nach § 6b Abs. 2 BDSG a. F. betraf: „Ein Verstoß gegen ein Beweiserhebungsverbot hat […] - auch im Falle personenbezogener Informationen [...] - nicht zwingend ein prozessuales Beweisverwertungsverbot zur Folge.“[72] Auch Daten, die durch private unter Verstoß

---

69 St. Rspr. des BGH, vgl. BGH Beschluss vom 17. März 1971, Az.: 3 StR 189/70, BGHSt 24, 125, 130; Beschluss vom 27. Februar 1992, Az.: 5 StR 190/91, BGHSt 38, 214, 219 f.; Beschluss vom 20. Mai 2015, Az.: 4 StR 555/14, NJW 2015, 2594, 2596; Urteil vom 17. Februar 2016, Az.: 2 StR 25/15, NStZ 2016, 551, 552.

70 Vgl. BVerfG, Kammerbeschluss vom 20. Mai 2011, Az.: 2 BvR 2072/10, NJW 2011, 2783 (2784 Rn. 14).

71 Vgl. die ausführliche Darstellung bei Betz, RdA 2018, 100.

72 Vgl. OLG Hamburg, Beschluss vom 27. Juni 2017, Az.: 1 Rev 12/17, juris Rz. 6 m. zustimmender Anmerkung von Popp, jurisPR-ITR 20/2017 Anm. 2; dagegen kritisch bzgl. Schutzrichtung, Eingriffsintensität und Abwägung des OLG Gubitz in ZD 2017, 727; gegen ein allg. Beweisverwertungsverbot bei Datenschutzverstößen wohl auch Kort, RdA 2018, 24 (33); Riesenhuber in: BeckOK DatenschutzR, 26. Auflage Stand 1. Mai 2018, § 32 BDSG (a. F.) Rn. 166.

gegen datenschutzrechtliche Bestimmungen erhoben wurden, „sind – verfassungsrechtlich unbedenklich – grundsätzlich verwertbar und unterliegen nicht zwingend per se einem Beweisverwertungsverbot“[73].

Das **BDSG** enthält auch **keine gesetzlich angeordneten Beweisverwertungsverbote** für mittels Videoüberwachung gewonnene Daten. § 4 Abs. 3 S. 3 BDSG beschränkt zwar die Änderung des Zweckes der Verarbeitung von in öffentlich zugänglichen Räumen durch Videobeobachtung erhobenen Daten, beinhaltet aber weder bei rechtmäßiger noch bei rechtswidriger Erhebung ein gesetzliches Beweisverwertungsverbot für das Straf- bzw. Ordnungswidrigkeitenverfahren. Das **OLG Stuttgart** hat diesbezüglich 2016 zum früheren § 6b Abs. 3 S. 2 BDSG a. F. (2003) ausgeführt: „Weder der Gesetzeswortlaut noch die Gesetzgebungsmaterialien geben Hinweise, dass der Gesetzgeber ein solches Beweisverwertungsverbot regeln wollte. Ein solches kennt das deutsche Strafprozessrecht […] ohnehin nur in Ausnahmefällen. In § 6b Abs. 3 Satz 2 BDSG ging es dem Gesetzgeber um eine Ausnahme von der strikten Zweckbindung des § 6b Absatz 3 Satz 1 BDSG für die durch Videoüberwachung gewonnenen Daten (BT-Drs. 14/5793, S. 62). Zur weitergehenden Frage eines Beweisverwertungsverbots im Straf- oder Bußgeldverfahren äußerte er sich jedoch gerade nicht, so dass auf die allgemeinen Grundsätze zurückzugreifen ist.“ [74] Die Regelung wurde in § 4 Abs. 3 S. 2 BDSG unverändert fortgeschrieben.

Im Ergebnis gelten daher auch bei Verstößen gegen datenschutzrechtliche Bestimmungen die allgemeinen Grundsätze für die Beweisverwertung (sh. dazu unter 3.1., S. 17 f.). Bei rechtswidrig durch Private erhobenen Informationen ist zu berücksichtigen, dass die Verwertung im Strafverfahren einen eigenständigen staatlichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellen kann.

***

73 OLG Stuttgart, Beschluss vom 4. Mai 2016, Az.: 4 Ss 543/15, juris Rz. 16 unter Verweis auf die Rechtsprechung zur Verwertbarkeit von „Steuer-CDs“ vgl. BVerfG, Kammerbeschluss vom 9. November 2010 – 2 BvR 2101/09, NStZ 2011, 103 Rn. 58; OVG Rheinland-Pfalz, NJW 2014, 1434 ff.).

74 OLG Stuttgart, Beschluss vom 4. Mai 2016, Az.: 4 Ss 543/15, juris.