Beschäftigtendatenschutz und Compliance

Thüsing

3. Auflage 2021
ISBN 978-3-406-71502-0
C.H.BECK

umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

mögliche Maßnahme der Terrorbekämpfung genannt wird.[70] *Maschmann* geht sogar davon aus, dass aufgrund des Beschäftigungsverbots der gelisteten Personen ein „Terrorlisten-Screening" notwendig ist.[71] Relevant sei dies vor allem für Exporteure, die sich um eine Zertifizierung als „Authorized Economic Operator" (AEO-Operator) bewerben, um zollrechtliche Erleichterungen (v. a. vereinfachte und zügigere Zollabfertigung) zu erhalten. In einer Entscheidung, welche noch zur Rechtslage vor der DS-GVO erging, hatte der BFH keine Bedenken, wenn die Erteilung des AEO Zertifikats davon abhängig gemacht wurde, dass in entsprechend sicherheitsrelevanten Bereichen der Beschäftigte einer Sicherheitsprüfung anhand der Anhänge der VO (EG) 2580/2001 und der VO (EG) 881/2002 (sog. „Terrorismusliste") unterzogen wurde. Die gesetzliche Rechtfertigungsgrundlage für einen dafür notwendigen datenschutzrechtlich relevanten Eingriff sah der BFH explizit in § 32 BDSG aF.[72] Diese Rechtsprechung dürfte auf die Situation nach In-Kraft-Treten der DS-GVO zu übertragen sein.[73]

47 Nach der Reform des AWG ist der fahrlässige Verstoß nicht mehr als Straftatbestand sondern als Ordnungswidrigkeit in § 19 Abs. 1 AWG zu finden. Die obigen Ausführungen der Literatur zum Sorgfaltsverstoß sind daher gleichermaßen zu berücksichtigen, auch wenn nicht die vormalige Rechtsfolge eintreten kann. Neuere Sanktionen könnte in Zukunft das geplante Gesetz zur Stärkung der Integrität der Wirtschaft bringen, das sich aktuell noch im Gesetzgebungsprozess befindet.[74]

48 Einige Stimmen der Literatur fordern für den Datenabgleich der Terrorlisten Einschränkungen. So hält *Sonnenberg*[75] den Abgleich für datenschutzwidrig, sofern kein Anlass dazu besteht. *Haszmons* und *Raben*[76] fordern, den Abgleich auf zwei Male im Jahr zu beschränken, da die Listen nicht öfter aktualisiert werden, und den Umfang auf die erforderlichen Daten zu begrenzen. Sie weisen daneben auf ein potentielles Mitbestimmungsrecht des Betriebsrates hin. Das BAG[77] erteilte dieser Aussage eine Absage und entschied, dass der Betriebsrat bei dem Datenabgleich kein Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG habe. Der Namensabgleich ist nicht dazu bestimmt, die Leistung oder das Verhalten des Arbeitnehmers am Arbeitsplatz zu überwachen. Über die Notwendigkeit der Maßnahme hatte das BAG aber nicht zu entscheiden.

49 All dies zeigt eine **Tendenz** auf: Es lässt sich festhalten, dass das Verbot, terroristische Gruppen indirekt mit Vermögenswerten auszustatten, hohe Anforderungen an die *Corporate Compliance* stellt. Nur mithilfe einer umfassenden Überwachung der Finanzströme eines Konzerns lässt sich erkennen, ob Gelder eventuell an terroristische Organisationen fließen, etwa in Form von Arbeitslöhnen oder Kaufpreisen. Es verfestigt sich der Gesamteindruck, dass der Staat zunehmend hohe Anforderungen an die interne Überwachung von Wirtschaftsunternehmen stellt.

II. Das Interesse der verantwortlichen Stelle

50 Der Datenabgleich in der Praxis ist also sowohl bei staatlichen wie nichtstaatlichen Stellen weit verbreitet. Auch im Bereich des europäischen Rechts ist er nicht unbekannt und wird höchstrichterlich in diesem Kontext für zulässig erachtet. Gleichwohl kann nur eine Ab-

[70] Bewährte Praktiken der EU für die Umsetzung restriktiver Maßnahmen, 8666/1/08 REV 1 v. 24. 8. 2008, S. 14 (Nr. 33 aE).
[71] *Maschmann* NZA-Beil. 2012, 50 (55).
[72] BFHE 237, 562; aA: *Möllenhoff/Ovie* AW-Prax 2010, 136 (137).
[73] Vgl. auch *Kort* RdA 2018, 24 (26), der die Zulässigkeit auf Grundlage von § 32 BDSG aF und § 26 BDSG nF annimmt.
[74] Referentenentwurf des Bundesjustizministeriums vom 22. 4. 2020: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Staerkung_Integritaet_Wirtschaft.html (zuletzt abgerufen am 15. 5. 2020).
[75] *Sonnenberg* JuS 2018, 917 (920).
[76] *Aszmons/Raben* DSB 2019, 220 (222).
[77] BAG NZA 2018, 673.

wägung der widerstreitenden Interessen endgültig Aufschluss über die Angemessenheit des einzelnen Datenabgleichs verschaffen. Die **Interessen der verantwortlichen Stelle am Datenabgleich** liegen regelmäßig auf der Hand. Der **hohe wirtschaftliche Schaden,** der durch regelwidrige Geschäfte zustande kommen kann, und die **Beeinträchtigung des Ansehens des Unternehmens** sind mit Händen zu greifen. Die Datenabgleiche dürfen aber nicht ohne Anlass sein, sondern müssen als Reaktion auf ein Verhalten erfolgen, das man vereinzelt beobachtet und nun effektiv verhindern will. Nichts anderes verlangt auch § 26 Abs. 1 S. 2 BDSG nF. Das Gewicht dieser Interessen muss umso höher angesetzt werden, als die Geschäftsleitung nicht aus freiem Antrieb handelt, sondern – wie in → § 2 Rn. 10 ff. eingangs dargestellt – aufgrund rechtlicher Verpflichtung. Mag es auch im „Wie" der Kontrolle frei sein, so ist es doch verpflichtet, die Vermeidung von Interessenkonflikten ernst zu nehmen. **Bloßes Vertrauen in die Belegschaft genügt keinesfalls.** Die Eigeninteressen der verantwortlichen Stelle decken sich hier zudem mit dem Interesse der Öffentlichkeit an einer effektiven **Verhinderung von Wirtschaftskriminalität.** Insbesondere vor dem Hintergrund des neuen Referentenentwurfs des Bundesjustizministeriums zum „Gesetz zur Stärkung der Integrität der Wirtschaft"[78] wird die Prävention von Straftaten besonders relevant. Danach drohen empfindliche Verbandssanktionen von bis zu 10 % des durchschnittlichen Jahresumsatzes, wenn eine Leitungsperson eine Verbandstat begeht (§§ 3 Abs. 1 Nr. 1, 9 Abs. 2 Nr. 1 des Entwurfs). Dies gilt es durch vorausschauende Compliance-Maßnahmen zu verhindern. Dies erkennt auch das Datenschutzrecht an. Dort wo die verantwortliche Stelle handelt, um rechtliche Pflichten zu erfüllen, darf sie das auch (s. Art. 6 Abs. 1 S. 1 Buchst. c DS-GVO). Zusätzlich wird in Erwgr. 47 S. 6 DS-GVO klargestellt, dass die Verhinderung eines Betruges in unbedingt erforderlichem Umfang ein berechtigtes Interesse iSd Art. 6 Abs. 1 S. 1 Buchst. f DS-GVO darstellt.

III. Das Interesse der betroffenen Arbeitnehmer

51 Auf der anderen Seite steht das **Interesse der betroffenen Arbeitnehmer** an der Wahrung ihres **Rechts auf informationelle Selbstbestimmung.** Auch dieses hat ein hohes Gewicht, wie das *BVerfG* in der bereits referierten Rechtsprechung (→ § 3 Rn. 38 ff.) deutlich macht. Es muss jedoch unterschieden werden zwischen den Beschäftigten, bei denen eine Übereinstimmung der Daten festgestellt wurde, und solchen, bei denen dies nicht der Fall war:

- Dort, wo **kein Treffer** erfolgt, werden auch keine weiteren Speicherungen von Daten vorgenommen. Hier liegt in Übereinstimmung mit der Rechtsprechung des *BVerfG* zur automatisierten Erfassung von KFZ-Kennzeichen und zur Kontenabfrage kein Eingriff in das Grundrecht der Beschäftigten auf informationelle Selbstbestimmung vor. Das überzeugt auch der Sache nach: Ein Transfer von Daten aus dem einen Vertragsverhältnis zum anderen hat im Hinblick auf diese Beschäftigten letztlich nicht stattgefunden, eine neue Aussage wurde nicht generiert.
- Anders verhält es sich im **Trefferfall:** Hier wurde (gegebenenfalls nach weiteren Nachforschungen) eine Aussage dahin generiert, dass der Beschäftigte auch Lieferant war. Das Gewicht dieses Eingriffs wird freilich dadurch relativiert, dass es sich hier meist um wenige Fälle verglichen mit der Gesamtbelegschaft handelt. Dies minimiert den Kreis der Betroffenen gerade auf die Personengruppe, nach der man gesucht hat. Eine Rechtfertigung sollte hier umso leichter fallen.

[78] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Staerkung_Integritaet_Wirtschaft.html (zuletzt abgerufen am 15. 5. 2020).

IV. Angemessenheit im engeren Sinne

Die Abwägung im Sinne einer **Angemessenheit im engeren Sinne** ist durch das Gesagte vorgezeichnet: 52

- Massive Interessen der Arbeitgeberseite stehen einem Eingriff in die Persönlichkeitsrechte allein derjenigen Beschäftigten gegenüber, die sich tatsächlich pflichtwidrig verhalten haben.
- Selbst dieser Eingriff ist entsprechend den Maßstäben der Rechtsprechung des BVerfG als gering zu werten, wenn es sich um „persönlichkeitsferne" Datenbestände ohne stigmatisierende Wirkung handelt. Das ist etwa bei Kontostammdaten oder Adressen anzunehmen.
- Hinzu kommt, dass der elektronische Datenabgleich durchaus üblich ist.
- Ferner ist zu beachten, dass der Datenabgleich eine umso geringere Belastung darstellt, wenn nur Daten zusammengeführt wurden, die beim Abgleichenden schon vorhanden waren. Hier muss die Rechtfertigungsschwelle niedriger sein als dort, wo der Datenabgleich auf externe Daten gestützt wird.

Ein Beispiel macht dies deutlich: Würde sich ein Arbeitgeber, der über eine geringere Anzahl von Beschäftigten verfügt, bei Erteilung eines Auftrags an einen Lieferanten daran erinnern, dass er diesen Namen auch schon einmal unter seinen Beschäftigten gehört hat, und würde er dann seinen Verdacht durch Nachfragen oder durch Blick in die Personalunterlagen verifizieren, so wäre dies kein datenschutzrechtliches Problem. Es spricht intuitiv weniger dafür, dass einem Arbeitgeber, der sehr viel mehr Arbeitnehmer hat, die Korruptionsbekämpfung datenschutzrechtlich schwerer gemacht wird.

Schließlich fällt entscheidend ins Gewicht, dass ein Eingriff in die Daten der Personen letztlich nur bei den Personengruppen vorliegt, die tatsächlich pflichtwidrig gehandelt haben. Gerade diese zu erfassen ist das Interesse des Arbeitgebers und das öffentliche Interesse. Eine geringe Beeinträchtigung des Rechts auf informationelle Selbstbestimmung steht hier einem Gewinn an effektiver Compliance gegenüber. Eine Rechtfertigung ist offensichtlich. 53

§ 9. Speicherung und Sichtung von E-Mails und E-Mail-Logfiles

Literatur:

Baumgarten, Birger, LAG Hessen: Sachvortragsverwertungsverbot bei Verstoß gegen Datenschutzrecht, ArbRAktuell 2019, 103; *Beckschulze, Martin,* Intranet- und E-Mail-Einsatz am Arbeitsplatz, DB 2009, 2097; *ders.,* Internet-, Intranet- und E-Mail-Einsatz am Arbeitsplatz, DB 2003, 2777; *Behling, Thorsten B.,* Neues EGMR-Urteil zur Überwachung der elektronischen Kommunikation am Arbeitsplatz: Datenschutzrechtliche Implikationen für deutsche Arbeitgeber, BB 2018, 52; *Besgen, Nicolai,* Handbuch Internet. Arbeitsrecht, 2009; *Brandt, Jochen,* Datenschutz und Betriebsrat, AiB 2009, 80; *Böhm, Wolf-Tassilo/Wybitul, Tim,* Sachvortragsverwertungsverbot – Kontrolle privater E-Mails – Schutz vertraulicher Kommunikation, NZA-RR 2019, 138; *Braun, Frank/Spiegl, Katarina,* E-Mail und Internet am Arbeitsplatz, AiB 2008, 393; *Brink, Stefan/Schwab, Sabrina,* Die private E-Mail-Nutzung am Arbeitsplatz, ArbR 2018, 111; *Chandna-Hoppe, Katja,* Beweisverwertung bei digitaler Überwachung am Arbeitsplatz unter Geltung des BDSG 2018 und der DS-GVO – Der gläserne Arbeitnehmer?, NZA 2018, 614; *Dann, Matthias/Gastell, Roland,* Geheime Mitarbeiterkontrollen: Straf- und arbeitsrechtliche Risiken bei unternehnehmensinterner Aufklärung; *Däubler, Wolfgang,* Gläserne Belegschaften, 2010; *de Wolf, Abraham,* Kollidierende Pflichten: zwischen Schutz von E-Mails und „Compliance" im Unternehmen, NZA 2010, 1206; *Dzida, Boris,* Überwachung der E-Mail-Kommunikation von Arbeitnehmern muss Recht auf Privatleben beachten, ArbRB 2017, 299; *Dzida, Boris/Klopp, Thorben,* Neue Vorgaben des EGMR für die Überwachung des E-Mail-Verkehrs im Arbeitsverhältnis – Ohne Transparenz geht nichts, ArbRB 2017, 376; *Eheleben, Moritz/Schirge, Barbara/Seipel, Matthias,* Datenschutz rund ums Arbeitsverhältnis, AiB 2009, 192; *Elschner, Günter,* Rechtsfragen der Internet- und E-Mail-Nutzung am Arbeitsplatz, Dissertation Münster 2004; *Erler, Andreas,* Die private Nutzung neuer Medien am Arbeitsplatz, Dissertation München 2003; *Ernst, Stefan,* Der Arbeitgeber, die E-Mail und das Internet, NZA 2002, 585; *Fuhlrott, Michael,* Ergebnis eines E-Mail-Screenings ins „Blaue hinein" ist unverwertbar, GWR 2019, 114; *Fuhlrott, Michael/Oltmanns, Sönke,* Arbeitnehmerüberwachung und interne Ermittlungen im Lichte der Datenschutz-Grundverordnung, NZA 2019, 1105; *Fülbier, Ulrich/Splittgerber, Andreas,* Keine (Fernmelde-) Geheimnisse vor dem Arbeitgeber?, NJW 2012, 1995; *Gola, Peter,* Datenschutz und Multimedia am Arbeitsplatz, 2008; *Hammann Dirk/Schmitz, Karl/Apitzsch, Wolfgang,* Überwachung und Arbeitnehmerdatenschutz, 2009; *Hanau, Peter/Hoeren, Thomas,* Private Internetnutzung durch Arbeitnehmer, 2003; *Henke, Jens,* IT und Datenschutz im Unternehmen, 2006; *Hilber, Marc/Frik, Roman,* Rechtliche Aspekte der Nutzung von Netzwerken durch Arbeitnehmer und den Betriebsrat, RdA 2002, 98; *Kempermann, Philip,* Strafbarkeit nach § 206 StGB bei Kontrolle von Mitarbeiter-E-Mails?, ZD 2012, 12; *Koch, Frank,* Rechtsprobleme privater Nutzung betrieblicher elektronischer Kommunikationsmittel, NZA 2008, 911; *Kock, Matrin/Francke, Julia,* Mitarbeiterkontrolle durch systematischen Datenabgleich zur Korruptionsbekämpfung; NZA 2009, 646; *Koeppen, Thomas,* Rechtliche Grenzen der Kontrolle der E-Mail- und Internetnutzung am Arbeitsplatz, Dissertation Berlin 2007; *Maschmann, Frank,* Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, 115; *Mattl, Tina,* Die Kontrolle der Internet- und E-Mail-Nutzung am Arbeitsplatz, Dissertation Tübingen 2008; *Mehrens, Christian,* Gewerkschaftswerbung per E-Mail – Zulässigkeit und Grenzen, BB 2009, 2086; *Mengel, Anja,* Kontrolle der E-Mail- und Internetkommunikation am Arbeitsplatz, BB 2004, 2014; *dies.,* Internal Investigations – Arbeitsrechtliche Lessons Learned und Forderungen an den Gesetzgeber, NZA 2017, 1494; *Oberwetter, Christian,* Arbeitnehmerrechte bei Lidl, Aldi & Co., NZA 2008, 609; *Olbertz, Klaus,* Einführung einer elektronischen Personalakte, ArbRB 2009, 86; *Ostmann, Petra/Kappel, Verena,* Arbeitnehmerdatenschutz – Reichweite der Rechte und Pflichten des Arbeitgebers, AuA 2008, 656; *Petri, Dirk/Brüssow, Rainer,* Arbeitnehmerüberwachung am Arbeitsplatz, PersV 2009, 90; *Raffler, Andrea/Hellig, Peter,* Unter welchen Voraussetzungen ist die Überwachung von Arbeitnehmer-E-Mails zulässig, NZA 1997, 862; *Sassenberg, Thomas/Mantz, Reto/Scheben, Barbara/Klos, Christian,* Analyse von Chatprotokollen und E-Mails – Was ist erlaubt? Was ist verwertbar?, CCZ 2013, 88; *Schmitt-Rolfes, Günther,* Kontrolle von Internet- und E-Mail- Nutzung am Arbeitsplatz, AuA 2008, 391; *Seifert, Achim,* Überwachung des E-Mail-Verkehrs von Arbeitnehmern – Urteil des Europäischen Gerichtshofs vom 5. 9. 2017 – Rechtssache Barbulescu/Rumänien, EuZA 2018, 502; *Ströbel, Lukas/Böhm, Wolf-Tassilo/Breunig, Christina/Wybitul, Tim,* Beschäftigtendatenschutz und Compliance: Compliance-Kontrollen und interne Ermittlungen nach der EU-Datenschutz-Grundverordnung und dem neuen Bundesdatenschutzgesetz, CCZ 2018, 14; *Stück, Volker,* Präventive und repressive Compliance: Datenschutz- und arbeitsrechtliche Aspekte nach DS-GVO sowie BDSG 2018, ArbRAktuell 2019, 216*; ders.,* Compliance: Überwachungsmöglichkeiten des Arbeitgebers im Lichte aktueller Rechtsprechung, ArbRAktuell 2018, 31; *Tinnefeld, Marie-Theres/Viethen, Hans Peter,* Arbeitnehmerdatenschutz und Internet- Ökonomie, NZA 2000, 977; *Wolf, Thomas/Mulert, Gerrit,* Die Zulässigkeit der Überwachung von E-Mail- Korrespondenz am Arbeitsplatz, BB 2008, 442; *Wytibul, Tim,* Das neue Bundesdatenschutzgesetz – Verschärfte Regeln für Compliance und interne Ermittlungen, BB 2009, 1582; *ders.*, Neue Spielregeln bei E-Mail-Kontrollen durch den Arbeitgeber, ZD 2011, 69.

A. Grundlagen

I. Zwecke der Speicherung und Sichtung des E-Mail-Verkehrs

1 Kaum ein Unternehmen kommt heutzutage mehr ohne ein eigenes E-Mail-System aus. Dessen Zweck ist es in erster Linie, die **dienstliche Kommunikation der Mitarbeiter** untereinander und nach außen zu ermöglichen. In der Praxis wird den Mitarbeitern außerdem häufig die Verwendung der E-Mail auch zu **privaten Zwecken** gestattet. Diese Zwecksetzungen stehen hier jedoch nicht im Vordergrund. Auch sie sind zwar datenschutzrechtlich zu rechtfertigen: Jede E-Mail enthält als personenbezogene Daten jedenfalls den Namen von Absender und Empfänger. Zusätzlich ist der Arbeitgeber – auch soweit private E-Mails versandt oder empfangen werden – jedenfalls auch Verantwortlicher (→ Rn. 15). Daher ist jede Übertragung und jede Speicherung von E-Mails im Grundsatz rechtfertigungsbedürftig. Sie gelingt aber nach § 26 Abs. 1 S. 1 BDSG ohne weiteres, weil der Einsatz moderner Kommunikationsmittel wie E-Mail im heutigen Arbeitsverhältnis unverzichtbar ist. Der Eingriff in das Persönlichkeitsrecht des Beschäftigten bleibt gering, weil nur Empfänger und Absender Einblick in die E-Mail nehmen. Hier kann also jeder bestimmen, was er dem anderen mitteilt.

2 Für den hiesigen Kontext interessant ist vielmehr, inwiefern der Arbeitgeber auf E-Mail und Verkehrsdaten **außerhalb der Sender-Empfänger-Beziehung** zugreifen kann. An einem solchen Zugriff hat er in vielen Fällen ein erhebliches Interesse:

3 Durch die Analyse des unternehmensinternen E-Mail-Verkehrs lässt sich ein **umfassendes Bild des Unternehmens** gewinnen. Die E-Mail-Korrespondenz bildet nicht nur die täglichen Geschäftsprozesse und die strategischen Entscheidungen ab, sondern zeigt auch, inwiefern sie tatsächlich umgesetzt werden. Ferner gibt sie auch Einblicke in die Beziehungen der Mitarbeiter untereinander.

4 Bei Maßnahmen der **Compliance** ist die Untersuchung des E-Mail-Verkehrs stets der erste Schritt. Spuren von Korruption oder Geheimnisverrat finden sich in den allermeisten Fällen auch in der unternehmensinternen Korrespondenz. Gleiches gilt für Kartellverstöße. Die Untersuchung kann dabei repressiv zur Aufklärung vergangener Verstöße erfolgen, aber auch präventiv zur Verhinderung neuer. Das Gesetz selbst nennt als Zweck der Datenerhebung die repressive Aufklärung von Straftaten (§ 26 Abs. 1 S. 2 BDSG).

5 Ein weiterer unmittelbar mit geschäftlichen Interessen in Zusammenhang stehender Zweck ist der **Zugriff** auf die in der E-Mail-Korrespondenz verkörperten **Informationen.** Es kann ganz konkret um an die Adresse gesandte Bestellungen gehen,[1] aber auch um das als E-Mail vorliegende Arbeitsergebnis. Die Eingliederung der Korrespondenz in die Knowledge Base des Unternehmens perpetuiert insbesondere das Wissen auch über Stellen- und Mitarbeiterwechsel hinweg. Teilweise ist das Unternehmen nach § 147 AO und § 257 HGB auch zur Aufbewahrung bestimmter E-Mails verpflichtet.[2]

6 Ein klassischer arbeitsrechtlicher Zweck ist ferner die **Leistungskontrolle.** Hierunter fällt die Analyse des E-Mail Verkehrs eines Arbeitnehmers, um die exzessive private Nutzung des Dienst-PC festzustellen. Daneben kann der Zugriff auf E-Mails aber auch Bedeutung für die Feststellung der Qualität der Arbeit haben.[3]

7 Die vorgenannten Zwecke erfordern in erster Linie einen Zugriff auf die Informationen, die der Absender der E-Mail ihrem Empfänger mitteilen wollte. Aus dem E-Mail-Verkehr lassen sich jedoch noch weit darüber hinausgehende Meta-Informationen gewinnen, die so nicht Inhalt der E-Mail sind, aber mittels **Big Data Technologie** erfasst werden können. Diese Daten sind meist nicht expliziter Inhalt der Kommunikation, sondern

[1] So in dem Fall des LAG Berlin-Brandenburg NZA-RR 2011, 342.
[2] Dazu *Sassenberg/Mantz* BB 2013, 889 (892).
[3] Etwa der Fall bei LAG Niedersachsen NZA-RR 2010, 406.

ergeben sich erst aus der „intelligenten" Verknüpfung verschiedener Datensätze miteinander. Ihre Existenz ist daher von Absender und Empfänger nicht ohne Weiteres zu steuern.

Sie können aber weitreichende Schlüsse erlauben: Moderne Analysesoftware deckt etwa anhand der unternehmensinternen Kommunikation auf, wie verschiedene Mitarbeiter zueinander stehen, wo es Animositäten und wo erfolgreiche Zusammenarbeit gibt. Die Analyse des E-Mail-Verkehrs ist daher in den USA bereits verbreitetes **Führungsmittel.** In anderen Bereichen werden Datenanalysen auch zur Bestimmung der Leistung der Mitarbeiter verwendet, um als Grundlage für Entlassungsentscheidungen zu dienen.[4] 8

Gleichzeitig können solche Analysen auch eine große Rolle im Rahmen der **Compliance-Organisation** spielen. In der Praxis werden etwa Insider Threats, dh aus der Organisation durch Mitarbeiter drohende Compliance-Risiken wie Insiderhandel, Untreue oder illegale Geschäfte, durch eine Analyse des E-Mail-Verkehrs aufgedeckt: Wer spricht in welchem Tonfall mit wem, wie verändert sich die Kommunikation im Laufe der Zeit?[5] 9

Wegen der großen Menge verfügbarer Daten lassen sich mit Big Data Techniken in vielen Fällen weitere Informationen über Mitarbeiter gewinnen. Diese können häufig für das Unternehmen selbst von Interesse sein – etwa was Krankheitszeiten oder mögliche Gesundheitsrisiken betrifft. Sie können aber auch für Werbezwecke anderer Unternehmen wertvolle Informationen darstellen. 10

II. Objekte des Zugriffs: Logfiles und E-Mails

Durch die technische Implementierung der für den E-Mail Verkehr verwandten Protokolle entstehen verschiedene Datensätze, auf die zugegriffen werden kann. Hier wird die Situation bei Verwendung der Protokolle SMTP und POP3 und Microsoft Exchange dargestellt. 11

Bei den sog. **E-Mail-Logfiles** handelt es sich um Protokolldateien, die Informationen über im E-Mail-Verkehr genutzte Verbindungen enthalten. So wird in diesen Protokolldateien festgehalten, zu welchem Zeitpunkt, wie lange und zwischen welchen Servern bzw. E-Mail- und/oder IP-Adressen eine Verbindung bestanden hat; darüber hinaus, welche Datenmengen in diesem Zusammenhang übertragen worden sind.[6] Auch ist es technisch möglich, die Betreffzeile einer E-Mail zu protokollieren. Das Logfile selbst enthält jedoch weder den eigentlichen Nachrichtentext noch die Anhänge. 12

Dieser eigentliche Inhalt der Nachrichten (Text und Anhänge) wird sowohl auf dem E-Mail Server als auch auf dem lokalen Rechner als abgrenzbarer Datensatz **(„E-Mail")** vorgehalten. Die einzelne E-Mail kann dann als solcher Gegenstand einer Datenerhebung sein. 13

Etwas anders ist die Situation bei der Verwendung eines Exchange Servers. Dieser erlaubt nicht nur die Versendung von E-Mails, sondern umfasst auch Kalenderfunktionen, die Verwaltung eines Aufgabenzettels und – auch als Add-on – zahlreiche weitere Funktionen. Entsprechend größer ist hier die Menge an verfügbaren Daten. 14

III. Verantwortlicher, Betroffene

Die Verantwortung des Arbeitgebers für die Verwendung seines E-Mail-Systems ist **umfassend** und gilt auch für das Versenden, Empfangen und Einsehen privater E-Mails. 15

[4] Vgl. den Bericht aus der Praxis *Markus Morgenroth* im Interview mit FAZ.net, „Datenanalyst Markus Morgenroth im Gespräch: Wer böse ist, bestimmt der Kunde" v. 12. 9. 2013.
[5] Vgl. den Bericht aus der Praxis *Markus Morgenroth* im Interview mit FAZ.net, „Datenanalyst Markus Morgenroth im Gespräch: Wer böse ist, bestimmt der Kunde" v. 12. 9. 2013.
[6] *Hanau/Hoeren* Internetnutzung S. 16.

Nach Art. 4 Nr. 7 DS-GVO ist der Arbeitgeber auch insofern jedenfalls (Mit-)Verantwortlicher, da er jedenfalls die Mittel der Verarbeitung bestimmt.

16 Von der Datenverarbeitung **Betroffener** ist der Beschäftigte (Art. 4 Nr. 1 DS-GVO). Gleiches gilt für **externe Adressaten** oder Absender von E-Mails. Der Eingriff in deren Rechte wiegt vergleichsweise gering, da sie damit rechnen müssen, dass ihre E-Mails in der Organisation des Arbeitgebers weitere Verbreitung finden. Das ist für sie ohne weiteres erkennbar, wenn eine berufliche Domain verwandt wird.[7] Insofern ist die Datenverarbeitung regelmäßig nach der jeweils einschlägigen Rechtsgrundlage (etwa Art. 6 Abs. 1 lit. b oder lit. f, § 26 Abs. 1 BDSG gerechtfertigt.

IV. Prüfungsrahmen: DS-GVO und BDSG oder TKG und StGB?

17 Bei dem Zugriff auf E-Mails und E-Mail-Logfiles stellt sich im ersten Schritt immer die Frage nach dem richtigen Prüfungsmaßstab. Unter → § 3 Rn. 73 ff. wurde ausführlich dargelegt, dass richtiger Maßstab nicht das TKG, sondern die DS-GVO und das **BDSG** ist – selbst bei erlaubter Privatnutzung. Daher wird in diesem Kapitel die Zulässigkeit in erster Linie anhand von DS-GVO und BDSG untersucht (→ Rn. 18 ff.). Da die Frage allerdings weiterhin umstritten ist und eine höchstrichterliche Klärung noch aussteht, wird *disputandi causa* auch die Zulässigkeit nach dem TKG und dem StGB ausgelotet (→ Rn. 70 ff.).

B. Erfordernis einer Rechtfertigung (Art. 5 Abs. 1 lit. a, 6 Abs. 1 DS-GVO, § 26 BDSG)

18 Jeder Zugriff auf E-Mail-Logfiles, ebenso wie auf den Inhalt der Kommunikation selbst, erfordert eine datenschutzrechtliche Rechtfertigung, da es sich stets um die Verarbeitung personenbezogener Daten handelt (Art. 5 Abs. 1 lit. a, 6 Abs. 1 DS-GVO).

I. E-Mail-Logfiles als personenbezogene Daten

19 Personenbezogene Daten sind nach der Legaldefinition des Art. 4 Nr. 1 DS-GVO „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)". E-Mail-Logfiles **personalisierter E-Mail-Adressen** werden nach allgemeiner Ansicht als personenbezogenes Datum eingestuft,[8] denn die typische E-Mail-Logfile gibt Auskunft darüber, wer an wen eine E-Mail welcher Größe zu welcher Zeit gesandt hat:

20
```
>tail syslog
September 21 16:32:06 tcs sendmail: from=<gregor.thuesing@email.de>, size=1150,
class=0
September 21 16:32:06 tcs sendmail: to=<sekretariat.thuesing@jura.uni-bonn.de>,
delay=00:00:01, stat=Sent
September 21 16:32:07 tcs sendmail: to=<professor.thuesing@jura.uni-bonn.de>,
delay=00:00:03, stat=Sent
```

[7] *Sassenberg/Mantz* BB 2013, 889 (891).
[8] S. nur NK-BDSG/*Dammann* BDSG § 3 Rn. 62; *Härting* CR 2008, 743 f.