Richtiges Verhalten in der Compliance-Krise

Engelhoven

2023
ISBN 978-3-406-79457-5
C.H.BECK

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

stößen geeignet. Der Einsatz solcher Techniken kann allerdings eine Datenschutz-Folgenabschätzung erforderlich machen (Art. 35 DS-GVO).

Beispiel: Kommt es innerhalb eines E-Mail-Programms zu ungewöhnlichen Tages- oder Nachtzeiten zum Versand auffällig vieler E-Mails mit großen Anhängen, erfasst der Bot diese Aktivität und versendet eine Information über seine Beobachtung an die dafür zuständige Stelle. So lässt sich etwa der Verrat von Geschäftsgeheimnissen frühzeitig aufdecken. 97

b) Beachtung datenschutzrechtlicher Vorschriften – insbes. Beschäftigtendatenschutz

aa) Problemstellung

Die vorstehend dargestellten vielfältigen technischen Möglichkeiten, einen Datenpool zu durchsuchen, dürfen nicht darüber hinwegtäuschen, dass dafür enge rechtliche Grenzen gesetzt sind, insbes. in Gestalt des Datenschutzrechts. 98

Denn klar ist: Jede Suche berührt das Recht von Arbeitnehmern auf informationelle Selbstbestimmung, sofern im Datenbestand personenbezogene Daten enthalten sind. Dann sind die Bestimmungen des gesetzlichen Datenschutzrechts zu beachten.[41] Rechtlich unbedenklich sind systematische Überprüfungen nur dann, wenn sie keine personenbezogenen oder personenbeziehbare Daten betreffen.[42] Eine Pseudonymisierung, die den Anforderungen von Art. 4 Nr. 5 DS-GVO genügt, kann daher die datenschutzrechtlichen Risiken einer Untersuchung deutlich verringern. 99

bb) Personenbezogene Daten im Datenpool

Das Recht auf informationelle Selbstbestimmung ist Teil des allgemeinen Persönlichkeitsrechts. Auf europäischer Ebene wird das Recht durch die seit 25.5.2018 geltende DS-GVO streng geschützt. Art. 6 DS-GVO legt fest, unter welchen Voraussetzungen personenbezogene Daten verarbeitet werden dürfen. Der Begriff des Verarbeitens ist in Art. 4 Nr. 2 DS-GVO äußerst weit definiert und erfasst insbes. das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, das Auslesen und die Übermittlung von Daten. Das Durchsuchen von Datenpools im Rahmen einer Untersuchung stellt also ohne jeden Zweifel ein datenschutzrechtlich relevantes Verarbeiten dar. 100

Das maßgebliche Kriterium für die Zulässigkeit, personenbezogene Daten zu verarbeiten, ist die Erforderlichkeit der Verarbeitung. Es gilt ein Verbot mit Erlaubnisvorbehalt, dh die Verarbeitung ist nur zulässig, wenn sie durch eine Vorschrift erlaubt ist. 101

Bei der Verarbeitung personenbezogener Daten von Beschäftigten bildet vor allem das BDSG den Maßstab. Der Gesetzgeber hat von der Öffnungsklausel Art. 88 DS-GVO Gebrauch gemacht und mit § 26 BDSG letztlich die bislang in § 32 BDSG aF geltenden Bestimmungen wiederholt. Im Kontext von Untersuchungen eines Datenpools ist entscheidend, dass § 26 Abs. 1 S. 2 BDSG ausdrücklich die repressive Aufklärung von Straftaten als erlaubten Zweck der Datenerhebung nennt. 102

Dieser Zweck rechtfertigt grds. den Zugriff auf die Informationen, die der Absender einer E-Mail dem Empfänger mitteilen wollte. Allerdings lassen sich E-Mails darüber hinaus zahlreiche weitere sog Meta-Daten entnehmen, die mittels Big Data Technologie ausgewertet werden können. Diese Daten sind nicht eigentlicher Inhalt der Kommunikation, sondern ergeben sich erst aus der Verknüpfung verschiedener Datensätze. Die Existenz dieser Meta-Daten ist weder vom Absender noch vom Empfänger genau vorherseh- und steuerbar.[43] Das ist iRd datenschutzrechtlich erforderlichen Abwägung relevant (s. sogleich → § 4 Rn. 116 ff.). 103

[41] Vgl. Kramer IT-ArbR/Oberthür B. Individualarbeitsrecht Rn. 452.
[42] Vgl. Kramer IT-ArbR/Oberthür B. Individualarbeitsrecht Rn. 456.
[43] Vgl. Thüsing Beschäftigtendatenschutz/Thüsing/Traut § 9 Rn. 7 ff.

cc) Zugriffsobjekte, Verantwortliche und Betroffene

(1) Zugriffsobjekte

104 Zugriffsobjekt bei Datenanalysen sind neben dem eigentlichen Text in den E-Mails inklusive Anhängen (nachfolgend: E-Mails) die in den sog E-Mail-Logfiles enthaltenen Meta-Daten. Dabei handelt es sich um Protokolldateien, in denen insbes. Informationen darüber enthalten sind, wann eine E-Mail gesendet, welche Datenmenge übertragen und zwischen welchen Servern eine Verbindung hergestellt wurde, sowie über die IP-Adressen von Absender und Empfänger.[44]

(a) E-Mails

105 E-Mails enthalten personenbezogene Daten – und zwar nicht nur bezogen auf Absender und Empfänger, sondern meist auch personenbezogene Daten anderer. Sowohl das händische als auch das automatisierte Durchsuchen und Strukturieren von E-Mails stellen datenschutzrechtlich relevante Verarbeitungsvorgänge dar, die einer Rechtfertigung bedürfen.

(b) E-Mail-Logfiles

106 E-Mail-Logfiles personalisierter E-Mail-Adressen enthalten ebenfalls personenbezogene Daten, weil die Logfiles Informationen darüber aufweisen, wer wann an wen eine E-Mail geschickt hat.[45] Etwas anderes gilt nur für vollständig pseudonymisierte E-Mail-Adressen, bei denen der Personenbezug regelmäßig nur für den Provider erkennbar ist, nicht hingegen für Dritte, also auch nicht den Arbeitgeber oder die Prüfer.[46] Die Betreffzeile von E-Mails, die auch Bestandteil der E-Mail-Logfiles sein kann, stellt ebenfalls ein personenbezogenes Datum dar.[47] Für die Verarbeitung dieser personenbezogenen Daten im Rahmen von Datenanalysen ist also eine Rechtfertigung erforderlich.

(c) Andere Datenpools

107 Die Erfahrung zeigt, dass E-Mails nicht nur wegen ihres digitalen Formats eine besonders ergiebige Quelle für Compliance-Verstöße sind. Oft kommunizieren Mitarbeiter in E-Mails sehr offen und dokumentieren dadurch ihre Vorhaben und Absichten. Deshalb lassen E-Mails schnell Rückschlüsse darauf zu, wer von was Kenntnis gehabt haben muss.

108 Aber auch andere Datenpools stellen selbstverständlich wichtige Erkenntnisquellen dar und sollten bei Datenanalysen nicht vernachlässigt werden. Bei diesen Dokumenten bestehen in der Regel nicht die datenschutzrechtlichen Einschränkungen wie bei E-Mails. Denn handelt es sich beispielsweise um Briefkorrespondenz, muss der Arbeitgeber Zugriff darauf haben, und zwar allein schon, um seine Verpflichtungen nach § 257 HGB, § 147 AO zu erfüllen. Sollte bei der Analyse ein Dokument eindeutig privater Natur auftauchen, muss durch eine schriftliche Arbeitsanweisung (→ § 4 Rn. 126) geregelt sein, dass das Dokument nicht zur Kenntnis genommen werden darf und sofort zu löschen ist.

(2) Verantwortliche und Betroffene

109 Bei der Untersuchung von E-Mails ist nach Art. 4 Nr. 7 DS-GVO der Arbeitgeber Verantwortlicher, da er die Mittel der Verarbeitung bestimmt. Betroffen nach Art. 4 Nr. 1 DS-GVO sind der Arbeitnehmer sowie externe Empfänger oder Versender von E-Mails.[48]

dd) Prüfungsmaßstab und Rechtfertigung

110 Sowohl die Durchsuchung – und mithin Verarbeitung – von E-Mails als auch von E-Mail-Logfiles ist nur mit einer Rechtfertigung gestattet. Dafür sind nach hier vertretener

---

[44] Bei der Verwendung der Protokolle SMTP (entspricht dem öffentlichen Postbriefkasten) und POP3 (entspricht dem Briefschlitz an der Haustür), vgl. Wikipedia, „E-Mail", https://de.wikipedia.org/wiki/E-Mail#Zustellung_einer_E-Mail:_beteiligte_Server_und_Protokolle (zuletzt abgerufen am 11.10.2022).
[45] Vgl. NK-BDSG/Dammann BDSG § 3 Rn. 62; Härting CR 2008, 743 f.
[46] Vgl. NK-BDSG/Dammann BDSG § 3 Rn. 62; BeckOK DatenschutzR/Schild DS-GVO Art. 4 Rn. 16.
[47] Vgl. VGH Kassel RDV 1991, 187.
[48] Vgl. Thüsing Beschäftigtendatenschutz/Thüsing/Traut § 9 Rn. 15 f.

Auffassung[49] die datenschutzrechtlichen Vorschriften der Art. 5 Abs. 1 Buchst. a DS-GVO, Art. 6 Abs. 1 DS-GVO sowie § 26 BDSG und nicht die Vorschriften des TTDSG einschlägig.

(1) Keine Geltung des Fernmeldegeheimnisses

Sofern der Arbeitgeber die Nutzung von Telekommunikationsdiensten für private Zwecke gestattet oder zumindest duldet, wird vertreten,[50] dass er als Anbieter von Telekommunikationsmedien anzusehen ist. Das hätte zur Folge, dass die Vorschriften des am 1.12.2021 in Kraft getretenen TTDSG anzuwenden sind. In diesem Fall wäre der Arbeitgeber gem. § 3 Abs. 2 Nr. 2 TTDSG[51] an das Fernmeldegeheimnis gebunden, und ein Zugriff auf die Mitarbeiter-E-Mails wegen Compliance-Verstößen wäre so gut wie ausgeschlossen. Bei einer Durchsuchung von E-Mails drohte dann auch eine Strafbarkeit nach §§ 202a, 202b, 206 StGB (s. dazu → § 4 Rn. 134) – und zwar selbst dann, wenn versucht wird, eine Einwilligung von Mitarbeitern zur E-Mail-Durchsicht einzuholen (→ § 4 Rn. 131 f.). Denn es kann nie absolut sichergestellt sein, dass tatsächlich alle Mitarbeiter einwilligen. 111

Der in seinen Konsequenzen folgenreiche Streit über die Geltung des Fernmeldegeheimnisses hat sich durch die neue Regelung in § 3 Abs. 2 Nr. 1, 2 TTDSG leider nicht erübrigt, sondern wird sich vermutlich nur verlagern. 112

§ 3 Abs. 2 Nr. 1 TTDSG ist allerdings schon wegen seines klaren Wortlauts („Anbieter von *öffentlich zugänglichen* Telekommunikationsdiensten") auf Arbeitgeber nicht anwendbar.[52] 113

Nach § 3 Abs. 2 Nr. 2 TTDSG ist es ausreichend, wenn der geschäftsmäßig angebotene Telekommunikationsdienst nicht vom Arbeitgeber selbst angeboten wird, sondern dieser an dem Angebot eines Dritten mitwirkt. Bedauerlicherweise definiert weder das TTDSG noch das TKG das „Mitwirken". Es wird aber vertreten, dass der Arbeitgeber als Mitwirkender anzusehen sei, da er Zugriff auf den Inhalt von E-Mails erlangen könne (insbes. beim Betrieb eines Exchange-Servers für E-Mails). Daher liege die technische Infrastruktur auch in der Sphäre des Arbeitgebers, und er wäre demnach zur Einhaltung des Fernmeldegeheimnisses verpflichtet.[53] Allerdings berücksichtigt diese Auffassung nicht hinreichend den Wortlaut der Vorschrift. § 3 Abs. 2 Nr. 2 TTDSG setzt voraus, dass an „*geschäftsmäßig* angebotenen Telekommunikationsdiensten" mitgewirkt wird. Zwar mag der Arbeitgeber rein faktisch an dem Dienst mitwirken, aber er tut dies nicht geschäftsmäßig. Es ist schon fraglich, ob betriebliche Kommunikationssysteme überhaupt ein Telekommunikationsdienst sein können; nach der Legaldefinition wird ein solcher Dienst gem. § 3 Abs. 2 S. 1 Nr. 2 TTDSG, § 2 Abs. 1 TTDSG iVm § 3 Nr. 61 TKG „in der Regel gegen Entgelt erbracht".[54] Für diese Sichtweise spricht auch, dass der Gesetzgeber mit der Änderung des TTDSG die ePrivacy-RL umsetzen wollte. Diese sieht Kommunikationsdienste ebenfalls als Dienste, die in der Regel gegen Entgelt verfügbar sind. Diese Voraussetzung ist im Verhältnis zwischen Arbeitgeber und Beschäftigten jedoch nicht gegeben, so dass § 3 TTDSG auch aufgrund teleologischer Reduktion auf Arbeitgeber letztlich keine Anwendung finden kann.[55] 114

[49] So auch: LAG Berlin-Brandenburg BB 2016, 891; 2011, 2298; LAG Niedersachsen NZA-RR 2010, 406; BeckOK DatenschutzR/Riesenhuber BDSG § 26 Rn. 169; Galle BB 2018, 564 (566); Thüsing Beschäftigtendatenschutz/Thüsing/Traut § 9 Rn. 28.

[50] Der Streitstand ist (allerdings noch zum TKG) ausführlich aufbereitet bei Thüsing Beschäftigtendatenschutz/Thüsing/Traut § 3 Rn. 73 ff., § 9 Rn. 41 f.

[51] Vor Inkrafttreten des TTDSG wurde der Arbeitgeber von den Vertretern dieser Auffassung als Dienstanbieter nach § 3 Nr. 6 TKG angesehen, der zur Einhaltung des Fernmeldegeheimnisses nach § 88 TKG (aF) verpflichtet sei.

[52] Ebenso Wünschelbaum NJW 2022, 1561 (1562).

[53] Vgl. Rossow DuD 2022, 93 (95 f.).

[54] Vgl. Wünschelbaum NJW 2022, 1561.

[55] Ähnlich Rossow DuD 2022, 93 (97); Wünschelbaum NJW 2022, 1561 (1562).

(2) Arbeitnehmer

(a) § 26 BDSG

115 Den wichtigsten gesetzlichen Rechtfertigungstatbestand für die Datenverarbeitung von Arbeitnehmern im Rahmen von Datenanalysen bildet § 26 BDSG, und zwar nach hier vertretener Ansicht auch dann, wenn der Arbeitgeber die private Nutzung von Telekommunikationsmitteln gestattet oder duldet.

116 § 26 Abs. 1 S. 2 BDSG enthält eine ausdrückliche Regelung der Verarbeitung personenbezogener Daten, sofern dies zum Zwecke der Aufklärung von Straftaten erforderlich ist. Erforderlich bedeutet, dass eine Abwägung stattzufinden hat.[56] Voraussetzung ist auch, dass es (zu dokumentierende → § 1 Rn. 329) tatsächliche Anhaltspunkte für den Verdacht einer Straftat (oder einer schwerwiegenden, jedoch nicht unbedingt strafbaren Pflichtverletzung[57]) gibt, die zu einem Beschäftigten hinführen und dass dessen schutzwürdige Interessen nicht überwiegen. Ein Anfangsverdacht oder ein „einfacher Verdacht" sind dem BAG zufolge ausreichend, bloße Mutmaßungen oder vage Anhaltspunkte hingegen nicht.[58]

117 Die Abwägung ist stets im Einzelfall vorzunehmen; dabei ist die Intensität der Beeinträchtigung in Einklang zu bringen mit den Interessen des Arbeitgebers an der Durchsuchung von E-Mails. Je schwerwiegender die (vermutete) Beeinträchtigung der Rechte des Unternehmens ist, desto mehr spricht für den Eingriff in die Rechte der Beschäftigten. Auf der anderen Seite steht das Recht der Arbeitnehmer auf informationelle Selbstbestimmung.[59]

118 IRd Abwägung spielt es eine Rolle, ob auf die E-Mails oder lediglich auf die E-Mail-Logfiles zugegriffen wird. Der Zugriff auf Logfiles ist grds. weniger eingriffsintensiv, weil sie nur Verkehrsdaten enthalten, also solche, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind (§ 3 Nr. 70 TKG). Daher sollte bei internen Untersuchungen ein gestuftes Vorgehen genutzt werden: Über die Auswertung von Logfiles wird zunächst ermittelt, welche Mitarbeiter mit einer verdächtigten Person in Kontakt standen; im nächsten Schritt können dann gezielt ausschließlich die E-Mails dieser Personen untersucht werden. Sofern lediglich eine Person im Verdacht steht, kann es jedoch auch weniger einschneidend sein, die E-Mails dieser Person selektiv zu durchsuchen – und nicht die Logfiles aller E-Mail-Nutzer. Auch das ist im Wege der Abwägung zu bestimmen.[60] Um den Eingriff in die Interessen von Nichtverdächtigen möglichst gering zu halten, kann es erforderlich sein, die Untersuchung zunächst auf zwischen Verdächtigen ausgetauschte E-Mails zu beschränken. Die sorgfältige und zurückhaltende Auswahl von Suchbegriffen, auf die E-Mails hin überprüft werden, kann sich ebenfalls als ein milderes Mittel darstellen und die Abwägung positiv beeinflussen.

119 Für die Abwägung ist auch relevant, ob E-Mails eher wie Telefonate oder wie Schriftstücke einzuordnen sind. Wären E-Mails, wie teilweise vertreten, eher als Telefonate anzusehen, wäre eine Inhaltskontrolle ohne Einwilligung des Arbeitnehmers weitgehend ausgeschlossen. Allerdings scheint richtigerweise die Ansicht herrschend, die E-Mails als Briefkorrespondenz ansieht, mit der Folge, dass der Arbeitgeber sich Kenntnis von jeder dienstlichen E-Mail verschaffen können muss.[61]

[56] Vgl. Kühling/Buchner/Maschmann BDSG § 26 Rn. 18; Thüsing Beschäftigtendatenschutz/Thüsing/Traut § 9 Rn. 28 ff.
[57] Vgl. BGH NZA 2017, 1327.
[58] Vgl. BGH NZA 2017, 443; 2017, 1327.
[59] Vgl. Galle BB 2018, 564 (567).
[60] Vgl. Kühling/Buchner/Maschmann BDSG § 26 Rn. 19; Thüsing Beschäftigtendatenschutz/Thüsing/Traut § 9 Rn. 31 ff.
[61] Vgl. Thüsing Beschäftigtendatenschutz/Thüsing/Traut § 9 Rn. 34 ff. mN zum Streitstand; Wolf/Mulert BB 2008, 442 (443).

Aufseiten des Arbeitgebers ist bei der Abwägung zu berücksichtigen, dass er selbst bestimmten Pflichten unterliegt, seine Arbeitnehmer zu überwachen, um seine Compliance zu gewährleisten.[62] 120

Ganz wesentlich ist iRd Abwägung, ob der Arbeitgeber die private Nutzung von Telekommunikationsmitteln erlaubt oder verboten hat. Sofern der Arbeitgeber die private Nutzung nicht gestattet hat, überwiegen nach herrschender Meinung die Interessen des Arbeitgebers. Man könne erwarten, dass sich der Arbeitnehmer korrekt verhält, deshalb alle seine E-Mails dienstlich sind, und der Arbeitgeber folglich ein uneingeschränktes Zugriffsrecht auf sie haben muss.[63] 121

Bei vom Arbeitgeber erlaubter oder geduldeter Nutzung von Telekommunikationsmitteln zu privaten Zwecken ist besonders zu prüfen, ob es weniger einschneidende Maßnahmen als den direkten Zugriff auf sämtliche E-Mails gibt. Jedenfalls zur Aufklärung von Straftaten muss es nach wohl herrschender Meinung grds. zulässig sein, E-Mails bei einem entsprechenden Verdacht einsehen zu können.[64] Hat der Arbeitgeber Vorkehrungen zur Trennung privater und dienstlicher Korrespondenz getroffen, wird dies iRd Abwägung ebenfalls berücksichtigt und erleichtert die Zugriffsmöglichkeiten. 122

Ein weiteres milderes Mittel im Rahmen einer Untersuchung ist die Aufforderung an einzelne Beschäftigte, bestimmte E-Mails herauszugeben. Allerdings ist diese Vorgehensweise möglicherweise nicht gleich effizient wie eine aktive Einsicht, etwa weil der Mitarbeiter nicht schnell genug reagiert. Sofern der Mitarbeiter nicht reagiert, sich weigert oder bereits ausgeschieden ist, wäre es dann auch bei erlaubter privater Nutzung zulässig, zunächst die für die Untersuchung einschlägigen E-Mails über die E-Mail-Logfiles zu identifizieren und dann auf einzelne E-Mails gezielt zuzugreifen.[65] 123

(b) Art. 6 Abs. 1 Buchst. f DS-GVO

Bei weniger gravierenden Pflichtverletzungen oder Ordnungswidrigkeiten von Beschäftigten – also dem Großteil von Compliance-Verstößen – kann die Prüfung von E-Mails nicht auf § 26 Abs. 1 S. 2 BDSG gestützt werden. 124

Dennoch kann das Durchsuchen von E-Mails zulässig sein, da diese Maßnahme nach Art. 6 Abs. 1 Buchst. f DS-GVO gerechtfertigt sein kann. Der Vorschrift zufolge dürfen personenbezogene Daten verarbeitet werden, wenn es für die Wahrung berechtigter Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen überwiegt.[66] 125

Ein berechtigtes Interesse liegt in der Regel dann vor, wenn ein Anfangsverdacht (→ § 1 Rn. 13, § 4 Rn. 4) zu bejahen ist. Ein Unternehmen hat unbestreitbar ein hohes Interesse daran, aufzuklären, ob es in Compliance-Verstöße verwickelt ist. Das gilt auch für Verstöße, die die Schwelle zur Straftat nicht überschreiten und betrifft alle Mitarbeiter des Unternehmens, solange durch Maßnahmen wie Schlagwort- und Zeitraumeingrenzung[67] sichergestellt ist, dass nicht unnötig viele Daten ausgewertet und gelesen werden. Eine derartige Eingrenzung lässt sich über die heute am Markt verfügbaren Softwarelösungen problemlos sicherstellen. Zur zusätzlichen Absicherung des Unternehmens sollte das Ermittlungsteam mit einer Dienstanweisung sensibilisiert werden. In jedem Fall ist es sinnvoll, den Ermittlern eine schriftliche Arbeitsanweisung[68] zu erteilen, dass erkennbar private E-Mails nicht gesucht werden und diese, bei zufälligem Auffinden, nicht zur Kenntnis genommen werden dürfen und sofort zu löschen sind. 126

[62] Vgl. Thüsing Beschäftigtendatenschutz/Thüsing/Traut § 9 Rn. 56 ff.
[63] Vgl. Kramer IT-ArbR B. Individualarbeitsrecht Rn. 309; Thüsing Beschäftigtendatenschutz/Thüsing/Traut § 9 Rn. 43.
[64] Vgl. Thüsing Beschäftigtendatenschutz/Thüsing/Traut § 9 Rn. 44 mN.
[65] Vgl. LAG Berlin-Brandenburg NZA-RR 2011, 342.
[66] Vgl. Galle BB 2018, 564 (567).
[67] Vgl. Thüsing Beschäftigtendatenschutz/Thüsing/Traut § 9 Rn. 45.
[68] Muster Arbeitsanweisung → § 4 Rn. 214

(c) Dokumentation der Interessenabwägung

127 Die Interessenabwägung muss im Vorfeld der Ermittlungsmaßnahme dokumentiert werden. Dafür sind der Verdacht und die konkreten Maßnahmen genau zu beschreiben (→ § 4 Rn. 118). Deshalb kann es sich auch empfehlen, die datenschutzrechtlichen Rahmenbedingungen einer Datenanalyse zunächst mit den zuständigen Aufsichtsbehörden abzuklären.

128 Die Dokumentation ist vor allem deshalb wichtig, weil das Unternehmen das Risiko für die Rechtmäßigkeit der Maßnahme trägt, falls sich der Verdacht nicht bestätigen sollte.

(d) Information der Arbeitnehmer

129 Es empfiehlt sich, die betreffenden Mitarbeiter vorab über Umfang und Zweck der Untersuchungsmaßnahme zu informieren. Der Grund liegt in den bestehenden gesetzlichen Anforderungen an Informationspflichten von Art. 5 Abs. 1 Buchst. a DS-GVO und Art. 13 DS-GVO. Überdies wird die Intensität eines Eingriffs dadurch verringert, dass der Betroffene vor der Durchführung einer ihn belastenden Maßnahme die Möglichkeit erhält, seine Interessen zu wahren, insbes. durch gerichtlichen (Eil-)Rechtsschutz.[69]

130 Wenn eine Vorabinformation aus ermittlungstaktischen Gründen unterbleiben soll, sollte dies vom Unternehmen ausführlich dokumentiert werden. Die Mitarbeiter sind dann im Nachhinein zu informieren. Die tatsächlichen Verhältnisse müssen vom Unternehmen vor der Ermittlungsmaßnahme ausführlich dokumentiert werden.[70]

(e) Einwilligung

131 Trotz der dargestellten rechtlichen Möglichkeiten einer Untersuchung von E-Mails sollten bei einer internen Untersuchung so viele Einwilligungen von Mitarbeitern (Formulierungsbeispiel § 4 Rn. 212) wie möglich eingeholt werden. Wenn alle Mitarbeiter einwilligen, ist die Maßnahme ohne weiteres zulässig.

132 Die Einwilligung ist im BDSG als Rechtfertigungsmöglichkeit in § 26 Abs. 2 BDSG vorgesehen. Sie muss den in § 26 Abs. 2 BDSG aufgezählten besonderen Anforderungen genügen und insbes. freiwillig abgegeben werden. Ein Nachteil ist freilich, dass die Einwilligung vom Arbeitnehmer jederzeit widerrufen werden kann.

(3) Externe

133 Externe Betroffene müssen damit rechnen, dass ihre E-Mails im Unternehmen verarbeitet und weiterverbreitet werden, etwa wenn E-Mails bei der Abwesenheit von Adressaten automatisch weitergeleitet werden. Das gilt auch, wenn Externe mit Beschäftigten privat per E-Mail in Kontakt treten. Der Eingriff in die Rechte Externer wiegt deshalb vergleichsweise gering. Daher wird die Datenverarbeitung in der Regel aufgrund von Art. 6 Abs. 1 Buchst. b oder Buchst. f DS-GVO, § 26 Abs. 1 BDSG gerechtfertigt sein.[71]

c) Strafrechtliche Risiken

134 Bei Beachtung der vorstehenden Grundsätze dürften strafrechtliche Risiken zwar zu vernachlässigen sein. Der Vollständigkeit halber seien aber folgende in Betracht kommende Straftatbestände erwähnt:

- Eine Strafbarkeit wegen Verletzung des Post- oder Fernmeldegeheimnisses gem. § 206 StGB scheidet nach hier vertretener Ansicht bereits deshalb aus, weil private Arbeitgeber bzw. deren Mitarbeiter nicht zum Täterkreis der Vorschrift zählen, da das TDDSG keine Anwendung findet.[72]
- Auch die Voraussetzungen des Ausspähens von Daten gem. § 202 a StGB und des Abfangens von Daten gem. 202 b StGB dürften nicht gegeben sein, sofern sich der Arbeit-

[69] Vgl. BVerfGE 118, 168; 120, 274; 120, 378.
[70] → § 1 Rn. 329.
[71] Vgl. Galle BB 2018, 564 (567); Thüsing Beschäftigtendatenschutz/Thüsing/Traut § 9 Rn. 16, 29.
[72] Zum Streitstand → § 4 Rn. 111.

geber den Zugriff auf seine Infrastruktur vorbehält bzw. wenn er Zugangsschranken durch Administratorenrechte überwinden kann – was regelmäßig bei E-Mail-Accounts der Fall sein wird. Eine Verwirklichung von § 202 a StGB wäre denkbar, wenn Daten eine besondere Zugangssicherung (zB einen Passwortschutz) haben und nicht für den Arbeitgeber bestimmt waren. Die Details sind umstritten.
- Die Voraussetzungen von § 42 BDSG kommen nur in Betracht bei gewerbsmäßigem Zugänglichmachen von Daten gegenüber einer großen Zahl von Personen oder beim Handeln gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen. In der Regel dürften diese Voraussetzungen bei Untersuchungen wegen Compliance-Verstößen nicht gegeben sein.

d) Auslandsbezug

Oft weist eine Datenanalyse Berührungspunkte zu anderen Staaten auf. Das ist etwa bereits dann der Fall, wenn personenbezogene Daten über Dienstleister in Drittstaaten verarbeitet oder Daten innerhalb eines Konzerns grenzüberschreitend ausgetauscht werden. 135

Trotz weitgehender datenschutzrechtlicher Harmonisierung durch die DS-GVO ist der Schutz personenbezogener Daten von Beschäftigten in der EU aufgrund von Öffnungsklauseln in der DS-GVO immer noch in den nationalen Rechtsordnungen der einzelnen Länder geregelt.[73] Deshalb können sich die Vorschriften zum Schutz von Beschäftigtendaten auch innerhalb der EU unterscheiden. Noch komplizierter ist die Lage, wenn eine Untersuchung Länder außerhalb der EU betrifft. Die Übermittlung von Daten setzt dann voraus, dass beim Empfänger ein angemessenes Datenschutzniveau gewährleistet ist. In der Praxis besonders bedeutsam ist dabei, dass die USA aus Sicht der EU kein ausreichendes Schutzniveau aufweisen.[74] Umgekehrt erlassen mehr und mehr Staaten Regelungen, die das Rückübertragen von Daten aus ihrem Hoheitsgebiet reglementieren und einschränken. 136

Deshalb sollten beim Austausch personenbezogener Daten über Grenzen hinweg vom Unternehmen rechtzeitig die Rahmenbedingungen für eine Datenübermittlung geschaffen werden. Dabei sollte insbes. geprüft werden, ob bei Untersuchungen eine Datenübermittlung auf Grundlage einer der Ausnahmeregelungen des Art. 49 DS-GVO zulässig ist, insbes. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 49 Abs. 1 Buchst. e DS-GVO). 137

Außerdem sollten innerhalb großer Unternehmen datenschutzrechtliche Regelungen und Betriebsvereinbarungen so gestaltet sein, dass der Austausch von Informationen bei Datenanalysen ermöglicht wird. Dazu gehört es auch, Prozesse, Organisationsstrukturen und IT-Systeme unter Berücksichtigung datenschutzrechtlicher Anforderungen wie Datenminimierung (zB durch elektronisches Filtern), Datenlokalisierung und Segmentierung zu gestalten. 138

Im Fall einer konkreten Datenanalyse gilt es, die Kooperation der einzelnen Gesellschaften unter datenschutzrechtlichen Gesichtspunkten zu strukturieren. Dabei sind neben den datenschutzrechtlichen alle anderen relevanten Stellen innerhalb des Konzerns zu beteiligen. 139

Auch an einen länderübergreifenden Datenaustausch mit Behörden muss ein Unternehmen denken, was verbindliche und unverbindliche Auskunftsanfragen bei den jeweiligen Behörden notwendig machen kann. 140

Die Dokumentation der Datenanalyse muss ebenfalls so erfolgen, dass gegenüber allen beteiligten Datenschutzaufsichtsbehörden einerseits die Einhaltung der rechtlichen Anforderungen hinreichend belegt werden kann. Andererseits muss im Hinblick auf mögliche Zugriffe durch Behörden sowie Einsichts- und Auskunftsrechte betroffener Personen bedacht werden, dass nur so viel wie nötig dokumentiert wird. 141

[73] Vgl. Moosmayer/Hartwig Untersuchungen/Kessler/Köhler I. Rn. 133.
[74] Vgl. EuGH NJW 2020, 2613.

6. Befragung von Mitarbeitern

a) Strategische Erwägungen

142 Die Befragung der Mitarbeiter des Unternehmens ist eine der wichtigsten Ermittlungsmaßnahmen. Oftmals lassen sich die aufgefundenen Dokumente und Korrespondenz nur dann richtig einordnen, wenn die betroffenen Mitarbeiter die Zusammenhänge erklären. Das Unternehmen ist daher idR darauf angewiesen, dass die Mitarbeiter in den Befragungen wahrheitsgemäße und vollständige Angaben machen. Dafür kann es erforderlich sein, den Mitarbeitern eine Amnestievereinbarung anzubieten.[75]

143 Auch die zeitliche Abfolge spielt eine wichtige Rolle. Nach einer Durchsuchung durch eine Ermittlungsbehörde kann es aufgrund des Zeitdrucks erforderlich sein, die betroffenen Mitarbeiter sofort zu befragen, weil bspw. in Kartellfällen Kronzeugenanträge und in Korruptionsfällen Selbstanzeigen erwogen werden müssen. Das hat zwar den Nachteil, dass der Sachverhalt noch nicht feststehen wird und daher nur schwer geprüft werden kann, ob die Mitarbeiter vollständige Angaben machen, jedoch hat das Unternehmen aufgrund des Zeitdrucks insoweit oftmals keine andere Wahl.[76] Besser ist die Situation, wenn der Compliance-Verstoß durch einen Hinweisgeber oder bei einem internen Audit aufgedeckt wird. In diesen Fällen hat das Unternehmen mehr Zeit und es kann zweckmäßig sein, zunächst die zur Verfügung stehenden Unterlagen durchzusehen, zB um den Mitarbeitern im Zuge der Befragung Dokumente vorgehalten werden.[77]

144 Der Ablauf der Mitarbeiter-Befragungen muss ebenfalls durchdacht werden. Wenn ausreichend Zeit zur Verfügung steht, sollten zunächst die Gespräche mit der Unternehmensleitung erfolgen und im Anschluss mit den nachgeordneten Mitarbeitern.[78] Wenn Zeitdruck besteht, sind aber die unmittelbar Tatverdächtigen vorzuziehen. Mehrere Tatverdächtige werden am besten gleichzeitig befragt, um Abstimmungen zwischen den Mitarbeitern zu vermeiden.

145 Die Befragungen sollten von geübten Personen durchgeführt werden, die sich auf das jeweilige Verhalten der befragten Mitarbeiter währen der Befragung schnell einstellen können. Grds. sollte auch bei Tatverdächtigen eine angenehme Gesprächsatmosphäre erzeugt werden. Dafür kann man bspw. den betroffenen Mitarbeiter bitten, den Sachverhalt aus seiner Sicht zu schildern, ohne dass man zuvor einen Vorwurf macht oder eine Beschuldigung ausspricht. Besonders wichtig ist es, bei der vor der Befragung erfolgenden Belehrung klarzumachen, dass nur die allgemeinen Verfahrensregeln zum Schutz des Mitarbeiters dargestellt werden und darin keine Vorverurteilung liegt. Abhängig von der Reaktion des Mitarbeiters kann es aber auch erforderlich sein, im Ton etwas deutlicher zu werden und dem Mitarbeiter seine Situation vor Augen zu führen.

146 Es ist empfehlenswert, die Befragungen mit zwei Ermittlern durchzuführen. Zum einen kann nicht ausgeschlossen werden, dass Tatverdächtige handgreiflich werden oder den Ermittlern drohen. Zum anderen ist es ratsam, zwei Zeugen für die Aussagen des Mitarbeiters zu haben.

b) Belehrung vor Mitarbeitergesprächen

147 Vor der Befragung, also zu Beginn des Gesprächs mit dem Mitarbeiter, muss der Mitarbeiter belehrt werden (→ § 4 Rn. 215).

148 Der Mitarbeiter ist darauf hinzuweisen, dass ein Protokoll über die Befragung erstellt wird. Insoweit ist dem Mitarbeiter zu erklären, dass das Unternehmen über das Protokoll

[75] → § 5 Rn. 64 ff.
[76] Galle BB 2018, 564 (565).
[77] Galle BB 2018, 564 (565).
[78] Galle BB 2018, 564 (565).