5. Jahrgang / Juli 2019 / Nr. 4

ZWF

Zeitschrift für Wirtschafts- und Finanzstrafrecht

Rainer Brandl | Severin Glaser | Robert Kert | Roman Leitner
Mario Schmieder | Norbert Schrottmeyer | Norbert Wess

Linde
www.lindeverlag.at

Datenschutzrechtliche Aspekte im Rahmen des „Dokumenten-Screenings" bei Internal Investigations

Katharina Dangl / Norbert Wess

Dr. Katharina Dangl ist Rechtsanwaltsanwärterin bei wkklaw Rechtsanwälte in Wien.

Dr. Norbert Wess, LL.M., M.B.L ist Rechtsanwalt und Partner bei wkklaw Rechtsanwälte in Wien.

Bei der Durchführung von Internal Investigations werden die involvierten privaten Ermittler mitunter nicht nur vor praktische, sondern auch rechtliche Herausforderungen gestellt. Technisch ist dabei oftmals mehr möglich, als rechtlich tatsächlich erlaubt ist. Hierbei ist es insb das Datenschutzrecht, das den privaten Ermittlern Grenzen auferlegt. Welche Vorgaben es konkret zu beachten gilt und wann eine Kontrollmaßnahme im Rahmen unternehmensinterner Ermittlungen zulässig ist, soll in diesem Beitrag[1] erläutert werden.

1. Grundlegendes

Internal Investigations – im deutschsprachigen Raum auch als unternehmensinterne Ermittlungen (UIE) bezeichnet – sind innerhalb eines Unternehmens durchgeführte, private Untersuchungen, die der systematischen Sachverhaltsaufklärung dienen.[2] Geführt werden sie entweder von Mitarbeitern des Unternehmens selbst oder (allenfalls auch gemeinsam) von extern beauftragten Rechtsanwalts- und/oder Wirtschaftsprüfungskanzleien und sind **anlassbezogen**, dh, sie werden bei Vorliegen eines konkreten Verdachts eines Rechts- oder Gesetzesverstoßes durchgeführt. Internal Investigations sind daher **Sonderuntersuchungen**.[3] Auch wenn sie von der Revisions- oder Compliance-Abteilung eines Unternehmens vorgenommen werden, sind Internal Investigations unabhängig von unternehmensinternen Kontrollprozessen und grundsätzlich kein Teil prozessunabhängiger Kontrollen (zB Interner Revision, Abschlussprüfung etc).[4]

Erster Schritt bei unternehmensinternen Untersuchungen ist zumeist das sog *„Dokumenten-Screening"*, bei dem sämtliches zur Verfügung stehende Datenmaterial, das mit dem zu untersuchenden Gegenstand in Zusammenhang steht, gesammelt, gesichtet und sichergestellt wird. Die internen Ermittler sind hierbei zwar nicht an die StPO und die dort normierten Schranken gebunden.[5] Dennoch haben sie eine Reihe materiellrechtlicher Grenzen zu beachten. Da es bei der Durchführung von Internal Investigations stets auch zur Verarbeitung personenbezogener Daten kommt, spielt das Datenschutzrecht eine entscheidende Rolle.

2. Allgemeines zum Datenschutzrecht

Das Datenschutzrecht ist seit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) im Mai 2018 in verschiedenen Rechtsquellen aufgesplittert: Wichtigste Rechtsquelle ist zunächst die DSGVO selbst. Daneben spielt auch das Datenschutzgesetz[6] (DSG) eine entscheidende Rolle, hier finden sich ergänzenden Regelungen zur DSGVO.

Die „Eintrittspforte" in den Anwendungsbereich der DSGVO bildet das Verarbeiten personenbezogener Daten. Unter personenbezogenen Daten versteht die DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art 4 Z 1 DSGVO). Verarbeitung meint *„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreiche im Zusammenhang mit personenbezogenen Daten"*. Als Beispiel werden in Art 4 Z 2 DSGVO etwa das Erheben, Erfassen, Organisieren, Speichern, Abfragen, Verwenden, Offenlegen etc aufgezählt. Da bei Kontrollen im Rahmen interner Untersuchungen regelmäßig personenbezogene Daten erhoben, gespeichert etc werden, sie also verarbeitet werden, liegen beide Voraussetzungen grundsätzlich vor. Am Personenbezug würde es zB bei der Verarbeitung von E-Mails mangeln, wenn die verwendete E-Mail-Adresse keiner Person eindeutig zuordenbar ist und sich

---

1 Bei diesem Beitrag handelt es sich um die erweiterte Fassung eines Vortrags der Autoren im Rahmen der Tagung „ERFA Herbst 2018" des Instituts für Interne Revision Österreich vom 8. 11. 2018.

2 Vgl zB *Zerbes*, Strafrechtliche Grundsatzfragen „interner Untersuchungen", in *Lewisch* (Hrsg), Jahrbuch Wirtschaftsstrafrecht und Organverantwortlichkeit 2013, 263 (274); *Madl*, Die Verwertung unternehmensinterner Mitarbeiterbefragungen im Strafverfahren (2018) 2; *Dangl*, Unternehmensinterne Untersuchungen (2019) 4; *Wess*, Unternehmensinterne Ermittlungen – Erfahrungen und Problemstellungen in Österreich, AnwBl 2013, 223; *Wess*, Die Privatisierung der Strafverfolgung, JSt 2014, 12.

3 *Greco/Caracas*, Internal Investigations und Selbstbelastungsfreiheit, NStZ 2015, 7; *Grützner*, Interne Ermittlungen, in *Momsen/Grützner* (Hrsg), Wirtschaftsstrafrecht (2013) Kap 4 Rz 7; *Wess*, AnwBl 2013, 223.

4 *Knyrim*, Erfordernisse und Grenzen der Internal Investigation, in *Rotsch* (Hrsg), Wissenschaftliche und praktische Aspekte der nationalen und internationalen Compliance-Diskussion (2012) 77 (79).

5 *Dangl*, Unternehmensinterne Untersuchungen, 30; *Wiederin* in *Fuchs/Ratz*, WK StPO, § 5 Rz 38.

6 Das DSG 2000 wurde durch das Datenschutz-Anpassungsgesetz 2018, BGBl I 2017/120, und das Datenschutz-Deregulierungs-Gesetz 2018, BGBl I 2018/24, weitgehend neu gestaltet.

auch nicht feststellen lässt, wer zum Zeitpunkt der Übermittlung den konkreten Computer verwendet hat.[7]

Die DSGVO kennt drei Hauptakteure: Bedeutend ist zunächst die **betroffene Person**, also jene natürliche Person, deren personenbezogene Daten verarbeitet werden sollen und auf die sich die Daten beziehen. Bei unternehmensinternen Untersuchungen ist die **betroffene Person idR der zu kontrollierende Mitarbeiter**, aber auch ein Dritter, dessen Daten verarbeitet werden (zB Daten von Mitarbeitern eines Kunden oder Kundenlisten). Daten juristischer Personen sind dem ausdrücklichen Wortlaut nach nicht umfasst; das Unternehmen selbst oder andere Unternehmen scheiden als betroffene Person aus.

Pendant zur betroffenen Person ist der **Verantwortliche**, also jene *„natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet"* (Art 4 Z 7 DSGVO).

Zuletzt kennt die DSGVO noch den **Auftragsverarbeiter** (Art 4 Z 8 DSGVO), der im Auftrag des Verantwortlichen die Daten verarbeitet.

Bei internen Untersuchungen ist das **Unternehmen als Verantwortlicher** zu qualifizieren, gleichgültig, ob es die Daten selbst verarbeitet, die Untersuchungen also intern durchgeführt werden, oder ob damit ein Auftragsverarbeiter beauftragt wird. Werden die Untersuchungen intern, zB durch die Revisionsabteilung, durchgeführt, werden die jeweiligen Mitarbeiter – obwohl „im Auftrag" des Unternehmens als Verantwortlicher – nicht als (eigenständige) Auftragsverarbeiter tätig, sondern handeln für das Unternehmen als Verantwortlicher und sind diesem zuzurechnen.[8]

Auch **Rechtsanwälte**, die vom Unternehmen mit der Durchführung der Internal Investigations betraut werden, sind idR nicht als Auftragsverarbeiter anzusehen: Aufgrund der weitreichend eigenständigen Entscheidungsbefugnis, die Rechtsanwälten gem § 9 Abs 1 RAO zukommt, sind auch sie als (zumindest gemeinsame) Verantwortliche iSd Art 4 Z 7 DSGVO anzusehen.[9]

Die DSGVO differenziert weiters zwischen verschiedenen Datenkategorien. Diese Unterscheidung spielt insb deswegen eine Rolle, weil es je nach vorliegender Datenkategorie einer unterschiedlichen Rechtfertigung für die Datenverarbeitung bedarf. So richtet sich die Rechtfertigung grundsätzlich nach Art 6 DSGVO.[10] Besonders relevant ist hierbei lit f, die eine Rechtfertigung durch Interessenabwägung ermöglicht. Handelt es sich hingegen um die in Art 9 DSGVO genannten *„besonderen Kategorien personenbezogener Daten"*, kann eine Rechtfertigung nur nach Art 9 Abs 2 DSGVO erfolgen; eine Interessenabwägung scheidet aus.

Für unternehmensinterne Untersuchungen besonders relevant sind die sog **strafrechtlich relevanten Daten**. Die Rechtfertigung richtet sich hierbei nach Art 10 DSGVO bzw § 4 Abs 3 DSG. Anders als Art 10 DSGVO, der nur von der Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln spricht, erweitert § 4 Abs 3 DSG den Anwendungsbereich auch auf personenbezogene Daten über den *Verdacht der Begehung von Straftaten*. Auch das Anstellen von Ermittlungen, um den Verdacht gegen eine bestimmte Person zu begründen, stellt eine Verarbeitung strafrechtlich relevanter personenbezogener Daten dar.[11] Bei der Abgrenzung ist auf den *Verwendungszweck* der Daten abzustellen. Es muss also danach gefragt werden, ob durch die Verarbeitung der konkrete Verdacht gegen eine bestimmte Person begründet werden soll.[12] Art 10 DSGVO bzw § 4 Abs 3 DSG gehen als *leges speciales* Art 6 und 9 DSGVO vor.[13] Auch hier ist eine Rechtfertigung durch Interessenabwägung möglich (§ 4 Abs 3 Z 2 DSG).

Bei unternehmensinternen Untersuchungen ist demnach zu differenzieren: Dienen die Untersuchungen der **Aufklärung eines strafrechtlich relevanten Verhaltens** *und* richten sie sich bereits **gegen eine bestimmte Person** oder den involvierten Personenkreis (wobei der individuelle Tatbeitrag der einzelnen Personen zur vermuteten Tat noch nicht gänzlich bekannt sein muss), handelt es sich um die *Verarbeitung strafrechtlich relevanter Daten*; die Rechtfertigung hat daher gem Art 10 DSGVO bzw § 4 Abs 3 DSG zu erfolgen. Soll durch die Untersuchungen lediglich zivil- oder arbeitsrechtswidriges Verhalten, etwa zur Geltendmachung von Schadenersatzansprüchen oder zur Aufdeckung eines Entlassungsgrundes, aufgeklärt werden oder handelt es sich bloß um generelle Er-

---

7 ZB die Adresse *office@FirmaXY.com*, die von mehreren Personen genützt wird; *Dangl*, Unternehmensinterne Untersuchungen, 81; *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsverhältnis, in *Resch* (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien 13 (25).

8 *Bergauer*, Die Rollenverteilung nach der DS-GVO – zugleich Überlegungen zu einem Übermittlungsprivileg im Konzern innerhalb enger Grenzen, jusIT 2018, 60 (63).

9 *Dangl*, Unternehmensinterne Untersuchungen, 62; aA noch zur alten Rechtslage *Feiler*, Datenschutzrechtliche Herausforderungen bei internen Compliance-Untersuchungen, in *Jahnel* (Hrsg), Jahrbuch Datenschutzrecht und E-Government 2013, 143 (158).

10 *Kastelitz*, Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten, in *Knyrim* (Hrsg), Datenschutzgrundverordnung (2016) 99 (105).

11 *Fritz*, Anwendungsbereich und Rechtfertigung – Alles neu macht die DSGVO? in *Jahnel* (Hrsg), Jahrbuch Datenschutzrecht 2016, 9 (16).

12 *Fritz* in *Jahnel*, JB Datenschutzrecht 2016, 16.

13 *Bergauer*, Personenbezogene Daten, in *Knyrim*, DSGVO, 43 (63).

mittlungen, ob überhaupt eine Straftat stattgefunden hat, richtet sich die Zulässigkeit der Verarbeitung daher nach Art 6 bzw – bei Vorliegen von Daten iSd Art 9 DSGVO – nach diesem.

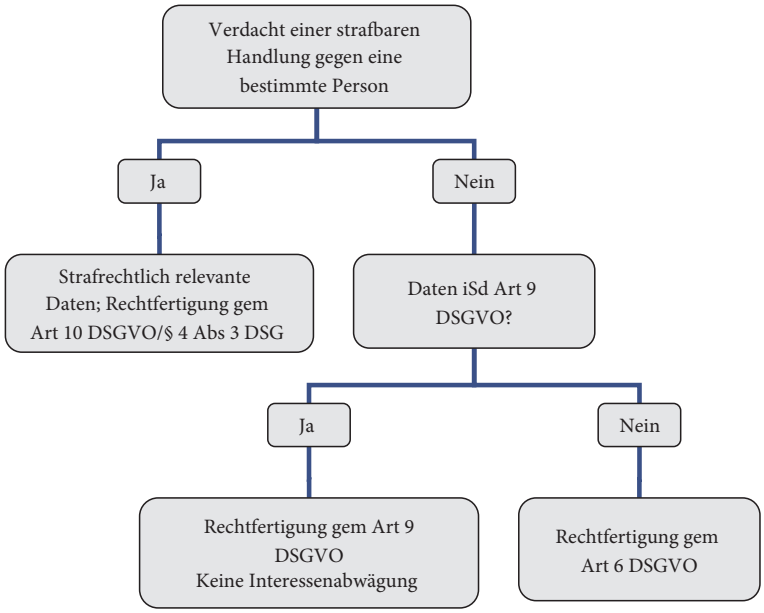

Abb 1: Entscheidungsbaum Datenschutz und Internal Investigations

3. Rechtmäßigkeit von Internal Investigations

3.1. Zweckbindung und Rechenschaftspflicht

Bei jeder Datenverarbeitung – unabhängig von der jeweiligen Datenkategorie – gilt es, die in Art 5 DSGVO genannten Grundsätze zu beachten. Für unternehmensinterne Untersuchungen bedeutsam ist insb dessen lit b, die den **Grundsatz der Zweckbindung** normiert: Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Wann eine Zweckänderung ausnahmsweise zulässig wäre, richtet sich nach Art 6 Abs 4 DSGVO. Die betroffene Person muss in die Zweckänderung entweder eingewilligt haben oder der neue Zweck mit dem ursprünglichen Zweck vereinbar sein. Sind Daten in einem Unternehmen bereits vorhanden, stellt deren (Weiter-)Verarbeitung zum Zweck interner Untersuchungen jedenfalls eine Zweckänderung dar; der neue Zweck (Aufklärung eines – möglicherweise strafrechtlich relevanten – Sachverhalts) ist aber idR nicht mit dem alten Zweck vereinbar, weshalb die (Weiter-)Verarbeitung – sofern der Arbeitnehmer und/oder Dritte als betroffene Person nicht eingewilligt haben – einer **neuerlichen Rechtfertigung** bedarf. Zu erwähnen ist auch die **Rechenschaftspflicht** gem Art 5 Abs 2 DSGVO: Gerade bei internen Untersuchungen ist die Dokumentation der Zulässigkeit der Verarbeitung, der Beachtung der Verhältnismäßigkeit und der Wahrung der schutzwürdigen Interessen besonders wichtig.[14]

3.2. Prüfschema

Internal Investigations werden durchgeführt, wenn der Verdacht besteht, ein Mitarbeiter habe gegen das Gesetz oder sonstige verbindliche Kodizes, interne Vorgaben, den Arbeitsvertrag etc verstoßen. Oftmals ist dem Unternehmen selbst oder aber der Allgemeinheit ein Schaden entstanden. Der Ablauf der Geschehnisse ist meist zumindest in groben Zügen bekannt, ebenso wie der involvierte bzw in Frage kommende Personenkreis. Die Rechtfertigung der Datenverarbeitung richtet sich gemäß den oben genannten Grundsätzen nach der Datenart und ist abhängig von der konkreten Verdachtslage und davon, ob der Verdacht einer Straftat oder (bloß) eines sonstigen (zB zivilrechtlichen) Rechtsverstoßes besteht.

Vor einer Verarbeitung personenbezogener Daten haben die privaten Ermittler folgende Prüfschritte zu beachten:

- Zu welchem **Zweck** soll die Verarbeitung erfolgen / welches Ziel hat die Verarbeitung?
- Welche **Daten (Datenkategorien)** sollen verarbeitet werden?[15]
  - Besteht ein begründeter konkreter Verdacht gegen eine bestimmte Person oder Personengruppe (zB aufgrund ihrer Funktion im Unternehmen)?

[14] Daneben trifft das Unternehmen als Verantwortlicher noch eine Reihe weiterer Pflichten, zB eine Informationspflicht der betroffenen Person gegenüber (Art 13 ff DSGVO) oder – im Fall eines *data breach* – die Pflicht zur Meldung an die Datenschutzbehörde bzw zur Information der von der Verletzung des Schutzes personenbezogener Daten betroffenen Personen (Art 33, 34 DSGVO).

[15] Vgl Entscheidungsbaum oben.

  - Besteht der Verdacht einer Straftatbegehung?
  - Falls nein: Handelt es sich um eine besondere Kategorie von Daten gem Art 9 DSGVO?
- Welche **Interessen** hat das Unternehmen als Verantwortlicher an der Verarbeitung?
- Bestehen besondere, schutzwürdige **Interessen der betroffenen Person**, die den Interessen des Unternehmens überwiegen?
- Sind die Daten zur Erreichung des Ziels **geeignet** *und* **erforderlich**?
- Handelt es sich um das **gelindeste Mittel**?

3.3 Anwendungsbeispiel: E-Mail-Screening

Veranschaulicht werden soll die weitere Prüfung am sog *E-Mail-Screening*. Darunter wird die systematische Kontrolle und Durchsicht aller ein- und ausgehenden E-Mails der Mitarbeiter in Hinblick auf ein bestimmtes Verdachtsmoment verstanden.[16] E-Mails enthalten grundsätzlich personenbezogene Daten des Senders sowie des Empfängers.[17] Ergeben können sich solche entweder aus Nutzungs-[18] oder Inhaltsdaten.[19] Bei der Rechtfertigung der konkreten Maßnahme muss in weiterer Folge danach unterschieden werden, ob die Privatnutzung des E-Mails-Accounts untersagt oder erlaubt ist.

3.3.1. Verbot privater Nutzung

Ist die Nutzung des beruflichen E-Mail-Accounts (auch) zu Privatzwecken untersagt, bedeutet dies zwar keineswegs, dass der Arbeitgeber nunmehr schrankenlos kontrollieren dürfte. Das Grundrecht des Arbeitnehmers auf Datenschutz bleibt trotz Verbots weiterhin bestehen.[20] Der Arbeitgeber darf jedoch davon ausgehen, dass sämtliche E-Mails der Arbeitnehmer nur dienstlichen Inhalts sind und somit – im Regelfall[21] – keine Daten iSd Art 9 DSGVO der betroffenen Person enthalten.[22]

Die Rechtfertigung der Datenverarbeitung hat daher – je nach Verdachtslage und damit zusammenhängend nach Datenkategorie – nach Art 6 DSGVO oder § 4 Abs 3 DSG zu erfolgen. In beiden Fällen kann die Rechtfertigung mittels **Interessenabwägung** erfolgen (Art 6 Abs 1 lit f DSGVO bzw § 4 Abs 3 Z 2 DSG):[23] Die Verarbeitung ist gerechtfertigt, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Ausreichend zur Rechtfertigung ist demnach bereits ein Interessengleichstand.[24]

Als berechtigtes Interesse des Arbeitgebers steht bei Internal Investigations die Sachverhaltsaufklärung im Vordergrund, zB um einen vom Arbeitnehmer gesetzten Entlassungsgrund offenzulegen. Auch das Interesse des Unternehmens an der Aufklärung von (Wirtschafts-)Straftaten kann in die Beurteilung miteinbezogen werden.[25] Entgegenstehendes Interesse bzw Grundrecht des Arbeitnehmers ist dessen Recht auf Privatsphäre sowie auf den Schutz seiner personenbezogenen Daten, während das Interesse, nicht einer Straftat überführt zu werden, mangels Schutzwürdigkeit nicht zu berücksichtigen ist.

Die **konkrete Rechtfertigung** ist zwangsläufig eine Einzelfallentscheidung, bei der verschiedenste Faktoren Berücksichtigung finden müssen: die Schwere der aus dem Fehlverhalten resultierenden Folgen für das Unternehmen, wobei auch mittelbare Folgen zu berücksichtigen sind; die Intensität des Verdachts, die Wahrscheinlichkeit, dass die Maßnahme neue Anhaltspunkte zutage fördert; der Umfang der zu verarbeitenden Daten; der zu untersuchende Zeitraum etc. Auch wiegt ein Eingriff in den Inhalt der E-Mails bedeutend schwerer als lediglich in die Verkehrsdaten.

Wurde die Privatnutzung untersagt, so wird die Interessenabwägung – insb vor dem Hintergrund, dass Interessengleichstand zur Rechtfertigung ausreichend ist – im Normalfall **zugunsten**

---

16 *Scharnberg*, Illegale Internal Investigations (2014) 124; *Dangl*, Unternehmensinterne Untersuchungen, 81.

17 *Burtscher*, Datenschutzrechtliche Aspekte bei Internal Investigations, in *Kustor* (Hrsg), Unternehmensinterne Untersuchungen (2010) 89 (95); *Brodil*, Die Kontrolle der Nutzung neuer Medien im Arbeitsverhältnis, ZAS 2004, 156 (157); *Kotschy/Reimer*, ZAS 2004, 167; *Rebhahn*, Mitarbeiterkontrolle am Arbeitsplatz (2009) 17.

18 Alle äußeren Daten, wie zB Angaben über Absender und Empfänger der E-Mail oder den Zeitpunkt sowie die Dauer der Verbindung.

19 Jene Informationen, die sich aus der E-Mail selbst ergeben.

20 *Kotschy/Reimer*, ZAS 2004, 168; so auch *Hattenberger* in *Resch*, Kontrolle, 13 (56).

21 Sofern es sich nicht um einen Arbeitsplatz handelt, bei dem die Verarbeitung besonderer Kategorien von Daten zum allgemeinen Geschäftsbetrieb gehört, zB in Krankenhäusern etc.

22 *Sacherer*, Datenschutzrechtliche Aspekte der Internetnutzung von Arbeitnehmern, RdW 2005, 173; *Gandjova/Mair/Müller*, (Computer-)forensische Untersuchungen – Status quo und Trends, in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht (2016) Kap 27 Rz 71.

23 Grundsätzlich könnte die Verarbeitung auch durch Einwilligung gerechtfertigt werden; vgl jedoch zur Frage der hierfür erforderlichen Voraussetzung der Freiwilligkeit *Braun/Hasenauer*, Die Rechtmäßigkeit der Verarbeitung gemäß Art 6 DSGVO in JB Datenschutzrecht 2018, 9 (19), sowie *Dangl*, Unternehmensinterne Untersuchungen, 66.

24 *Fercher/Riedl*, DSGVO: Entstehungsgeschichte und Problemstellung aus österreichischer Sicht, in *Knyrim*, DSGVO, 7 (20); *Fritz* in *Jahnel*, JB Datenschutzrecht 2016, 29.

25 ErwGr 47 DSGVO.

des Arbeitgebers bzw des **Unternehmens** ausfallen und die **Datenverarbeitung daher zulässig** sein, sofern es sich hierbei um das gelindeste Mittel handelt.

Sollte bei der Durchführung der internen Untersuchungen doch private Korrespondenz gefunden werden, ist deren Verarbeitung im Regelfall mangels berechtigten (Kontroll-)Interesses untersagt. Im Einzelfall jedoch kann auch hier die Interessenabwägung zugunsten des Unternehmens ausfallen; etwa wenn bereits ein konkreter, starker Verdacht gegen einen bestimmten Mitarbeiter vorliegt, es sich also um das Verarbeiten strafrechtlich relevanter Daten handelt, und die Durchsuchung durchgeführt wird, um die Ermittlungsergebnisse zur Vorlage als Beweismittel in einem staatlichen Verfahren verwenden zu können. Dies ergibt sich aus einem Vergleich der Rechtfertigung strafrechtlich relevanter Daten mit den besonderen Datenkategorien des Art 9 DSGVO: So entfalten die in Art 9 Abs 2 DSGVO aufgezählten Rechtfertigungsgründe Indizwirkung auch auf die im Rahmen von § 4 Abs 3 Z 2 DSG vorzunehmende Interessenabwägung: Der Verordnungsgeber hat in Art 9 DSGVO taxativ Gründe aufgezählt, die sogar die Verarbeitung besonders schutzwürdiger Daten rechtfertigen. Die hier genannten Gründe sind nun aber wohl jedenfalls ein **berechtigtes Interesse iSd Art 6 Abs 1 lit f DSGVO**, auf den § 4 Abs 3 Z 2 DSG wiederum verweist. Liegt daher ein **in Art 9 DSGVO aufgezählter Fall** vor, ist **von einem berechtigten Interesse des Verantwortlichen auszugehen**; ein entgegenstehendes Interesse der betroffenen Person, das eine Rechtfertigung in solchen Fällen verhindern könnte, wird wohl **nur in Ausnahmefällen denkbar** sein.[26]

Auch hier muss es sich aber um das **gelindeste Mittel** handeln: Gerechtfertigt ist die Verarbeitung daher nur, wenn die Durchsicht der privaten E-Mails unbedingt notwendig ist, um den vorliegenden Verdacht der Begehung einer Straftat durch den konkreten Mitarbeiter zu bestätigen, etwa weil sich nur hieraus Rückschlüsse auf das (straf)rechtswidrige Verhalten ziehen lassen.

3.3.2. Zulässige Privatnutzung

Ist die Privatnutzung des E-Mail-Accounts hingegen zulässig (oder fehlt es an einer entsprechenden Vereinbarung), kann im Gegensatz zum bisher Ausgeführten nicht ausgeschlossen werden, dass bei der Kontrolle der E-Mails auch personenbezogene Daten iSd Art 9 DSGVO des Arbeitnehmers (oder Dritter) zutage gefördert werden. Es muss daher stets der strengere Rechtfertigungsmaßstab des Art 9 DSGVO angewendet werden,[27] sofern es sich nicht gleichzeitig auch um strafrechtlich relevante Daten handelt.

Die Verarbeitung besonderer Kategorien von Daten kann im Fall interner Untersuchungen insb gerechtfertigt sein, wenn die **Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen** oder bei Handlungen der Gerichte in ihrer gerichtlichen Eigenschaft erforderlich ist (Art 9 Abs 2 lit f DSGVO) oder eine entsprechende Betriebsvereinbarung vorliegt (Art 9 Abs 2 lit b DSGVO).[28] Eine **Interessenabwägung scheidet** jedoch **aus**.

Wie festgehalten, wird es sich bei der Durchführung interner Untersuchungen zumeist jedoch ohnehin um die **Verarbeitung strafrechtlich relevanter Daten** handeln; auch hier ist die Rechtfertigung somit durch Interessenabwägung möglich: Ist die Privatnutzung zulässig, wird der Arbeitnehmer üblicherweise ein besonders hoch zu bewertendes Interesse am Schutz seiner Daten und an Geheimhaltung haben. Gleichzeitig handelt es sich aber um einen strafrechtlich relevanten Vorfall – auch das Interesse des Unternehmens auf Sachverhaltsaufklärung wird ungleich höher zu bewerten sein. Es gilt wiederum: **Interessengleichstand ist zur Rechtfertigung ausreichend.**

Auch hier variiert das Ergebnis naturgemäß. Regelmäßig wird man im Rahmen der vorzunehmenden Interessenabwägung zu dem Ergebnis kommen, dass der Zugriff auf die *Nutzungsdaten* idR sowohl bei dienstlichen als auch bei privaten E-Mails zulässig ist. Im Gegensatz dazu beschränkt sich der Zugriff auf *Inhaltsdaten* im Regelfall auf dienstliche E-Mails, wogegen es grundsätzlich unzulässig ist, auf die Inhaltsdaten privater Kommunikation zuzugreifen.[29]

In der Praxis empfiehlt es sich, Mitarbeiter – im Idealfall im Beisein einer Vertrauensperson des Unternehmens oder eines Mitglieds des Betriebsrats – vor der Durchsuchung zu beauftragen, alle privaten E-Mails auszusortieren und/oder zu löschen, sofern private E-Mails nicht ohnehin stets als *„privat"* zu kennzeichnen sind.[30] Dem Ermittlungsteam ist aber stichprobenartige Einsicht in die als *„privat"* gekennzeichneten Dateien zu gewähren, um zu überprüfen, ob sich hinter einem harmlos erscheinenden Betreff nicht vielleicht doch relevante Informationen für die Untersuchung verbergen.[31] Dieses Vorgehen ist gem § 4 Abs 3 DSG iVm Art 6 Abs 1 lit f DSGVO jedenfalls gerechtfertigt und stellt das gelindeste Mittel dar.

Haben sich die internen Ermittler bei der Überprüfung der Inhaltsdaten daher grundsätzlich auf dienstliche E-Mails zu beschränken, so kann gerade bei Untersuchungen, die der Aufklärung eines

---

26 *Dangl*, Unternehmensinterne Untersuchungen, 85.
27 Sog potenziell-sensible Daten: *Jahnel*, Datenschutzrecht, Rz 3/97.
28 *Dangl*, Unternehmensinterne Untersuchungen, 70, 89.
29 *Brodil*, ZAS 2004, 156 (161).
30 Diese wären in Folge von der Durchsuchung auszunehmen; *Kristoferitsch* in *Lewisch*, JB Wirtschaftsstrafrecht 2013, 291.
31 *Kristoferitsch* in *Lewisch*, JB Wirtschaftsstrafrecht 2013, 292.

strafrechtswidrigen Verhaltens eines Mitarbeiters dienen, bei Vorliegen einer besonderen Verdachtslage auch der **Einblick in private Korrespondenz gerechtfertigt** sein, da in diesem Fall das Interesse des Mitarbeiters auf Geheimhaltung die Interessen des Arbeitgebers nicht überwiegt.[32] Dies etwa bei Verdacht auf Verrat eines Geschäfts- oder Betriebsgeheimnisses, sofern anzunehmen ist, dass nur aus den privaten E-Mails eine Aufklärung zu erwarten ist, und hiermit Rechtsansprüche vor Gericht geltend gemacht werden sollen (vgl Pkt 3.3.1.).

3.4. Dokumentation

In jedem Fall kommt der umfassenden Dokumentation der gesamten Untersuchung entscheidende Bedeutung zu: So ist nicht nur die Verdachtslage zu dokumentieren, insb warum von einem strafrechtlich relevanten Vorfall ausgegangen werden muss, sondern auch zu begründen, warum und durch welche analytischen Schritte eine Aufklärung auf Verdächtigtenebene zu erfolgen hat. Festzuhalten ist auch, wie und welche Interessen des Unternehmens betroffen sind, welche Schäden bereits entstanden sind oder zu entstehen drohen und wie diese durch die Untersuchung hintangehalten werden können. Zuletzt sollten auch die Überlegungen zur Verhältnismäßigkeit festgehalten werden.[33]

3.5. Sonderfall: präventive Sonderuntersuchungen

Von Sonderuntersuchungen iS unternehmensinterner Untersuchungen als repressive Maßnahme zu unterscheiden sind präventive Untersuchungen, etwa präventive Analysen von Risikogebieten iS einer **forensischen Due Diligence**. Da die Interessen des Unternehmens als Verantwortlicher der Datenverarbeitung hier deutlich geringer und jene der Arbeitnehmer auf Geheimhaltung umso höher einzustufen sind, lässt sich das eben Ausgeführte nur bedingt übertragen. Es empfiehlt sich, die zu verarbeitenden personenbezogenen Daten zu anonymisieren bzw pseudonymisieren (also in einer Weise zu verarbeiten, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können) und sich auf Stichprobenkontrollen zu beschränken. Erst bei ausreichend dringender Verdachtslage sollte eine Wiederherstellung der Verknüpfung zum konkreten Personenbezug erfolgen.[34]

► Auf den Punkt gebracht

Kommt es im Rahmen unternehmensinterner Untersuchungen zur Verarbeitung personenbezogener Daten, so hängt deren Rechtfertigung maßgeblich von der Verdachtslage sowie davon ab, ob sich der Vorwurf auf strafbares Verhalten bezieht. Werden interne Untersuchungen wegen des (konkreten) Verdachts einer strafbaren Handlung durchgeführt, handelt es sich um die Verarbeitung strafrechtlich relevanter Daten – eine Rechtfertigung ist im Wege einer Interessenabwägung möglich. Die Ausführungen zeigen, dass die Verarbeitung personenbezogener Daten aus dienstlichen E-Mails und Dokumenten idR zulässig ist, die Verarbeitung personenbezogener Daten aus privaten Unterlagen oder Kommunikation hingegen bloß in Einzelfällen.

Ist der Verdacht einer strafbaren Handlung hingegen noch zu unbestimmt, um von strafrechtlich relevanten Daten zu sprechen, oder steht lediglich ein anderer (zivilrechtlicher) Rechtsverstoß im Raum, muss zwischen der Erlaubnis zur privaten Nutzung und einem privaten Nutzungsverbot unterschieden werden: Besteht ein Nutzungsverbot, kann der Arbeitgeber im Normalfall davon ausgehen, dass es sich bei den zu verarbeitenden Daten lediglich um *„allgemeine"* Daten iSd Art 6 DSGVO handelt, die der Rechtfertigung durch Interessenabwägung zugänglich sind. Ist die private Nutzung jedoch erlaubt, kann das Vorliegen von Daten von besonderer Kategorie iSd Art 9 DSGVO nicht ausgeschlossen werden; es muss zur Rechtfertigung einer der in Art 9 Abs 2 DSGVO explizit genannten Gründe vorliegen: Die internen Untersuchungen müssen daher entweder durchgeführt werden, um einen Rechtsanspruch durchzusetzen, oder es ist eine entsprechende Betriebsvereinbarung erforderlich.

---

32 So auch *Determann/Hitz*, Die private Nutzung von Internet und E-Mail, ASoK 2019, 53 (54).

33 Zur Frage, ob derartige Dokumentationen, ebenso wie auch der – uU anwaltlich angefertigte – Endbericht in Folge von den Strafverfolgungsbehörden sichergestellt werden können, vgl *Wess*, JSt 2014, 12 (12 ff).

34 Vgl auch *Institut für Interne Revision Österreich*, Leitfaden zum Datenschutz in der Internen Revision (2018) 85 f.

Linde
Zeitschriften

Linde

Auch online verfügbar:
lindedigital.at

Starten Sie gut ins neue Jahr!

ZWF-Jahresabo 2020
(6. Jahrgang, Heft 1–6)

€ 201,60*
statt € 252,–*

Jetzt Jahresabo 2020 bestellen und 20 % sparen!

Bestellformular
Ja, ich bestelle

ZWF-Jahresabo 2020
(6. Jahrgang 2020, Heft 1-6)

EUR 201,60
statt EUR 252,–

Name/Firma

Kundennummer

Straße/Hausnr.

PLZ/Ort

E-Mail/Telefon

Datum/Unterschrift

○ Ich stimme zu, dass die Linde Verlag GmbH meine angegebenen Daten für den Versand von Newslettern verwendet. Diese Einwilligung kann jederzeit durch Klick des Abbestelllinks in jedem zugesendeten Newsletter widerrufen werden.

Linde Verlag Ges.m.b.H
Scheydgasse 24, 1210 Wien
Handelsgericht Wien
FB-Nr: 102235X, ATU 14910701
DVR: 000 2356

Jetzt bestellen! lindeverlag.at, office@lindeverlag.at, T 01 24 630, F 01 24 630-23