



Dr. Ferdinand Graf, LL.M. (N.Y.U.)/Dr. Ruth Riesenhuber
Graf & Pitkowitz Rechtsanwälte GmbH

■ jusIT 2009/72, 143

Whistleblowing-Hotline: Bescheid der DSK zu GZ K178.274/0010-DSK/2008 vom 5. 12. 2008 – Einige gelöste, viele offene Fragen

Am 5. 12. 2008 hat die Datenschutzkommission (in der Folge kurz „DSK“) eine richtungsweisende Entscheidung im Zusammenhang mit sog Whistleblowing-Hotlines getroffen. Der Inhalt dieser Entscheidung wird im Folgenden kurz dargestellt und die damit einhergehenden datenschutzrechtlichen Fragen näher erörtert.

Deskriptoren: Datenschutzrecht, Whistleblowing-Hotline, SOX, Übermittlung und Überlassung von Daten in das Ausland, Finanzdaten, Vorabkontrolle, Art 29 Datenschutzgruppe

Normen: DSG 2000: §§ 8, 10, 12, 13

1. Sachverhalt und Tenor der Entscheidung

In ihrer Entscheidung vom 5. 12. 2008 hat sich die DSK eingehend mit den datenschutzrechtlichen Aspekten von „Whistleblowing-Hotlines“ befasst.¹⁾ Unter einer „Whistleblowing-Hotline“ wird üblicherweise ein Meldesystem verstanden, das Mitarbeitern eines Unternehmens die Möglichkeit gibt, über mutmaßliche Missstände, insbesondere im Bereich der Rechnungslegung und Bilanzierung, an eine eigens eingerichtete (unternehmensinterne oder externe) Stelle zu berichten.²⁾

Im Entscheidungssachverhalt wurde der Genehmigungsantrag von einer GmbH mit Sitz in Wien gestellt („Antragstellerin“), die Teil eines internationalen Konzerns war, dessen Konzernspitze in den USA niedergelassen war. Entsprechend den Vorgaben nach US-Bundesrecht im

*Sarbanes-Oxley-Act*³⁾ (in der Folge kurz: „SOX“) war in diesem Konzern die Einrichtung einer Whistleblowing-Hotline vorgesehen. Nach dem Konzept der Antragstellerin konnten die Mitarbeiter ihre Beschwerden über Telefon und Internet (in der Folge kurz „Hotline“) bei einem von der Konzernspitze beauftragten, ebenfalls in den USA domizilierten Unternehmen (in der Folge kurz „Hotline-Betreiberin“) erheben. Daten aus dem Anwendungsbereich des SOX (in der Folge kurz „Finanzdaten“), also von Meldungen über Missstände aus den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität (in der Folge kurz „schwere Verstöße“⁴⁾), sollten von der Hotline-Betreiberin an die Konzernspitze weitergeleitet werden, die die „Aufarbeitung“ der Sachverhalte selbst vornehmen sollte. Meldungen über andere Missstände (in der Folge kurz „leichte Verfehlungen“) sollten von der Hotline-Betreiberin zwar ebenfalls an die Konzernspitze weitergeleitet werden, diese

sollte die gemeldeten Daten (in der Folge kurz „sonstige Daten“) aber nur für die betroffene Konzerngesellschaft speichern und dieser zur Verfügung stellen.

Die Antragstellerin beantragte gem § 13 Abs 1 und 2 DSG 2000 eine Genehmigung zur Übermittlung und zur Überlassung von personenbezogenen Mitarbeiter-Daten aus einer registrierten Datenanwendung⁵⁾ in die USA. Die Genehmigung wurde – unter Auflagen und einer aufschiebenden Bedingung – teilweise erteilt und teilweise abgewiesen. Genehmigt wurde die Datenübermittlung an die Konzernspitze und zwar hinsichtlich bestimmter Daten von Entscheidungsträgern, über die im Wege der Hotline schwere Verstöße gemeldet wurden, sowie hinsichtlich bestimmter Daten von Mitarbeitern, die eine Meldung erstattet haben. Neben einigen Auflagen wurde die Genehmigung unter die aufschiebende Bedingung gestellt, dass mit der Betreiberin der Hotline eine Dienstleistervereinbarung mit einem bestimmten Mindestinhalt getroffen, und dass für die Überlassung der Daten an die Hotline-Betreiberin eine entsprechende

1) S zu dieser Entscheidung auch DSK-Datenpost, Newsletter Nr 6/Dezember 2008 Pkt 5; König, Entscheidungsübersicht Datenschutzkommission – Dezember 2008 bis Jänner 2009, jusIT 2009/12, 25; Leissler, „Whistleblowing“ in Österreich – die ersten Schritte..., ecolex 2009, 361; Spring, „Whistleblowing-Hotlines“, ecolex 2009, 363; Reis, Zur Zulässigkeit von Whistleblowing-Hotlines, RdW 2009, 396.

2) Zum Begriff der Whistleblowing-Hotline s insb Lehner, Whistleblowing-Hotlines gemäß SOX, in: Jahnell/Siegwart/Fercher (Hrsg), Aktuelle Fragen des Datenschutzrechts 149.

3) Sarbanes-Oxley Act of 2002, Pub.L. 107-204, 116 Stat. 745, in Kraft seit 30. Juli 2002; abrufbar auf http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ204.107.

4) Die Bezeichnung als „schwere Verstöße“ bzw „leichte Verfehlungen“ erfolgt in Anlehnung der Bezeichnungen in der DSK-Entscheidung.

5) Die Bezeichnung der registrierten Datenanwendung lautete „Internes Verfahren zur Erfassung von Meldungen über mutmaßliche Missstände im Unternehmen in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität“.

Genehmigung eingeholt wird. Im Übrigen wurde der Antrag abgewiesen. Von der Abweisung betroffen sind sohin insb. Meldungen über mögliche Vergehen von anderen Personen als „Entscheidungssträgern“.

2. Kritische Analyse der Entscheidung

2.1. Einteilung in Übermittlung und Überlassung

Die DSK stellt klar, dass es sich bei der Aufzeichnung der Meldungen durch die Hotline-Betreiberin um eine Dienstleistung für die Antragstellerin handelt. Der Datenaustausch zwischen der Antragstellerin und der Hotline-Betreiberin stellt sohin eine Datenüberlassung iSd § 4 Z 11 DSGVO dar.

Die Qualifikation des Austauschs von Daten über schwerwiegende Verstöße zwischen der Antragstellerin und der Konzernspitze als Datenübermittlung iSd § 4 Z 12 DSGVO wird in der Entscheidung nicht infrage gestellt, sondern stillschweigend als gegeben vorausgesetzt.⁶⁾ Die Übermittlung erfolgt rechtlich gesehen von der Antragstellerin an die Konzernspitze, technisch gesehen jedoch über die Hotline-Betreiberin, die die Daten nur an die Konzernspitze weiterleitet, sodass eine gesonderte Beurteilung der Weiterleitung von der Hotline-Betreiberin an die Konzernspitze nicht erfolgte. In Bezug auf die weitere Verwendung der Daten heißt es im Sachverhalt lediglich, dass Meldungen über schwere Verstöße von der Konzernspitze selbst weiterbearbeitet werden. Genauere Angaben zur Verwendung der Daten durch die Konzernspitze sind im Sachverhalt nicht enthalten. Aus der unterstellten Qualifikation als Datenübermittlung und der diesbezüglichen Definition resultiert jedoch, dass der Konzernspitze gewisse Entscheidungsbefugnisse im Hinblick auf die Verwendung der Daten zukommen.⁷⁾

Meldungen, die leichte Verfehlungen betreffen, sollen hingegen – nach den

Sachverhaltsangaben in der Entscheidung – von der Konzernspitze lediglich gespeichert werden und sodann nur den betreffenden Tochterunternehmen zur weiteren Bearbeitung zur Verfügung stehen. Daraus folgt, dass der diesbezügliche Datenaustausch – wieder zwischen Antragstellerin und Konzernspitze, funktional durchgeführt durch die Hotline-Betreiberin – als Überlassung iSd § 4 Z 11 DSGVO zu qualifizieren ist. Auch dies wird in der Entscheidung lediglich angenommen und nicht näher thematisiert.⁸⁾

2.2. Unternehmen als Auftraggeber

Die DSK führt in der Entscheidung zutreffend aus, dass die Mitarbeiter bei derartigen Meldungen letztlich in Erfüllung der für sie verpflichtenden unternehmensinternen Verhaltensregeln tätig werden. Die Meldungen sind ihnen deshalb nicht als Privatperson sondern als Organ des Unternehmens zuzurechnen, sodass datenschutzrechtlich handelndes Rechtssubjekt das Unternehmen ist. Daher ist der Antragstellerin die Eigenschaft eines Auftraggebers zuzuerkennen und zwar sowohl im Hinblick auf die Übermittlung der Daten an die Konzernspitze als auch im Hinblick auf die Überlassung der Daten an die Hotline-Betreiberin.⁹⁾

2.3. Datenüberlassung an die Konzernspitze

Die DSK beruft sich bei der Beurteilung der Rechtsgrundlage nicht auf den SOX, da ausländische Bestimmungen nicht als Rechtsgrundlage für eine Datenanwendung nach österreichischem Recht

herangezogen werden können.¹⁰⁾ Die Zulässigkeit einer Überlassung richtet sich daher nach § 8 Abs 1 Z 4 DSGVO.

Im Vergleich zu einer Übermittlung ist die Missbrauchsgefahr bei Überlassungen aufgrund der eingeschränkten Verwendungsbefugnis der Konzernspitze, welche die Daten ja bloß speichern soll, – zumindest schuldrechtlich – eingeschränkt. Dennoch ist für den Bedarf einer Überlassung der sonstigen Daten an die Konzernspitze im Entscheidungssachverhalt kein sachlich nachvollziehbarer Grund ersichtlich. Im Gegenteil: Wenn diese Daten von der Hotline-Betreiberin an die Konzernspitze weitergeleitet werden sollen, um dort ausschließlich gespeichert und sodann an das betreffende Tochterunternehmen weitergeleitet zu werden, so muss die Hotline-Betreiberin ohnehin zuvor eine Einordnung dahingehend vornehmen, ob die Meldung schwere Verstöße oder leichte Verfehlungen betrifft. Andernfalls wäre die Konzernspitze gezwungen, die Daten nicht nur zu speichern, sondern diese auch abzurufen, um die Einordnung selbst vorzunehmen. Die Überlassung dieser Daten an die Konzernspitze erscheint daher entbehrlich. Im Sinne der allgemeinen Grundsätze des Datenschutzrechtes, insbesondere der Grundsätze der Sparsamkeit und Verhältnismäßigkeit, ist daher von dieser Datenanwendung abzusehen. Insofern ist der Entscheidung der DSK beizupflichten.

2.4. Datenübermittlung an die Konzernspitze

2.4.1. Umfang der Entscheidung und Rechtsgrundlage

Die Prüfung der Zulässigkeit der Datenübermittlung beschränkt sich in der gegenständlichen Entscheidung entsprechend der Antragstellung auf die Übermittlung von Finanzdaten an die Konzernspitze. Gem § 12 Abs 5 DSGVO ist Voraussetzung für die Zulässigkeit der geplanten Übermittlung die Rechtmäßigkeit der Datenanwendung im Inland gem § 7 Abs 2 DSGVO. Die DSK führt aus, dass Daten nur übermittelt werden dürfen, wenn

- sie aus einer zulässigen Datenanwendung stammen;
- die rechtliche Befugnis des Empfängers für eine derartige Übermittlung ausreichend glaubhaft ist und

6) Vgl etwa Pkt.1.3 oder die Überschrift von Pkt 3.2b.

7) Dies ergibt sich daraus, dass eine Übermittlung gem § 4 Z 12 DSGVO nur vorliegt, wenn Daten weitergegeben werden an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister. Die Konzernmutter ist jedenfalls weder Betroffene noch die Auftraggeberin der gegenständlichen Datenübermittlung. Von einem Dienstleister unterscheidet sie sich aber nur dann, wenn ihr Entscheidungsbefugnisse in Bezug auf die Verwendung der Daten zukommen. Vgl hierzu *Knyrim*, Datenschutzrecht (2003) 18 ff, 189 ff.

8) Vgl etwa Pkt 1.4 oder die Überschrift von Pkt 3.2c.

9) Insb dieser Punkt der Entscheidung wird von *Leissler*, *ecolox* 2009, 361 kritisiert, der der Meinung ist, dass – mangels Kontrolle über die Hotline – nicht die Antragstellerin, sondern die Konzernspitze als Auftraggeber anzusehen sei. Dies würde in der Folge dazu führen, dass kein Fall der Datenübermittlung zwischen Auftraggebern, sondern nur eine Datenermittlung durch die US Konzernspitze in Österreich vorliegen würde. Unserer Ansicht nach spricht aber viel dafür, dass die österreichische Konzerngesellschaft als Auftraggeber anzusehen ist, da nur sie – durch Ausübung ihres Weisungsrechtes – in der Lage ist, die Mitwirkung ihrer Mitarbeiter an der Hotline zu ermöglichen; sie ist es auch, die – jedenfalls nach dem Konzept der DSK – gegenüber der Hotline-Betreiberin die Grenzen der Datenverwendung (auch in Bezug auf die Weitergabe an die Konzernspitze) vorgibt. Ob diese Grenzen in der Umsetzung tatsächlich eingehalten werden – also die österreichische Gesellschaft als „Herrin der Daten“ akzeptiert wird – ist allerdings eine andere Frage.

10) S § 8 Abs 1 Z 1 DSGVO; vgl hierzu *Lehner* in: *Jahnel/Sieglwart/Fercher* (Hrsg), *Aktuelle Fragen des Datenschutzrechts* 149; *Dohr/Pollierer/Weiss*, *DSG* § 8 Anm 5.

- die Übermittlung iSd §§ 8, 9 DSGVO ihrer Art nach auch im Inland zulässig wäre.

Zum überwiegenden berechtigten Interesse iSd § 8 Abs 1 Z 4 DSGVO führt die DSK aus, dass im Umfang der Meldung von schweren Verstößen, die Mitarbeitern der Antragstellerin in Führungspositionen angelastet werden, das überwiegende berechnete Interesse an der Übermittlung an die Konzernspitze anerkannt werde.

2.4.2. Beschränkung auf „Entscheidungsträger“ greift zu kurz

Die Beschränkung der von der DSK erteilten Genehmigung in Bezug auf Finanzdaten resultiert bereits aus dem Antrag. Die Beschränkung auf vermutete Vergehen von Entscheidungsträgern war von der Antragstellerin hingegen nicht vorgesehen. In der Sachverhaltsdarstellung wird eine Aussage aus dem Antrag zitiert, wonach schwere Verstöße „vor allem Entscheidungsträger des Antragstellers betreffen.“ Weiters wird dort die Antragstellerin wie folgt zitiert:

„In solchen Fällen ist es natürlich nicht angebracht, dass diese Personen gegen sich selbst Maßnahmen aussprechen. Aus diesem Grund obliegt die Entscheidungsgewalt der Konzernspitze.“

In der Begründung heißt es dann, die Antragstellerin habe selbst Argumente in ihrem Antrag vorgebracht, die erkennen lassen würden, dass ein überwiegendes berechtigtes Interesse dann bestehe, wenn schwere Verstöße durch Entscheidungsträger vorliegen. In diesem Umfang werde das überwiegende berechnete Interesse anerkannt, da nur auf diese Weise mit hinlänglicher Sicherheit eine objektive Aufklärung der erhobenen Vorwürfe zu erwarten sei. Unserer Ansicht nach ist ein berechtigtes Interesse aber nicht nur bei vermuteten Vergehen von Entscheidungsträgern gegeben.

2.4.2.1. Nicht die Person des „Täters“ sondern das „Delikt“ muss aus Sicht der Konzernspitze relevant sein

Das von der DSK gewählte Unterscheidungskriterium ist bereits der Art nach ungeeignet. Objektiv betrachtet hat die Konzernspitze zweifellos an der Kenntniserlangung von schweren Verstößen – unabhängig davon, von wem sie begangen werden – ein berechtigtes Interesse. Auf diesen systematischen Fehler der Entscheidung hat bereits *Spring* zu Recht verwiesen.¹¹⁾

2.4.2.2. Ein überwiegendes berechtigtes Interesse besteht an einem einheitlichen System der „Aufklärung“

Durch eine „Whistleblowing-Hotline“ soll für den Einzelnen eine transparente und durch ihm bekannte Verfahrensgarantien abgesicherte Möglichkeit geschaffen werden, erkannte Unregelmäßigkeiten zu melden. Wer der eigentliche Urheber der Unregelmäßigkeit ist bzw mit wem dieser kooperiert, wird für einen zur Meldung bereiten Mitarbeiter nicht immer klar sein. Bürdet man nun dem Mitarbeiter, der bereit ist, den – in vielen Fällen nicht leichten – Schritt zur Meldung zu gehen, auch noch die Last der Beurteilung auf, welcher Mechanismen er sich bedienen muss (direkte Meldung an den Vorgesetzten, wenn der Täter voraussichtlich keine Führungskraft ist, oder Hotline, wenn eine Führungskraft betroffen ist), so wird dies oft zu einem Unterbleiben der Meldung führen.

In diesem Zusammenhang ist auch auf das arbeitsrechtliche Gleichbehandlungsgebot zu verweisen; die Hotline wird – in der Regel – zu einer gleichartigen Reaktion auf vergleichbare Vorwürfe führen. Bei einer Meldung im Einzelfall an den jeweiligen Vorgesetzten ist diese Vergleichbarkeit der Reaktion weniger leicht zu gewährleisten.

2.4.2.3. Unklare Formulierung

Diese Beschränkung ist aber auch insofern bedenklich, als der Begriff „Entscheidungsträger“¹²⁾ kein eindeutiges Abgrenzungskriterium darstellt. Es ist keineswegs klar, ob damit nur Personen gemeint sind, die innerhalb des Unternehmens keine Vorgesetzten haben, oder etwa all jene Personen, denen irgendwelche Entscheidungskompetenzen zukommen. Der Begriff an sich ist daher schon unklar.

Darüber hinaus ist es aber selbst nach Herleitung einer bestimmten Definition fraglich, ob jedem Mitarbeiter bekannt ist, welche Personen als „Entscheidungsträger“ einzustufen sind.

Last but not least wie soll der (bemühte) Mitarbeiter der Hotline-Betreiberin, der den Anruf des „Meldungslegers“ entgegennimmt, zwischen Entscheidungsträger nach österreichischem Recht und sonstigen Personen unterscheiden!

Die vorliegende Beschränkung der Zulässigkeit auf Meldungen betreffend

Entscheidungsträger ist daher nicht nur wegen des unklaren Begriffs zweifelhaft, sondern auch im Hinblick auf die praktischen Schwierigkeiten bei der Realisierung.

2.4.2.4. Weitere Überlegungen

Folgt man der Begründung der DSK, so besteht ein – durch die Entscheidung nun anerkanntes – überwiegendes berechtigtes Interesse der Konzernspitze an der objektiven Aufklärung von Vorwürfen gegen „Entscheidungsträger“. Dies schließt aber nicht aus, dass an Vergehen anderer Personen möglicherweise ein *anderes* überwiegendes berechtigtes Interesse bestehen kann. Auf den – durchaus ein solches Interesse darstellenden – Faktor Einheitlichkeit wurde bereits zu 2.4.2.2 verwiesen.

Darüber hinaus hat die Konzernspitze im vorliegenden Fall auch ein im SOX begründetes berechtigtes Interesse, da die SOX-Bestimmungen für sie verbindlich sind. Auch wenn der SOX nicht gem § 8 Abs 1 Z 1 DSGVO herangezogen werden kann, so kann er dennoch in die Erwägungen im Rahmen des § 8 Abs 1 Z 4 DSGVO betreffend das überwiegende berechnete Interesse einfließen. Die Vorgaben im SOX beschränken sich *nicht* auf Entscheidungsträger, sondern sehen eine Hotline für Meldungen vor, die sämtliche Mitarbeiter – unabhängig von deren Position im Unternehmen – betreffen können. Insofern hat die Konzernspitze aufgrund der im SOX vorgesehenen Verpflichtungen ein berechtigtes Interesse an der Einrichtung einer Hotline für Meldungen sowohl hinsichtlich der Entscheidungsträger als auch hinsichtlich der übrigen Mitarbeiter.

3. Offene Fragen

3.1. Übermittlung von sonstigen Daten an die Konzernspitze

3.1.1. Keine Beurteilung in der vorliegenden Entscheidung

Über die Zulässigkeit einer Übermittlung von sonstigen Daten an die Konzernspitze wurde in der vorliegenden Entscheidung nicht ausdrücklich entschieden, da eine solche Datenanwendung in dem der Entscheidung zugrunde liegenden Antrag letztlich nicht vorgesehen war.¹³⁾ Unter

11) *Spring*, *ecolex* 2009, 363.

12) In der Entscheidungsbegründung ist auch von „Führungskräften“ die Rede.

13) So heißt es im Sachverhalt, Pkt. 1 der Entscheidung: „(...) hat die Antragstellerin den ursprünglich bezeichneten Übermittlungsumfang ausdrücklich eingeschränkt auf Daten über schwerwiegende Missstände (...)“

Pkt 3.2b, in welchem die Rechtsgrundlage für die Übermittlung geprüft wird, heißt es lediglich:

„Ein überwiegendes berechtigtes Interesse der Konzernspitze an der Kenntnis von allen Verstößen gegen die konzerninternen Verhaltensregeln wird demgegenüber nicht anzunehmen sein (...).“

Mit dieser Aussage scheint die DSK eine negative Haltung zur Übermittlung von sonstigen Daten zu implizieren. Eine prinzipielle Ablehnung ist jedoch hieraus nicht abzuleiten, da eine solche Datenanwendung nicht zwingend die Kenntnis von „allen“ Verstößen zur Folge haben muss. So könnte – bleibt man ungeachtet der zu 2.4.2 aufgezeigten Bedenken im Entscheidungssystem der DSK – der Übermittlungsumfang etwa auf Daten betreffend Verstöße durch „Entscheidungsträger“ eingeschränkt werden. Diese Auslegung steht auch nicht im Widerspruch zu dem darauf folgenden Satz, in welchem es heißt, dass ein überwiegendes berechtigtes Interesse der Konzernspitze dann besteht, „wenn mutmaßliche schwere Verstöße durch Entscheidungsträger der österreichischen Tochtergesellschaft vorliegen.“ Diese Aussage schließt nämlich nicht aus, dass auch ein überwiegendes berechtigtes Interesse in Bezug auf leichte Verfehlungen durch Entscheidungsträger anerkannt wird.

Auch ein Größenschluss von der Ablehnung der Überlassung sonstiger Daten auf die Übermittlung dieser Daten erscheint hier nicht angebracht. Die Ablehnung der Zulässigkeit der Datenüberlassung basiert im Wesentlichen auf der *in concreto* fehlenden Eignung der Konzernspitze als Dienstleister. Das Argument der mangelnden Eignung als Dienstleister fällt aber in Bezug auf eine Übermittlung weg. Auch die Beurteilung der Überlassung der sonstigen Daten als obsolet lässt keine Schlüsse hinsichtlich der Beurteilung einer Übermittlung solcher Daten zu, da für die Erforderlichkeit einer Übermittlung Argumente herangezogen werden können, welche in Bezug auf die Überlassung nicht greifen würden. So könnte etwa argumentiert werden, dass auch für eine objektive Aufklärung von mutmaßlichen sonstigen Verstößen durch Entscheidungsträger die Mitwirkung von gesellschaftsexternen Personen, die in der Konzernhierarchie über den betreffenden Entscheidungsträgern stehen, von Vorteil ist.¹⁴⁾

Eine (bloße) Überlassung dieser Daten an die Konzernspitze würde eine solche Mitwirkung jedoch nicht zulassen, so dass dieses Argument eben nur in Bezug auf die Datenübermittlung greift. Die in der vorliegenden Entscheidung angeführten Gründe bieten sohin keine Anhaltspunkte für die Beurteilung einer Übermittlung der betreffenden Daten durch die DSK.

Da in der vorliegenden Entscheidung über die Übermittlung von sonstigen Daten an die Konzernspitze mangels eines diesbezüglichen Antrages nicht abzusprechen war und die angeführten Entscheidungsgründe keine eindeutigen Anhaltspunkte für die Beurteilung einer solchen Datenanwendung liefert, kann anhand dieser Entscheidung nicht beurteilt werden, wie eine diesbezügliche Entscheidung der DSK ausfallen würde.

3.1.2. Aussagen der Art 29 Datenschutzgruppe

Die Art 29 Datenschutzgruppe¹⁵⁾ hat anerkannt, dass es ein wesentliches Anliegen für eine Aktiengesellschaft (in der Folge kurz „AG“), insbesondere eine börsennotierte AG ist, zu gewährleisten, dass Berichte über mutmaßliche Rechnungslegungsmanipulationen oder fehlerhafte Rechnungslegung, die sich auf die Jahresabschlüsse des Unternehmens auswirken und sich auf die berechtigten Interessen der Betroffenen an der finanziellen Stabilität des Unternehmens auswirken können, den Vorstand auch erreichen, damit angemessene Folgemaßnahmen ergriffen werden können.¹⁶⁾ Sie hat diese – auf den Bereich Finanzdaten eingeschränkte – Stellungnahme allerdings ausdrücklich unter der Voraussetzung getroffen, dass sie über die mögliche Vereinbarkeit von EU-Datenschutzvorschriften mit internen Verfahren zur Meldung von sonstigen Verfehlungen, wie zB Gesundheit und Sicherheit am Arbeitsplatz, Umweltschä-

gar geboten. Die DSK anerkennt ja nicht SOX als rechtliche Grundlage, sondern „nur“ die Schwierigkeit der Aufdeckung von Vergehen von Entscheidungsträgern. Dieses Problem – „Wer überwacht die Überwacher“ – besteht aber nicht nur bei SOX relevanten Daten, sondern bei allen Vergehen.

15) Die Datenschutzgruppe wurde gem Art 29 der RL 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der EU in Fragen des Datenschutzes. Ihre Aufgaben sind in Art 30 der RL 95/46/EG und in Art 14 der RL 97/66/EG festgelegt.

16) WP 117 Pkt. IV.1.(ii); die Stellungnahme ist online abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_de.pdf.

den oder -gefahren und Straftaten, weiter nachdenken muss. Sie hat angekündigt, ihre Untersuchungen fortzusetzen, um zu entscheiden, ob auch für diese Themen EU-Leitlinien erforderlich sind.¹⁷⁾ Bis dato ist jedoch keine diesbezügliche Stellungnahme ergangen.

3.1.3. Eigene Beurteilung

Bei der Beurteilung, ob sich das überwiegende berechnete Interesse auf schwere Verstöße beschränkt oder an Meldungen von sonstigen Verfehlungen ebenfalls ein überwiegendes berechtigtes Interesse besteht, ist eine differenzierte Interessensabwägung vorzunehmen.

Für eine Berechtigung zur Übermittlung von sonstigen Daten spricht die Tatsache, dass der Konzern ein berechtigtes Interesse an der Durchsetzung sämtlicher Konzernvorgaben hat, das sich nicht auf Daten des Finanzbereichs beschränkt. Am Vorliegen eines Interesses an der Durchsetzung von Vorgaben außerhalb des Finanzbereichs kann kein Zweifel bestehen, denn ansonsten brauchte der Konzern derartige Vorgaben ja nicht festlegen. Dass dieses Interesse auch berechtigt ist, resultiert einerseits daraus, dass es sich bei den Prinzipien des „Corporate Governance“ um anerkannte Grundsätze für eine verantwortungsvolle Unternehmensführung handelt. Im Übrigen sind die Grenzen zwischen bilanzrelevanten SOX Daten/Verfehlungen und sonstigen Verfehlungen ohnedies nicht scharf zu ziehen. Etwas vereinfacht gesprochen: Früher oder später wirkt sich jedes Handeln eines Wirtschaftssubjektes in seiner Bilanz und – die Erreichung gewisser Größenordnungen vorausgesetzt – auch in der (US) Konzernbilanz aus.

Sofern der SOX nicht als Rechtsgrundlage herangezogen wird, ist auch kein Grund für eine Differenzierung zwischen Finanzdaten und sonstigen Daten ersichtlich. Die von der DSK ins Treffen geführte Begründung, dass die Einrichtung einer Hotline erforderlich ist, um mit hinlänglicher Sicherheit eine objektive Aufklärung der erhobenen Vorwürfe gegen Entscheidungsträger zu erreichen, stellt jedenfalls kein Argument für die Beschränkung der Zulässigkeit auf Verstöße im Finanzbereich dar. Ein allfälliger Mangel an Objektivität der „Selbstprüfung“ dieser Entscheidungsträger besteht unabhängig von der Art des Vorwurfs.

14) Im Entscheidungssystem der DSK wäre eine solche Ausweitung unserer Ansicht nach so-

17) WP 117 Pkt. I.

Es sprechen daher einige gute Gründe für die Zulässigkeit der Übermittlung sonstiger Daten, und es ist kein Grund ersichtlich für eine Beschränkung der Zulässigkeit auf Hotlines, die nur für Meldungen von schweren Verstößen zur Verfügung stehen.

3.2. Sensible Daten

Nicht näher erörtert wurde in der vorliegenden Entscheidung die Frage nach dem Umgang mit sensiblen Daten iSd § 4 Z 2 DSGVO. Der Verhaltenskodex nach amerikanischem Muster enthält häufig Verbote der Diskriminierung oder Regelungen zum Schutz der sexuellen Integrität. Meldungen über solche Verfehlungen können daher durchaus sensible Daten enthalten. Die Verwendung sensibler Daten kann jedoch nicht durch ein überwiegendes berechtigtes Interesse gerechtfertigt werden, denn für sensible Daten gilt der taxative Katalog des § 9 DSGVO. Daher wird für die Verwendung dieser Daten häufig die ausdrückliche Zustimmung der Betroffenen erforderlich sein. Unter Berücksichtigung der strengen Auflagen für eine gültige Zustimmung iSd § 4 Z 14 DSGVO wird die Einholung der Zustimmung sämtlicher Betroffenen, insbes bei größeren Unternehmen, jedoch nicht praktikabel sein.

Ein möglicher Ausweg besteht darin, die Meldungserstatter darüber zu informieren, dass sensible Daten im Rahmen der Hotline nicht aufgenommen werden können. Darüber hinaus ist die Hotline-Betreuerin anzuweisen, Meldungen, die sensible Daten enthalten, nicht aufzunehmen, und die Betroffenen insofern auf den unternehmensinternen Beschwerdeweg (oder die Behörden) zu verweisen. Dies scheint der einzig mögliche Weg zu sein, um die Verwendung sensibler Daten zu verhindern.

Wie die DSK zu einer solchen Lösung steht, geht aus der vorliegenden Entscheidung nicht hervor. Es kann aber wohl nie gänzlich ausgeschlossen werden, dass Meldungen im Rahmen einer solchen Hotline sensible Daten enthalten. Dies gilt wohl auch für den vorliegenden Fall. Angesichts der Tatsache, dass sie die Überlassung von sonstigen Daten an die Hotline-Betreiberin aber grundsätzlich zulässt, und eine andere Option nicht ersichtlich ist, ist aber davon auszugehen, dass dies auch aus der Sicht der DSK ein möglicher Lösungsweg ist.

3.3. Erforderlichkeit einer Vorabkontrolle

Für die Übermittlung oder Überlassung von Daten in das Ausland ist gem § 13 Abs 1 DSGVO die Genehmigung der DSK einzuholen, sofern der Datenverkehr mit dem Ausland nicht gem § 12 DSGVO genehmigungsfrei ist. Beide Datenempfänger, also sowohl die Konzernspitze als auch die Hotline-Betreiberin, sind in den USA ansässig.¹⁸⁾ Die USA fallen nicht unter den Ausnahmetatbestand für EU-Staaten gem § 12 Abs 1 DSGVO und sind auch kein Staat mit angemessenem Datenschutzniveau iSd § 12 Abs 2 DSGVO.¹⁹⁾ In der vorliegenden Entscheidung liegt auch keine materielle Ausnahme iSd § 12 Abs 3 DSGVO vor, sodass die Einholung einer Genehmigung durch die DSK erforderlich war. In vielen Fällen wird jedoch keine Genehmigungspflicht bestehen, zB wenn US-amerikanische Datenempfänger über ein Safe Harbor-Zertifikat verfügen. In diesen Fällen ist aber jedenfalls zu berücksichtigen, dass die Übermittlung der Daten eine Meldepflicht iSd § 17 DSGVO auslöst. Die DSK vertritt allerdings die Ansicht, dass in Fällen wie dem vorliegenden eine Vorabkontrolle durchzuführen sei, da auch „strafrechtliche relevante Daten“ iSd § 18 Abs 4 Z 4 DSGVO umfasst seien. Diese Auffassung erscheint jedoch – insbesondere unter Berücksichtigung der europarechtlichen Vorgaben – zweifelhaft.

Wird die Übermittlung von sensiblen Daten ausgeschlossen, so kommt die Vorabkontrolle gem § 18 Abs 2 Z 2 DSGVO noch in Betracht, wenn die Datenanwendung strafrechtlich relevante Daten iSd § 8 Abs 4 DSGVO enthält. Strafrechtlich relevante Daten iSd § 8 Abs 4 DSGVO sind Daten über

- gerichtlich oder
- verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den

- Verdacht der Begehung von Straftaten, sowie über
- strafrechtliche Verurteilungen oder
- vorbeugende Maßnahmen.

Diese Bestimmung ist richtlinienkonform auszulegen.²⁰⁾ Sie geht zurück auf Art 8 Abs 5 der Datenschutzrichtlinie²¹⁾ (in der Folge kurz „DS-RL“). Dort ist – soweit hier relevant – eine Sonderregelung festgelegt für Daten, die

- Straftaten,
 - strafrechtliche Verurteilungen oder
 - Sicherungsmaßregeln
- betreffen. Unter „Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln“ iSd Art 8 Abs 5 DS-RL sind alle Angaben zu verstehen, mit denen eine Person als Täter einer Straftat bezeichnet wird, sowie Angaben, die eine Person als tatverdächtig bezeichnen. Für den Begriff der Straftat kommt es nicht darauf an, ob sämtliche strafrechtlichen Voraussetzungen für eine Verurteilung vorliegen. Eine Straftat liegt auch vor, wenn sich aus den Daten ergibt, dass jemand eine Straftat begangen hat und wegen Schuldunfähigkeit nicht verurteilt wird. Sicherungsmaßregeln sind Maßnahmen in Bezug auf einen Straftäter, die keinen Strafcharakter haben.²²⁾ Die Meldung über mutmaßliche schwere Verstöße im Rahmen der Hotline zielt idR darauf ab, das Unternehmen vor finanziellen Verlusten zu schützen. Eine strafrechtliche Verfolgung wird damit jedoch nicht in Gang gesetzt. Der strafrechtliche Gehalt steht sohin nicht im Vordergrund der Meldungen. Würde jede Art von Anschuldigung und jede Datenart, welche irgendwie auf einen strafrechtlichen Gehalt schließen lassen könnte, unter die Bestimmung des Art 8 Abs 5 DS-RL fallen, so würde der Anwendungsbereich dieser Bestimmung ausufern. Eine Hotline, im Rahmen derer Meldungen über das Verhalten anderer Mitarbeiter erstattet werden, das in Einzelfällen möglicherweise einen strafrechtlichen Tatbestand verwirklicht, ist daher von der Formulierung des Art 8 Abs 5 DS-RL nicht umfasst. Die Verpflichtung zur Durchführung einer Vorabkontrolle für eine Hotline steht somit im Widerspruch zu den gemeinschaftsrechtlichen Vorgaben und ist aufgrund der Notwen-

18) In der Entscheidung wird bei der Beurteilung der Genehmigungspflicht – vermutlich aus Versehen – nur auf die Konzernmutter als Übermittlungsempfängerin Bezug genommen. Dieselben Erwägungen müssen aber auch für die Hotline-Betreiberin als Überlassungsempfängerin gelten.

19) Ein solcher Fall der Genehmigungsfreiheit gem § 12 Abs 2 DSGVO würde – jedenfalls nach der gängigen Praxis der DSK – hingegen vorliegen, wenn die Empfänger Safe Harbor-registriert wären. Zur Problematik der mangelnden Umsetzung der diesbezüglichen Entscheidung der EU-Kommission s *Knyrim*, Datenschutzrecht (2003) 134 sowie die FN 289 und 342.

20) EuGH 6. 11. 2003, Rs C-101/01.

21) RL 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.

22) *Damman/Simitis*, EG-Datenschutzrichtlinie (1996) 170.

digkeit der richtlinienkonformen Auslegung unzulässig.

4. Zusammenfassung

Mit der vorliegenden Entscheidung wird die Zulässigkeit der Einführung einer Whistleblowing-Hotline – bei Vorliegen bestimmter Voraussetzungen – anerkannt. Im Rahmen dieser Hotline dürfen zwar grundsätzlich sowohl Meldungen über schwere Verstöße, als auch Meldungen über leichte Verfehlungen erstattet werden. Es dürfen jedoch nur Daten aus Meldungen über schwere Verstöße an die Konzernspitze übermittelt werden. Die Überlassung von Daten aus Meldungen über leichte Verfehlungen an die Konzernspitze ist hingegen unzulässig. Solche Daten dürfen nur dem österreichischen Tochterunternehmen zur Verfügung gestellt werden. Zu beachten ist dabei, dass das österreichische Tochterunternehmen Auftraggeber sowohl in Bezug auf die Datenübermittlung an die Konzernspitze ist, als auch in Bezug auf die Datenüberlas-

sung an die Hotline-Betreiberin. Dies bedeutet, dass mit der Hotline-Betreiberin ein entsprechender Dienstleistervertrag iSd § 10 DSGVO abzuschließen ist. Sofern sowohl die Konzernspitze als auch die Hotline-Betreiberin in einem Land niedergelassen sind, die kein angemessenes Datenschutzniveau iSd § 12 DSGVO aufweisen, ist für beide Datenanwendungen grundsätzlich eine Genehmigung der DSK einzuholen. Bei der Verfassung der relevanten Dokumente sind die Vorgaben der Art 29 Datenschutzgruppe und die dort vorgeschlagenen Sicherheitsmaßnahmen zu berücksichtigen. Darüber hinaus wird regelmäßig auch eine Klarstellung dahingehend, dass sensible Daten im Rahmen der Hotline nicht aufgenommen werden, und ein entsprechender Nachweis der diesbezüglichen Anweisung der Hotline-Betreiberin, erforderlich sein.

Die Entscheidung der DSK ist insofern zu begrüßen, als nunmehr klargestellt ist, dass die Einrichtung einer Hotline aus datenschutzrechtlicher Sicht grundsätzlich zulässig ist. Es ist der DSK insofern

zuzustimmen, als eine Überlassung der Daten an die Konzernspitze überflüssig und daher im Sinne des Grundsatzes der Datensparsamkeit unzulässig ist. Die generelle Beschränkung der Zulässigkeit auf Meldungen bezüglich Entscheidungsträger erweist sich hingegen als unrichtig. Zur Zulässigkeit der Übermittlung von sonstigen Daten an die Konzernspitze hat sich die DSK nicht abschließend geäußert. Insofern bleibt die Haltung der DSK zu dieser Frage abzuwarten. Es sprechen jedoch einige Gründe für die Zulässigkeit einer solchen Datenanwendung, und die von der DSK herangezogene Begründung – welche den SOX als Rechtsgrundlage ausschließt – lässt kaum einen Raum für eine Differenzierung zwischen Finanzdaten und sonstigen Daten in Bezug auf die Zulässigkeit der Übermittlung. Die Fragen betreffend sensible Daten und die Erforderlichkeit einer Vorabkontrolle wurden in der vorliegenden Entscheidung nicht erörtert, sodass die diesbezügliche Einschätzung der DSK ebenfalls abzuwarten bleibt.



Die Autoren:

Dr. Ferdinand Graf ist Partner, Dr. Ruth Riesenhuber Rechtsanwältin bei Graf & Pitkowitz Rechtsanwälte GmbH; beide sind regelmäßig mit datenschutzrechtlichen Fragestellungen befasst und vertreten in Verfahren vor der DSK.



Dr. Gregor König, LL.M.

Österreichische Datenschutzkommission

■ jusIT 2009/73, 148

Entscheidungsübersicht Datenschutzkommission – Juni bis Juli 2009

1. Fotografie für den Zweck Kriminalpolizei

K121.476/0008-DSK/2009,
5. 6. 2009

Sachverhalt: Die Beschwerdeführerin behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass ein Beamter der Bundespolizei, dessen Handlungen der Bezirkshauptmannschaft (Beschwerdegegnerin) zuzurechnen seien, während einer Amtshandlung (ohne Androhung oder Anwendung von Befehls- oder

Zwangsgewalt) von ihr nachdrücklich verlangt habe, die Anfertigung von zwei Lichtbildern mithilfe einer Digitalkamera zu dulden, worauf sie in das Fotografieren eingewilligt habe. Da aber die Voraussetzungen für die Durchführung erkennungsdienstlicher Maßnahmen gem § 65 SPG nicht vorgelegen seien, sei diese Ermittlung erkennungsdienstlicher Daten rechtswidrig erfolgt. Die Beschwerdeführerin beantragte die bescheidmäßige Feststellung dieser Rechtsverletzung. Der Polizeibeamte erhielt von einem ihm bekannten, aber nicht namentlich

genannten Informanten aus der Suchtgiftszene telefonisch den Tipp, eine Frau, die als „eine kleine Dicke“ beschrieben wurde, verkaufe in einem Lokal im Bahnhofsviertel, das als „offene Drogenszene“ bekannt ist, Heroin. Er begab sich zum angeblichen Tatort und begegnete dort der Beschwerdeführerin, die das Lokal gerade verlassen wollte. Da sie nach entsprechender Aufforderung verneinte, Drogen bei sich zu haben, den Inhalt ihrer Taschen aber nicht vorzeigen wollte und auch keinen Lichtbildausweis dabei hatte, wurde sie aufgefordert, zur gegenüber