

Entscheidende Behörde

Datenschutzkommission

Entscheidungsdatum

05.12.2008

Geschäftszahl

K178.274/0010-DSK/2008

Text

[Anmerkung Bearbeiter: Namen (Firmen), (Internet-)Adressen, Aktenzahlen (und dergleichen), Rechtsformen und Produktbezeichnungen etc. sowie deren Initialen und Abkürzungen können aus Anonymisierungsgründen abgekürzt und/oder verändert sein. Offenkundige Rechtschreib-, Grammatik- und Satzzeichenfehler wurden korrigiert.]

B E S C H E I D

Die Datenschutzkommission hat unter dem Vorsitz von Dr. SPENLING und in Anwesenheit der Mitglieder Dr. KOTSCHY, Dr. ROSENMAYR-KLEMENZ, Dr. BLAHA, Mag. HEILEGGER und Dr. STAUDIGL sowie des Schriftführers Dr. KÖNIG in ihrer Sitzung vom 05. Dezember 2008 folgenden Beschluss gefasst:

S P R U C H

A. Der G**** GmbH in Wien wird auf Grund ihres Antrags vom 11. Juli 2007, modifiziert mit Schreiben vom 20. August 2007, gemäß § 13 Abs. 1 und 2 DSG 2000 die Genehmigung erteilt, aus der beim DVR unter der Nummer xxxxxxx/yyy gemeldeten Datenanwendung (Bezeichnung: "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") die folgenden Daten an die G**** Inc., USA, zu übermitteln:

1) von Mitarbeitern der Antragstellerin, die

- Entscheidungsträger sind und
- über die im Wege der von S**** Inc. (USA) im Auftrag der G**** Inc. (USA) betriebenen Hotline ein schwerer Verstoß gegen Regeln des für alle Mitarbeiter geltenden "Code of Business Conduct des G****-Konzerns" betr. die Bereiche Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität gemeldet wird:
- Vor- und Familienname,
- Titel/akademischer Grad
- Firmenname (Bezeichnung des Unternehmens, dessen Mitarbeiter der Entscheidungsträger ist)
- Stellenbezeichnung (nähere Bezeichnung der Stellung des Entscheidungsträgers im Unternehmen)
- Telefonnummer
- E-Mail-Adresse
- Art des Verstoßes

2) Von Mitarbeitern, die im Wege der genannten Hotline Meldung über Missstände erstatten, und hiebei ihre Identität angegeben haben

- Vor- und Familienname, Titel/akademischer Grad
- Firmenname (Bezeichnung des Unternehmens, dessen Mitarbeiter der Meldende ist)
- Stellenbezeichnung (Bezeichnung der Stellung des Meldenden im Unternehmen)
- Telefonnummer
- E-Mail-Adresse

Die Genehmigung wird unter der Auflage erteilt, dass im internen Verfahren für die Behandlung von Missbrauchsmeldungen folgende Maßnahmen garantiert sind:

1. G**** lässt anonyme Meldungen zwar zu, fördert sie aber nicht, sondern sichert vielmehr den Meldern volle Vertraulichkeit hinsichtlich ihrer Identität zu, wenn sie diese angeben.
2. Die mit der Bearbeitung von Meldungen betrauten Stellen sind von den anderen Konzernstellen strikt getrennt und haben nur Personen als Mitarbeiter, die besonders geschult und ausdrücklich verantwortlich für die Vertraulichkeit der gemeldeten Daten sind.
3. Die Beschuldigten haben grundsätzlich Zugang zu Anschuldigungen.
4. Die Identität des Meldenden wird nur dann offengelegt, wenn sich nachträglich herausstellt, dass die Anschuldigung bewusst falsch erhoben wurde.
5. Die eingemeldeten Daten werden spätestens 2 Monate nach Beendigung der Untersuchung gelöscht.

Die Genehmigung wird weiters unter der aufschiebenden Bedingung erteilt, dass die Antragstellerin vor Aufnahme der Übermittlungen an die G**** Inc (USA) die Genehmigung der Datenschutzkommission zur Überlassung der Daten eingeholt hat, die an die Betreiberin der Hotline, S**** Inc (USA) im Wege der Hotline von Mitarbeitern der Antragstellerin gemeldet werden. In der der Überlassung zugrundeliegenden Dienstleistervereinbarung ist festzulegen, dass die Betreiberin der Hotline als Dienstleisterin der Auftraggeberin nur Meldungen mit dem in 1) bezeichneten Inhalt an die G**** Inc. (USA) übermittelt, während die restlichen Meldungen nur der Antragstellerin zugänglich gemacht werden. Weiters ist zu vereinbaren, dass der Inhalt von Meldungen nach ihrer Übermittlung an die G**** Inc. bzw. nach ihrer Überlassung an die Antragstellerin beim Dienstleister umgehend gelöscht wird.

B. Im Übrigen wird der Antrag auf Genehmigung des internationalen Datenverkehrs vom 11. Juli 2007, modifiziert mit Schreiben vom 20. August 2007, abgewiesen.

C. Gemäß § 78 des Allgemeinen Verwaltungsverfahrensgesetzes (AVG), BGBl Nr. 51/1991 idF. BGBl I Nr. 65/2002, iVm §§ 1, 3 Abs. 1 und TP 1 Bundesverwaltungsabgabenverordnung 1983, BGBl Nr. 24 i.d.F. BGBl II Nr. 460/2002 (BVwAbgV), hat die Antragstellerin eine Verwaltungsabgabe in Höhe von

Euro 6,50

zu entrichten.

B e g r ü n d u n g

1. Sachverhalt:

Die G**** GmbH (in weiterer Folge "Antragstellerin") hat mit Schreiben vom 11. Juli 2007, eine Genehmigung zur Übermittlung wie auch zur Überlassung von personenbezogenen Daten über Mitarbeiter in die USA beantragt.

1.1 Die vom Antrag betroffenen Daten sind von der Antragstellerin als Daten über Verstöße (auch "incidents" genannt) gegen den "Code of Business Conduct of the G**** group of companies" näher bezeichnet worden (vgl. "Description of the transfers" in Appendix B der Anlage ./1 zum ursprünglichen Antrag vom 11. Juli 2007).

Die Übermittlung bzw. Überlassung dieser Daten soll im Wege eines konzerninternen Verfahrens unter Zuhilfenahme einer Hotline (Telefon- und Web-basiert) geschehen, die zur Meldung mutmaßlicher Missstände für den gesamten Konzern eingerichtet ist und von einem von der Konzernmuttergesellschaft beauftragten US-Unternehmen (S**** Inc) als Dienstleister betrieben wird.

1.2 Die Rollenverteilung der involvierten Unternehmen wird im ergänzenden Antrag vom 20. August 2007 so geschildert, dass Meldungen über schwere Missstände ("serious incidents") in den sogenannten "SOX-relevanten" Bereichen (Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität) von der US-amerikanischen Muttergesellschaft selbst weiterbearbeitet werden sollen. Meldungen, die nur leichte Verfehlungen betreffen, sollen von der US-Muttergesellschaft als Service für die übrigen Konzerngesellschaften gespeichert werden und stehen sodann, wenn die Meldung z.B. die österreichische Tochtergesellschaft betrifft, nur der österreichischen Tochtergesellschaft zur weiteren Bearbeitung zur Verfügung.

Weiters wird im ergänzenden Antrag ausgeführt, dass "schwerwiegende Fälle vor allem Entscheidungsträger des Antragstellers betreffen", welche im Verdacht stehen, gegen SOX-relevante Regeln des Code of Conduct verstoßen zu haben:

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

1.3 In ihrer ergänzenden Klarstellung vom 20. August 2007 hat die Antragstellerin den ursprünglich bezeichneten Übermittlungsumfang ausdrücklich eingeschränkt auf Daten über schwerwiegende Missstände ("serious incidents") in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität. Dies mit dem Hinweis, dass nach dem 2002 erlassenen US Sarbanes-Oxley Act (Pub. L. No. 107-204, 116 Stat. 745), die rechtliche Verpflichtung für an US-Börsen notierende Unternehmen bestünde, besondere Verfahren zur Meldung von solchen Missständen eingerichtet zu haben. Es werde als Rechtsgrundlage für die Übermittlung von solchen Missstandsmeldungen somit auf Art. 7 f der RL 95/46 und überdies auf die Äußerung der Art. 29 Gruppe in WP117 verwiesen, die "whistle blowing"-Hotlines bei Einrichtung von bestimmten besonderen Schutzmaßnahmen als vereinbar mit der zitierten Richtlinienbestimmung angesehen hat.

1.4 Die ebenfalls zur Genehmigung beantragte Überlassung von Daten hätte im Gegensatz zur beantragten Übermittlung sämtliche Meldungen betreffen sollen, die mit Hilfe der genannten Hotline erstattet werden, also auch betr. "minor incidents". In ihrer Rolle als Dienstleister hat G**** Inc. (USA) der Antragstellerin auch zugesagt, die relevanten datenschutzrechtlichen Verpflichtungen vertraglich zu überbinden, falls Sub-Dienstleister herangezogen werden.

1.5 Hinsichtlich der Art und Weise des Betriebs der Hotline werden im Antrag besondere organisatorische Vorkehrungen zum Schutz von Betroffenenrechten genannt. So wird etwa im Antrag beschrieben, dass die mit der Bearbeitung von Meldungen betrauten Stellen von den anderen Konzernstellen strikt getrennt sind und Personen als Mitarbeiter haben, die besonders geschult und für die Vertraulichkeit der Meldedaten verantwortlich sind; die Beschuldigten haben grundsätzlich Zugang zu Anschuldigungen – freilich zur Identität des Meldenden nur dann, wenn sich nachträglich herausstellt, dass die Anschuldigung bewusst falsch erhoben wurde; Meldedaten werden 2 Monate nach Beendigung der Untersuchung gelöscht. G**** lässt anonyme Meldungen zwar zu, fördert sie aber nicht, sondern sichert vielmehr den Meldern volle Vertraulichkeit hinsichtlich ihrer Identität zu, wenn sie diese angeben.

2. Anzuwendende Rechtsvorschriften:

§ 13 Abs. 1 und 2 DSGVO 2000 lauten unter der Überschrift "Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland" wie folgt:

"§ 13. (1) Soweit der Datenverkehr mit dem Ausland nicht gemäß § 12 genehmigungsfrei ist, hat der Auftraggeber vor der Übermittlung oder Überlassung von Daten in das Ausland eine Genehmigung der Datenschutzkommission (§§ 35 ff) einzuholen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen binden.

(2) Die Genehmigung ist unter Beachtung der gemäß § 55 Z 2 ergangenen Kundmachungen zu erteilen, wenn die Voraussetzungen des § 12 Abs. 5 vorliegen und wenn, ungeachtet des Fehlens eines im Empfängerstaat generell geltenden angemessenen Datenschutzniveaus,

1. für die im Genehmigungsantrag angeführte Übermittlung oder Überlassung im konkreten Einzelfall angemessener Datenschutz besteht; dies ist unter Berücksichtigung aller Umstände zu beurteilen, die bei der Datenverwendung eine Rolle spielen, wie insbesondere die Art der verwendeten Daten, die Zweckbestimmung sowie die Dauer der geplanten Verwendung, das Herkunfts- und das Endbestimmungsland und die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen, Standesregeln und Sicherheitsstandards; oder
2. der Auftraggeber glaubhaft macht, daß die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Hiefür können insbesondere auch vertragliche Zusicherungen des Empfängers an den Antragsteller über die näheren Umstände der Datenverwendung im Ausland von Bedeutung sein."

3. Rechtlich war zu erwägen:

3.1 Zur Genehmigungspflichtigkeit:

Die beantragte **Übermittlung und Überlassung von Daten** ist gemäß § 13 Abs. 1 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999, **genehmigungspflichtig**, da die Empfängerin G**** Inc. nicht in einem

Staat mit angemessenem Datenschutzniveau im Sinne des § 12 Abs. 2 DSG 2000 ansässig ist und auch kein Fall eines gemäß § 12 Abs. 3 DSG 2000 genehmigungsfreien Datenverkehrs vorliegt.

Bedingung für die Erteilung einer Genehmigung für genehmigungspflichtige Datentransfers ins Ausland ist das Vorliegen der Voraussetzungen des § 12 Abs. 5 DSG 2000 und der Nachweis des Bestehens eines angemessenen Datenschutzniveaus beim ausländischen Datenempfänger.

3.2 Vorliegen der Voraussetzungen nach § 12 Abs. 5 DSG 2000:

Gemäß § 12 Abs. 5 DSG 2000 ist Voraussetzung für die Rechtmäßigkeit einer geplanten Übermittlung, dass die Bedingungen des § 7 Abs. 2 DSG 2000 erfüllt sind. Danach dürfen Daten nur dann übermittelt werden, wenn sie

- aus einer zulässigen Datenanwendung stammen, und wenn
- die rechtliche Befugnis des Empfängers für eine derartige Übermittlung ausreichend glaubhaft ist und wenn
- die Übermittlung im Sinne der §§ 8 bzw. 9 DSG 2000 ihrer Art nach auch im Inland zulässig wäre.

Die Rechtmäßigkeit einer Überlassung an einen Dienstleister ist gemäß § 10 DSG 2000 an den Abschluss einer (schriftlichen) Vereinbarung geknüpft, in der der Auftraggeber für den Dienstleister die in concreto einzuhaltenden datenschutzrechtlichen Verpflichtungen festlegt.

a) Die vom Antrag umfassten Datenflüsse werden wie folgt gewertet:

Es erfolgt eine Ermittlung von Daten durch die Antragstellerin, wenn ihre Mitarbeiter wahrgenommene Missstände in *Verfolg der generellen Empfehlung ihres Arbeitgebers* melden und diese Meldungen - sei es von der Antragstellerin selbst oder auch in ihrem Auftrag von einem Dienstleister - elektronisch aufgezeichnet werden. Da die Mitarbeiter bei derartigen Meldungen letztlich in Erfüllung der für sie verpflichtenden unternehmensinternen Verhaltensregeln tätig werden, sind ihnen derartige Meldungen nicht als Privatperson sondern als Organ des Unternehmens zuzurechnen, sodass datenschutzrechtlich handelndes Rechtssubjekt das Unternehmen ist. Der Antragstellerin ist daher die Eigenschaft eines Auftraggebers für die Verwendung von gemeldeten Missbrauchsdaten zuzuerkennen – die (elektronischen) Aufzeichnungen stellen eine Datenanwendung der Antragstellerin dar, die im Übrigen von ihr auch beim Datenverarbeitungsregister zur Registrierung gemeldet wurde.

Wenn nun Missbrauchsdaten im Wege der hierfür eigens eingerichteten Hotline ermittelt werden, geschieht auch dies nach dem vorstehend dargestellten Verständnis des Sachverhalts "für die Antragstellerin", da ihre Mitarbeiter als ihre Organe handeln. Die Aufzeichnung der Meldungen durch den Hotline-Betreiber ist daher – in dieser ersten Phase – als Dienstleistung für die Antragstellerin zu begreifen. Dementsprechend bedarf es besonderer Vereinbarungen, wie der Dienstleister mit den für die Antragstellerin ermittelten Daten zu verfahren hat. Die Verpflichtung zum Abschluss einer derartigen Vereinbarung mit einem vorgegebenen Inhalt ist im Bescheidspruch als aufschiebende Bedingung der Genehmigungserteilung für die Übermittlung von Missbrauchsdaten an die Muttergesellschaft enthalten – erst nachdem die Genehmigung der Datenschutzkommission eingeholt wurde zur (bloß logischen) Überlassung der mit Hilfe der Hotline ermittelten Daten an den als Dienstleister fungierenden Hotline-Betreiber, darf von der vorliegenden Genehmigung zur Übermittlung von Daten an die G**** Inc. Gebrauch gemacht werden.

b) Zur Rechtsgrundlage der beantragten Übermittlungen:

aa) Wie im Sachverhalt ausgeführt, sind Maßstab für den zu meldenden "Missbrauch" die konzerninternen Verhaltensregeln, die in ihrem bilanz- und finanzrelevanten Teil den Verpflichtungen des Sarbanes-Oxley Act nachgebildet sind. Für die Mitarbeiter der Antragstellerin haben diese Regeln rechtliche Relevanz durch ihren Arbeitsvertrag, in dem die Verpflichtung zur Einhaltung der konzerninternen Verhaltensregeln als Weisungen des Arbeitgebers bedungen wurde. Verstöße gegen diese Verhaltensregeln werden daher zumindest arbeitsrechtlich nicht irrelevant sein, sodass dem Arbeitgeber ein überwiegendes berechtigtes Interesse an der Kenntnis von solchen Verstößen zuzubilligen ist.

Ein überwiegendes berechtigtes Interesse der Konzernspitze an der Kenntnis von allen Verstößen gegen die konzerninternen Verhaltensregeln wird demgegenüber nicht anzunehmen sein, da dies unverhältnismäßig wäre. Die Antragstellerin hat selbst Argumente in ihrem Antrag vorgebracht, die erkennen lassen, wann überwiegende berechnete Interessen der Konzernspitze in dieser Frage bestehen, nämlich dann, wenn mutmaßliche schwere Verstöße durch Führungskräfte der österreichischen Tochtergesellschaft vorliegen.

Im Umfang der Meldung von schwerwiegenden Verstößen ("serious incidents"), die Mitarbeitern der Antragstellerin in Führungspositionen angelastet werden, anerkennt die Datenschutzkommission das Bestehen eines überwiegenden berechtigten Interesses an der Übermittlung der Meldungsdaten an die Konzernspitze, da nur auf diese Weise mit hinlänglicher Sicherheit eine objektive Aufklärung der erhobenen Vorwürfe zu erwarten ist. Im Spruch war daher die Genehmigung auf die Übermittlung von Daten über Meldungen über solche Verdachtsfälle zu beschränken.

bb) Die Zulässigkeit der Übermittlung von Missbrauchsdaten bedarf angesichts ihres hohen Schadenspotentials für den Beschuldigten besonderer Begleitmaßnahmen, um eine Verletzung von Datenschutzrechten hintanzuhalten. Die Antragstellerin hat jene organisatorischen Begleitmaßnahmen im Antrag beschrieben, die im antragsgegenständlichen internen Verfahren zum Schutz von Betroffenenrechten vorgesehen sind. Sie entsprechen weitgehend jenen besonderen Garantien, die in der Äußerung WP 117 der Art. 29 Gruppe für eine datenschutzkompatible Führung einer "whistle blowing hotline" verlangt werden. Da diese Begleitmaßnahmen wesentlich sind für die Zulässigkeit der Datenanwendung, war ihre Umsetzung im Falle von Übermittlungen als Auflage in die Genehmigung aufzunehmen.

c) Zur Ablehnung der Genehmigung der Überlassung der Meldedaten an die Konzernspitze:

Nach § 10 DSGVO 2000 ist ein Auftraggeber zwar an sich in der Auswahl seiner Dienstleister frei, doch darf nur ein solcher Dienstleister bestellt werden, der nicht infolge eines offensichtlichen Interessenskonflikts Gefahr läuft, seine Rolle als Dienstleister zu überschreiten.

Angesichts der erheblichen Nachteile, die die Meldung des Verdachts eines Missbrauchs für den Beschuldigten haben kann, muss der Kreis derjenigen, denen diese Daten zur Kenntnis kommen, so eng wie möglich gehalten werden. Die Datenschutzkommission erachtet es daher für erforderlich, dass dem Hotline-Betreiber, der nach dem vorliegenden Konzept jede einzelne Meldung zunächst bearbeiten muss, die Prüfung der eingehenden Meldungen im Hinblick auf ihre Einordnung als "serious incident" und im Hinblick auf die Stellung des Beschuldigten als Führungskraft übertragen wird. Nur Meldungen über schwerwiegende Verfehlungen, die Führungskräften vorgeworfen werden, dürfen nach der vorliegenden Genehmigung an die Konzernspitze übermittelt werden – andere Meldungen wären der Antragstellerin zurückzumitteln, was als Überlassung von (für den Auftraggeber ermittelten) Daten vom Dienstleister an den Auftraggeber zu werten wäre.

3.3 Glaubhaftmachung des angemessenen Datenschutzes beim Übermittlungsempfänger im Ausland:

Zur Glaubhaftmachung des angemessenen Datenschutzes beim Empfänger im Ausland haben die Antragstellerin als „Exporteur“ von Daten und G**** Inc. als „Importeur“ einen Vertrag abgeschlossen, der den in der **Entscheidung der Kommission 2004/915/EG vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (Set II)**, Amtsblatt Nr. L 385 S. 74–84, CELEX: 32004D0915, vorgesehenen Standardvertragsklauseln entsprechen. Der Nachweis ausreichenden Datenschutzes bei den ausländischen Datenempfängern gilt daher als erbracht im Sinne des § 13 Abs. 2 Z 2 DSGVO 2000.

3.4 Die Verwaltungsabgabe war gemäß § 78 Abs. 1 AVG iVm §§ 13, 53 Abs. 1 DSGVO 2000 vorzuschreiben. Demnach ist für Anträge nach § 13 DSGVO 2000 keine Befreiung von Verwaltungsabgaben normiert.