Entscheidende Behörde

Datenschutzkommission

Entscheidungsdatum

24.02.2012

Geschäftszahl

K506.237-020/0002-DVR/2012

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. KURAS und in Anwesenheit der Mitglieder Dr. SOUHRADA-KIRCHMAYER, Dr. BLAHA, Mag. MAITZ-STRASSNIG, Mag. HEILEGGER und Dr. HEISSENBERGER sowie des Schriftführers Mag. HILD in ihrer Sitzung vom 24. Februar 2012 folgenden Beschluss gefasst:

S p r u c h

Unter Zugrundelegung der im Mängelrügeverfahren nach § 20 Abs. 1 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 idgF, verbesserten Registrierungsmeldung der T**** GmbH vom 21. Oktober 2009 betreffend die Datenanwendung "Whistleblowing-Hotline" wird die Registrierung dieser Datenanwendung gemäß § 21 Abs. 2 DSG 2000 unter Erteilung folgender Auflagen verfügt:

1. Die Übermittlung von personenbezogenen Daten von Beschuldigten ist nur hinsichtlich leitender Angestellter zulässig, die eines maßgeblichen Verstoßes (oder der Teilnahme daran) gegen die konzernintern verbindlichen Regelungen ("SOP for the T**** Compliance Helpline") betreffend Korruption und Bestechung, Verstöße gegen Buchführungsvorschriften und Steuerhinterziehung, illegale Praktiken im Zusammenhang mit Banken wie Geldwäsche und Betrug im Zusammenhang mit Bankgeschäften sowie Fälschung von Finanzunterlagen und Insiderhandel bezichtigt werden.

2. Die mit der Bearbeitung von Meldungen betraute Stelle ist von den anderen Konzernstellen strikt getrennt und hat nur Personen als Mitarbeiter, die besonders geschult und ausdrücklich verantwortlich für die Vertraulichkeit der gemeldeten Daten sind.

3. Die Antragsstellerin lässt anonyme Meldungen zwar zu, fördert sie aber nicht, sondern sichert vielmehr den Meldern volle Vertraulichkeit hinsichtlich ihrer Identität zu, wenn sie diese angeben.

4. Die Beschuldigten haben grundsätzlich Zugang zu Anschuldigungen.

5. Die Identität des Meldenden wird nur dann offengelegt, wenn sich nachträglich herausstellt, dass die Anschuldigung bewusst falsch erhoben wurde.

6. Die eingemeldeten Daten werden spätestens 2 Monate nach Beendigung der Untersuchung gelöscht.

7. Die Registrierung ist an die Auflage geknüpft, dass die Mitarbeiter arbeitsvertraglich zur Einhaltung des der Behörde vorgelegten "Standard Operating Procedure" und zur Meldung an den Arbeitgeber über wahrgenommene Verstöße gegen diesen Code verpflichtet wurden.

8. Die Registrierung wird weiters unter der Auflage vorgenommen, dass die Antragstellerin vor Aufnahme der Übermittlungen an T*** Company (USA) die Behandlung der an die Hotline gemeldeten Daten vertraglich geregelt hat. In dieser Vereinbarung ist festzulegen, dass die U**** Inc (USA) als Betreiberin der Hotline und Dienstleisterin der Antragstellerin nur Meldungen mit den im Spruch bezeichneten Inhalten weiterbearbeitet und an die Konzernmutter weitergibt, während die restlichen über die Hotline allenfalls eingebrachten Meldungen nur der Antragstellerin zugänglich gemacht werden. Weiters ist zu vereinbaren, dass der Inhalt von Meldungen nach ihrer Übermittlung an die T**** Company bzw. nach ihrer Rück-Überlassung an die Antragstellerin beim Dienstleister umgehend gelöscht wird.

B e g r ü n d u n g

I. Sachverhalt

Die T**** GmbH hat mit Schreiben vom 21. Oktober 2009 eine Meldung für eine Datenanwendung mit der Bezeichnung "Whistleblowing-Hotline" (Datenanwendungsnummer xxxxxxx/yyy), beim Datenverarbeitungsregister eingebracht. Diese Meldung dient zur Einrichtung eines internen Verfahrens zur Meldung mutmaßlicher Missstände an die Konzermutter in den USA. Dies ergibt sich aus der Standard Operating Procedure (SOP) für die Hotline, deren letzte Version mit E-Mail vom 3. März 2010 vorgelegt wurde ("SOP for the T**** Compliance Helpline").

Bei den zu verfolgenden Missständen handelt es sich um schwerwiegende Vergehen.

Da die Antragsstellerin wegen ihrer geringen Größe keinen Betriebsrat hat, mit dem eine Betriebsvereinbarung abgeschlossen werden könnte, wurde stattdessen eine Zustimmung der Arbeitnehmer gemäß § 10 Abs. 1 und 2 Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG), BGBl. Nr. 459/1993 idgF, eingeholt. Diese Zustimmung wurde für fünf Jahre ab dem 1. März 2010 vereinbart.

Die Empfängergesellschaft, T**** Company in den USA hat sich zur Einhaltung der Regeln des "Safe Harbor" verpflichtet.

Zum Betrieb der Hotline wird ein Dienstleister in den USA eingesetzt, die U**** Inc, ein auf den Betrieb solcher Dienste spezialisiertes Unternehmen. U**** Inc ist ebenfalls Mitglied im "Safe Harbor".

II. Rechtliche Erwägungen:

1. Anzuwendende Rechtsvorschriften:

§ 7 Abs. 1 DSG 2000 lautet unter der Überschrift "Zulässigkeit der Verwendung von Daten":

"§ 7 (1) Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen."

§ 12 Abs. 2 DSG 2000 lautet:

"(2) Keiner Genehmigung gemäß § 13 bedarf weiters der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutz. Welche Drittstaaten angemessenen Datenschutz gewährleisten, wird unter Beachtung des § 55 Z 1 durch Verordnung des Bundeskanzlers festgestellt. Maßgebend für die Angemessenheit des Schutzes ist die Ausgestaltung der Grundsätze des § 6 Abs. 1 in der ausländischen Rechtsordnung und das Vorhandensein wirksamer Garantien für ihre Durchsetzung."

§ 17 Abs. 1 DSG 2000 lautet unter der Überschrift "Meldepflicht des Auftraggebers":

"§ 17 (1) Jeder Auftraggeber hat, soweit in den Abs. 2 und 3 nicht anderes bestimmt ist, vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission mit dem in § 19 festgelegten Inhalt zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten. Diese Meldepflicht gilt auch für Umstände, die nachträglich die Unrichtigkeit und Unvollständigkeit einer Meldung bewirken."

§ 18 Abs. 2 DSG 2000 lautet:

"(2) Meldepflichtige Datenanwendungen, die weder einer Musteranwendung nach § 19 Abs. 2 entsprechen, noch innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften noch die Verwendung von Daten im Katastrophenfall für die in § 48a Abs. 1 genannten Zwecke betreffen, dürfen, wenn sie

1. sensible Daten enthalten oder
2. strafrechtlich relevante Daten im Sinne des § 8 Abs. 4 enthalten oder
3. die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder
4. in Form eines Informationsverbundsystems durchgeführt werden sollen,

erst nach ihrer Prüfung (Vorabkontrolle) durch die Datenschutzkommission nach den näheren Bestimmungen des § 20 aufgenommen werden."

§ 21 Abs. 2 DSG 2000 lautet:

"(2) Bei Datenanwendungen, die gemäß § 18 der Vorabkontrolle unterliegen, können auf Grund der Ergebnisse des Prüfungsverfahrens dem Auftraggeber Auflagen, Bedingungen oder Befristungen für die Vornahme der Datenanwendung durch Bescheid erteilt werden, soweit dies zur Wahrung der durch dieses Bundesgesetz geschützten Interessen der Betroffenen notwendig ist."

§ 10 Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG) BGBl. Nr. 459/1993 idgF, lautet samt Überschrift:

"Kontrollmaßnahmen

§ 10. (1) Die Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren, ist unzulässig, es sei denn, diese Maßnahmen werden durch eine Betriebsvereinbarung im Sinne des § 96 Abs. 1 Z 3 ArbVG geregelt oder erfolgen in Betrieben, in denen kein Betriebsrat eingerichtet ist, mit Zustimmung des Arbeitnehmers.

(2) Die Zustimmung des Arbeitnehmers kann, sofern keine schriftliche Vereinbarung mit dem Arbeitgeber über deren Dauer vorliegt, jederzeit ohne Einhaltung einer Frist schriftlich gekündigt werden."

2. rechtliche Schlussfolgerungen:

2.1 Zur Vorabkontrolle und Erteilung von Auflagen:

Die Meldung betrifft strafrechtlich relevante Daten gemäß § 18 Abs. 2 Z DSG 2000 und unterliegt damit der Vorabkontrolle. Weiters kann die Datenschutzkommission bei Datenanwendungen, die der Vorabkontrolle unterliegen, dem Auftraggeber Auflagen für die Vornahme der Datenanwendung durch Bescheid erteilen.

Die Datenschutzkommission hat von dieser Möglichkeit bereits in früheren, ähnlich gelagerten Fällen Gebrauch gemacht, wie im Bescheid Zahl K600.074/0002-DVR/2010 vom 20. Jänner 2010. Weiters wurden Übermittlungen aus Whistleblowing-Hotlines gemäß § 13 DSG 2000 mit Bescheid genehmigt, wobei vergleichbare Auflagen erteilt wurden (Zahl K178.305/0004- DSK/2009 vom 24. Juli 2009, alle veröffentlicht im RIS).

2.2 Zur Zulässigkeit der Übermittlung und Überlassung von Daten in die USA:

Hinsichtlich der Übermittlung von Daten an T**** Company und U**** Inc in den USA besteht Genehmigungsfreiheit, da diese Unternehmen dem Safe Harbor beigetreten sind, sodass angemessener Datenschutz bei diesen in den USA ansässigen Unternehmen besteht. Eine separate Genehmigung gemäß § 13 DSG 2000 ist daher nicht erforderlich.

Die U**** Inc arbeitet als Dienstleister der Konzerntöchter (und auch der Antragsstellerin), wenn sie Beschwerden entgegennimmt, aber nicht selbst weiterbehandelt, sondern an die Töchter übergibt. Um diesem rechtlichen Verhältnis gerecht zu werden, wurde im Spruch der Abschluss einer Vereinbarung angeordnet.

2.3 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 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 hiefür 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 Auflage für die Übermittlung von Missbrauchsdaten an die Muttergesellschaft enthalten – erst wenn ein Vertrag zur Überlassung der mit Hilfe der Hotline ermittelten Daten an den als Dienstleister fungierenden Hotline-Betreiber abgeschlossen wurde, darf die Antragstellerin von der vorliegenden Genehmigung zur Übermittlung von Daten an die T**** Company Gebrauch machen.

2.4 Zur Rechtsgrundlage der beantragten Übermittlungen:

a) 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, einem amerikanischen Gesetz, das für US-Konzerne gilt und die Einrichtung von Meldungssystemen an die Konzernmutter vorsehen. Für die Mitarbeiter der Antragstellerin haben diese Regeln rechtliche Relevanz durch die Standard Operation Procedure, in der das Recht und auch die Aufforderung zur Meldung von schwerwiegenden Verstößen festgehalten ist. 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.

Die schutzwürdigen Geheimhaltungsinteressen der Mitarbeiter sind gewahrt, weil die Antragstellerin als Arbeitgeber um einem Konsens mit den Arbeitnehmern bemüht ist, und statt einer Betriebsvereinbarung, die wegen der geringen Größe der Belegschaft nicht möglich ist, eine Zustimmung der Arbeitnehmer gemäß § 10 Abs. 1 und 2 AVRAG eingeholt hat. Diese Zustimmung ist nicht als datenschutzrechtlich gültige Zustimmung zur Übermittlung zu werten (siehe § 8 Abs. 1 Z 2 DSG 2000), aber geeignet, die schutzwürdigen Geheimhaltungsinteressen der Betroffenen zu wahren, und repräsentiert auch ohne Betriebsrat ein Element der betrieblichen Mitbestimmung.

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. Eine sachliche Rechtfertigung für die Übermittlung von Missbrauchsdaten **zum Zweck der Aufklärung und Untersuchung** von Vorfällen wird nur dann anzunehmen sein, wenn dieser Zweck bei der Antragstellerin selbst nicht zweifelsfrei erreicht werden kann: Im Umfang der Meldung von maßgeblichen Verstößen, die Mitarbeitern der Antragstellerin in Führungspositionen oder vergleichbar hochgestellten Positionen 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 und vollständige 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. Die Meldung von Vorfällen, die keine leitenden Angestellten betreffen wäre nicht zulässig, weil in solchen Fällen die Antragstellerin selbst ohne Hilfe der Konzernmutter das Problem bereinigen kann. In dem Fall, dass ein Mitarbeiter von geringerem Einfluss auf die Unternehmensführung einen schwerwiegenden Verstoß verursacht, wäre eine Meldung an die Konzernspitze dann zulässig, wenn die Vorgesetzten ihre Aufsichtpflicht nicht korrekt wahrnehmen und dadurch ihrerseits maßgeblich gegen die Konzernrichtlinien verstoßen.

b) 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 für die Zulässigkeit der Datenanwendung wesentlich sind, war ihre Umsetzung im Falle von Übermittlungen als Auflage in die Genehmigung aufzunehmen.