TE Dsk BescheidRegistrierung 2014/5/13 DSB-D600.328-001/0001-DSB/2014

JUSLINE Entscheidung

Veröffentlicht am 13.05.2014

Norm

DSG 2000 §17 Abs1
DSG 2000 §18 Abs2
DSG 2000 §18 Abs2 Z2
DSG 2000 §21 Abs2
AVRAG §10 Abs1
AVRAG §10 Abs2
DSG 2000 §8 Abs1 Z2
DSG 2000 §7 Abs1

Text

GZ: DSB-D600.328-001/0001-DSB/2014 vom 13. 5. 2014

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

BESCHEID

SPRUCH

Die Datenschutzbehörde verfügt unter Zugrundelegung der im Mängelrügeverfahren nach § 20 Abs. 1 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 idgF, verbesserten Meldung der C**** GmbH Niederlassung Österreich vom 6. Juni 2011 betreffend die Datenanwendung „Whistleblowing-Hotline“ (DVR-Nummer 0**0***) die Registrierung dieser Datenanwendung gemäß § 21 Abs. 2 DSG 2000 unter Erteilung folgender Auflagen:

1. Die Übermittlung von personenbezogenen Daten von Beschuldigten an die C**** Inc. (USA) und die C**** A**** BV (Niederlande) ist nur hinsichtlich leitender Angestellter (oder vergleichbar verantwortlichen Personen) zulässig, die eines maßgeblichen Verstoßes (oder der Teilnahme daran) gegen den Verhaltenskodex des C****-Konzerns („C**** - D**** of Ethics Point for Austria v2“) betreffend Betrug, Buchfälschung, Verstoß gegen Buchhaltungsvorschriften, Insiderhandel, wirtschaftliche Interessenskonflikte, Manipulation von Optionen, Untreue, Wettbewerbsverstöße, Bestechung von Amtsträgern, Finanzierung des Terrorismus und illegaler Handel mit Kriegsmaterial 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 Antragstellerin 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 wird unter der Auflage vorgenommen, dass die Mitarbeiter im Arbeitsvertrag oder sonst durch generelle Weisung oder Betriebsvereinbarung zur Meldung an den Arbeitgeber über wahrgenommene Verstöße in den obengenannten Punkten verpflichtet wurden;

8. Die Registrierung wird unter der Auflage vorgenommen, dass bei der Bearbeitung von Meldungen durch Personen, die nicht Mitarbeiter sind, die Rechte der Betroffenen auf ein faires Verfahren gewahrt bleiben;

9. Die Registrierung wird unter der Auflage vorgenommen, dass die Antragstellerin vor Aufnahme der Übermittlungen an die Empfänger die Behandlung der an die Hotline gemeldeten Daten vertraglich geregelt hat. In dieser Vereinbarung ist festzulegen, dass die M****, 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 bzw. nach ihrer Rück-Überlassung an die Antragstellerin beim Dienstleister umgehend gelöscht wird.

BEGRÜNDUNG

A. Vorbringen und Sachverhalt:

Die C**** GmbH Niederlassung Österreich hat am 6. Juni 2011 die Datenanwendung „Whistleblowing“ (DVR-Nummer 0**0***) beim Datenverarbeitungsregister gemeldet.

Das System dient zur Aufdeckung von Verstößen gegen den Verhaltenskodex des C****-Konzerns (vorgelegt mit dem Dokument „ - Description for Austria v2“). Der Antrag betrifft Meldungen zu Verstößen in den folgenden Bereichen wobei neben der englischen Originalbezeichnung aus dem Verhaltenskodex die deutsche Übersetzung eingefügt wurde:

- (Betrug, Buchfälschung) Fraud, deliberate error, or misrepresentation in the preparation, evaluation, review, or audit of any financial statements of the company
- (Verstoß gegen Buchhaltungsvorschriften) Fraud, deliberate error, or misrepresentation in the recording and maintaining of financial records of the Company
- (Verstoß gegen Buchhaltungsvorschriften) Deficiencies in or noncompliance with the company’s internal accounting controls
- (Buchfälschung) Misrepresentation or false statements regarding a matter contained in the Company’s financial records, financial reports, or audit reports
- (Buchfälschung) Deviation from full and fair reporting of the company’s financial condition
- (Buchfälschung) Falsification or destruction of financial or accounting records
- (Insiderhandel) Insider trading
- (wirtschaftliche Interessenskonflikte) Conflicts of interest (related to these financial, audit or controls areas)
- (Manipulation von Optionen) Improper treatment of stock options
- (Untreue) Improper expenditure of company funds
- (Wettbewerbsverstöße) Anti-competition or anti-trust violations (related to any of the above)

- (Steuerhinterziehung) Tax evasion
- (Betrug) Employment of fictitious personnel
- (Bestechung von Amtsträgern) Bribery of governmental and quasi-governmental public officials (including health care professionals) or any other customers, vendors or suppliers
- (Finanzierung des Terrorismus) Funding of terrorist activities
- (illegaler Handel mit Kriegsmaterial) Illegal trading with war materials
- (Vertuschung eines der genannten Verstöße) Efforts to conceal any of the above

Die Mitarbeiter werden aufgefordert und ermächtigt, die genannten Verstöße zu melden.

Die Daten werden an die europäische Zentrale (C**** E**** BV in den Niederlanden) sowie die Muttergesellschaft (C**** Inc. in den USA) übermittelt. Zum Betrieb des Systems wird die Firma M**** Inc. in den USA eingesetzt. Die C**** Inc. und die M**** Inc. sind Mitglieder im „Safe Harbor".

Als weitere Rechtsgrundlage werden Zustimmungserklärungen gemäß § 10 AVRAG eingeholt, weil die Antragsstellerin keinen Betriebsrat hat, mit dem eine Betriebsvereinbarung abgeschlossen werden könnte.

Die Meldung sieht vor, dass auch andere Personen als Mitarbeiter Meldungen erstatten können. Dies betrifft insb. Kunden und Lieferanten.

B. In rechtlicher Hinsicht folgt daraus:

1.1 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 Datenschutzbehörde bei Datenanwendungen, die der Vorabkontrolle unterliegen, dem Auftraggeber Auflagen für die Vornahme der Datenanwendung durch Bescheid erteilen.

Die Datenschutzbehörde 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).

1.2 Zur Zulässigkeit der Übermittlung und Überlassung von Daten in das Ausland:

Hinsichtlich der Übermittlung von Daten an das Konzernunternehmen in den Niederlanden besteht Genehmigungsfreiheit, da dieses Unternehmen seinen Sitz in einem EWR-Land hat (§ 12 Abs. 1 DSG 2000). Die Übermittlung an die Konzernmutter in den USA und die Überlassung von Daten an den Dienstleister M*** Inc in den USA sind gemäß § 12 Abs. 2 DSG 2000 ohne Genehmigung zulässig, weil beide Empfänger Mitglieder im „Safe Harbor" sind.

Eine separate Genehmigung gemäß § 13 DSG 2000 ist daher nicht erforderlich.

1.3 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 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 stellt daher eine Dienstleistung für die Antragstellerin dar. 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.

1.4 Zur Rechtsgrundlage der beantragten Übermittlungen:

aa) Wie im Sachverhalt ausgeführt, sind Maßstab für den zu meldenden „Missbrauch" die konzerninternen Verhaltensregeln. Für die Mitarbeiter der Antragstellerin haben diese Regeln rechtliche Relevanz durch den Verhaltenskodex, in dem das Recht zur Meldung von schwerwiegenden Verstößen festgehalten sind. 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 ist 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 Datenschutzbehörde 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 oder Personen in vergleichbar hochgestellten Positionen 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 Aufsichtspflicht nicht korrekt wahrnehmen und dadurch ihrerseits maßgeblich gegen die Konzernrichtlinien verstoßen.

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

cc) Das Meldesystem sieht auch Meldungen durch andere Personen als Mitarbeiter vor, also insb. Kunden und Lieferanten. Es ist daher möglich, dass bei einer derartigen Meldung geschäftliche Interessen im Spiel sind, die eine fragwürdige Entscheidung zu Lasten eines beschuldigten Mitarbeiters möglich machen, wenn z.B. die Antragstellerin mit einer fragwürdigen Beschwerde eines Großkunden konfrontiert ist und sich entscheiden muss, ob sie ein unangemessenes Ansinnen des Kunden zurückweist oder den wichtigen Kunden zufriedenstellt indem sie den Mitarbeiter ohne Nachweis eines Fehlverhaltens versetzt. Diese Gefahr ist deutlich geringer, wenn beide Parteien - Anzeiger und Angezeigter - Mitarbeiter desselben Konzerns sind.

Es wurde daher eine besondere Auflage formuliert, die die Antragstellerin an ihre Verpflichtungen gegenüber ihren Mitarbeitern mahnen soll.

Eingaben im Registrierungsverfahren sind gemäß § 53 Abs. 1 DSG 2000 von den Verwaltungsabgaben des Bundes befreit.

Schlagworte

Registrierung, Auflagenbescheid, Whistle-Blowing, nicht-genehmigungspflichtiger IDVK, Datenempfänger im Safe Harbor, Safe-Harbor-Zertifizierung, Datenverwendung im Konzern, Übermittlung, Mitarbeiterdaten, Meldung mutmaßlicher Missstände, Whistle-Blower Hotline, keine Betriebsvereinbarung möglich, leitende Angestellte und Mitarbeiter mit eigenem Verantwortungsbereich

European Case Law Identifier (ECLI)

ECLI:AT:DSB:2014:DSB.D600.328.001.0001.DSB.2014

Zuletzt aktualisiert am

10.06.2015