

TE Dsk BescheidRegistrierung 2013/11/22 K600.326-001/0002- DVR/2013

JUSLINE Entscheidung

© Veröffentlicht am 22.11.2013

Norm

DSG 2000 §7;

DSG 2000 §12 Abs2;

DSG 2000 §17 Abs1;

DSG 2000 §18 Abs2;

DSG 2000 §20 Abs2;

AVRAG §10 Abs2;

1. AVRAG § 10 heute
2. AVRAG § 10 gültig ab 01.01.1995 zuletzt geändert durch BGBl. Nr. 450/1994
3. AVRAG § 10 gültig von 01.07.1993 bis 31.12.1994

Text

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

B E S C H E I D B E S C H E römisch eins D

Die Datenschutzkommission hat unter dem Vorsitz von Dr. Gerhard KURAS und in Anwesenheit der Mitglieder Dr. Gregor KÖNIG, Dr. Michaela BLAHA, Dr. Claudia ROSEN MAYR-KLEMENZ, Mag. Daniela ZIMMER und Dr. Klaus HEISSENBERGER sowie des Schriftführers Mag. Dr. Amrita MONTAGNI in ihrer Sitzung vom 22. November 2013 folgenden Beschluss gefasst:

Spruch

Unter Zugrundelegung der im Mängelrügeverfahren nach § 20 Abs. 1 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 idgF, verbesserten Registrierungsmeldung der P**** GmbH vom 31. August 2011 betreffend die Datenanwendung "P**** Integrity System" (DVR-Nummer xxxxxxxx/yyy) wird die Registrierung dieser Datenanwendung gemäß § 21 Abs. 2 DSG 2000 unter Erteilung folgender Auflagen verfügt: Unter Zugrundelegung der im Mängelrügeverfahren nach Paragraph 20, Absatz eins, Datenschutzgesetz 2000 (DSG 2000), Bundesgesetzblatt Teil

eins, Nr. 165 aus 1999, idgF, verbesserten Registrierungsmeldung der P**** GmbH vom 31. August 2011 betreffend die Datenanwendung "P**** Integrity System" (DVR-Nummer xxxxxx/yyy) wird die Registrierung dieser Datenanwendung gemäß Paragraph 21, Absatz 2, DSG 2000 unter Erteilung folgender Auflagen verfügt:

1. Die Übermittlung von personenbezogenen Daten von Beschuldigten an die P**** SA in Belgien ist nur hinsichtlich leitender Angestellter (oder vergleichbar verantwortlichen Personen) zulässig, die eines maßgeblichen Verstoßes (oder der Teilnahme daran) gegen den Verhaltenskodex des P****-Konzerns betreffend Rechnungslegung, interne Rechnungslegungskontrolle, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität, 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 Genehmigung ist an die Auflage geknüpft, 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 Genehmigung wird weiters unter der Auflage vorgenommen, dass die Antragstellerin vor Aufnahme der Übermittlungen an die P**** SA die Behandlung der an die Hotline gemeldeten Daten vertraglich geregelt hat. In dieser Vereinbarung ist festzulegen, dass die P**** SA als Dienstleister der Antragstellerin nur Meldungen mit den im Spruch bezeichneten Inhalten weiterbearbeitet und in ihrer Funktion als Konzernmutter auswertet, während die restlichen über die Hotline allenfalls eingebrachten Meldungen nur der Antragstellerin zugänglich gemacht werden. Die Rollen der P**** SA als Dienstleister und als Empfänger von Meldungen sind dabei zu trennen. Weiters ist zu vereinbaren, dass der Inhalt von Meldungen nach ihrer Übermittlung an die P**** SA bzw. nach ihrer Rück-Überlassung an die Antragstellerin beim Dienstleister umgehend gelöscht wird.

B e g r ü n d u n g

A. Vorbringen und Sachverhalt:

Die P**** Gesellschaft m.b.H. hat am 31. August 2011 die Datenanwendung "P**** Integrity System" (DVR-Nummer xxxxxx/yyy) beim Datenverarbeitungsregister gemeldet.

Die P**** Gesellschaft m.b.H. ist eine österreichische Tochter der P***** SA, mit Sitz in Belgien.

Das System dient zur Aufdeckung von Verstößen gegen den Verhaltenskodex des P****-Konzerns (P**** Code of Conduct). Der Antrag betrifft Meldungen zu Verstößen in den Bereichen Rechnungslegung, internen Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung und in der Bekämpfung von Korruption, Banken- und Finanzkriminalität hinsichtlich leitender Angestellter/Führungskräfte. Der Kodex umfasste noch andere Art von Verstößen, aber die Antragstellerin hat in der Meldung den Umfang der zu bekämpfenden Missstände auf die oben genannten Kategorien eingegrenzt (Meldung mit Stand 15. November 2011).

Die Konzernmutter P**** SA in Belgien betreibt die Hotline. Die P**** SA verarbeitet die Daten der Beschwerden auch in Fällen, in denen eine Beschwerde zurück an die Antragstellerin verwiesen wird, und handelt dabei als Dienstleister. Nur die Daten bezüglich gravierender Verstöße leitender Angestellter werden von der Konzernmutter als Übermittlungsempfänger bearbeitet.

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

hat, mit dem eine Betriebsvereinbarung abgeschlossen werden könnte.

B. In rechtlicher Hinsicht folgt daraus:

1. Anzuwendende Rechtsvorschriften

§ 7 Abs. 1 DSG 2000 lautet unter der Überschrift "Zulässigkeit der Verwendung von Daten" Paragraph 7, Absatz eins, 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: Paragraph 12, Absatz 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." "(2) Keiner Genehmigung gemäß Paragraph 13, bedarf weiters der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutz. Welche Drittstaaten angemessenen Datenschutz gewährleisten, wird unter Beachtung des Paragraph 55, Ziffer eins, durch Verordnung des Bundeskanzlers festgestellt. Maßgebend für die Angemessenheit des Schutzes ist die Ausgestaltung der Grundsätze des Paragraph 6, Absatz eins, in der ausländischen Rechtsordnung und das Vorhandensein wirksamer Garantien für ihre Durchsetzung."

§ 17 Abs. 1 DSG 2000, lautet unter der Überschrift "Meldepflicht des Auftraggebers" Paragraph 17, Absatz eins, 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." "§ 17. (1) Jeder Auftraggeber hat, soweit in den Absatz 2 und 3 nicht anderes bestimmt ist, vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission mit dem in Paragraph 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: Paragraph 18, Absatz 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" "(2) Meldepflichtige Datenanwendungen, die weder einer Musteranwendung nach Paragraph 19, Absatz 2, entsprechen, noch innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften noch die Verwendung von Daten im Katastrophenfall für die in Paragraph 48 a, Absatz eins, genannten Zwecke betreffen, dürfen, wenn sie

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

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

Bestimmungen des Paragraph 20, aufgenommen werden."

§ 21 Abs. 2 DSG 2000 lautet: Paragraph 21, Absatz 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." "(2) Bei Datenanwendungen, die gemäß Paragraph 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: Paragraph 10, Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG) Bundesgesetzblatt Nr. 459 aus 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. Paragraph 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 Paragraph 96, Absatz eins, Ziffer 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 1 DSG 2000 und unterliegt damit der Vorabkontrolle. Weiters kann die Datenschutzkommission bei Datenanwendungen, die der Vorabkontrolle unterliegen, dem Auftraggeber Bedingungen oder Auflagen für die Vornahme der Datenanwendung durch Bescheid erteilen. Die Meldung betrifft strafrechtlich relevante Daten gemäß Paragraph 18, Absatz 2, Ziffer eins, DSG 2000 und unterliegt damit der Vorabkontrolle. Weiters kann die Datenschutzkommission bei Datenanwendungen, die der Vorabkontrolle unterliegen, dem Auftraggeber Bedingungen oder 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). 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 Paragraph 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 nach Belgien:

Hinsichtlich der Übermittlung von Daten an die P**** SA in Belgien besteht Genehmigungsfreiheit, da dieses Unternehmen seinen Sitz in einem EWR-Land hat (§ 12 Abs. 1 DSG 2000). Eine separate Genehmigung gemäß § 13 DSG 2000 ist daher nicht erforderlich. Hinsichtlich der Übermittlung von Daten an die P**** SA in Belgien besteht Genehmigungsfreiheit, da dieses Unternehmen seinen Sitz in einem EWR-Land hat (Paragraph 12, Absatz eins, DSG 2000). Eine separate Genehmigung gemäß Paragraph 13, DSG 2000 ist daher nicht erforderlich.

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 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. Dies ist vor allem wichtig, weil die Konzernmutter, die P**** SA, hier sowohl als Dienstleister (in der Funktion als Hotline-Betreiber) als auch als Empfänger (hinsichtlich der Daten über gravierende Verstöße leitender Angestellter) auftritt.

2.4 Zur Rechtsgrundlage der beantragten Übermittlungen:

aa) Wie im Sachverhalt ausgeführt, sind Maßstab für den zu meldenden "Missbrauch" die konzerninternen Verhaltensregeln (P**** Code of Conduct). Für die Mitarbeiter der Antragstellerin haben diese Regeln rechtliche Relevanz durch den Verhaltenskodex, in dem das Recht und auch die Aufforderung 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.

Eine Zustimmung der Arbeitnehmer gemäß § 10 Abs. 1 und 2 AVRAG wurde eingeholt. Damit wurden die Voraussetzungen für die Rechtmäßigkeit der Übermittlung unter dem Aspekt dieser Bestimmung erfüllt. Eine Zustimmung der Arbeitnehmer gemäß Paragraph 10, Absatz eins und 2 AVRAG wurde eingeholt. Damit wurden die Voraussetzungen für die Rechtmäßigkeit der Übermittlung unter dem Aspekt dieser Bestimmung erfüllt.

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 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 "whistleblowing 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. 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 Artikel 29, Gruppe für eine datenschutzkompatible Führung einer "whistleblowing 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.

Schlagworte

Registrierung, Auflagenbescheid, nicht-genehmigungspflichtiger IDVK, Datenempfänger im EWR, Datenverwendung im Konzern, Übermittlung, Mitarbeiterdaten, Meldung mutmaßlicher Missstände, Whistle-Blowing, Whistle-Blower Hotline, Abschluss einer Betriebsvereinbarung erforderlich

Zuletzt aktualisiert am

24.04.2014

Quelle: Datenschutzbehörde Dsb, <https://www.dsb.gv.at>

© 2026 JUSLINE

JUSLINE® ist eine Marke der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH.

www.jusline.at