TE Dsk Empfehlung 2018/1/17 DSB-D213.503/0004-DSB/2017

JUSLINE Entscheidung

Veröffentlicht am 17.01.2018

Norm

DSG 2000 §1 Abs1
DSG 2000 §6 Abs1 Z3
DSG 2000 §11 Abs1 Z1
DSG 2000 §11 Abs1 Z2
DSG 2000 §10 Abs1
DSG 2000 §10 Abs2
AMSG §32 Abs3
DSGVO Art25 Abs2
DSG 2000 §30 Abs3
DSG 2000 §30 Abs6

Text

GZ: DSB-D213.503/0004-DSB/2017 vom 17.1.2018

[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.]

EMPFEHLUNG

Die Datenschutzbehörde spricht aus Anlass einer anonymen Anzeige vom 09. Dezember 2016 betreffend Zugang auf das eAMS-Konto für Weiterbildungsinstitutionen („Partnerinstitutionen"), bereitgestellt durch das AMS Österreich, ****, Dienstleistungsunternehmen des öffentlichen Rechts (im Folgenden: AMS), folgende Empfehlung aus:

1. Das AMS möge sicherstellen,

i) dass für Partnerinstitutionen des AMS tätige Trainer über das eAMS-Konto nicht mehr auf die Geschäftsfälle aller anderen Trainer und somit auf die Daten von deren Kursteilnehmern zugreifen können,

ii) insbesondere indem es die Partnerinstitutionen verpflichtet, das eService „Projekt-Veranstaltungszuordnung" zur Vornahme einer „Projekt-Veranstaltungszuordnung" zu verwenden, um somit eine technische Barriere zu errichten.

2. Für die Umsetzung dieser Empfehlung wird eine Frist von drei Monaten gesetzt.

3. Der Datenschutzbehörde sind nach Ablauf dieser Frist die zur Herstellung des rechtmäßigen Zustandes gemäß Punkt 1 aufgetragenen Maßnahmen vorzuweisen, die das AMS zur Umsetzung dieser Empfehlung ergriffen hat.

Rechtsgrundlagen: § 1 Abs. 1, § 6 Abs. 1 Z 3, § 10, § 11 Abs. 1 Z 1 und Z 2, § 30 Abs. 2 des Datenschutzgesetzes 2000 (DSG 2000), BGBl. I Nr. 165/1999 idgF; § 32 Abs. 3 des Arbeitsmarktservicegesetzes (AMSG), BGBl. Nr. 313/1994 idgF.

Gründe für diese Empfehlung

A. Vorbringen der Beteiligten und Verfahrensgang

Die Datenschutzbehörde nahm eine anonyme Anzeige vom 09. Dezember 2016 zum Anlass, ein amtswegiges Prüfverfahren einzuleiten. Der anonyme Anzeiger besitze als Trainer von AMS-Kursen Zugang auf das eAMS-Konto für Unternehmen und habe dadurch auf alle Geschäftsfälle aller anderen Trainer seines Arbeitgebers Zugriff gehabt. Somit könnten alle Trainer über Daten der Kursteilnehmer aller Gruppen der etwa 100 Trainer verfügen, insbesondere: Sozialversicherungsnummer, Lebenslauf inkl. Adresse und Telefonnummer, Berichte über Kursteilnehmer und auch Krankenstände.

Mit Schreiben vom 13. Jänner 2017 brachte das AMS der Datenschutzbehörde Ihre Stellungnahme zur Kenntnis und fügte als Anhang eine Muster-Datenschutzvereinbarung sowie die Handouts „eServices für Partnerinstitutionen Projekt-/Veranstaltungszuordnung“ und „eServices für Partnerinstitutionen Berechtigungen“ bei. Es wird zusammengefasst vorgebracht, dass das AMS gemäß § 32 Abs. 3 AMSG gesetzlich vorgegebene Dienstleistungen an geeignete Einrichtungen übertragen könne. Es würden beispielsweise Qualifizierungsmaßnahmen für arbeitslose Personen durch Weiterbildungsinstitutionen („Partnerinstitution“) erbracht. Mit diesen Partnerinstitutionen werde auch eine Datenschutzvereinbarung gemäß § 10 DSG 2000 abgeschlossen.

Das eAMS-Konto für Unternehmen und Partnerinstitutionen diene der sicheren elektronischen Kommunikation zwischen dem AMS und den Weiterbildungseinrichtungen. Die Partnerinstitutionen seien verpflichtet, bestimmte eServices zu verwenden, um die Administration von Teilnehmern von AMS-Kursen durchzuführen. Innerhalb dieses eAMS-Kontos gäbe es eine Berechtigungsstruktur, die zwischen Superuser, Poweruser und User unterscheide (beispielsweise bei Partnerinstitutionen mit Niederlassung in mehreren Bundesländern). Der Superuser müsse bestätigen, dass er in Vertretung der Partnerinstitution berechtigt wäre, die eServices des eAMS-Kontos zu nutzen, wobei ein Nachweis für die Vertretungsbefugnis zu erbringen sei.

In Folge sei die Partnerinstitution für die weitere Verteilung von Berechtigungen an Poweruser und User verantwortlich, wobei hier zwischen drei Varianten zu unterscheiden sei:

Variante 1: Durch das eService „Projekt-Veranstaltungszuordnung“ könne der Superuser oder der Poweruser einzelnen Usern die Nutzung für bestimmte Projekte/Veranstaltungen ermöglichen, für die sie zuständig wären. Im Sinne einer „Berechtigungsmatrix“ seien im Vorfeld der Projekt-/Veranstaltungszuordnung auch jedem einzelnen User die jeweiligen eServices zuzuordnen, die er für seine Tätigkeit benötigen würde. Somit sei sichergestellt, dass die User nur jene Daten einsehen könnten, die sie konkret für die Erfüllung des Auftrages benötigen würden.

Variante 2: Das AMS verpflichte die Partnerinstitutionen nicht, das eService „Projekt-/Veranstaltungszuordnung“ des eAMS-Kontos zu nutzen. Würde von einer Partnerinstitution dieses eService nicht benutzt und dadurch keine technische Barriere zur Einsicht in andere Projekte bzw. Veranstaltungen errichtet werden, so habe die Partnerinstitution geeignete Maßnahmen zu treffen, damit die Daten Unbefugten nicht zugänglich gemacht würden.

Variante 3: Die Partnerinstitution könne eine elektronische Datenerfassung außerhalb des eAMS-Kontos durchführen und die Daten gesammelt mittels einer CSV-Importierungsmöglichkeit an das AMS übertragen.

Im telefonischen Kontakt zwischen der Datenschutzbehörde und dem AMS am 21. September 2017 (Aktenvermerk vom 21. September 2017 liegt dem Akt bei) wurden Herr Karl O*** und Herr Harald T*** vom AMS befragt, ob es dazu kommen könne, dass ein Trainer über das eAMS-Konto auf die Geschäftsfälle aller anderen Trainer und somit auf die Daten von deren Kursteilnehmer zugreifen könne, sofern die Partnerinstitution keine „Projekt-/Veranstaltungszuordnung“ vornehme, oder wenn der Superuser (die Partnerinstitution) bzw. der Poweruser dem Standarduser als Trainer eine überbordende Geschäftsfallansicht einräumen würde; dies wurde vom AMS bejaht.

Mit Stellungnahme vom 22. September 2017 legte das AMS Screenshots des eAMS-Kontos vor und skizzierte anhand eines Beispiels die Vergabe von Berechtigungen.

Auf Ersuchen der Datenschutzbehörde konkretisierte das AMS seine Stellungnahme mit Schreiben vom 07. Dezember 2017 und bejahte die Frage der Datenschutzbehörde, „[..] ob ein Trainer über das eAMS-Konto auf die Geschäftsfälle aller anderen TrainerInnen und somit auf die Daten von deren KursteilnehmerInnen zugreifen kann, wenn die Partnerinstitution des AMS über das eService „Projekt-Veranstaltungszuordnung“ (...) keine „Projekt-Veranstaltungszuordnung“ vornimmt oder wenn der Superuser bzw. der Poweruser dem Standard-User eine Geschäftsfallansicht einräumt [...]“

B. Sachverhaltsfeststellungen

Die Datenschutzbehörde gelangte auf Grundlage der Ergebnisse des Ermittlungsverfahrens zu folgenden Sachverhaltsfeststellungen:

Das AMS ist ein Dienstleistungsunternehmen des öffentlichen Rechts und kann gesetzlich vorgegebene Dienstleistungen an geeignete Einrichtungen übertragen. Es werden unter anderem Qualifizierungsmaßnahmen für arbeitslose Personen durch Weiterbildungsinstitutionen („Partnerinstitution“) erbracht. Zwischen dem AMS und den Partnerinstitutionen wird jeweils eine Datenschutzvereinbarung abgeschlossen. Punkt II dieser Datenschutzvereinbarung lautet auszugsweise:

„Das AMS wird als Auftraggeber im Sinne des § 4 Z 4 DSG 2000 (nachfolgend nur „Auftraggeber“) dem <Name des Unternehmens>, das als Dienstleister im Sinne des § 4 Z 5 DSG 2000 (nachfolgend nur „Dienstleister“) tätig wird, zur Durchführung des Vertrages personenbezogene Daten im Sinne des § 4 Z 1 erster Halbsatz DSG 2000 (nachfolgend kurz: „Daten“) aus seinen Datenanwendungen überlassen.“

Das eAMS-Konto dient der elektronischen Kommunikation zwischen dem AMS und den Partnerinstitutionen. Die Partnerinstitutionen werden verpflichtet, bestimmte eServices im Rahmen des eAMS-Kontos zu nutzen, um die Administration von Teilnehmern von AMS-Kursen durchzuführen: So sind insbesondere Eintritte/Ergebnisse der Informationsveranstaltungen, Teilnahmelisten (z.B. bezugsunterbrechende Zeiten), Lebensläufe, individuelle Teilnahmeberichte sowie individuelle Ausbildungsinhalte/Lern- und Prüfungserfolge unter Verwendung des eAMS-Kontos an das AMS zu senden.

Nicht verpflichtet sind die Partnerinstitutionen jedoch, das eService „Projekt-/Veranstaltungszuordnung“ des eAMS-Kontos zu nutzen.

Innerhalb dieses eAMS-Kontos gibt es eine Berechtigungsstruktur, die zwischen Superuser (Partnerinstitution), Poweruser und Standarduser unterscheidet. Jedenfalls dann, wenn eine Partnerinstitution über das eService „Projekt-Veranstaltungszuordnung“ keine „Projekt-Veranstaltungszuordnung“ vornimmt, kann es zum Ausgangsfall kommen, wonach Standarduser über das eAMS-Konto Einsicht auf die Geschäftsfälle aller anderen Standarduser und somit auf die Daten von deren Kursteilnehmern haben. Bei den Daten handelt es sich insbesondere um: Sozialversicherungsnummer, Lebenslauf inkl. Adresse und Telefonnummer, Berichte über Kursteilnehmer und auch Krankenstände.

Beweiswürdigung: Diese Feststellungen beruhen auf dem Vorbringen des AMS vom 13. Jänner 2017, 20. Februar 2017, 22. September 2017 und 07. Dezember 2017 sowie den beiliegenden Dokumenten, insbesondere der Muster-Datenschutzvereinbarung („Datenschutzvereinbarung für Einzelprojekte“).

C. In rechtlicher Hinsicht folgt daraus:

Allgemeines

Gemäß § 10 Abs. 1 DSG 2000 dürfen Auftraggeber bei ihren Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten.

Darüber hinaus ist gemäß § 10 Abs. 2 DSG 2000 [...] die beabsichtigte Heranziehung eines Dienstleisters durch einen Auftraggeber des öffentlichen Bereichs im Rahmen einer Datenanwendung, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegt, der Datenschutzbehörde mitzuteilen, es sei denn, dass die Inanspruchnahme des Dienstleisters auf Grund ausdrücklicher gesetzlicher Ermächtigung erfolgt [...].

Gemäß § 32 Abs. 3 AMSG kann das AMS gewisse Dienstleistungen, die es nicht selbst bereitstellen kann oder deren Bereitstellung unzweckmäßig oder unwirtschaftlich wäre, an andere geeignete Einrichtungen übertragen. Dabei dürfen schutzwürdige Interessen Dritter im Sinne des § 1 Abs. 1 des Datenschutzgesetzes nicht verletzt werden.

Daten dürfen gemäß § 6 Abs. 1 Z 3 DSG 2000 nur verwendet werden, soweit sie für den Zweck der Datenanwendung wesentlich sind und über diesen Zweck nicht hinausgehen.

Dienstleister haben gemäß § 11 Abs. 1 Z 1 DSG 2000 die Pflicht, bei der Verwendung von Daten für den Auftraggeber die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden [...].

Dienstleister haben gemäß § 11 Abs. 1 Z 2 DSG 2000 die Pflicht, alle gemäß § 14 DSG 2000 erforderlichen Datenschutzmaßnahmen zu treffen [...].

In der Sache

Wie festgestellt, ist das AMS ein Dienstleistungsunternehmen des öffentlichen Rechts. Somit ist gemäß § 10 Abs. 2 DSG 2000 zu prüfen, ob eine Voraussetzung für die Heranziehung eines Dienstleisters durch einen Auftraggeber des öffentlichen Bereichs vorliegt. Eine entsprechende gesetzliche Ermächtigung findet sich in § 32 Abs. 3 AMSG, sodass die Heranziehung eines Dienstleisters durch das AMS grundsätzlich zulässig ist.

In weiterer Folge war zu prüfen, ob durch die Heranziehung von Dienstleistern (Partnerinstitutionen)schutzwürdige Interessen Dritter im Sinne des § 1 Abs. 1 DSG 2000 verletzt werden (§ 32 Abs. 3 letzter Satz DSG 2000):

Bei der in Rede stehenden Datenanwendung handelt es sich um das „eAMS-Konto für Unternehmen (Partnerinstitutionen) bzw. die eServices für Partnerinstitutionen". Bestimmte eServices, zu deren Verwendung - nach den getroffenen Feststellungen – die Partnerinstitutionen verpflichtet sind, dienen ausschließlich dem Zweck der zwischen dem AMS und den Partnerinstitutionen erfolgenden „Verwaltung der Kursteilnehmer": So müssen bestimmte Informationen (insbesondere Eintritte/Ergebnisse der Informationsveranstaltungen, Teilnahmelisten (z.B. bezugsunterbrechende Zeiten), Lebensläufe, individuelle Teilnahmeberichte sowie individuelle Ausbildungsinhalte/Lern- und Prüfungserfolge) von den Partnerinstitutionen unter Verwendung des eAMS-Kontos an das AMS gesendet werden. Das bedeutet, dass sich die Verwendung von Daten durch einen Trainer dann im Rahmen des Zwecks „Verwaltung der Kursteilnehmer" halten wird, wenn er etwas zu diesem Zweck beitragen kann, indem er die vom AMS gewünschten Informationen über die an seinen eigenen Kursen teilnehmenden Arbeitsuchenden mit dem AMS austauschen kann. Zur Erfüllung des Zwecks „Verwaltung der Kursteilnehmer" ist es aber nicht notwendig und daher überschießend, dass der jeweilige Trainer über die Daten seiner Kursteilnehmer hinaus auch Zugriff auf die Daten von Kursteilnehmern anderer Trainer hat.

Ein solch überschießender Zugriff auf Daten ist unzulässig, da er insbesondere dem datenschutzrechtlichen Grundsatz gemäß § 6 Abs. 1 Z 3 DSG 2000 widerspricht, wonach Daten nur verwendet werden dürfen, soweit sie für den Zweck der Datenanwendung wesentlich sind und soweit sie über diesen Zweck nicht hinausgehen.

Zu einem solch uneingeschränkten Zugriff auf die Daten nicht nur der eigenen, sondern aller Kursteilnehmer kommt es nach den getroffenen Feststellungen jedenfalls in jenen Fällen, in denen über das eService „Projekt-Veranstaltungszuordnung" keine „Projekt-Veranstaltungszuordnung" vorgenommen wird.

Es war folglich gemäß § 30 Abs. 6 DSG 2000 zur Herstellung des rechtmäßigen Zustandes die obige Empfehlung zu erteilen, die Zugriffsberechtigungen auf das notwendige Ausmaß zu beschränken.

In diesem Zusammenhang ist auch auf die ab 25. Mai 2018 anwendbare Datenschutz-Grundverordnung (DSGVO) hinzuweisen, wonach Verantwortliche gemäß Art. 25 Abs. 2 DSGVO verpflichtet sind, datenschutzfreundliche Voreinstellungen zu treffen, sodass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Schlagworte

Empfehlung, amtswegiges Prüfverfahren, AMS, eServices, eAMS-Konto, Partnerinstitutionen, Heranziehung von Dienstleistern, Kursveranstalter, Pflichtenüberbindung, Datenerfassung, Beschränkung der Zugriffsberechtigung, datenschutzfreundliche Voreinstellungen

European Case Law Identifier (ECLI)

ECLI:AT:DSB:2018:DSB.D213.503.0004.DSB.2017

Zuletzt aktualisiert am

20.02.2018

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