EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
STELLVERTRETENDER DATENSCHUTZBEAUFTRAGTER

Dr. Udo HELMBRECHT
Exekutivdirektor
Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA)
Postfach 1309
710 01 Heraklion,
Kreta
GRIECHENLAND

Brüssel, den 31. März 2016
WW/XK/sn/D(2016)0756 **C 2011-1149**
Bitte richten Sie alle Schreiben an:
edps@edps.europa.eu

Betr.: **Stellungnahme zur Vorabkontrolle der Verarbeitung von Gesundheitsdaten bei der Agentur der Europäischen Union für Netz- und Informationssicherheit (Fall 2011-1149)**

Sehr geehrter Herr Dr. Helmbrecht,

am 15. Dezember 2015 erhielt der Europäische Datenschutzbeauftragte („EDSB“) eine Meldung zur Vorabkontrolle der Verarbeitung von Gesundheitsdaten gemäß Artikel 27 Absatz 2 Buchstabe a der Verordnung (EG) Nr. 45/2001 („Verordnung“)[1]. Der Zweck dieser Verarbeitung besteht darin, die Einhaltung der Anforderungen sicherzustellen, die im Statut der Beamten im Zusammenhang mit ärztlichen Einstellungsuntersuchungen, jährlichen ärztlichen Kontrolluntersuchungen und Krankenurlaub der Bediensteten der Agentur vorgesehen sind. Folgende Unterlagen wurden dem EDSB übersandt:

- ein Entwurf einer Strategie für die Verarbeitung von Gesundheitsdaten bei der ENISA,
- eine Datenschutzerklärung betreffend die Verarbeitung gesundheitsbezogener Daten,
- ein Auszug aus der Vertraulichkeitserklärung der ENISA mit Verweisen auf Artikel 10 Absatz 3 und Artikel 7 Absatz 3 und
- Kopien von Auszügen aus Verträgen (betreffend Vertraulichkeit und Datenschutz) mit dem externen medizinischen Dienstleister.

[1] Die Meldung wurde dem EDSB am 10. Dezember 2011 übermittelt, doch fehlten wichtige Informationen und Dokumente. Daraufhin fand ein Briefwechsel zwischen dem EDSB und dem damaligen Datenschutzbeauftragten statt. Am 19. Juni 2015 stattete der EDSB der ENISA einen Besuch ab.

Da die Verarbeitung bereits angelaufen ist, gilt die Frist von zwei Monaten für die Abgabe der Stellungnahme des EDSB nicht.

Die Analyse der Meldung und der entsprechenden Unterlagen erfolgt vor dem Hintergrund der Leitlinien des EDSB für die Verarbeitung von Gesundheitsdaten am Arbeitsplatz („Leitlinien")[2]. Die gemeinsame Stellungnahme zur Verarbeitung von Daten über die Gesundheit durch 18 Agenturen[3] ist im vorliegenden Fall ebenfalls anwendbar.

Der EDSB wird nur auf diejenigen Praktiken der ENISA eingehen, die nicht mit den Grundsätzen der Verordnung sowie den Leitlinien im Einklang zu stehen scheinen, und der ENISA entsprechende Empfehlungen unterbreiten.

1) Verarbeitung personenbezogener Daten im Auftrag des für die Verarbeitung Verantwortlichen

Die ENISA hat einen Vertrag mit einem externen medizinischen Dienstleister abgeschlossen, und gemäß diesem Vertrag wurde für die Erbringung medizinischer Dienstleistungen für die Bediensteten der ENISA ein ärztlicher Berater ausgewählt.

In Artikel I.9 des Vertrags, in dem es um Datenschutz geht, werden die Rechte des externen Auftragnehmers erwähnt. Natürlich hat die ENISA Pflichten im Hinblick auf die Verarbeitung personenbezogener Daten des Auftragnehmers und hat dieser wiederum sich aus der Verordnung ergebende Rechte. Gegenstand des Vertrags ist jedoch die Erbringung medizinischer Dienstleistungen für die Bediensteten der ENISA. Die ENISA sollte daher einen Absatz zu den **Pflichten** des Auftragnehmers bei der Verarbeitung der personenbezogenen Daten der Bediensteten der Agentur aufnehmen.

In Anbetracht der Schutzwürdigkeit der hier zu prüfenden Verarbeitungen hätte die ENISA eine maßgeschneiderte Klausel ausarbeiten können, anstatt eine Standarddatenschutzklausel zu verwenden. Auch wenn bedauerlicherweise der Vertrag bereits unterzeichnet wurde, empfiehlt der EDSB der ENISA eine Überarbeitung des Vertrags und die Hinzufügung einer Klausel betreffend die **Pflichten** des Auftragnehmers bei der Verarbeitung personenbezogener Daten der Bediensteten der Agentur. Über die dem Auftragnehmer aus der Verordnung erwachsenden Rechte sollte die ENISA den Auftragnehmer besser im Wege eines Datenschutzhinweises oder eines anderen von ihr als angemessen betrachteten Instruments informieren.

2) Aufbewahrungsfristen

Die Meldung besagt, dass die **Diensttauglichkeitsatteste vor der Einstellung** in der Personalakte unbefristet aufbewahrt werden. Mit Blick auf Artikel 4 Absatz 1 Buchstabe e sollte die ENISA eine Höchstaufbewahrungsfrist festlegen, die für den Zweck erforderlich ist, für den die Diensttauglichkeitsatteste erhoben wurden. Der EDSB empfiehlt, die Diensttauglichkeitsatteste in der Personalakte maximal zehn Jahre nach dem Ende des Zeitraums aufzubewahren, in dem der Bedienstete im aktiven Dienst war oder die letzte Ruhegehaltszahlung erhalten hat.

[2] Angenommen im September 2009 und auf der Website des EDSB veröffentlicht.
[3] Angenommen am 11. Februar 2011; es ging darin um 18 Agenturen; Fall 2010-0071.

Die ENISA sollte in der Meldung angeben, dass die **medizinischen Daten der Einstellungsuntersuchungen** vom medizinischen Dienst der Kommission maximal 30 Jahre nach Hinzufügen des letzten Dokuments in die Gesundheitsakte aufbewahrt werden.

Zu den **vom externen ärztlichen Berater aufbewahrten medizinischen Daten** heißt es in der Meldung, dass sie für ein Jahr gespeichert werden, während im Entwurf der Strategie im Einklang mit den Vorgaben des EDSB von 30 Jahren die Rede ist. Diese Unstimmigkeit sollte beseitigt werden.

Die ENISA sollte deshalb in der Meldung klar die oben genannten Aufbewahrungsfristen angeben.

3) Informationspflicht gegenüber der betroffenen Person

Die ENISA hat für das Intranet den Entwurf einer Strategie für die Verarbeitung von Gesundheitsdaten erstellt, in dem das Verfahren und bewährte Datenschutzverfahren im Zusammenhang mit ärztlichen Einstellungsuntersuchungen, jährlichen ärztlichen Pflichtuntersuchungen und Attesten erläutert werden. Dessen ungeachtet sollten gemäß Artikel 11 der Verordnung Bedienstete zur Gewährleistung einer Verarbeitung nach Treu und Glauben und aus Gründen der Transparenz über die Verarbeitung ihrer personenbezogenen Daten informiert werden, **bevor** die Daten erhoben werden.

Datenschutzerklärungen zur Einstellungsuntersuchung und zu den jährlichen ärztlichen Kontrolluntersuchungen

Der dem EDSB vorgelegte Datenschutzhinweis betrifft nur die Verarbeitung ärztlicher Atteste bei Fehlzeiten. Die ENISA sollte zwei klare und präzise Datenschutzhinweise zu den Einstellungsuntersuchungen und zu den jährlichen Kontrolluntersuchungen ausarbeiten, die alle in den Artikeln 11 und 12 der Verordnung geforderten Informationen enthalten.

Der Datenschutzhinweis zu den Einstellungsuntersuchungen sollte dem Einladungsschreiben zur Durchführung der Einstellungsuntersuchung, das dem erfolgreichen Bewerber übermittelt wird, beigelegt werden.

Der Datenschutzhinweis zu den jährlichen Kontrolluntersuchungen sollte allen Bediensteten einfach zugänglich gemacht werden, sobald diese die Durchführung ihrer jährlichen Kontrolluntersuchung entweder beim externen ärztlichen Berater der ENISA oder bei einem Hausarzt beantragen.

Identität des für die Verarbeitung Verantwortlichen

Gemäß Artikel 11 Absatz 1 Buchstabe a und Artikel 12 Absatz 1 Buchstabe s ist es wichtig, dass in allen drei Datenschutzhinweisen (auch in dem zu Attesten) eine Kontaktperson in der Personalabteilung angegeben wird, sodass sich Bedienstete direkt an den zuständigen Sachbearbeiter wenden können und schriftliche Ersuchen und Wahrung der Vertraulichkeit möglich sind. Der EDSB erinnert daran, dass in der Praxis die Personalabteilung der ENISA für die interne Verwaltung der hier zu prüfenden Verarbeitungen verantwortlich ist. Aus rechtlicher Perspektive ist die ENISA der für diese Verarbeitungen Verantwortliche.

Recht auf Auskunft und Berichtigung

Ausgehend von Artikel 11 Absatz 1 Buchstabe e und Artikel 12 Absatz 1 Buchstabe e der Verordnung sollte die ENISA in allen Datenschutzhinweisen erklären, auf welche Weise die

betroffenen Personen ihre Rechte auf Auskunft und Berichtigung ausüben können, sodass sie ihre Rechte uneingeschränkt verstehen.

Die ENISA sollte erwähnen, dass die Bediensteten indirekt – und nicht direkt – über einen von ihnen benannten Arzt[4] Zugang zu ihren psychiatrischen und psychologischen Gutachten erhalten können.

Mit Blick auf das Recht auf Berichtigung sollte die ENISA erwähnen, dass Bedienstete das Recht haben, nicht nur administrative Fehler in ihrer medizinischen Akte zu berichtigen, sondern auch die Akte um Stellungnahmen anderer Ärzte zu ergänzen, um die Vollständigkeit der Akte sicherzustellen.

Fristen für die Aufbewahrung der Daten

Im Sinne der Artikel 11 Absatz 1 Buchstabe f Ziffer ii und 12 Absatz 1 Buchstabe f Ziffer ii der Verordnung sollte die ENISA in dem jeweiligen Datenschutzhinweis die Aufbewahrungsfrist für Gesundheitsdaten sowie für Diensttauglichkeitsatteste bei der Einstellung angeben.

Die ENISA sollte alle Empfehlungen des EDSB umsetzen, um im Einklang mit der Verordnung zu stehen, und die Meldung erforderlichenfalls aktualisieren. Als Folgemaßnahme erwartet der EDSB, dass die ENISA alle aktualisierten sachdienlichen Dokumente innerhalb einer Frist von drei Monaten als Nachweis für die Umsetzung der obigen Empfehlungen übermittelt.

Mit freundlichen Grüßen

(unterzeichnet)

Wojciech Rafał WIEWIÓROWSKI

Verteiler: Herrn Aidan RYAN, Verwaltungsdirektor.
Frau Athena BOURKA, Datenschutzbeauftragte

[4] Diesbezüglich sollte sich die ENISA an die Schlussfolgerung 221/04 des Kollegiums der Verwaltungschefs vom 19. Februar 2004 halten.