WOJCIECH RAFAŁ WIEWIÓROWSKI
STELLVERTRETENDER DATENSCHUTZBEAUFTRAGTER

[…]
Datenschutzbeauftragte®
Europäische Bankenaufsichtsbehörde
One Canada Square, Canary Wharf
London E14 5AA
Vereinigtes Königreich

Brüssel, den 19. Dezember 2016
WW/OL/ssp/D(2016)2764 **C 2016-1113**
Bitte richten Sie alle Schreiben an
edps@edps.europa.eu

Betr.: **Meldung zur Vorabkontrolle der Verwendung von ECAS bei der EBA (EDSB Fall 2016-1113)**

Sehr geehrte(r) […],

am 30. November 2016 ging beim Europäischen Datenschutzbeauftragten (EDSB) Ihre Meldung zur Vorabkontrolle gemäß Artikel 27 der Verordnung (EG) Nr. 45/2001[1] (Verordnung) der Nutzung des Authentifizierungssystems der Europäischen Kommission (European Commission Authentication System / EU Login (ECAS)) ein, über das EBA-Bedienstete Zugang zu bestimmten Anwendungen auch außerhalb des EBA-Netzwerks erhalten.[2]

1. Sachverhalt

Die EBA plant den Einsatz von ECAS / EU Login für ihre Bediensteten, damit diese Zugang zu mehreren Anwendungen, darunter JSIS online (Joint Sickness Insurance Scheme - Erstattung von Kosten für ärztliche Behandlung) auch von außerhalb des EBA-Netzwerks haben, beispielsweise von zu Hause.

Um ECAS / EU Login von außerhalb der Netzwerke der Organe und Agenturen nutzen zu können, muss eine doppelte Authentifizierung vorgenommen werden. Neben der Kombination von Nutzername und Passwort wird ein Zugangscode an eine vom Bediensteten angegebene Mobiltelefonnummer (für ein privates oder ein Diensthandy) geschickt. Damit dies möglich ist, müssen Bedienstete eine solche Mobiltelefonnummer angeben, die an die Europäische Kommission weitergegeben wird, die ECAS / EU Login verwaltet.

[1] ABl. L 8 vom 12.1.2001, S. 1.
[2] Gemäß Artikel 27 Absatz 4 der Verordnung hat der EDSB seine Stellungnahme innerhalb von zwei Monaten nach Eingang der Meldung abzugeben (Aussetzungen fallen nicht unter diese Frist). Der EDSB muss seine Stellungnahme also bis spätestens 30. Januar 2017 abgeben.
2017.

In dem Formblatt, in dem EBA-Bedienstete diese Nummer angeben sollen, werden sie auch aufgefordert, in die Weitergabe ihrer Telefonnummer an die Europäische Kommission zwecks Übersendung des SMS-Token einzuwilligen.

In der Meldung wird die Verarbeitung von Gesundheitsdaten als Grund für die Einreichung zur Vorabkontrolle angeführt.

2. Rechtliche Prüfung

In Artikel 27 Absatz 2 der Verordnung sind die Kriterien aufgelistet, aufgrund derer Verarbeitungen „besondere Risiken beinhalten können" und daher einer Vorabkontrolle zu unterziehen sind. Unter Buchstabe a dieses Absatzes wird die „Verarbeitung von Daten über Gesundheit" genannt.

Wird ECAS dazu verwendet, EBA-Bediensteten Zugang zu JSIS online von außerhalb des Netzwerks der Agentur zu gewähren, kommt es in der Tat zur Verarbeitung von Gesundheitsdaten. Allerdings ist ECAS / EU Login nur der Zugangskanal, während die eigentliche Verarbeitung personenbezogener Daten in JSIS online oder anderen über ECAS / EU Login aufgerufenen Anwendungen stattfindet.[3]

Somit ist ECAS als solches **keiner Vorabkontrolle zu unterziehen** (bei einigen Verarbeitungen durch Anwendungen, auf die über ECAS / EU Login zugegriffen wird, mag dies anders sein). Dessen ungeachtet möchte der EDSB zu den gemeldeten Verarbeitungen eine Anmerkung machen:

Die EBA ersucht ihre Bediensteten um die Einwilligung, die Mobiltelefonnummer an die Europäische Kommission weiterzugeben. Damit eine Einwilligung gültig ist, muss sie unter anderem „ohne Zwang gegeben" worden sein.[4] Aufgrund des Kräfteungleichgewichts zwischen Arbeitgeber und Beschäftigtem ist die Einwilligung in einem Beschäftigungsverhältnis nur schwer heranzuziehen. Sie sollte nur dann verwendet werden, wenn Mitarbeiter eine echte Wahlmöglichkeit zwischen Einwilligung und Nicht-Einwilligung haben.[5] Im vorliegenden Fall können Bedienstete Anwendungen, bei denen der Zugang von außerhalb des EBA-Netzwerks über ECAS / EU Login erfolgt, nur nutzen, wenn sie in die Weitergabe ihrer Telefonnummer an die Europäische Kommission einwilligen. Verweigern Bedienstete diese Einwilligung, können sie die Anwendungen noch immer innerhalb des EBA-Netzwerks nutzen; die Heranziehung der Einwilligung ist also hier möglich, wenn die Bediensteten umfassend informiert werden. Die EBA sollte also dafür Sorge tragen, dass die Bediensteten umfassend über ihre Entscheidung und deren Konsequenzen aufgeklärt werden; das Einwilligungsformblatt, dass EBA-Bedienstete zu unterzeichnen haben, sowie die Datenschutzerklärung zu ECAS / EU Login bieten entsprechende Informationen. Im Einwilligungsformblatt könnte allerdings deutlicher zum Ausdruck gebracht werden, dass bei Verweigerung der Einwilligung die einzige Konsequenz darin besteht, dass eine Nutzung von über ECAS / EU Login zugänglichen Anwendungen außerhalb des EBA-Netzwerks nicht möglich ist.

3. Schlussfolgerung

Wie bereits erläutert, sind die gemeldeten Verarbeitungen **keiner Vorabkontrolle gemäß Artikel 27** der Verordnung zu unterziehen.

---

[3] Siehe die Vorabkontrollstellungnahme des EDSB vom 10. Juli 2007 zur Verwaltung des Krankheitsfürsorgesystems im Hinblick auf die Erstattung von Kosten für ärztliche Behandlung (ASSMAL) durch die Kommission (Fall 2004-0238).

[4] Siehe Artikel 29-Datenschutzgruppe, Stellungnahme 15/2011 zur Definition von Einwilligung, insbesondere S. 13, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf

[5] Ein Beispiel wäre die freiwillige Aufnahme von Bildern in ein internes Verzeichnis.

Der EDSB empfiehlt jedoch, im Einwilligungsformblatt deutlicher zum Ausdruck zu bringen, dass bei Verweigerung der Einwilligung die einzige Konsequenz darin besteht, dass eine Nutzung von über ECAS / EU Login zugänglichen Anwendungen außerhalb des EBA-Netzwerks nicht möglich ist. Vor dem Hintergrund des Grundsatzes der Rechenschaftspflicht erwartet der EDSB von der EBA die entsprechende Umsetzung der obigen Empfehlung und hat daher beschlossen, **den Fall abzuschließen**.

Mit freundlichen Grüßen

[gezeichnet]

Wojciech Rafał WIEWIÓROWSKI