



WOJCIECH RAFAŁ WIEWIÓROWSKI
STELLVERTRETENDER DATENSCHUTZBEAUFTRAGTER

Direktor der Abteilung Humanressourcen
Amt der Europäischen Union für geistiges
Eigentum
Avenida de Europa 4
E-3008 Alicante
Spanien

Brüssel,
WW/ZS/sn/ D(2017) 6. Dezember 2017
C 2017-0813
Bitte richten Sie alle Schreiben an
edps@edps.europa.eu

Betr.: Stellungnahme zur Vorabkontrolle des Feedback-Events 2017 beim Amt der Europäischen Union für geistiges Eigentum (EDSB Fall 2017-0813)

Sehr geehrte(r) ...,

am 18. September 2017 erhielt der Europäische Datenschutzbeauftragte („EDSB“) vom Datenschutzbeauftragten („DSB“) des Europäischen Amtes für geistiges Eigentum („EUIPO“)¹ eine Meldung zur Vorabkontrolle des „Feedback-Events 2017“ gemäß Artikel 27 der Verordnung (EG) Nr. 45/2001² („Verordnung“).

Wie vom DSB erwähnt, ist die Meldung eine Aktualisierung der Meldung zur Vorabkontrolle von „Peer-Feedback-Fragebogen beim HABM“³. Diese Verarbeitung weist ferner starke Ähnlichkeiten mit anderen gemeldeten Fällen von Feedback-Tools für Führungskräfte auf, die der EDSB bereits einer Vorabkontrolle unterzogen hat.⁴ Daher enthält die vorliegende Stellungnahme keine vollständige Analyse aller Datenschutzaspekte. Sie geht vielmehr hauptsächlich auf Punkte ein, die von anderen Fällen abweichen, oder auf Punkte, die von der

¹ Gemäß Artikel 27 Absatz 4 der Verordnung hat der EDSB seine Stellungnahme innerhalb von zwei Monaten nach Eingang der Meldung abzugeben (Aussetzungen aufgrund von Ersuchen um weitere Informationen fallen nicht unter diese Frist). Die Frist wurde ausgesetzt zwischen 22. und 25. September, 10. und 14. November, 14. und 16. November, 21. November und 6. Dezember und am 6. Dezember die Konsultation des DSB. Der EDSB muss seine Stellungnahme also bis spätestens 12. Dezember 2017 abgeben.

² ABl. L 8 vom 12.1.2001, S. 1.

³ EDSB Fall 2015-0733, Stellungnahme vom 24. November 2015.

⁴ Fälle 2009-0215, 2013-1290, 2014-0906, 2014-1146, 2015-0733, 2015-0772, 2016-0002, 2016-1007 und 2017-0588.

früheren Meldung zum „Peer-Feedback-Fragebogen beim HABM“ abweichen oder anderweitig der Verbesserung bedürfen.⁵

1. Sachverhalt und Analyse

1.1. Rechtmäßigkeit der Verarbeitung

Rechtsgrundlage für die Verarbeitung sind Artikel 24a des Beamtenstatuts sowie die Artikel 11 und 81 der Beschäftigungsbedingungen für die sonstigen Bediensteten.

Als Gründe für die Rechtmäßigkeit führte das EUIPO an, die Verarbeitung personenbezogener Daten beruhe auf der unmissverständlichen, ausdrücklichen, informierten und freien Einwilligung der betroffenen Person (Artikel 5 Buchstabe d⁶ der Verordnung).

Die Einwilligung der betroffenen Person ist in Artikel 2 Buchstabe h der Verordnung definiert als „*jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass sie betreffende personenbezogene Daten verarbeitet werden*“. Der EDSB weist jedoch darauf hin, dass in einem Beschäftigungskontext die Einwilligung mit Vorsicht herangezogen werden sollte. Eine solche Einwilligung dürfte kaum Rechtsgrundlage für eine Datenverarbeitung im Arbeitsumfeld sein, es sei denn, Beschäftigte können sie verweigern, ohne nachteilige Folgen befürchten zu müssen. Beschäftigte sind aufgrund der Abhängigkeitsbeziehung zwischen Arbeitgeber/Arbeitnehmer praktisch nie in der Lage, freiwillig eine Einwilligung zu erteilen, sie zu verweigern oder zurückzunehmen. Aufgrund des Machtungleichgewichts können Beschäftigte nur unter außergewöhnlichen Umständen aus freien Stücken eine Einwilligung erteilen, wenn nämlich mit der Annahme oder Ablehnung eines Angebots überhaupt keine Konsequenzen verbunden sind.

In der Meldung heißt es ganz klar, dass die Teilnahme an der Verarbeitung sowohl für die Beurteilten als auch die Beurteilenden freiwillig ist. Ob die betroffene Person teilnimmt oder nicht hat keinerlei Konsequenzen für sie. Teilnehmer können jederzeit aussteigen. Aus der Datenschutzerklärung geht jedoch nicht hervor, dass die Einwilligung jederzeit, auch wenn das Verfahren bereits läuft, widerrufen werden kann. Der Vollständigkeit halber sollte in der Datenschutzerklärung eindeutig erklärt werden, dass sich die Einwilligung auf das gesamte Verfahren bezieht und damit auch auf die Gruppenberichte (siehe weiter unten Punkt 1.2).

Der EDSB **empfiehlt**, in der Datenschutzerklärung klar zum Ausdruck zu bringen, dass sich die Einwilligung auf das gesamte Verfahren einschließlich der Gruppenberichte bezieht und dass die Teilnehmer jederzeit und ohne nachteilige Folgen aus der Verarbeitung aussteigen können.

⁵ Gegenstand der Meldung sind 1) eine Zufriedenheitsumfrage bei den Mitarbeitern bezüglich der Arbeitsweise des EUIPO, 2) ein Peer-Feedback, das Mitarbeitern dabei helfen soll, eine Selbstbeurteilung vorzunehmen und Feedback über ihre und von ihren Kollegen zu geben und zu empfangen, und 3) ein 360°-Feedback für Führungskräfte, die von ihren Kollegen und von unmittelbaren Vorgesetzten und Vorgesetzten, denen sie Bericht erstatten, Feedback bezüglich ihrer Führungsqualitäten erhalten. Am 14. November bestätigte das EUIPO, dass sich die Meldung zur Vorabkontrolle nur auf das Peer-Feedback und das 360°-Feedback bezieht, da die Zufriedenheitsumfrage bei den Mitarbeitern wohl keine spezifischen Risiken für die Rechte und Freiheiten betroffener Personen beinhaltet. Daher befasst sich die vorliegende Stellungnahme nur mit Verarbeitungsvorgängen im Zusammenhang mit dem Peer-Feedback und dem 360°-Feedback.

⁶ Personenbezogene Daten dürfen nur verarbeitet werden, wenn die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat.

1.2. Verarbeitung von Gruppenberichten

Laut Meldung werden die bereitgestellten Informationen automatisch sowohl zu Gruppenberichten als auch zu individuellen Feedback-Berichten verarbeitet (einschließlich konsolidierter Daten, die eine Identifizierung der Feedbackgeber verhindern). Während die individuellen Feedback-Berichte nur der betroffenen Person zugänglich sind, können die Gruppenberichte vom Exekutivdirektor, dem Direktor Humanressourcen und einer begrenzten Zahl anderer Mitarbeiter eingesehen werden.⁷ Gruppen-Feedback-Berichte werden erstellt, um einen die Organisation betreffenden Überblick über die Ergebnisse des Peer-Feedback und des 360°-Feedback zu erhalten. Sie geben dem EUIPO Auskunft über Stärken und die Bereiche, in denen Verbesserungen erforderlich sind. Sie umfassen einen Teamleader-Gruppenbericht, einen Manager-Gruppenbericht und einen Mitarbeiter-Gruppenbericht. Zur Wahrung der Vertraulichkeit enthalten diese Bericht nur aggregierte und anonymisierte Daten und werden nur freigegeben, wenn eine Mindestzahl⁸ an Einzelberichten vorliegt.

Die Gruppenberichte ermöglichen keine Identifizierung einzelner Antworten auf die Fragen des Online-Fragebogens. In Anbetracht des fakultativen Charakters der Verarbeitung begrüßt der EDSB die Einführung eines Kriteriums betreffend eine Mindestanzahl von Teilnehmern, die für die Erstellung von Einzel- und Gruppenberichten benötigt wird. Wir unterstreichen jedoch nachdrücklich, dass unbedingt zu gewährleisten ist, dass die Berichte keine Daten enthalten, die eine Identifizierung von Personen erlauben, indem sie aggregierte Daten in personenbezogene Daten umwandeln.

Des Weiteren gehen wir davon aus, dass die Weitergabe von Gruppenberichten nicht dem gleichen Zweck dient wie die Erstellung von Einzelberichten⁹, und die Datenschutzerklärung enthält weder Angaben zum Zweck der Erzeugung von Gruppenberichten noch zu den darin enthaltenen Datenkategorien.

Der EDSB **empfiehlt**, in der Datenschutzerklärung klar zum Ausdruck zu bringen, welches die jeweiligen (unterschiedlichen) Ziele der Gruppenberichte sind und welche Datenkategorien sie enthalten.

1.3. Verarbeitung im Auftrag des für die Verarbeitung Verantwortlichen

Den vom EUIPO vorgelegten Informationen und der Datenschutzerklärung ist zu entnehmen, dass die Verarbeitung der personenbezogenen Daten einem externen Anbieter auf der Grundlage eines Rahmenvertrags übertragen wurde. Der Auftragnehmer arbeitet mit einem spezifischen Unterauftragnehmer am Peer-Feedback und am 360°-Feedback. Alle personenbezogenen Daten werden verarbeitet und gespeichert auf externen Tools im Besitz des Auftragnehmers, der seinen Sitz im Vereinigten Königreich hat. Das EUIPO teilte ferner mit, dass der Auftragnehmer nach ISO 27001 zertifiziert ist und einen Cloud-Diensteanbieter nutzt, dessen Server sich in der EU befinden. Der Cloud-Diensteanbieter wendet die Normen ISO 27001, 27017 und 27018 an.

⁷ Nicht zugänglich sind hingegen Daten in einigen Bereichen wie „Zusammenfassung Manager-Heatmap“, „Zusammenfassung Teamleader-Heatmap“, „Zusammenfassung Mitarbeiter-Heatmap“.

⁸Für die Gruppenberichte sind mindestens zehn Einzelberichte erforderlich, und mindestens drei Personen sollten Input für die individuellen Feedback-Berichte geben, damit die Berichte freigegeben werden.

⁹ Der Zweck der Einzelberichte für das Peer-Feedback besteht darin, Mitarbeitern eine Selbstbeurteilung zu ermöglichen sowie Feedback über ihre Kollegen und von ihren Kollegen zu geben und zu empfangen. Beim 360°-Feedback für Manager besteht der Zweck darin, Feedback von den Kollegen und von unmittelbaren Vorgesetzten und Vorgesetzten, an die sie berichten, Feedback zu ihren Führungsqualitäten zu erhalten.

Am 14. November teilte das EUIPO dem EDSB mit, dass möglicherweise Mitarbeiter eines Auftragnehmers in einem Drittland ohne Angemessenheitsentscheidung auf die Daten zugreifen müssen. Das EUIPO reichte die Musterstandardvertragsklauseln ein, die der Auftragnehmer in seinen Verträgen mit Unterauftragnehmern verwendet und bestätigte schließlich am 16. November, dass der Auftragnehmer garantiert, dass keine Stelle außerhalb der Europäischen Union auf die vom EUIPO bereitgestellten Daten zugreifen kann.

Der Auftragnehmer hat einen Unterauftragnehmer mit Sitz in den USA. Dieser Unterauftragnehmer ist abgedeckt durch das Datenschutzschild und dort als aktiver Teilnehmer registriert. Der EDSB begrüßt, dass der für die Verarbeitung Verantwortliche zum Abfedern potenzieller Risiken in Vorbereitung einer umfassenden Risikobewertung die Maßnahmen des Unterauftragnehmers in den Bereichen Organisation, Technik und IT prüft.

Der EDSB begrüßt, dass der Rahmenvertrag die Anwendung der Verordnung (EG) Nr. 45/2001¹⁰ auf alle Verarbeitungen personenbezogener Daten im Zusammenhang mit dem Vertrag vorsieht und auch detaillierte Bestimmungen zu den Rechten und Pflichten des Auftragnehmers einschließlich der Vergabe von Unteraufträgen enthält¹¹. Des Weiteren nimmt der EDSB zur Kenntnis, dass sowohl der Auftragnehmer als auch sein Unterauftragnehmer in der Datenschutzerklärung ausdrücklich erwähnt werden.

...

2. Schlussfolgerung

In dieser Stellungnahme hat der EDSB mehrere Empfehlungen ausgesprochen, damit der Verordnung Genüge getan wird, und verschiedene Verbesserungsvorschläge formuliert. Der EDSB erwartet die **Umsetzung** der folgenden in dieser Stellungnahme ausgesprochenen Empfehlungen, erwartet aber keinen schriftlichen Nachweis dieser Umsetzung:

1. Klarstellung der Datenschutzerklärung dahingehend, dass die Einwilligung für das gesamte Verfahren einschließlich Gruppenberichte gilt und dass Teilnehmer jederzeit aussteigen können.
2. Definition des jeweiligen Zwecks der Gruppenberichte und der unter die Datenschutzerklärung fallenden Kategorien von Daten.

Vor dem Hintergrund des Grundsatzes der Rechenschaftspflicht erwartet der EDSB vom EUIPO die Umsetzung der obigen Empfehlungen und hat daher beschlossen, **den Fall abzuschließen**.

Mit freundlichen Grüßen

(unterzeichnet)

Wojciech Rafał WIEWIÓROWSKI

Verteiler: DSB, EUIPO

¹⁰ Artikel 1 Absatz 9.

¹¹ Artikel 12 und 13 der Allgemeinen Bedingungen.