Stellungnahme zur Vorabkontrolle
über die Bereitstellung externer Beratungsdienste
bei der Europäischen Arzneimittelagentur

Brüssel, den 15. Oktober 2015
(Fall 2013–0627)

1. Verfahren

Am 11. Juni 2013 erhielt der Europäische Datenschutzbeauftragte („EDSB“) vom Datenschutzbeauftragten („DSB“) der Europäischen Arzneimittelagentur („EMA“) eine Meldung für eine Vorabkontrolle gemäß Artikel 27 Absatz 2 der Verordnung (EG) Nr. 45/2001 („die Verordnung“) über die Verarbeitung personenbezogener Daten im Zusammenhang mit externen Beratungsdiensten. Auf Antrag des EDSB legte die EMA nachträgliche Erläuterungen vor.

Da die Verarbeitungen **bereits angelaufen sind** (es sich somit um eine Ex-post-Vorabkontrolle handelt), gilt die Frist von zwei Monaten für die Abgabe der Stellungnahme des EDSB nicht. Wir haben uns dennoch bemüht, den Fall angemessen zu prüfen.

2. Verarbeitung

Die EMA hat eine Klinik vertraglich verpflichtet, medizinische Dienste für die Mitarbeiter zu erbringen (im Folgenden „der Vertragsnehmer“). Hierzu zählen auch **Beratungsdienste**. Lediglich die letztgenannten Dienste sind Gegenstand der von der EMA übermittelten Meldung. Das **Ziel** der Bereitstellung solcher Dienste ist die Unterstützung von Mitarbeitern, die während oder nach einer Störung der Kontinuität der Geschäftstätigkeit unter einer seelischen Belastung leiden. Die Beratungsdienste werden auch bei Mobbing, sexueller Belästigung und Konflikten am Arbeitsplatz angeboten, oder um Mitarbeiter zu unterstützen, die aus anderen Gründen in ihrem Leben unter Stress leiden. Außerdem bei Ängsten, Depressionen, Beziehungsproblemen, Streitfällen vor Gericht und Familienstreitigkeiten, Traumata, Stressmanagement sowie für psychologische Gutachten.

Das Rechtsverhältnis zwischen der EMA und dem Vertragsnehmer wird von einem Dienstleistungsrahmenvertrag (Framework Service Contract, FSC) sowie einer Dienstgütevereinbarung (Service Level Agreement, SLA) bestimmt.

Dieses Verfahren umfasst zwei Arten von Datenverarbeitung: Einmal wird die Verarbeitung direkt von der EMA durchgeführt und einmal direkt vom Vertragsnehmer, wenn es sich um die Beratungsgespräche handelt.

Zu den **personenbezogenen Daten**, die direkt von der EMA verarbeitet werden, zählen:

- Antrag auf Beratungsgespräche durch die betroffene Person,
- ein zusammenfassender Bericht des Vertragsnehmers darüber, dass die sechs Gespräche, die der betroffenen Person zustehen, abgeschlossen wurden. Dieser Bericht enthält weder Informationen bezüglich des Inhalts der Beratung noch eine Diagnose. Eine Empfehlung für weitere Gespräche kann jedoch enthalten sein,
- Rechnungen für die geleisteten Dienste, die eine Vorgangsnummer und das Geburtsdatum der betroffenen Person aufweisen, und
- „Kopien nicht-medizinischer Dokumente aus den Akten von Mitarbeitern" (gemäß der SLA).

Zu den vom Vertragsnehmer verarbeiteten personenbezogenen Daten zählen:

- alle oben genannten Daten, sowie
- alle personenbezogenen Daten, die aus den Beratungsgesprächen resultieren und damit in Verbindung stehen.

Sowohl der Leiter des Bereichs Humanressourcen (HR) als auch ein Anweisungsbefugter haben Zugang zu den direkt von der EMA verarbeiteten Daten.

Vor Beginn der Beratung findet ein mündliches und informelles Treffen zwischen dem Leiter des Bereichs HR und dem betroffenen Mitarbeiter statt. Anschließend wird der Antrag auf die sechs Beratungsgespräche von der Abteilung HR der EMA an den Vertragsnehmer übermittelt. Die Termine werden von dem Mitarbeiter direkt mit dem Dienstleister vereinbart. Der zusammenfassende Bericht und die Rechnung, auf denen anstatt des Namens der betroffenen Person eine zugewiesene Vorgangsnummer vermerkt ist, werden nach Abschluss der Gespräche an die EMA übermittelt.

3. Rechtliche Prüfung

3.1. Anwendungsbereich der Stellungnahme

Anwendungsbereich. Diese Stellungnahme befasst sich mit der Datenverarbeitung durch die EMA und deren externen Vertragsnehmer bei der Bereitstellung von **Beratungsdiensten**. Die Verarbeitung personenbezogener Daten durch den externen Vertragsnehmer bei der Bereitstellung medizinischer Dienste *im eigentlichen Sinne* wird nicht erörtert. Zu diesem Thema sollte die EMA daher eine gesonderte Meldung übermitteln.

Leitlinien. Die Verarbeitung fällt in den Anwendungsbereich der **EDSB**-Leitlinien für die Verarbeitung von **Gesundheitsdaten** am Arbeitsplatz durch Organe und Einrichtungen der EU (die „Leitlinien")[1].

Der DSB betonte, dass sich die vorliegende Verarbeitung von der Verarbeitung im Zusammenhang mit Beratungen gegen Mobbing und sexuelle Belästigung unterscheidet. Letztgenannte unterlag bereits einer Vorabkontrolle durch den EDSB.[2]

[1] *Leitlinien für die Verarbeitung von Gesundheitsdaten am Arbeitsplatz durch Organe und Einrichtungen der Gemeinschaft*, angenommen im September 2009 und abrufbar auf der Website des EDSB https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/09-09-28_Guidelines_Healthdata_atwork_DE.pdf

[2] Siehe Stellungnahme vom Februar 2011 zum Fall 2010-0598 (Vertrauenspersonen/Informelles Verfahren bei der EMA).

Diese Stellungnahme konzentriert sich auf die Aspekte, die, wie in den oben genannten Leitlinien dargestellt, der Verordnung offenbar nicht in vollem Umfang entsprechen, bei denen Verbesserungsbedarf besteht oder anderweitige Erläuterungen angebracht sind.

3.2. Begründung der Vorabkontrolle

Da im Rahmen der Beratungsdienste Gesundheitsdaten verarbeitet werden könnten, unterliegen diese gemäß Artikel 27 Absatz 2 Buchstabe a der Verordnung einer Vorabkontrolle.

3.3. Rechtmäßigkeit

Gemäß Artikel 5 Buchstabe a der Verordnung ist die Verarbeitung rechtmäßig, wenn diese „*für die Wahrnehmung einer Aufgabe erforderlich [ist], die aufgrund der Verträge zur Gründung der Europäischen Gemeinschaften oder anderer aufgrund dieser Verträge erlassener Rechtsakte im öffentlichen Interesse […] ausgeführt wird*".

Artikel 1e des Beamtenstatuts dient als Rechtsgrundlage der beurteilten Verarbeitung. Demnach haben „*Beamte im aktiven Dienst […] Zugang zu sozialen Maßnahmen der Organe, einschließlich spezieller Maßnahmen zur Vereinbarung von Berufs- und Familienleben*". Auch steht sie im Einklang mit Erwägung 27 der Verordnung, wonach die Verarbeitung personenbezogener Daten für die Wahrnehmung von Aufgaben im öffentlichen Interesse „*die Verarbeitung personenbezogener Daten, die für die Verwaltung und das Funktionieren dieser Organe und Einrichtungen erforderlich ist*", einschließt. Ferner wird in dem internen Memorandum vom 19. Juni 2008[3] erwähnt, dass die Dienste in Situationen, wie beispielsweise bei „Konflikten am Arbeitsplatz" und „Mobbing" zur Verfügung stehen, „um Mitarbeiter zu unterstützen, die aus anderen Gründen in ihrem Leben unter Stress leiden."

Angesichts des sensiblen Charakters der fraglichen Datenverarbeitung und angesichts der Tatsache, dass die entsprechende Rechtsgrundlage für die Beratung von Mitarbeitern lediglich in einem internen Memorandum dargelegt wird, sollte die EMA die Modalitäten des Beratungsdienstverfahrens in besonderen Rechtsnormen (Strategie, Mitteilung, Beschluss), die auf ihre eigenen Bediensteten Anwendung finden, näher beschreiben.[4] Solch ein Schritt würde nicht nur für Klarheit und Transparenz hinsichtlich der Verfahren sorgen, sondern würde zudem dazu beitragen, dass die Mitarbeiter die Einzelheiten der Verarbeitung sensibler Daten anerkennen.

Die von der EMA eingeführte Verarbeitungsmethode scheint für die Lösung von beschäftigungsbezogenen Problemen erforderlich zu sein und zu einer generellen Verbesserung des Arbeitsumfeldes[5] bei der EMA beizutragen.

---

[3] Memorandum (Ref.: EMEA/312151/2008 310) übermittelt durch den Leiter des Referats Verwaltung an das Sekretariat der EMA bezüglich der Beratungsdienste.

[4] Siehe diesbezüglich *Leitlinien für die Verarbeitung personenbezogener Daten bei der Auswahl von Vertrauenspersonen und in informellen Verfahren bei Belästigung in europäischen Organen und Einrichtungen*, angenommen im Februar 2011 (abrufbar unter https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/11-02-18_Harassment_Guidelines_DE.pdf), S. 4.

In Anbetracht dieser Bewertung, ist die Verarbeitung nach Artikel 5 Buchstabe a der Verordnung rechtmäßig, vorausgesetzt, die Rechtsgrundlage wird mit einer von der EMA angenommenen Strategie bzw. einem solchen Beschluss gestützt.

3.4. Verarbeitung besonderer Datenkategorien

Zu den personenbezogenen Daten, die von der EMA (und dem Vertragsnehmer im Auftrag der EMA) im Zusammenhang mit dem Beratungsdienst verarbeitet werden, zählen gesundheitsbezogene Daten.

Wie der EDSB in den Leitlinien[6] festlegt, zählen zu den Gesundheitsdaten:
- medizinische Daten (z. B. ärztliche Überweisungen und Verschreibungen, medizinische und psychologische Untersuchungsberichte) – im vorliegenden Fall werden solche Daten vom Vertragsnehmer verarbeitet, und
- gesundheitsbezogene Verwaltungs- und Finanzdaten (z. B. medizinische Termine, Rechnungen für erbrachte Gesundheitsleistungen, Angaben zur Anzahl der Krankheitstage, Verwaltung der Fehlzeiten wegen Krankheit) – im vorliegenden Fall werden solche Daten von der EMA und dem Vertragsnehmer verarbeitet.

Die Verarbeitung personenbezogener Daten über Gesundheit oder Sexualleben ist untersagt, es sei denn, dies kann nach Artikel 10 Absatz 2 der Verordnung begründet werden. Gemäß Artikel 10 Absatz 2 Buchstabe b ist eine solche Ausnahme vorgesehen, wenn die Verarbeitung erforderlich ist, um den Pflichten und spezifischen Rechten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen. In diesem Fall findet sich die Begründung für die Verarbeitung gesundheitsbezogener Daten in dem Beamtenstatut (Artikel 1e), das mit einer von der EMA angenommenen Strategie/Beschluss zu Beratungsdiensten ergänzt werden muss (siehe Abschnitt 3.3 oben).

Aufgrund des sensiblen Charakters der im vorliegenden Fall verarbeiteten personenbezogenen Daten, sind gemäß Artikel 22 der Verordnung konkrete organisatorische Maßnahmen zu treffen (siehe Abschnitt 3.6 unten).

3.5. Rechte der betroffenen Person

1) Information

Laut der Meldung, erhalten die Mitarbeiter der EMA einen allgemeinen Datenschutzhinweis zu allen Verarbeitungen im Zusammenhang mit HR-Verfahren. Ein allgemeiner Hinweis zum Schutz der Privatsphäre ist hingegen auf der externen Website erhältlich. Ansonsten erhalten die Mitarbeiter keinen weiteren konkreten Datenschutzhinweis. Der betroffene Mitarbeiter erhält Kopien des Schriftverkehrs zwischen dem Leiter des Bereichs Humanressourcen und dem externen Beratungsdienstleister.

Die von der EMA vorgelegte „Datenschutzerklärung“ kommt den Anforderungen nach Artikel 11 und 12 der Verordnung nicht nach. So werden in der Erklärung beispielsweise weder die Zweckbestimmungen der Verarbeitung noch die Empfänger oder Kategorien der Empfänger erwähnt. Die EMA sollte die betroffenen Personen im Rahmen eines spezifischen Datenschutzhinweises zu Beratungsdiensten informieren. Der Hinweis ist auf der Website oder im Intranet zu veröffentlichen.[7]

[6] Siehe die oben genannten *Leitlinien zu Gesundheitsdaten*, S. 2.
[7] Siehe diesbezüglich die oben genannten *Leitlinien für Verfahren bei Belästigung*, Punkt 1.

Die Strategie bzw. der Beschluss der EMA hinsichtlich des Beratungsdienstverfahrens (siehe Abschnitt 3.3 oben) sollte außerdem vorsehen, dass die betroffene Person im Falle eines Antrags auf Beratung spezifische Informationen erhält. Dies sollte während des ersten Treffens zwischen dem Leiter des Bereichs HR und der betroffenen Person geschehen. In dieser Hinsicht hat die EMA bereits ein Informationssystem im Zusammenhang mit dem informellen Verfahren gegen Belästigung eingeführt, das der EDSB als bewährtes Verfahren erachtet.[8] Für das vorliegende Verfahren sollte die EMA das gleiche System einführen.

2) Ausübung ihrer Rechte durch die betroffenen Personen

Die EMA muss nicht nur von ihrem Vertragsnehmer verlangen, den betroffenen Personen Zugang zu ihren personenbezogenen Daten zu ermöglichen (siehe Abschnitt 3.7. unten), sondern auch selbst Zugang zu den von ihr verarbeiteten personenbezogenen Daten gewähren und Mittel zur Ausübung der Rechte auf Berichtigung und Löschung zur Verfügung stellen. In dieser Hinsicht sollte der Datenschutzhinweis genaue Informationen darüber enthalten, wie die betroffene Person seine/ihre Rechte gegenüber der EMA und dem Vertragsnehmer geltend machen kann. Die Meldung (Abschnitt 8) muss entsprechend aktualisiert werden.

3.6. Sicherheit

[...]

3.7. Outsourcing

Artikel 23 Absatz 1 der Verordnung besagt, dass für den Fall, dass „*die Verarbeitung im Auftrag des für die Verarbeitung Verantwortlichen vorgenommen [wird], [...] dieser einen Auftragsverarbeiter auszuwählen [hat], der hinsichtlich der für die Verarbeitung nach Artikel 22 zu treffenden technischen und organisatorischen Sicherheitsvorkehrungen ausreichende Gewähr bietet, und [...] für die Einhaltung dieser Maßnahmen zu sorgen [hat]*". Außerdem ist in Artikel 23 Absatz 2 der Verordnung festgelegt, dass „*die Durchführung einer Verarbeitung im Auftrag [...] auf der Grundlage eines Vertrags oder Rechtsakts [erfolgt], durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere Folgendes vorgesehen ist:*
a) der Auftragsverarbeiter handelt nur auf Weisung des für die Verarbeitung Verantwortlichen;
b) die in den Artikeln 21 [Vertraulichkeit] *und 22* [Sicherheit] *genannten Verpflichtungen gelten auch für den Auftragsverarbeiter, es sei denn, der Auftragsverarbeiter unterliegt aufgrund von Artikel 16 oder Artikel 17 Absatz 3 zweiter Gedankenstrich der Richtlinie 95/46/EG bereits Verpflichtungen in Bezug auf Vertraulichkeit und Sicherheit, die in den nationalen Rechtsvorschriften von einem der Mitgliedstaaten festgelegt sind*".

In diesem Fall wurde zwischen der EMA und dem Auftragsverarbeiter ein Vertrag (FSC und SLA) geschlossen.

[8] Siehe die oben genannte Stellungnahme in Fall 2010-0598, Punkt 3.8.

1) Verpflichtung des Auftragsverarbeiters, nur auf Weisung der EMA zu handeln

Der FSC enthält lediglich einen Artikel zum Datenschutz (Artikel II.7). Dieser enthält jedoch keinen Hinweis auf die Verpflichtung des Auftragsverarbeiters, gemäß Artikel 23 Absatz 2 Buchstabe a der Verordnung „*nur auf Weisung des für die Verarbeitung Verantwortlichen*" zu handeln. Der bloße Hinweis auf die Verordnung, der im FSC enthalten ist, reicht nicht aus, um klarzumachen, nach welcher rechtlichen Voraussetzung die Daten verarbeitet werden können. Daher sollte der Vertrag so geändert werden, dass er diese Verpflichtung enthält.

2) Vertraulichkeit

Der Vertragsnehmer ist einem Mitgliedstaat der EU (Vereinigtes Königreich) eingetragen. Daher unterliegt er den in Richtlinie 95/46/EG verankerten Verpflichtungen und deren Umsetzungsbestimmungen, einschließlich der Vertraulichkeits- und Sicherheitsverpflichtungen. Die im FSC (Artikel II.9) vorgesehene Vertraulichkeitsklausel sollte auch einen Hinweis auf die geltenden nationalen Datenschutzvorschriften enthalten.[9]

3) Sicherheitsmaßnahmen

[...]

4) Ausübung ihrer Rechte durch die betroffenen Personen im Zusammenhang mit der Verarbeitung durch den Vertragsnehmer

Um die Wirksamkeit des Auskunftsrechts der betroffenen Person zu gewährleisten, sollte Punkt 14 der SLA hinsichtlich „Akten" mit Bestimmungen ergänzt werden, die klarmachen, dass die betroffene Person nach Artikel 13 der Verordnung das Recht auf Zugang zu ihrer eigenen Akte hat und nicht nur nach Artikel 26a des Beamtenstatuts (Punkt 14.1 der SLA). Ebenso sollte Punkt 14.2 der SLA ergänzt werden, indem festgelegt wird, dass der Vertragsnehmer nach Artikel 14 der Verordnung den von den EMA-Mitarbeitern vorgelegten Aufforderungen zur Berichtigung und Löschung nachkommen wird.

Der EDSB weist darauf hin, dass die betroffene Person gemäß der allgemeinen Regelung hinsichtlich des Zugangsrechts weiterhin direkten Zugang zu den Gesundheitsdaten erhält, die direkt vom Vertragsnehmer verarbeitet werden. Nach Artikel 20 Absatz 1 Buchstabe c der Verordnung, kann der Zugang zu Daten psychologischer oder psychiatrischer Natur jedoch *indirekt* gewährt werden, wenn sich anhand einer Einzelfallbewertung herausstellt, dass angesichts der gegebenen Umstände ein indirekter Zugang für den Schutz der betroffenen Person erforderlich ist.[10]

Schlussfolgerungen

Es gibt keinen Grund zu der Annahme, dass die Bestimmungen der Verordnung (EG) Nr. 45/2001 missachtet werden, vorausgesetzt, die Empfehlungen, die in der vorliegenden Stellungnahme enthalten sind, werden in vollem Umfang berücksichtigt. Die EMA sollte insbesondere

[9] Siehe Stellungnahme in Fall 2007-0489 (Datenverarbeitung durch den Sozialberater bei der EZB), 6. Dezember 2007, Punkt 3.9.
[10] Siehe *Leitlinien*, Punkt 6.

- besondere Bestimmungen mit Rechtscharakter erlassen (Strategie, Mitteilung, Beschluss), in denen die Modalitäten des Beratungsdienstverfahrens dargelegt werden;
- eine vollständige Datenschutzerklärung erstellen und veröffentlichen, die die Verarbeitung im Zusammenhang mit Beratungsdiensten betrifft, und die die Anforderungen der Artikel 11 und 12 der Verordnung erfüllt. Hierzu zählen auch Informationen darüber, wie die betroffene Person ihre Rechte ausüben kann. In der Strategie bzw. dem Beschluss zu den Beratungsleistungen sollte vorgeschrieben sein, dass die betroffene Person die Datenschutzerklärung während des ersten Treffens mit dem Leiter des Bereichs HR erhält;
- spezifische Vertraulichkeitserklärungen erstellen, die von den Mitarbeitern zu unterschreiben sind, die für die Verarbeitung verantwortlich sind, die direkt bei der EMA durchgeführt wird und sich auf die Verarbeitung von Gesundheitsdaten im Zusammenhang mit Beratungsdiensten bezieht;
- den Vertrag und die SLA mit dem Beratungsdienstleister ändern, sodass diese
    - die Verpflichtung des Dienstleisters enthalten, gemäß Artikel 22 Absatz 2 Buchstabe a der Verordnung, *„nur auf Weisung des für die Verarbeitung Verantwortlichen“* zu handeln;
    - in der Vertraulichkeitsklausel auf die geltenden nationalen Datenschutzvorschriften hinweisen;
    - [...];
    - [...];
    - Punkt 16 der SLA hinsichtlich „Akten“ gemäß Artikel 13 und 14 der Verordnung ergänzen und auf diese Weise die Rechte der betroffenen Person gewährleisten;
    - eine für den Vertragsnehmer geltende Verpflichtung enthalten, wonach jeder seiner Mitarbeiter im Rahmen des Vertrages eine spezifische Vertraulichkeitserklärung im Zusammenhang mit der Verarbeitung von Gesundheitsdaten der EMA-Mitarbeiter unterschreiben muss;
- [...]
- die Meldung aktualisieren, um die Verfahren zur Ausübung der Rechte der betroffenen Personen sowohl hinsichtlich der Daten, die vom Vertragsnehmer verarbeitet werden, als auch hinsichtlich der Daten, die direkt von der EMA verarbeitet werden, mit aufzunehmen;
- den EDSB über die Verarbeitung Gesundheitsdaten durch den Vertragsnehmer bei der Bereitstellung medizinischer Dienste *im eigentlichen Sinne* informieren.

15. Oktober 2015

(unterzeichnet)

Wojciech WIEWIÓROWSKI
Stellvertretender Europäischer Datenschutzbeauftragter