Stellungnahme des EDSB zur Meldung für eine Vorabkontrolle über *„Belastungstests auf Grundlage der Herzfrequenzvariabilität (Bewertung der Lebensweise)“* beim Ausschuss der Regionen

Brüssel, den 17. Dezember 2015 (Fall 2015-0509)

1. Verfahren

Am 11. Juni 2015 erhielt der Europäische Datenschutzbeauftragte („der EDSB“) vom Datenschutzbeauftragten („dem DSB“) des Ausschusses der Regionen („AdR“) eine Meldung für eine Vorabkontrolle gemäß Artikel 27 Absatz 2 Buchstabe a der Verordnung (EG) Nr. 45/2001 („die Verordnung“). Die Meldung betrifft eine neue Verarbeitung bezüglich der Messung und Bewertung des Stressniveaus der Mitarbeiter auf Grundlage ihrer Herzfrequenzvariabilität und ihrer täglichen Gewohnheiten.

Gemäß Artikel 27 Absatz 4 der Verordnung muss diese Stellungnahme innerhalb von zwei Monaten, also bis zum 17. Dezember 2015, abgegeben werden. Diese Frist kann jedoch bis zum Vorliegen weiterer Auskünfte ausgesetzt werden[1].

2. Sachverhalt

Zweck und betroffene Personen

Im Zusammenhang mit der Belastungs- und Burn-Out-Prävention des AdR beabsichtigt sein ärztlicher Dienst, seinen Mitarbeitern die Möglichkeit anzubieten, sich einer Messwertermittlung des Stressniveaus bei einem externen Auftragnehmer zu unterziehen. Dieser Test stellt ihnen einen Bewertungsbericht darüber aus, wie sie Belastungen und psychosoziale Risiken am Arbeitsplatz besser bewältigen. Mitarbeiter können freiwillig an diesem Programm teilnehmen.

Rechtsgrundlage und Rechtmäßigkeit

- Artikel 3 und 8 der belgischen Königlichen Verordnung vom 10. April 2014 bezüglich der Vorbeugung psychologischer Risiken am Arbeitsplatz; diese Bestimmungen verpflichten den Arbeitgeber, mögliche psychologische Risiken am Arbeitsplatz zu analysieren und auszuwerten.
- Die Teilnahme am Test ist gemäß Artikel 5 Buchstabe d der Verordnung freiwillig.

[1] Dieser Fall wurde wegen eines Ersuchens um weitere Auskünfte vom 16. Juni 2015 bis zum 26. Juni 2015, vom 23. Juli 2015 bis zum 29. September 2015 bzw. 20. November 2015 und wegen eines Ersuchens um Kommentierung durch den DSB und den für die Verarbeitung Verantwortlichen vom 3. Dezember bis zum 10. Dezember 2015 ausgesetzt.

Verfahren und verarbeitete Daten

Der AdR wird einen Dienstleistungsvertrag über ein Jahr mit einem externen finnischen Auftragnehmer (Firstbeat) aushandeln. Ein Vertragsentwurf sowie damit verbundene Dokumente wurden dem EDSB zugesandt.

Gemäß Vertragsentwurf *„können personenbezogene Daten einzeln oder zusammen mit den personenbezogenen Dateien von Firstbeat und seiner Tochtergesellschaften verarbeitet werden. Jede Übermittlung personenbezogener Daten außerhalb solcher Unternehmen unterliegt der gesonderten Einwilligung der betroffenen Person ... Personenbezogene Daten können von Firstbeat, einem Unterauftragnehmer oder einem Drittanbieter (der von Firstbeat ein Nutzungsrecht der Dienstleistung erworben hat und die Dienstleistung für seine Kunden als Dienstleister anbietet) und von einem ermächtigten externen Gesundheitsspezialisten gemäß finnischem Datenschutzgesetz verarbeitet werden. Dieser ermächtigte externe Gesundheitsspezialist darf die Dienstleistung unabhängig, wie mit Firstbeat vereinbart, nutzen."* Der erwähnte *„ermächtigte externe Gesundheitsspezialist"* ist die Krankenpflegekraft des AdR. Es wird auch erwähnt, dass personenbezogene Daten *„anonym für statistische und Marktforschungszwecke verwendet werden".*

Die erste Kontaktaufnahme der Teilnehmer findet mit der Krankenpflegekraft des ärztlichen Dienstes des AdR statt, die zur Messung des Herzschlags ein Messgerät mit Elektroden an der Brust des Teilnehmers anbringt. Die Teilnehmer können sich dann in einen Online-Server einloggen, eine Sprache auswählen und auf „Start" klicken und die folgenden Angaben machen: Vorname, Nachname, Geburtsdatum, Geschlecht, Größe, Gewicht, berufliche Einstufung, Einschätzung der aeroben Fitness, langfristige medikamentöse Behandlung und Krankheiten, zehn Fragen zur körperlichen Bewegung, Essgewohnheiten, Alkoholkonsum, Belastung, Energieniveau, ausreichender Schlaf usw. Die Teilnehmer sollten dann das Datum und die Uhrzeit ihres Messbeginns einstellen. Darüber hinaus erhalten sie die Möglichkeit, ein Tagebuch mit Informationen zu den Messtagen und weiteren Informationen, wie entspannende oder belastende Momente oder Trainingseinheiten, auszufüllen, um höheren Nutzen aus der Bewertung zu ziehen. Es steht den Teilnehmern frei, ob sie Firstbeat ihre Anschrift und Telefonnummer oder zusätzliche Angaben über den Online-Server mitteilen.

Der Messzeitraum und die Online-Bereitstellung entsprechender Informationen an den Server sollten mindestens drei Tage und drei Nächte betragen.

Wenn der Messzeitraum beendet ist, geben die Teilnehmer das Messgerät an die Krankenpflegekraft des AdR zurück. Die Krankenpflegekraft wird das Gerät mit dem Server von Firstbeat verbinden und die Messungen hochladen. Zu diesem Zeitpunkt steht den Teilnehmern ein Bewertungsbericht zur Verfügung. Die Teilnehmer können über ihre individuelle Kontoverbindung, die sie zu Beginn der Messungen erstellt hatten, auf ihren Bericht zugreifen.

Die Krankenpflegekraft des AdR wird vom externen Auftragnehmer geschult, damit sie den Teilnehmern die Ergebnisse ihres Bewertungsberichts erklären und sie zur Verbesserung ihres täglichen Lebens anleiten kann.

Recht auf Information

Die Teilnehmer werden durch einen *„rechtlichen Hinweis zur Datenverarbeitung in Bezug auf den Test zur „Bewertung der Lebensweise" informiert"* (Datenschutzhinweis). Dieses Dokument wird im Intranet des ärztlichen Dienstes verfügbar sein, und die Teilnehmer erhalten eine Kopie, wenn ihnen das Gerät zur Herzfrequenzmessung übergeben wird.

Recht auf Auskunft und Berichtigung

Die Meldung gibt an, dass die Teilnehmer ihr Recht auf Auskunft und Berichtigung ausüben können, indem sie eine E-Mail an den ärztlichen Dienst des AdR senden. Sie können unrichtige oder unvollständige personenbezogene Daten in ihrer medizinischen Akte korrigieren. Sie können darum bitten, dass ihr Bewertungsbericht aus ihrer medizinischen Akte entfernt wird.

Allerdings gab der AdR in Beantwortung der Fragen des EDSB an, dass dies nicht länger der Fall sei, da der ärztliche Dienst des AdR nicht den Bewertungsbericht, sondern nur die Liste der Teilnehmer aufbewahren werde.

Datenaufbewahrung

Der ärztliche Dienst des AdR wird Firstbeat vorschlagen, einen zweijährigen Aufbewahrungszeitraum anzunehmen, damit Teilnehmer, falls sie sich entscheiden, den Test innerhalb dieses Zeitraums zu wiederholen, in der Lage sind, die Ergebnisse zu vergleichen.

Anonyme Daten werden für statistische und Marktforschungszwecke verwendet. Das bedeutet, dass Namen, E-Mail-Adressen und Gruppeninformationen, wie eine Person identifiziert werden kann, vom Firstbeat-Server gelöscht werden. Firstbeat wird die Herzfrequenzmessungen sowie die Informationen zum Alter und zum Geschlecht aufbewahren.

Aufbewahrung und Sicherheitsmaßnahmen

Der ärztliche Dienst wird keine Akten in Papier- oder elektronischer Form aufbewahren. Der Bewertungsbericht wird dem Teilnehmer direkt ausgehändigt.

Bezüglich der Frage, ob eine Bewertung der Informationssicherheitsrisiken bezüglich der Unterauftragsvergabe der Verarbeitung an Firstbeat vorgenommen wurde, antwortete der AdR, dass keine solche Bewertung durchgeführt worden sei, da Firstbeat ein seriöses finnisches Unternehmen mit Servern in Finnland sei.

3. Rechtliche Aspekte

3.1. Vorabkontrolle

Die Verarbeitung von zu analysierenden, personenbezogenen Daten wird von einem EU-Organ, dem AdR, durchgeführt. Darüber hinaus erfolgt die Verarbeitung sowohl manuell - die Teil eines Ablagesystems bildet bzw. bilden soll (auf Papier ausgedruckter Bewertungsbericht) - als auch automatisch (Informationen, die von den Teilnehmern über den Online-Server des Bewertungsinstruments von Firstbeat bereitgestellt werden, und Erstellung des Bewertungsberichts). Die Verordnung ist folglich anwendbar.

Die Verarbeitung umfasst die Verarbeitung von Daten über Gesundheit, wie Herzfrequenzmessungen, chronische Krankheiten, Medikation und Essgewohnheiten. Der Verarbeitungszweck besteht darin, das Stressniveau der Teilnehmer zu bewerten und ihnen durch die Krankenpflegekraft des AdR eine Anleitung, wie sie ihr tägliches Leben besser bewältigen können, zukommen zu lassen. Aufgrund des sensiblen Charakters der verarbeiteten Daten könnte die Verarbeitung besondere Risiken für die Rechte und Freiheiten der Bewerber bergen und unterliegt daher einer Vorabkontrolle durch den EDSB[2].

[2] Artikel 27 Absatz 2 der Verordnung enthält eine Liste von Verarbeitungen, die aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können, einschließlich Buchstabe a Verarbeitungen von Daten über die Gesundheit.

Der EDSB wird die Praktiken des AdR ermitteln, die den Grundsätzen der Verordnung offenbar nicht entsprechen, und dem AdR geeignete Empfehlungen unterbreiten.

3.2. Einwilligung

Die zu analysierende Verarbeitung stützt sich auf die freiwillige Teilnahme der Mitarbeiter des AdR. Der EDSB weist den AdR darauf hin, dass die Einwilligung im Rahmen eines Beschäftigungsverhältnisses eine sensible Angelegenheit ist, da bezweifelt werden kann, dass eine solche Einwilligung ohne Zwang erfolgt. Daher ist es wichtig, dass der AdR sicherstellt, dass jeder Teilnehmer gemäß Artikel 5 Buchstabe d der Verordnung eindeutig seine Einwilligung gibt, bevor er am Test teilnimmt. Das bedeutet, dass die Einwilligung der Teilnehmer ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage, dass ihre Daten durch die verschiedenen Schritte der Verarbeitung erhoben werden, erfolgen muss[3]. Daher sollte der AdR alle Teilnehmer angemessen darüber unterrichten, dass ihre Teilnahme und ihre Datenerhebung freiwillig ist (Artikel 11 Absatz 1 Buchstabe d der Verordnung) und dass sie ihre Einwilligung jederzeit zurückziehen können.

3.3. Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter sowie Artikel 23 der Verordnung

Wie vorstehend erklärt, wird der AdR für Durchführung der Messung und Bewertung des Stressniveaus auf Grundlage der Herzfrequenzvariabilität und der täglichen Gewohnheiten der Teilnehmer einen Vertrag mit einem externen finnischen Auftragnehmer, Firstbeat, unterzeichnen.

In Anbetracht von Artikel 23 der Verordnung handelt Firstbeat im Namen des AdR und muss somit als Auftragsverarbeiter angesehen werden, während der AdR der für die Verarbeitung Verantwortliche ist. Das bedeutet, dass der AdR das für die Entscheidung über die Zwecke und Mittel der Verarbeitung verantwortliche EU-Organ ist (Artikel 2 Buchstabe d der Verordnung) und Firstbeat verpflichtet ist, die Verarbeitung nur auf Weisung des AdR durchzuführen (Artikel 23 Absatz 2 Buchstabe a).

Insbesondere sollte der AdR als der für die Verarbeitung Verantwortliche (Artikel 4 Absatz 2 der Verordnung) im Vertragsentwurf die folgenden Bedingungen festlegen:

i) Firstbeat sollte nur angemessene, sachdienliche und nicht übermäßig umfangreiche Daten verarbeiten, und die verarbeiteten Daten (Herzfrequenzmessungen, von den Teilnehmern eingegebene Informationen und Bewertungsbericht) werden nur für den erhobenen Zweck verarbeitet;

ii) Firstbeat sollte nicht zur Übermittlung von verarbeiteten Informationen oder zur Auslagerung einer Dienstleistung an einen Unterauftragnehmer oder einen Drittanbieter ermächtigt werden, es sei denn der AdR stimmt zu;

iii) Firstbeat sollte keine Daten für andere unrechtmäßige Zwecke weiterverarbeiten (d. h. Übermittlung an andere Unternehmen zu Marketingzwecken);

[3] In Artikel 2 Buchstabe h der Verordnung heißt es, dass die Einwilligung der betroffenen Person *„jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass die sie betreffenden personenbezogenen Daten verarbeitet werden“* bedeutet.

iv) Firstbeat sollte den vom AdR geforderten Datenaufbewahrungszeitraum einführen und

v) falls ein Teilnehmer Auskunft über seine von Firstbeat verarbeiteten Rohdaten wünscht, sollte Firstbeat in der Lage sein, dieses Recht zu gewährleisten.

In Bezug auf die Verpflichtungen von Firstbeat zu Vertraulichkeit, Datenschutz und Sicherheitsmaßnahmen gemäß Artikel 23 Absatz 2 Buchstabe b der Verordnung sollte der AdR sicherstellen, dass dem Vertragsentwurf spezifische Bestimmungen bezüglich dieser Verpflichtungen hinzugefügt werden. Im Hinblick auf die Verpflichtungen zu Vertraulichkeit und Sicherheit und da der Auftragsverarbeiter ein finnisches Unternehmen ist, sollte dieses grundsätzlich Artikel 16 und Artikel 17 Absatz 3 zweiter Spiegelstrich der Richtlinie 95/46/EG, die in finnisches Recht über Datenschutz umgesetzt wurde (siehe Absatz 3.7), unterliegen.

3.4. Recht auf Auskunft und Berichtigung

Im Sinne von Artikel 4 Absatz 1 Buchstabe d der Verordnung sollte der AdR sicherstellen, dass die Daten der Teilnehmer sachlich richtig und auf den neusten Stand gebracht werden; daher hat er alle angemessenen Maßnahmen zu ergreifen, damit im Hinblick auf die Zwecke, für die sie verarbeitet werden, nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden. Das bedeutet, dass der AdR dafür sorgen muss, dass die Teilnehmer ihr Recht auf Auskunft (Artikel 13 der Verordnung) und Berichtigung (Artikel 14 der Verordnung) ausüben können.

Der EDSB hält fest, dass die Krankenpflegekraft des AdR mit jedem Teilnehmer den Bewertungsbericht besprechen und den Teilnehmer anleiten wird, wie er seine Belastung bewältigen und seinen Alltag verbessern kann. Die Teilnehmer können den Test auch wiederholen und die Ergebnisse vergleichen. Der AdR möchte keine Kopie des Bewertungsberichts aufbewahren. Falls allerdings ein Teilnehmer darum bittet, dass eine Kopie des Berichts und gegebenenfalls damit verbundene Anmerkungen in seiner medizinischen Akte aufbewahrt werden, sollte der AdR diesem Wunsch nachkommen können. Die Teilnehmer sollten dann jederzeit ihr Recht auf Auskunft über ihren Bewertungsbericht und ihr Recht auf Berichtigung/Aktualisierung ausüben können, wenn sie den Test wiederholen möchten.

Darüber hinaus hebt der EDSB hervor, dass der AdR, falls ein Teilnehmer Auskunft über seine Rohdaten (die von Firstbeat verarbeiteten Informationen) verlangt, dafür sorgen sollte, dass Firstbeat in der Lage ist, dieses Recht zu gewähren.

Der AdR sollte unrichtige in der Meldung genannte Informationen löschen und die vorgenannten Empfehlungen sowohl in der Meldung als auch im Vertragsentwurf deutlich niederlegen.

3.5. Datenaufbewahrung

Als allgemeiner Grundsatz dürfen personenbezogene Daten gemäß Artikel 4 Absatz 1 Buchstabe e der Verordnung nur so lange, wie es für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht.

Der EDSB hält fest, dass Firstbeat bereit ist, verarbeitete Daten nach Aufforderung des AdR zu löschen. Wenn der AdR beabsichtigt, einen Einjahresvertrag mit Firstbeat abzuschließen, scheint der zweijährige vom AdR vorgesehene Aufbewahrungszeitraum über den Zweck der

Verarbeitung hinauszugehen. Der EDSB empfiehlt, dass der AdR einen notwendigen und angemessenen, nicht über die Länge des Vertrags mit Firstbeat hinausgehenden Aufbewahrungszeitraum festlegt und dafür sorgt, dass der Auftragsverarbeiter diesen Aufbewahrungszeitraum umsetzt. Der AdR sollte im Vertragsentwurf ausdrücklich angeben, dass Firstbeat geeignete Garantien vorsehen muss, um sicherzustellen, dass diese Daten nicht für andere Zwecke verarbeitet oder für Maßnahmen oder Entscheidungen gegenüber einem speziellen Teilnehmer verwendet werden. Die Meldung sollte entsprechend aktualisiert werden.

In Anbetracht des Absatzes 3.1 sollte der AdR auch einen Aufbewahrungszeitraum für den Bewertungsbericht und mögliche Anmerkungen der Krankenpflegekraft vorsehen, falls ein Teilnehmer wünscht, dass diese Informationen in seiner medizinischen Akte aufbewahrt werden.

Gemäß den vorgelegten Informationen werden „anonymisierte" Daten von Firstbeat für statistische und Marktforschungszwecke genutzt. Selbst wenn Namen, E-Mail-Adressen und Gruppeninformationen gelöscht werden, ist das Risiko einer Wiedererkennung so sensibler Daten sehr hoch[4]. Die Firstbeat anvertrauten Daten sollten als personenbezogene Daten angesehen werden, auch wenn die vorgenannten Angaben gelöscht werden. Der EDSB empfiehlt daher, dass der AdR eine Bestimmung in den Vertragsentwurf aufnimmt, die die Sensibilität der Daten und das hohe Risiko einer Wiedererkennung hervorhebt. Folglich sollte Firstbeat keine anonymisierten oder anderen Daten auf seinem Server für statistische oder Marketingzwecke weiterverarbeiten.

Falls der AdR anonyme Daten nur zu statistischen Zwecken nutzen will, empfiehlt der EDSB, dass die anonymisierten Daten nicht im Internet veröffentlicht und nur für die ordnungsgemäße Verwaltung des Organs und im Interesse der Mitarbeiter verwendet werden.

3.6. Informationen, die den Teilnehmern bereitzustellen sind

Artikel 11 und Artikel 12 der Verordnung beziehen sich auf die Informationen, die den betroffenen Personen bereitzustellen sind, um eine faire und transparente Verarbeitung ihrer personenbezogenen Daten zu gewährleisten. Im vorliegenden Fall werden einige Daten direkt von den Teilnehmern erhoben und andere Informationen von anderen Stellen (d. h. der Bewertungsbericht von Firstbeat und die Bewertung der Ergebnisse und Anleitung durch die Krankenpflegekraft). Somit finden beide Artikel Anwendung.

In Bezug auf den Inhalt des Datenschutzhinweises sollte der AdR
i) die Rolle von AdR und Firstbeat klären, da es hierfür keine Bezugnahme im Datenschutzhinweis gibt;

ii) gegenüber den Teilnehmern erwähnen, dass sie ihr Recht auf Auskunft und Berichtigung ihres Bewertungsberichts und der damit verbundenen Anmerkungen sowie der Rohdaten (von Firstbeat verarbeitete Informationen), wie unter Absatz 3.3 erklärt, ausüben können; und

iii) den Aufbewahrungszeitraum der vom ärztlichen Dienst des AdR und von Firstbeat aufbewahrten Daten angeben.

[4] Siehe die Stellungnahme 05/2014 der Artikel-29-Datenschutzgruppe über Anonymisierungstechniken, angenommen am 10. April 2014 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp2l 6_en.pdf)

Der AdR sollte alle vorgenannten Empfehlungen in den Datenschutzhinweis aufnehmen und die aktualisierte Fassung im Intranet veröffentlichen, bevor die Verarbeitung aufgenommen wird.

3.7. Sicherheit

Selbst wenn der AdR die personenbezogenen Daten nicht direkt verarbeitet, ist er an Artikel 23 der Verordnung gebunden: *„Wird eine Verarbeitung im Auftrag des für die Verarbeitung Verantwortlichen vorgenommen, so hat dieser einen Auftragsverarbeiter auszuwählen, der hinsichtlich der für die Verarbeitung nach Artikel 22 zu treffenden technischen und organisatorischen Sicherheitsvorkehrungen ausreichende Gewähr bietet, und er hat für die Einhaltung dieser Maßnahmen zu sorgen.“* Zu diesem Zweck sollte der AdR eine formelle Garantie (d. h. eine Sicherheitsbescheinigung) einholen, dass Firstbeat tatsächlich seinen Verpflichtungen zu Vertraulichkeit und Sicherheit der anvertrauten personenbezogenen Daten nachkommt.

4. Schlussfolgerung

Es besteht kein Grund zu der Annahme, dass gegen die Bestimmungen der Verordnung verstoßen wird, sofern die folgenden Erwägungen berücksichtigt werden. Der AdR sollte insbesondere:

- im Vertragsentwurf mit Firstbeat die Rollen des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters klären und im Vertragsentwurf alle in Absatz 3.3 erläuterten Bedingungen angeben;

- die in der Meldung angegebenen unrichtigen Informationen löschen und angeben, dass die Teilnehmer ihr Recht auf Auskunft und Berichtigung des Bewertungsberichts und der damit verbundenen Anmerkungen sowie Rohdaten ausüben können (Absatz 3.4);

- einen bestimmten Aufbewahrungszeitraum der für Firstbeat und für den AdR erhobenen Daten festlegen;

- alle in Absatz 3.6 des Datenschutzhinweises genannten Informationen aufnehmen und eine aktualisierte Fassung im Intranet veröffentlichen, bevor die Verarbeitung aufgenommen wird;

- eine formelle Garantie (d. h. eine Sicherheitsbescheinigung) von Firstbeat einholen, dass die anvertrauten Informationen in Übereinstimmung mit den Anforderungen zu Vertraulichkeit und Sicherheit gemäß der Verordnung (Absatz 3.7) aufbewahrt werden.

Im Rahmen des Follow-up-Verfahrens bitten wir Sie, dem EDSB innerhalb von drei Monaten und vor Beginn der Verarbeitung eine überarbeitete Fassung der Meldung, des Datenschutzhinweises, des Vertragsentwurfs und der Sicherheitsgarantie von Firstbeat zu senden, um zu zeigen, dass die vorgenannten Empfehlungen des EDSB umgesetzt wurden.

Brüssel, den 17. Dezember 2015

(unterzeichnet)
Wojciech Rafal WIEWIOROWSKI