Stellungnahme zu einer vom Datenschutzbeauftragten des Europäischen Zentrums für die Prävention und die Kontrolle von Krankheiten erhaltenen Meldung für eine Vorabkontrolle hinsichtlich der Bereitstellung von vertraulicher Mitarbeiterberatung

Brüssel, 22. April 2016
(Fall 2013–0790)

1. Verfahren

Am 1. Juli 2013 erhielt der Europäische Datenschutzbeauftragte („EDSB“) vom Datenschutzbeauftragten („DSB“) des Europäischen Zentrums für die Prävention und die Kontrolle von Krankheiten („ECDC“) 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 der Bereitstellung von vertraulicher Mitarbeiterberatung.

Da es sich um eine Ex-Post-Sache handelt, greift die Zweimonatsfrist, innerhalb derer der EDSB seine Stellungnahme abgeben muss, nicht. Zusätzliche Informationen über die Meldung wurden am 3. Juli 2013 vom ECDC versandt. Weitere Informationen hinsichtlich der Meldung wurden am 19. August 2014 vom ECDC angefordert, wozu das ECDC am 29. August 2014 Stellung nahm. Der Entwurf der Stellungnahme wurde dem DSB am 19. Januar 2015 mit der Bitte um Anmerkungen übermittelt. Eine Antwort ging beim EDSB am 27. Januar 2015 ein.

2. Einzelheiten des Verarbeitungsvorgangs

Der Beratungsdienst für ECDC-Mitarbeiter wird von einer externen psychologischen und psychotherapeutischen Klinik auf vertraglicher Grundlage bereitgestellt. Die kurzfristige vertrauliche Beratung steht Bediensteten und abgeordneten nationalen Sachverständigen zur Verfügung. ECDC-Mitarbeiter können sich mit verschiedenen Problemen, zu denen unter Umständen auch angebliche Belästigung zählen kann, an den Berater wenden. Jeder Mitarbeiter ist zu fünf Beratungsterminen pro Kalenderjahr berechtigt. Es ist dem ECDC nicht gestattet, von der Klinik eine Berichterstattung über einzelne Probleme zu fordern.

Termine sind vertraulich und werden vom Mitarbeiter über den ECDC-internen Arzt gebucht. Die Empfehlung der Inanspruchnahme beratender Unterstützung kann auch von der Humanressourcen(HR)-Abteilung des ECDC ausgehen, wenn sich ein Mitarbeiter an ECDC HR wendet und diesbezüglich um Hilfe bittet. Die Überweisung erfolgt zwar durch die Organisation, aber der Inhalt des Beratungsaustauschs zwischen dem Berater und dem Mitarbeiter ist streng vertraulich.

Mitarbeiter erhalten Tickets, dank derer sie innerhalb einer bestimmten Frist Zugang zu Beratungsdiensten haben. Gemäß der Meldung dient das Ticket-System zwar in erster Linie der Wahrung der Anonymität der Beratungsdienstnutzer, die Tickets sind aber auch Belege für die erfüllte Sorgfaltspflicht bei den Haushaltsausgaben. Informationen über ECDC-

Mitarbeiter, die um beratende Unterstützung bitten, werden vom ECDC weder gespeichert noch aufbewahrt. Ein Register, in dem eine bestimmte Ticket-Nummer einem bestimmten Mitarbeiter zugeordnet ist, wird nur von der Klinik geführt, während das ECDC nur über die Ticket-Nummern Buch führt.

Während die Klinik Daten für 10 Jahre ab dem letzten Eintrag in das Beratungsjournal aufbewahrt, wird die Festlegung eines Aufbewahrungszeitraums für Ticket-Nummern, die elektronisch gespeichert werden, durch das ECDC nicht in Betracht gezogen.

Aus Vertraulichkeitsgründen besteht seitens des ECDC nicht die Absicht, die beiden Register – eines für die „Beratungsticket-Nummern", das vom ECDC zu Haushaltszwecken geführt wird, und das zweite für die Namen von Mitarbeitern, die die Beratungsdienste nutzen, das lediglich vom externen Diensteanbieter geführt wird, – miteinander zu verbinden. Die Verarbeitung personenbezogener Daten durch das ECDC beschränkt sich daher auf die Speicherung von Ticket-Nummern ohne zugeordnete Namen / persönliche Kennzeichen.

3. Rechtliche Prüfung

3.1. Vorabkontrolle

Die vorliegende Verarbeitung weist Ähnlichkeiten zu zwei Arten von Verarbeitungen auf, zu denen vom EDSB ausgegebene Leitlinien vorliegen. Erstens handelt es sich bei den im vorliegenden Fall verarbeiteten personenbezogenen Daten um Gesundheitsdaten und um gesundheitsbezogene administrative Daten. Daher gelten die Leitlinien für die Verarbeitung von Gesundheitsdaten am Arbeitsplatz[1]. Zweitens ähnelt die vom Auftragnehmer durchgeführte Verarbeitung dem informellen Verfahren bei Belästigung, für das die Leitlinien für Verfahren zur Bekämpfung von Belästigung gelten[2]. Diese Stellungnahme konzentriert sich daher auf jene Aspekte, die von den Leitlinien abweichen, verbessert werden müssen oder anderweitig zu erläutern sind. Die Besonderheit der vorliegenden Sachlage besteht in erster Linie in der Existenz des externen Auftragnehmers, der Daten über die psychologische Gesundheit der betroffenen Personen verarbeitet.

3.2. Rechtmäßigkeit

Nach dem Dafürhalten des EDSB ist die Verarbeitung gemäß Artikel 5 Buchstabe a der Verordnung rechtmäßig.
Da es bei der betreffenden Verarbeitung um sensible Daten geht, empfiehlt der EDSB, dass der für die Verarbeitung Verantwortliche die Modalitäten des Beratungsdienstverfahrens im Einzelnen in spezifischeren Regeln (Grundsätze, Mitteilung, Entscheidung), die für seine internen Mitarbeiter gelten, festlegt[3].

---

[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 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).

[3] Wie S. 4.

3.3. Verarbeitung besonderer Datenkategorien

Wir stellen fest, dass es sich bei allen vom ECDC im Zusammenhang mit dem Beratungsdienst verarbeiteten Daten um gesundheitsbezogene Daten handelt. Zu den verarbeiteten Gesundheitsdaten gehören sowohl i) medizinische Daten (z. B. ärztliche Überweisungen und Verschreibungen, ärztliche Untersuchungsberichte) – die vom Auftragnehmer verarbeiteten Daten – als auch ii) mit der Gesundheit in Zusammenhang stehende administrative und finanzielle Daten (z. B. Arzttermine, Rechnungen für erbrachte Gesundheitsleistungen, Angabe der Anzahl der Krankenurlaubstage, Verwaltung des Krankenurlaubs)[4] – die direkt vom ECDC verarbeiteten Daten.

In Anbetracht der Tatsache, dass in der Meldung mehrmals erwähnt wird, dass das ECDC personenbezogene Daten nicht direkt verarbeitet[5], sollte verdeutlicht werden, dass es sich bei den vom ECDC verarbeiteten und um Beratung bittenden Mitarbeitern zugeordneten Ticket-Nummern um „personenbezogene Daten" handelt. Gemäß Artikel 2 Buchstabe a der Verordnung bezeichnet der Ausdruck „personenbezogene Daten" alle Informationen über eine bestimmte oder bestimmbare natürliche Person; als bestimmbar wird eine Person angesehen, „*die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer (...)*". In diesem Fall kann die betroffene Person identifiziert werden, wenn die Aufzeichnungen des ECDC den Aufzeichnungen des Auftragnehmers gegenübergestellt werden. Die Tatsache, dass Mitarbeitern im Zusammenhang mit Daten, die zu administrativen Zwecken in Verbindung mit dem Beratungsdienst verarbeitet werden, eindeutige Nummern zugeordnet werden, so dass nicht alle einzelnen Verarbeiter dieser Daten die um Beratung bittende Person identifizieren können, ist eine gute Praxis, die wir begrüßen. Es handelt sich dabei jedoch um personenbezogene Daten, die denselben Garantien unterliegen wie Informationen über eine bestimmte Person.

3.4. Verantwortung für die Verarbeitung und Zuweisung von Zuständigkeiten

Das ECDC ist der für die vorliegende Datenverarbeitung Verantwortliche und somit für ihre Rechtmäßigkeit, einschließlich der Erfüllung der Anforderungen hinsichtlich Datenqualität, Aufbewahrung, Übermittlungen, Information, Rechten der betroffenen Personen und Sicherheit, zuständig.

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*]". „Die Durchführung einer Verarbeitung im Auftrag", so heißt es in Artikel 23 Absatz 2, „erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist [...]". Dies gilt für die vorliegende Verarbeitung, für die ein Vertrag zwischen dem ECDC und dem Auftragsverarbeiter geschlossen wurde.

Wir begrüßen es, dass sowohl die Datensicherheitspflichten gemäß Artikel 22 der Verordnung als auch die Verpflichtung des Auftragsverarbeiters, ausschließlich unter der Aufsicht des für die Verarbeitung Verantwortlichen zu handeln, im Vertrag verankert sind.

[4] Siehe die oben genannten *Leitlinien zu Gesundheitsdaten*, S. 2.
[5] Siehe Punkte 5, 6, 8, 10 der Meldung.

Um der Eindeutigkeit willen ist anzumerken, dass sich der Vertrag nicht auf die Rechte der Personen beziehen sollte, die den Auftragnehmer in ihrer Eigenschaft als „betroffene Personen“ vertreten, was aus Verordnung 45/2001 stammt (siehe Artikel 11.6.2 und 11.6.3 des Vertrags). Diesbezüglich reicht es aus, dass die Personen, die für den für die Verarbeitung Verantwortlichen arbeiten, gemäß den Artikeln 11 und 12 der Verordnung über die Einzelheiten der Verarbeitung, die ihre personenbezogenen Daten betreffen kann, informiert werden.

Darüber hinaus empfehlen wir die Einfügung einer Klausel, in der der Auftragsverarbeiter dazu verpflichtet wird, den für die Verarbeitung Verantwortlichen darüber zu informieren, wenn der Auftragsverarbeiter die Absicht hat, die Verarbeitung an einen Unterauftragnehmer zu vergeben, und in der es dem Auftragnehmer untersagt wird, irgendwelche seiner Verarbeitungen ohne das vorherige Einverständnis des für die Verarbeitung Verantwortlichen an einen Unterauftragnehmer zu vergeben.

3.5. Rechte der betroffenen Person

Die betroffene Person hat Auskunftsrecht (Artikel 13 der Verordnung) und das Recht auf Berichtigung (Artikel 14). In dem Abschnitt über „Verfahren zur Gewährung der Rechte der betroffenen Personen“ gab das ECDC in der Meldung an, dass „das ECDC keine natürliche Personen betreffenden Daten erhebt“. Bei den elektronischen Informationen über Tickets handelt es sich um personenbezogene Daten (siehe Absatz 3.2 oben); aus diesem Grund müssen den betroffenen Personen Auskunftsrecht und das Recht auf Berichtigung gewährt werden.

3.6. Informationspflicht gegenüber der betroffenen Person

Gemäß Artikel 11 und 12 der Verordnung sind jene, die personenbezogene Daten erheben, verpflichtet, die betroffenen Personen darüber zu unterrichten, dass ihre Daten erhoben und verarbeitet werden. Die betroffenen Personen haben überdies das Recht, u. a. über die Zwecke der Verarbeitung, die Empfänger der Daten und über die spezifischen Rechte, die ihnen als betroffene Personen zustehen, unterrichtet zu werden.

Die Informationen über die vorliegende Datenverarbeitung, die über das Intranet zugänglich sind und vom ECDC am 29. August 2014 versandt wurden, können nicht als „Datenschutzerklärung“ im Sinne von Artikeln 11 und 12 der Verordnung gelten. Die bereitgestellten Informationen betreffen den Zweck der Beratung im Allgemeinen, die Terminvereinbarungsverfahren und die Adresse der Klinik sowie eine Beschreibung des Wegs zur Klinik. Die Formulierung zur Vertraulichkeit reicht nicht aus, als dass die Anforderungen der Unterrichtung der betroffenen Person als erfüllt gelten können.

Zur Gewährleistung einer transparenten Verarbeitung nach Treu und Glauben in Bezug auf eine derartig sensible Verarbeitung unter Wahrung der Rechte der Mitarbeiter empfehlen wir, dass das ECDC eine Datenschutzerklärung gemäß Artikeln 11 und 12 der Verordnung verabschiedet.

Wir begrüßen es, dass die verfügbaren Informationen im Intranet sind, und wir empfehlen, dass die Datenschutzerklärung ebenfalls im Intranet veröffentlicht wird. Darüber hinaus empfehlen wir, dass die Mitarbeiter im Falle einer Bitte um Beratungsdienste an die betroffene Person über die Verarbeitung informiert werden, ggf. bevor die Verarbeitung

beginnt[6]; beispielsweise zu dem Zeitpunkt, an dem sie den internen Arzt oder die Personalabteilung ansprechen und um eine Ticket-Nummer für den Beratungstermin bitten.

Abschließend weisen wir darauf hin, dass die betroffene Person gemäß der allgemeinen Regelung hinsichtlich des Zugangsrechts weiterhin direkten Zugang zu den Gesundheitsdaten erhält, die direkt vom Auftragsnehmer 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[7].

3.7. Datenaufbewahrung

Gemäß der Meldung speichert das ECDC die elektronischen Ticket-Informationen (wie Identifikationsnummern, Ausgabedatum, Rückgabedatum als Beleg für die Rechnungsstellung) für Haushaltszwecke und als Buchungskontrolle für finanzielle Zwecke. Das ECDC teilte dem EDSB mit, „dass auf den Tickets keine personenbezogenen Daten erscheinen; aus diesem Grund wurde für diese Daten kein spezifischer Aufbewahrungszeitraum in Erwägung gezogen“.

Angesichts der Tatsache, dass die Personen, denen Tickets zugeordnet wurden, identifizierbar sind und es sich bei den Tickets um personenbezogene Daten handelt, empfehlen wir, dass das ECDC unter Einhaltung von Artikel 4 Absatz 1 Buchstabe e der Verordnung einen Aufbewahrungszeitraum festlegt.

[6] Siehe diesbezüglich die oben genannten *Leitlinien für Verfahren zur Bekämpfung von Belästigung*, Abschnitt 7.
[7] Siehe die oben genannten *Leitlinien für die Verarbeitung von Gesundheitsdaten*, Abschnitt 6.

Schlussfolgerung

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

1. die Modalitäten des Beratungsdienstverfahrens im Einzelnen in spezifischeren Regeln (Grundsätze, Mitteilung, Entscheidung), die für seine internen Mitarbeiter gelten, festlegen;
2. den Vertrag mit dem Dienstleister ändern, so dass eine Klausel eingefügt wird, in der der Auftragsverarbeiter dazu verpflichtet wird, den für die Verarbeitung Verantwortlichen darüber zu informieren, wenn der Auftragsverarbeiter die Absicht hat, die Verarbeitung an einen Unterauftragnehmer zu vergeben, und in der es dem Auftragnehmer untersagt wird, irgendwelche seiner Verarbeitungen ohne das vorherige Einverständnis des für die Verarbeitung Verantwortlichen an einen Unterauftragnehmer zu vergeben;
3. die Verweise auf die Rechte des „Auftragnehmers“, was aus der Verordnung stammt (siehe Teile von Artikeln 11.6.2 und 11.6.3 des Vertrags), aus dem Vertrag streichen;
4. den betroffenen Personen das Auskunftsrecht und das Recht auf Berichtigung für die personenbezogenen Daten gewähren, die vom ECDC direkt verarbeitet werden;
5. eine Datenschutzerklärung gemäß den Artikeln 11 und 12 der Verordnung verabschieden und sicherstellen, dass Mitarbeiter zu dem Zeitpunkt, an dem sie den internen Arzt oder die Personalabteilung ansprechen und um Beratung bitten, über die Einzelheiten der Verarbeitung informiert werden;
6. gemäß Artikel 4 Absatz 1 Buchstabe e der Verordnung einen Aufbewahrungszeitraum für die Daten festlegen, die direkt vom ECDC verarbeitet werden.

Geschehen zu Brüssel, 22. April 2016

(unterzeichnet)

Wojciech Rafał WIEWIÓROWSKI