PETER HUSTINX
EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER

Herrn Jonathan FAULL
Generaldirektor
GD Binnenmarkt und Dienstleistungen
Europäische Kommission
BRU-SPA2 08/020
1049 Brüssel
BELGIEN

Brüssel, 27. Juli 2010
PH/ZB/ktl/ D(2010)1194 **C 2010-0025**

Bericht der EU-Kommission über den Stand des Datenschutzes im Binnenmarkt-Informationssystem (IMI) (KOM(2010) 170 endgültig)

Sehr geehrter Herr Faull,

wie bereits in den informellen Kommentaren zum Entwurf eines Berichts der Kommission angekündigt, möchte der EDSB nach dessen Annahme nun eine erste Bilanz ziehen: Was wurde bisher erreicht und welche Schritte sind bezüglich der im Bericht aufgeworfenen Fragen noch zu ergreifen? Eine Kopie dieses Schreibens wird auf unserer Website veröffentlicht und den nationalen Datenschutzbehörden übermittelt.

Allgemeine Kommentare

Zunächst möchte ich erwähnen, dass wir den bisherigen Fortschritt begrüßen und mit der guten Zusammenarbeit zwischen unseren Ressorts auf der Grundlage des vorher abgestimmten schrittweisen Vorgehens sehr zufrieden sind. Wir schätzen die gute Arbeit Ihres Teams und bitten Sie, dem Datenschutz auch bei der weiteren Entwicklung des Systems und dessen Ausweitung auf andere Bereiche der Binnenmarktvorschriften Rechnung zu tragen.

Dies schließt die Umsetzung weiterer Datenschutzgarantien in der Praxis und den Grundsatz des eingebauten Datenschutzes (Privacy by Design) mit ein. Außerdem erachten wir die Zusammenarbeit mit Interessenvertretern, darunter der nationalen Datenschutzbehörden, als notwendig, damit deren Belange gewahrt werden. Die Prüfungen und regelmäßigen Berichterstattungen, auf die im Bericht kurz eingegangen wurde, bewerten wir besonders

Postanschrift: rue Wiertz 60 – B-1047 Brüssel
Büro: rue Montoyer 63, Brüssel, Belgien
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu

Tel.: (32-2) 283 19 00 - Fax : (32-2) 283 19 50

positiv. Wir unterstützen deren Umsetzung, um zu gewährleisten, dass Richtlinien und die gute Verwaltungspraxis eingehalten werden.

Umfassender Rahmen

Unser wichtigster Kommentar bezieht sich auf die Annahme eines neuen Rechtsinstruments, vorzugsweise einer Verordnung des Rates und des Parlaments, die wir für die Schaffung eines umfassenden Rahmens notwendig erachten, der die Funktionsweise des Binnenmarktinformationssystems ermöglicht und die rechtliche Sicherheit sowie ein höheres Datenschutzniveau garantiert. In unserer bisherigen Intervention zur Entwicklung des IMI, haben wir wiederholt die Bedeutung eines solchen Rahmens unterstrichen.

In Anbetracht des voraussichtlichen Umfangs und der Komplexität des Systems sowie der Tatsache, dass die Kommission und die Mitgliedstaaten zunächst praktische Erfahrungen im Umgang mit IMI sammeln müssen, begrüßen wir den Vorschlag der Kommission für ein schrittweises Vorgehen. Hit Hilfe dieser Vorgehensweise wurde bereits ein maßgeblicher Fortschritt erzielt, der – neben den Fortschritten im praktischen und technischen Bereich – die Annahme folgender Dokumente beinhaltet:

- Entscheidung der Kommission vom 12. Dezember 2007 über den Schutz personenbezogener Daten bei der Umsetzung des Binnenmarkt-Informationssystems (IMI) (2008/49/EG);
- Empfehlung der Kommission vom 26. März 2009 zu Datenschutzleitlinien für das Binnenmarkt-Informationssystem (IMI) (K(2009) 2041 endgültig);
- Entscheidung der Kommission vom 2. Oktober 2009 zur Festlegung der praktischen Regelungen für den Informationsaustausch auf elektronischem Wege zwischen den Mitgliedstaaten gemäß Kapitel VI der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt; sowie der kürzlich verabschiedete
- Bericht der Kommission vom 22. April 2010 über den Stand des Datenschutzes im Binnenmarkt-Informationssystem (IMI) (KOM(2010) 170 endgültig).

Wir sind mit den bisherigen Ergebnissen des schrittweisen Vorgehens sehr zufrieden. Dennoch halten wir die Annahme eines verbindlichen Rechtsinstruments für ein so wichtiges und komplexes europäisches Informationssystem wie das IMI für unerlässlich. Dieser weitere Schritt sollte vorzugsweise in einem ordentlichen Gesetzgebungsverfahren durchgeführt werden. Die Annahme dieses Rechtsinstruments sollte nicht unangemessen verzögert werden. Wie bereits mit Ihrem Ressort besprochen, sind bei der Konzeption eines solchen Rechtsinstruments die ersten Erfahrungen mit dem IMI zu berücksichtigen und die Schritte zur Erarbeitung sobald wie möglich einzuleiten.

Der Bericht zeigt, dass sich das System bereits deutlich ausgeweitet hat. Bis Ende Januar 2010 wurden über 4 500 zuständige Behörden für die Nutzung des Binnenmarktinformationssystems registriert. Im Jahr 2009 gingen rund 2 700 Informationsanfragen ein. Diese Zahl hat sich von ca. 300 Anfragen im ersten Quartal 2009 auf über 1 100 Anfragen im vierten Quartal exponentiell gesteigert, was hauptsächlich auf Neuerungen, die im Rahmen der Dienstleistungsrichtlinie eingeführt wurden, zurückzuführen ist. Obwohl sich das System noch in einer relativ frühen Phase befindet, zeigt dies, dass bereits eine große Datenmenge verarbeitet wurde und umfangreiche Datenschutzgarantien immer unerlässlicher werden. Jedoch bleibt festzuhalten, dass der Rechtsetzungsprozess einige Zeit in Anspruch nehmen wird und angemessene Bestimmungen notwendig sind, bevor sich das IMI zu einem großen Informationssystem entwickeln kann.

Aus diesem Grund möchten wir Sie dazu anhalten, die notwendigen Schritte für die Schaffung eines umfassenden Rechtsrahmens so bald wie möglich einzuleiten.

Fortschritt in der praktischen Umsetzung

Was den Fortschritt bei der praktischen Umsetzung anbelangt, begrüßen wir die Einbeziehung von nationalen Datenschutzbehörden in vielen Ländern, die Verbreitung von Datenschutzhinweisen auf nationaler und lokaler Ebene und die Integration des Datenschutzes in die Benutzerschulung für das System.

Wir freuen uns außerdem, dass die IMI-Website der Kommission einen umfangreichen Überblick der Funktionsweise des IMI und der damit verbundenen Datenschutzaspekte bietet. Die Einbeziehung von Interessenvertretern, einschließlich nationaler und ggf. subnationaler Datenschutzbehörden, sowie Schulungen, Sensibilisierungskampagnen und Transparenz sind besonders wichtige Sicherungsmaßnahmen für eine angemessene Datenverarbeitung im IMI.

Wir bewerten es weiterhin als positiv, dass Schritte zur Prüfung und Wahrung der Sicherheit des Systems unternommen wurden und die Kommission für 2010 die Durchführung einer neuen Risikoanalyse für das IMI und eine dementsprechende Aktualisierung ihres Sicherheitsplans von 2009 vornehmen möchte.

Darüber hinaus möchten wir die Kommission dazu anhalten zu prüfen, wo die bestehenden Authentifizierungsmechanismen verbessert werden können. Dies ist ausschlaggebend, um das Vertrauen der Benutzer gegenüber dem System zu gewinnen – insbesondere in der jetzigen Situation, in der aufgrund des unterschiedlichen Standes bei der Harmonisierung des Datenschutzes zwischen den einzelnen Mitgliedstaaten noch immer unterschiedliche Praktiken existieren. Wir unterstützen die im Bericht für Anfang 2011 vorgeschlagene externe Prüfung, die einige für den Datenschutz relevanten Punkte, darunter insbesondere die Datensicherheit, abdecken könnte.

Was den Vorwarnmechanismus anbelangt, erachten wir es als äußerst wichtig, dass die Informationsverbreitung strikt auf das notwendige Mindestmaß beschränkt wurde. Die zuständigen Behörden und IMI-Benutzer können z. B. nicht automatisch Vorwarnungen senden und empfangen, da diese Funktion separat aktiviert werden muss. Des Weiteren müssen vor dem Senden von Informationen Kontroll-Listen ausgefüllt werden, um Notwendigkeit und Verhältnismäßigkeit zu prüfen. Informationen werden standardmäßig nur in den Niederlassungsmitgliedstaat gesendet. Die Vorwarnungskoordinatoren prüfen zusätzlich, dass keine unnötigen Vorwarnungen verbreitet werden. Schließlich erhält die Kommission zwar Vorwarnungen, kann aber nicht auf personenbezogene Daten zugreifen.

Des Weiteren begrüßen wir, dass im Bericht deutlich festlegt ist, dass die Vorwarnung von den verantwortlichen Behörden des Niederlassungsmitgliedstaates aufgehoben werden muss, wenn das Risiko, das den Alarm ausgelöst hat, nicht mehr besteht. Wir erachten es zudem als positiv, dass die zuständigen Behörden per E-Mail Erinnerungen zur Aufhebung der Vorwarnungen erhalten, dass die Vorwarnungen nach Behebung des Risikos unsichtbar werden und dass alle personenbezogenen Daten, die im Zusammenhang mit der Vorwarnung erfasst wurden, vom System automatisch spätestens 6 Monate nach der Aufhebung gelöscht werden.

Weitere Datenschutzgarantien

Hinsichtlich der Speicherung personenbezogener Daten im bilateralen Informationsaustausch würden wir es begrüßen, wenn den verantwortlichen Mitarbeitern eine Frist für die „manuelle“ Aufhebung von Fällen gesetzt werden würde. Da das System keine Funktion zur automatischen Aufhebung inaktiver Fälle umfasst, könnte es vorkommen, dass einige Fälle unnötigerweise und für einen unangemessen langen Zeitraum offen bleiben.

Die Statistik für die Richtlinie über die Anerkennung von Berufsqualifikationen 2009 zeigt, dass die gewünschten Informationen in ca. sieben Prozent der Fälle nicht innerhalb von acht Wochen bereitgestellt werden und diese Fälle daher potenziell für einen längeren Zeitraum offen und inaktiv bleiben können. Obwohl diese Zahl nicht besonders groß erscheinen mag, darf nicht außer Acht gelassen werden, dass sie langfristig zunehmen und zu zahlreichen inaktiven aber offenen Fällen mit potenziell veralteten Daten führen kann.

Aus diesem Grund begrüßen wir Ihr Vorhaben, technische Datenschutzsicherungen wie Dringlichkeitslisten und Erinnerungen in das System zu integrieren, um dadurch eine zügige Aufhebung von Fällen sicherzustellen. Diese Sicherungsmaßnahmen sollten unverzüglich eingeführt werden. Sie sind besonders beim Austausch von Informationen aus dem Strafregister oder anderen Informationen, die mit der Zeit veraltet oder fehlerhaft werden können, von Bedeutung.

Wir empfehlen Ihnen, die Situation zu beobachten (Zahl der seit langer Zeit offenen Fälle mit entsprechender Begründung) und weitere Maßnahmen zu prüfen, die eine zügige Aufhebung der Fälle bewirken. Eine Möglichkeit, die wir bereits vorgeschlagen haben, ist der Einsatz neuer „Standardeinstellungen“ für die Aufhebung von Fällen: Wenn ein Fall z. B. seit sechs Monaten nach seiner letzten Bearbeitung inaktiv ist, sollten automatisch eine oder mehrere Erinnerungen versendet werden. Falls danach noch immer keine offizielle Aufhebung oder andere Aktivität erfolgt ist, sollte der Fall automatisch vom System gelöscht werden. Ein vergleichbarer Mechanismus könnte die sofortige Aufhebung von nicht mehr benötigten Fällen bewirken.

Vor diesem Hintergrund sollte das Vorhaben, die Aufbewahrungszeit von derzeit sechs Monaten nach Aufhebung zu erhöhen, sorgfältig überdacht werden. Dies bedeutet, dass zunächst eine sehr spezifische und genaue Begründung vorgelegt werden sollte, warum die aktuell geltenden sechs Monate nicht ausreichen und wie viel zusätzliche Zeit benötigt wird. Zweitens könnte auch die „Blockierung“ von Daten eine Möglichkeit sein, um wirklich notwendige Informationen für einen begrenzten Zeitraum im System zu behalten. Diese Möglichkeit sollte gründlich geprüft werden. Außerdem sollte eindeutig festgelegt werden, wer blockierte Daten einsehen darf und zu welchem Zweck.

Drittens sollte ein begrenzter Zeitraum definiert werden. Über eine Verlängerung der derzeitigen Aufbewahrungszeit von Daten sollte nicht leichtfertig entschieden werden: Je länger die Daten aufbewahrt werden, umso höher ist das Risiko des „function creep“ (schleichende Ausweitung der Zweckbestimmung): Da im IMI zahlreiche sensible Daten, darunter Vorwarnungen und Strafregistereinträge, gespeichert sind, muss besonders darauf geachtet werden, dass die gespeicherten Daten nicht für unvorhergesehene Zwecke genutzt oder an unbefugte Empfänger weitergeleitet werden, die sie für zusätzliche, unrechtmäßige Zwecke verwenden könnten. Die Entscheidungen des Gerichtshofes in der Sache *Rijkeboer* (C-553/07) sollten ebenfalls beachtet werden.

Im Sinne des Grundsatzes des eingebauten Datenschutzes („Privacy by Design“) empfehlen wir Ihnen den „Einbau“ spezieller Mechanismen in die Systemarchitektur, um die Zusammenarbeit zwischen den zuständigen Behörden zu erleichtern, falls diese eine Auskunfts- oder Berichtigungsanfrage erhalten und miteinander kommunizieren müssen. Dadurch können sie diese Anfragen leichter autorisieren bzw. eine Berichtigung oder Aktualisierung von Daten für das gesamte System vornehmen.

Wenn diese Art von Zusammenarbeit zwischen den zuständigen Behörden notwendig ist, um Auskünfte zu erhalten oder Berichtigungen durchzuführen, sollte das Potenzial des IMI-Systems genutzt werden: Die zuständigen Behörden müssen in Bezug auf Auskunfts- oder Berichtigungsanfragen auf dieselbe effiziente Art und Weise miteinander kommunizieren können wie bei ihren Fragebögen zum Informationsaustausch im Rahmen der Richtlinie über die Anerkennung von Berufsqualifikationen oder der Dienstleistungsrichtlinie. Obwohl im gegenwärtigen frühen Funktionsstadium des Systems noch keine bedeutende Menge an Auskunfts- oder Berichtigungsanfragen registriert wurde, sollte dennoch rechtzeitig und präventiv eine effiziente Vorgehensweise für diese Anfragen erarbeitet werden.

In Bezug auf die nationale Nutzung des IMI begrüßen wir die ausdrückliche Erwähnung im Bericht, dass die nationalen Datenschutzbehörden vor der Autorisierung jeder nationalen Nutzung des IMI kontaktiert und deren Bedenken berücksichtigt werden sollten. In einigen Ländern gibt es möglicherweise keine gesetzliche Grundlage für die nationale Nutzung des Vorwarnmechanismus, während es bei anderen Arten von bilateralem Informationsaustausch keine Probleme mit dem Datenschutz gibt.

Berücksichtigung der Kommentare

Wir hoffen, dass Ihnen die oben erwähnten Kommentare weiterhelfen. Wir würden uns freuen, wenn Sie uns in einem nächsten Schritt Ihre Sichtweise zu den Kommentaren mitteilen könnten.

Wir sind insbesondere an Ihrem Feedback bezüglich konkreter Schritte für die Einführung eines umfassendem rechtlichen Rahmens für das IMI, vorzugsweise in einem ordentlichen Gesetzgebungsverfahren, interessiert.

Weiterhin sind wir besonders an Ihren Antworten zu folgenden Punkten interessiert:

a) Verpflichtung zur Einbeziehung des Datenschutzes bei Prüfungen und regelmäßigen Berichterstattungen im IMI (einschließlich der Datenschutzaspekte);
b) Vorschläge für Schritte und Fristen für den praktischen Einsatz der im Abschnitt 7.1 des Berichts der Kommission genannten „technischen Verbesserungen“ (Erinnerungen und Dringlichkeitslisten);
c) Vorschläge für weitere „technische Verbesserungen“, die in diesem Schreiben angesprochen wurden und dem Grundsatz des eingebauten Datenschutzes („Privacy by Design“) folgen, einschließlich Standardeinstellungen für die automatische Aufhebung von inaktiven Fällen (sowohl Vorwarnungen als auch Austausch) sowie Vorschläge für den „Einbau“ von Mechanismen, die die Zusammenarbeit zwischen den zuständigen Behörden bezüglich Auskunfts- und Berichtigungsanfragen erleichtern;
d) Eine spezifische und genaue Begründung für jegliche Verlängerungen der derzeit geltenden sechs Monate Aufbewahrungsfrist von Daten, dazu ausführliche

Erklärungen zur Umsetzung derartiger Verlängerungen und dem Vorschlag angemessener Datenschutzbestimmungen für einen eventuellen „Blockierungszeitraum“.

Wir freuen uns auf die Zusammenarbeit mit Ihnen beim schrittweisen Aufbau eines umfassenden datenschutzrechtlichen Rahmens für das IMI.

Im Rahmen Ihres Feedbacks werden wir auch eine gemeinsame Sitzung mit nationalen und ggf. subnationalen Datenschutzbehörden zu gegebener Zeit in Erwägung ziehen, um die Fragen, die im Rahmen der Aufsicht oder einer späteren Beratung hinsichtlich des IMI entstehen können, zu analysieren.

Mit freundlichen Grüßen

(unterzeichnet)

Peter HUSTINX