GIOVANNI BUTTARELLI
STELLVERTRETENDER DATENSCHUTZBEAUFTRAGTER

Frau Laraine LAUDATI
Datenschutzbeauftragte
Europäische Kommission
Europäisches Amt für Betrugsbekämpfung
(OLAF)
1049 Brüssel

Brüssel, den 10. August 2012
Unser Zeichen: D(2012)1681 **C 2012-0279**
Bitte richten Sie alle Schreiben an edps@edps.europa.eu

Betrifft: Meldung des Datenschutzbeauftragten des Europäischen Amtes für Betrugsbekämpfung (OLAF) für eine Vorabkontrolle der Verarbeitung personenbezogener Daten im Zusammenhang mit der „Search Facility"

Sehr geehrte Frau Laudati,

ich schreibe Ihnen im Zusammenhang mit der von Ihnen am 23. März 2012 eingereichten Meldung zur Vorabkontrolle der „Search Facility" (Suchfazilität). Ausgelöst wurde die Meldung durch eine Empfehlung des EDSB in seiner Stellungnahme zur Vorabkontrolle neuer Untersuchungsverfahren vom 3. Februar 2012. Ursprünglich war die „Search Facility" nämlich im Zusammenhang mit diesem Verfahren der Vorabkontrolle gemeldet worden. In seiner Stellungnahme war der EDSB zu dem Schluss gekommen, dass ihm für eine Analyse der neuen „Search Facility" keine ausreichenden Informationen vorlagen, weshalb er OLAF zur Einreichung einer eigenen Meldung aufforderte.

In Ihrem Anschreiben zur Meldung wiesen Sie darauf hin, dass OLAF nach weiteren Überlegungen bei der Vorbereitung der Meldung zu der Auffassung gelangt ist, dass eine Vorabkontrolle dieser Verarbeitung nicht erforderlich ist, da sie in den Geltungsbereich der Meldung betreffend OLAF „Intelligence Databases" fällt („Meldungen von 2007") (siehe Stellungnahme des EDSB vom 21. November 2007 zu den verbundenen Fällen 2007-27 und 2007-28, nachstehend als „Stellungnahme von 2007" bezeichnet).

Die „Search Facility" ist eine neue iBase-Datenbank, die in der Hauptsache den befugten Mitarbeitern im Referat Untersuchung – Auswahl und Prüfung (Referat 0.1), die für die Auswahl von Fällen zuständig sind, die eine elektronische Suche nach Datenteilsätzen im Fallverwaltungssystem (CMS) von OLAF ermöglicht, anhand derer sie überprüfen, ob neue Informationen in Verbindung zu einem bekannten Fall stehen; auf diese Weise lässt sich die Eröffnung eines zweiten Verfahrens zu identischen Sachverhalten vermeiden. Die Fazilität nimmt Abgleiche folgender Datenfelder vor, die aus den Tabs „Organisation" und „Person" des CMS extrahiert werden: Name, Kommentar zur Verwicklung, Kommentar zur

Organisation, Anschrift(en), Kontakt(e), Arbeitsplatz/-plätze, Art der betroffenen Personen, Alias-Namen, Geburtsdatum, Geburtsort, Kommentar zur Person, Land, Programm. Die Suchergebnisse weisen auf Dokumente hin, in denen die gesuchten Daten auftauchen.

Die Datenbank enthält folgende Unterlagen: Stellungnahmen zur Eröffnungsentscheidung (Erstbeurteilung vor dem 1. Februar 2012), Neunmonatsberichte, Zwischenberichte und Abschlussberichte. Die Fazilität steht in Verbindung mit den neuen Untersuchungsverfahren, mit denen ein Auswahlverfahren für die Bewertung neuer Informationen über potenzielles Interesse an einer Untersuchung eingeführt worden ist (siehe Stellungnahme des EDSB zur Vorabkontrolle vom 3. Februar 2012 zu den Fällen 2011-1127, 2011-1129, 2011-1130, 2011-1131, 2011-1132). Wie andere Intelligence-Datenbanken kann die „Search Facility" von den OLAF-Analysten auch für die Zwecke und unter den Bedingungen verwendet werden, die in den Meldungen von 2007 und der entsprechenden Stellungnahme genannt werden. Anders als bei anderen Intelligence-Datenbanken haben zur „Search Facility" jedoch auch Bedienstete des Referats 0.1 für Zwecke der Fallauswahl Zugang.

In den Meldungen von 2007 sind die Bedingungen dargestellt, unter denen OLAF Daten zu Intelligence-/Analysezwecken und für operative Tätigkeiten sowie zur Unterstützung konkreter Fallersuchen, von Vorgängen und Untersuchungen verarbeiten darf, damit ein Höchstmaß an Genauigkeit und Relevanz der Informationen gewährleistet ist, die zu Intelligence-Zwecken und zur Verwendung in den Bereichen Finanzen und Verwaltung sowie in Disziplinar- und Gerichtsverfahren eingehen, verbreitet und anderweitig verarbeitet werden. Die Intelligence-Datenbanken (iBase) wurden als eines des Instrumente des „Information and Intelligence Data Pool" bezeichnet. Daher sind das bei der Verarbeitung eingesetzte IT-Tool (iBase-Datenbank), das in den verbundenen Fällen 2007-0027 und 2007-0028 sowie im vorliegenden Fall geschildert wurde, deckungsgleich. Dessen ungeachtet bestehen einige Unterschiede. Die verbundenen Fälle 2007-0027 und 2007-0028 decken ein breiteres Szenario ab. Die „Search Facility" dient hingegen im Wesentlichen der Beantwortung der Frage, ob die neuen Informationen in Verbindung mit einem bereits bestehenden Fall stehen, so dass die Eröffnung eines weiteren Falls zu identischen Sachverhalten vermieden werden kann. Ihr Inhalt ist genau festgelegt (Stellungnahmen zur Eröffnungsentscheidung (Erstbeurteilung vor dem 1. Februar 2012), Neunmonatsberichte, Zwischenberichte und Abschlussberichte).

Trotz des engeren Anwendungsbereichs und anderer Unterschiede (z. B. Zugriff gewährt für Referat 0.1) hat es aufgrund der vorliegenden Informationen den Anschein, als würde die „Search Facility" ebenfalls die Standardmerkmale der Intelligence-Datenbanken enthalten und damit in den Geltungsbereich der entsprechenden Meldungen fallen. In der Meldung von 2007 wurden eher Standardstruktur, Konzeption, Prüfpfad, Managementkontrolle und Zugangsrechte von Datenbanken im iBase-Umfeld und weniger eine bestimmte Datenbank beschrieben. Solange die neue Datenbank die in dieser Meldung beschriebenen Merkmale aufweist, fällt sie unter diese Meldung von 2007 und eine eigene Meldung ist nicht erforderlich. Auf eine entsprechende Anfrage hat OLAF bestätigt, dass die „Search Facility" diese Standardmerkmale aufweist. Daher gelten gegebenenfalls die Anmerkungen und Empfehlungen des EDSB in seiner Stellungnahme von 2007 auch für den vorliegenden Fall.

Des Weiteren sollte bedacht werden, dass die mit Hilfe der „Search Facility iBase-Datenbank vorgenommene Verarbeitung eine in den Fällen 2011-1127, 2011-1129, 2011-1130, 2011-1131, 2011-1132 beschriebene allgemeine Verarbeitungstätigkeit ist (genauer gesagt die „Auswahlphase"). Diese Verarbeitungstätigkeit sollte daher auch im Einklang mit den Anmerkungen und Empfehlungen des EDSB in seiner Stellungnahme vom 3. Februar 2012 stehen, soweit diese anwendbar sind.

In Anbetracht dessen sind wir der Auffassung, dass die hier zu prüfende Verarbeitung keine vollständige Vorabkontrolle erfordert, da sie bereits durch die Meldungen betreffend den „Information and Intelligence Data Pool“ und die Intelligence-Datenbanken von OLAF (Fälle 2007-0027 und 2007-0028) sowie die neuen Untersuchungsverfahren von OLAF (interne Untersuchungen, externe Untersuchungen, abgewiesene Fälle und eingehende Hinweise ohne Ermittlungsinteresse, Koordinierungsfälle und Umsetzung der OLAF-Empfehlungen) (Fälle 2011-1127, 2011-1129, 2011-1130, 2011-1131, 2011-1132) abgedeckt ist. Wir verweisen auf die Empfehlungen in den endgültigen Stellungnahmen des EDSB in diesen Fällen, die im Allgemeinen auch auf die hier zu prüfende Datenbank anzuwenden sind. Insbesondere unterstreichen wir die Bedeutung, die der Gewährleistung der Datenqualität und dem Erfordernis zukommt, hinsichtlich der Erfordernisse der jeweiligen Untersuchung bei der Nutzung der Datenbank im Einzelfall den Grundsatz der Notwendigkeit und Verhältnismäßigkeit zu wahren.

Im Hinblick auf die für die Datenbank geltenden Sicherheitsvorkehrungen weist der EDSB OLAF auf Folgendes hin:

- Sicherheitskontrollen sollten auf einer Informationsrisikoanalyse beruhen. Im Idealfall würde sich ein Informationssicherheitsmanagementsystem (ISMS) bei der Einrichtung eines neuen Systems melden und die Durchführung einer Risikoanalyse verlangen, die wiederum OLAF dabei helfen würde, alle erforderlichen technischen und organisatorischen Sicherheitskontrollen vorzunehmen.

- Zur Nutzerverwaltung:
    - Nach dem Verständnis des EDSB soll ein Verzeichnisdienst für die Nutzer-Authentifizierung verwendet werden und sollen die Nutzerkonten einmal jährlich überprüft werden. Der Überprüfung dieser Nutzerkonten kommt entscheidende Bedeutung zu, denn sie sorgt dafür, dass nur befugte Personen Zugang zum System haben; daher müssen diese Überprüfungen sorgfältig geplant und durchgeführt werden.
    - Schließlich sollten die Verfahren für die Gewährung, die Änderung oder den Entzug des Zugangs zu diesem System eindeutig dokumentiert und kommuniziert werden; diese Verfahren sollten regelmäßig überprüft werden, damit sichergestellt ist, dass ausreichend Sicherheitskontrollen durchgeführt wurden und greifen.

- Zu Protokollierung und Überwachung:
    - Zur Aufdeckung von Angriffsversuchen sollten die Protokolle des Verzeichnisdienstes regelmäßig überprüft werden. Es könnten ferner weitere Sicherheitskontrollen (wie Einbruchmeldesysteme oder Einbruchverhütungssysteme (IDS/IPS)) in Erwägung gezogen werden.
    - Die iBase Audit-Datenbank und Sicherheitsdatenbank sollten gegen Verlust an Vertraulichkeit und Integrität, auch durch die Administratoren, gesichert werden.
    - Die iBase Audit-Datenbank sollte so verwaltet werden, dass auch bei einer Betriebsunterbrechung keine Log-Informationen verloren gehen.
    - Mit einem dokumentierten Verfahren sollte sichergestellt werden, dass die dreijährige Aufbewahrungsfrist für Protokolle eingehalten wird. Im Idealfall sollte dies automatisch geschehen (d. h., das System sollte Protokolle, die älter als drei Jahre sind, automatisch löschen). Ausnahmen könnten nach einem ordnungsgemäß dokumentierten Verfahren für interne Untersuchungszwecke vorgesehen werden.

- Zu dem in Ihrer Meldung erwähnten und für den Aufbau der iBase-Datenbank erforderlichen Auszug historischer Daten und den später erfolgten Datenimporte in diese iBase-Datenbank:

- Es sollte sorgfältig darauf geachtet werden, dass alle Schritte und hier vor allem manuelle Schritte zur Aufdeckung von Fehlern (Gewährleistung der Datenqualität) ausreichend kontrolliert werden.
- Alle vorläufigen Kopien der Daten (auch Teilkopien) sollten gegen Verlust der Vertraulichkeit und Integrität gesichert und vernichtet werden, sobald sie nicht mehr benötigt werden.

Sollten Sie weitere Auskünfte zu der vorliegenden Verarbeitung benötigen, stehen Ihnen die Mitarbeiter des EDSB selbstverständlich zur Verfügung.

Mit freundlichen Grüßen

(**unterzeichnet**)

Giovanni BUTTARELLI