Stellungnahme zur Meldung des Datenschutzbeauftragten der Europäischen Eisenbahnagentur (ERA) für eine Vorabkontrolle des Internet-Systems der ERA

Brüssel, den 6. Dezember 2012 (Fall 2012-0135)

1. VERFAHREN

Am 10. Februar 2012 erhielt der Europäische Datenschutzbeauftragte („**EDSB**“) eine Meldung des Datenschutzbeauftragten („**DSB**“) der Europäischen Eisenbahnagentur („**ERA**“ oder „**Agentur**“) zur Vorabkontrolle des Internet-Systems der ERA. Vor Einreichen der Meldung konsultierte die ERA den EDSB zur Notwendigkeit der Vorabkontrolle gemäß Artikel 27 Absatz 3 der Verordnung (EG) Nr. 45/2001 („**Verordnung**“). Der Meldung waren folgende Entwürfe beigefügt:

- Policy 2.0 Use of ERA ICT[1] Owned Resources (Strategie 2.0 Nutzung der ERA-eigenen IKT-Ressourcen) („**ICT**“);
- Policy 2.1 Identity and Access Management (Strategie 2.1 Identitäts- und Zugangsmanagement) („**IAM**“);
- Policy 2.2 Internet Acceptable Use Policy (Strategie 2.2 Strategie der annehmbaren Nutzung des Internets) („**Internet Policy**“);
- Policy 2.3 Electronic Communication Policy (Strategie 2.3 Strategie der elektronischen Kommunikation) („**ECP**“);
- Policy 2.4 E-mail Acceptable Use (Strategie 2.4 Annehmbare Nutzung der E-Mail) („**E-mail Policy**“);
- Policy 2.5 Electronic Information Security Policy (Strategie 2.5 Strategie der Sicherheit elektronischer Informationen) („**EISP**“).

Der EDSB forderte die ERA am 2. April, 2. Juli, 7. und 28. September sowie am 17., 23. und 26. Oktober 2012 auf, einige ergänzende Informationen vorzulegen. Die Antworten gingen am 4. Mai, 5. und 25. September, 15., 17., 18. und 24. Oktober sowie am 15. November 2012[2] ein. Am 10. Mai 2012 beschloss der EDSB, die Frist für die Abgabe einer Stellungnahme in Übereinstimmung mit Artikel 27 Absatz 4 der Verordnung aufgrund der Komplexität der Angelegenheit um zwei Monate zu verlängern. Am 10. Oktober 2012 fand zur weiteren Klärung einiger offener Fragen ein Treffen zwischen dem EDSB und Dienststellen der ERA statt. Der Entwurf der Stellungnahme wurde dem DSB am 15. November 2012 zur Kommentierung vorgelegt; seine Bemerkungen gingen beim EDSB am 4. Dezember 2012 ein.

[1] Informations- und Kommunikationstechnologie.

[2] Die vollständigen Antworten für alle am 2. Juli und 7. September 2012 gestellten Fragen gingen erst am 17. Oktober 2012 ein. Der EDSB betrachtete daher den Zeitraum zwischen dem 2. Juli und dem 17. Oktober als eine fortgesetzte Aussetzung.

2. SACHVERHALT

Die vorliegende Stellungnahme zur Vorabkontrolle betrifft die Internet-Strategie der ERA wie in den Dokumenten Internet Policy und ECP beschrieben. Nach Angaben der ERA ist das Referat Verwaltung (Administration Unit) der Teil der Organisation der Agentur, der mit der Verarbeitung befasst ist.

Neben der Meldung übermittelte die ERA dem EDSB ihre schriftlich niedergelegten Strategien zu ICT, IAM und EISP als Hintergrunddokumente. Obwohl diese Dokumente fachlich gesehen nicht Gegenstand der vorliegenden Stellungnahme sind, wird sich der EDSB auf sie beziehen, sofern sie relevant sind.

2.1. Zwecke der Verarbeitung

Die von der ERA angegebenen Zwecke der Internet-Strategie lauten wie folgt:

- Darstellung der angemessenen und der unangemessenen Nutzung der Internet-Dienste der Agentur;
- Sicherstellung, dass die Systeme und Internet-Dienste der Agentur für Zwecke eingesetzt werden, die dem Aufgabenbereich der Agentur entsprechen;
- Information der Mitarbeiter und Nutzer der Agentur über die Anwendbarkeit der Regeln und Strategien der ERA, wenn sie auf die Internet-Systeme und –Dienste der Agentur zugreifen;
- Verhinderung von Störungen und Missbrauch der Infrastruktur der ERA.

Angemessene und unangemessene Nutzung des Internets

Abschnitt IV der Internet-Strategie („Allowable Use“ [Zulässige Nutzung]) legt dar, was nach Ansicht der ERA als angemessene bzw. unangemessene Nutzung anzusehen ist. Gemäß diesem Dokument gefährdet jegliche unsachgemäße Nutzung des Internets den rechtlichen Status der Agentur und wird nicht geduldet. Zudem wird die „unangemessene Nutzung“ in dem Dokument u. a. wie folgt definiert:

a. Das Internet darf nicht für illegale oder ungesetzliche Zwecke eingesetzt werden, wenn der Zugang über die Infrastruktur der ERA erfolgt[3].
b. Das Internet darf nicht in einer Weise verwendet werden, welche die Strategien, Vorschriften oder Verwaltungsanweisungen der ERA verletzt, oder in einer Weise, die nicht dem Aufgabenbereich der Agentur entspricht.
c. Die Mitarbeiter sollten ihre private Internetnutzung über die Infrastruktur der ERA beschränken. Die ERA erlaubt eine beschränkte private Nutzung für die Kommunikation mit Familie und Bekannten, unabhängiges Lernen und die Inanspruchnahme öffentlicher Dienstleistungen. Die ERA untersagt unerbetene Massensendungen, den Zugang zu Ressourcen und Netzwerkeinrichtungen der ERA durch Nicht-Mitarbeiter, konkurrierende kommerzielle Tätigkeiten und die Verbreitung von Kettenbriefen.
d. Personen dürfen Daten, Software, Dokumente oder Datenmitteilungen, die der ERA oder einem anderen Bediensteten gehören, nicht ohne Genehmigung ansehen, kopieren, verändern oder vernichten.
e. Die Benutzer dürfen keine unangemessen großen E-Mail-Anhänge versenden.

[3] Darunter u. a. Verletzung von Urheberrechten, Obszönität, Beleidigung, Verleumdung, Betrug, Diffamierung, Plagiat, Belästigung, Einschüchterung, Fälschung, Nachahmung, illegales Glücksspiel, Aufforderung zu illegalen Pyramidensystemen und Computermanipulationen (z. B. durch Computerviren).

Abschnitt V der Internet-Strategie enthält weitere Regeln für die Internet-Sicherheit. Dort ist u. a. Folgendes bestimmt:

a. Konten- oder Passwort-Informationen dürfen nicht gemeinsam genutzt werden;
b. das Herunterladen von Software ist nicht zulässig;
c. wenn ein neues Programm oder ein Update einer vorhandenen Software erforderlich scheinen, ist der ICT Service Desk mit der Angelegenheit zu befassen.

Überwachung der Nutzung

Die ICT besagt, dass die Agentur die Nutzungsmuster der IKT-Ressourcen routinemäßig überprüft, um die Funktionsfähigkeit der Informations- und Kommunikationssysteme der ERA sicherzustellen und Sicherheitsverstöße zu verhindern. Der Inhalt von Mitteilungen wird in keinem Fall überwacht. Abweichungen von den Vorschriften müssen durch die Bedürfnisse der Dienststelle gerechtfertigt sein und ausdrücklich vom ITFM-Leiter[4] und/oder dem IKT-Sicherheitsbeauftragten nach Konsultation des IT Governing Committee genehmigt werden. Der gesamte ein- und ausgehende Internet-Verkehr wird automatisch von einem oder mehreren Sicherheitstools verarbeitet, um Viren, Malware oder Spyware zu entdecken. Der gesamte von außerhalb der Agentur eingehende Internet-Verkehr wird automatisch durch eine Antiviren-Software gescannt. Beim Auftreten eines Problems wird eine automatische Desinfizierung durchgeführt[5].

Die Agentur setzt Software-Filter und andere Techniken ein, um den Zugang zu unangemessenen Informationen zu beschränken. Wird der Zugang verweigert, erhält der Benutzer eine klare, persönliche Mitteilung mit Angabe der Gründe, aus denen der Zugang verweigert wurde. Die Zugangsversuche werden somit für die oben genannten Zwecke protokolliert. Die ERA erklärte, dass die Aufzeichnungen nicht verwendet werden, um das individuelle Verhalten zu überwachen; ausgenommen hiervon sind nur die Fälle, die in Artikel 20 der Datenschutzverordnung erwähnt werden. Im Anhang zur Strategie hat die ERA eine Liste gefilterter Kategorien vorgelegt.

Gemäß ihrer Internet-Strategie darf die ERA jegliche Internet-Tätigkeit in ihren Ausrüstungen oder Konten überwachen. Die Agentur bewahrt die Protokolle des Internet-Verkehrs auf, um die Funktionsfähigkeit ihrer Systeme zu gewährleisten und Sicherheitsverstöße zu verhindern. Die Logdateien enthalten Folgendes:

- URL-Zugriffsprotokoll: Name des ERA-Servers, der die Anfrage verarbeitet, Datum und Uhrzeit, Client-IP, Server-IP, Domäne, Pfad, Kategorie, Protokoll, Anzahl der Zugriffe, empfangene MB. Die Client-IP wird dynamisch geleast;
- URL-Sperrprotokoll: Datum und Uhrzeit, Kategorie, Regel, Scan-Typ, IOOID, URL, Protokoll;
- URL-Filterprotokoll: Datum und Uhrzeit, Kategorie, Regel, Scan-Typ, Filteraktion, URL, Protokoll[6].

Es sei darauf hingewiesen, dass die ERA die Protokolle des Dienstes für die Zuweisung der IP-Adressen (DHCP-Protokolle) nicht aufbewahrt.

2.2. Kategorien betroffener Personen

Es gibt folgende Kategorien betroffener Personen:

[4] IT und Facility Management.
[5] Internet-Strategie, S. 10.
[6] Ebenda S. 11.

- Mitarbeiter der ERA,
- Auftragnehmer der ERA,
- Einzelpersonen, die beruflich mit der ERA zusammenarbeiten, und
- alle Personen, die über die von der Agentur bereitgestellte Infrastruktur auf einen Internet-Dienst zugreifen.

2.3. Kategorien personenbezogener Daten

Laut Meldung sind folgende Datenkategorien (d. h. vom System registrierte Datenfelder) betroffen:

- Name des ERA-Servers, der die Anfrage verarbeitet,
- IP-Adresse,
- Zeitstempel der Verarbeitung der Abfrage (Eingang, Zuweisung, Modifizierung, Auflösung usw.)
- Informationen zum angeforderten/aufgerufenen Dienst,
- alle Informationen, welche die betroffene Person im Rahmen der Transaktion bereitstellt.

2.4. Datenübermittlungen/Empfänger

Die Meldung besagt, dass es sich bei den Empfängern der Daten um den IKT-Sicherheitsbeauftragten und den ITFM-Leiter handelt.

Im weiteren Schriftwechsel mit dem EDSB fügte der für die Verarbeitung Verantwortliche folgende interne Empfänger hinzu:

- Leitender Direktor,
- Datenschutzbeauftragter,
- Leiter des Referats Verwaltung,
- Leiter des betroffenen Referats,
- Leiter des betroffenen Bereichs,
- Leiter des Bereichs Humanressourcen,
- IT-Systemadministrator,
- IT-Dienstleister.

Unter bestimmten Umständen können Daten vorübergehend an folgende Stellen weitergeleitet werden:

- auf Antrag den Richtern des Gerichts für den öffentlichen Dienst oder
- auf Antrag der Staatsanwaltschaft oder
- dem OLAF und/oder dem IDOC (Untersuchungs- und Disziplinaramt) im Rahmen ihrer Untersuchungen oder
- dem Bürgerbeauftragten auf dessen Antrag
- oder dem Europäischen Datenschutzbeauftragten auf dessen Antrag.

Die Meldung erwähnt auch Datenübermittlungen an die Staatsanwaltschaft.

2.5. Datenaufbewahrung

Logdateien (und andere betroffene Daten) werden verarbeitet und für einen Zeitraum von höchstens 90 Tagen aufbewahrt.

2.6. Rechte der betroffenen Personen

Die Meldung gibt an, dass die betroffenen Personen durch einen Vermerk für die Mitarbeiter mit dem Titel „Use of ERA's ICT owned resources" (Nutzung der ERA-eigenen IKT-Ressourcen), die ICT und die Internet-Strategie informiert wurden.

Die betroffenen Personen können ihr Recht auf Auskunft und Berichtigung ausüben, indem sie eine E-Mail mit Angabe des Rechts, das sie ausüben möchten, an ein funktionales Postfach senden. Der Antrag wird von dem für die Verarbeitung Verantwortlichen innerhalb von einem Monat bzw. drei Monaten bearbeitet, je nachdem, ob es in dem Antrag um Auskunft oder die Sperrung/Löschung geht.

2.7. Sicherheitsmaßnahmen

Es bestehen mehrere systemspezifische Sicherheitsmaßnahmen, die in der Internet-Strategie beschrieben sind:

- Das System ist in das von der Agentur eingerichtete IAM-System integriert. Die Benutzer werden darüber informiert, dass sie ihr Passwort nicht weitergeben dürfen, auch nicht an den Service Desk.
- Um Viren zu bekämpfen, wird der eingehende Datenverkehr von außerhalb des Netzes der ERA automatisch auf Viren, Malware und Spyware gescannt und gegebenenfalls bereinigt.
- Die ERA verwendet eine Filtersoftware, um den Zugang zu unangemessenen Daten (z. B. Material mit obszönem, rassistischem oder den Terrorismus unterstützendem Inhalt usw.) zu beschränken.
- Der Zugriff auf Logdateien ist den IKT-Systemadministratoren der ERA und dem IT-Sicherheitsbeauftragten der ERA vorbehalten.

Weitere Maßnahmen, die alle Systeme abdecken, sind in der EISP beschrieben und umfassen:

- die Notwendigkeit eines Risikomanagements und die Notwendigkeit, kosteneffiziente Kontrollen zur Vorbeugung gegen diese Risiken festzusetzen;
- eine Beschreibung der Aufgaben und Zuständigkeiten, die auch Sicherheitsaspekte abdeckt;
- Vorschriften für Verschlusssachen;
- eine Liste der festzulegenden erforderlichen Sicherheitsverfahren;
- operative und technische Kontrollen (Backup, Korrektur- und Änderungsmanagementprozesse usw.);
- die Notwendigkeit von Schulung und Sicherheitsbewusstsein.

3. RECHTLICHE ASPEKTE

3.1. Vorabkontrolle

Gegenstand dieser Stellungnahme zu einer Vorabkontrolle sind die Strategien der ERA für die Internet-Nutzung innerhalb der Agentur einschließlich der Datenverarbeitungstätigkeiten zur Überwachung des Benutzerverhaltens. In der Stellungnahme wird also beurteilt, inwieweit die oben beschriebenen Datenverarbeitungstätigkeiten der zuständigen Akteure der ERA im Einklang mit der Verordnung stehen.

3.1.1. Anwendbarkeit der Verordnung

Die Verordnung gilt für die *„ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind“* und für die Verarbeitung *„durch alle Organe und Einrichtungen [der EU], soweit die Verarbeitung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des EU-Rechts fallen“*. Aus den nachstehend dargelegten Gründen sind alle Elemente vorhanden, die die Anwendung der Verordnung auslösen.

Erstens bringt die Überwachung der Nutzung des Internets das Erfassen und Weiterverarbeiten *personenbezogener Daten* mit sich, wie sie in Artikel 2 Buchstabe a der Verordnung definiert sind. Wie tatsächlich in der Meldung beschrieben, werden personenbezogene Daten der Internet-Nutzer erfasst und weiterverarbeitet. Dazu gehören IP-Adressen, besuchte URL, Datum und Uhrzeit, Daten zum Internet-Verkehr usw. Selbst wenn die Verkehrs- und anderen Daten über die Nutzung der elektronischen Kommunikationsmittel nicht direkt mit einem bestimmten Nutzer verknüpft sind, kann die Anonymität jederzeit aufgehoben werden, wenn die ERA beschließt, eine gründliche Untersuchung vorzunehmen, indem sie die Internet-Protokolle mit Protokollen aus anderen ERA-Systemen abgleicht. Somit sind die betroffenen Personen bestimmbar.

Im Schriftwechsel mit dem EDSB stellte die ERA klar, dass die Überwachung der Internet-Protokolle automatisiert und *„anonym“* erfolgt, da laut ERA IP-Adressen dynamisch an Clients vergeben werden und sie keine Aufzeichnungen über die Zuweisung und Vergabe der IP-Adressen (DHCP-Protokolle) führt. Daher ist es nach Aussage der ERA nicht möglich, jeden Eintrag zur Internet-Überwachung zu einem bestimmten Computer zurückzuverfolgen. Allerdings ist der EDSB der Ansicht, dass die ERA andere Protokolle (beispielsweise E-Mail-Protokolle, IAM-Protokolle usw.) verwenden könnte, um die in den Internet-Protokollen enthaltenen Informationen zu korrelieren und so die meisten individuellen Zugriffe auf das Internet zurückzuverfolgen. Die Tatsache, dass keine DHCP-Protokolle vorhanden sind, bedeutet, dass einige der Internet-Zugriffe nicht einfach zurück verfolgbar sind, doch liefern in der Praxis andere Protokolle der ERA ausreichend Informationen, um bestimmen zu können, welcher Nutzer zu welchem Zeitpunkt eine bestimmte IP-Adresse verwendet hat.

Zweitens werden, wie in der Internet-Strategie und anderen Dokumenten beschrieben, die erhobenen personenbezogenen Daten einer *„Verarbeitung mit automatisierten Verfahren“* gemäß Artikel 2 Buchstabe b der Verordnung unterzogen. Alle Daten werden mit Hilfe automatisierter Verfahren erfasst und analysiert. Eine bestimmte Teilmenge der Daten darf auch manuell vom Systemadministrator analysiert werden, wenn eine weitere Analyse erforderlich ist, beispielsweise bei mutmaßlich gefährlichem Inhalt wie Viren usw. In diesen Fällen werden die personenbezogenen Daten tatsächlich zunächst automatisch unmittelbar bei den Internet-Nutzern erfasst (automatische Registrierung der Logdateien) und dann vom IKT-Systemadministrator analysiert.

Schließlich erfolgt die Verarbeitung durch ein Organ/eine Agentur/eine Einrichtung der EU, in diesem Fall durch die ERA, im Rahmen des EU-Rechts (Artikel 3 Absatz 1 der Verordnung). Somit liegen alle Elemente vor, die die Anwendung der Verordnung auslösen.

3.1.2. Gründe für die Vorabkontrolle

In Artikel 27 Absatz 1 der Verordnung ist festgelegt, dass *„Verarbeitungen, die aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können“*, vom EDSB vorab kontrolliert werden. Die Verarbeitung von Daten in Verbindung mit Kommunikationsnetzen weist spezielle

Aspekte hinsichtlich des Datenschutzes auf, weshalb zu diesen Aspekten ein eigenes Kapitel (Kapitel IV) verfasst wurde. So ist insbesondere in Artikel 36 der Grundsatz der Vertraulichkeit des Kommunikationsverkehrs festgelegt und enthält Artikel 37 Bestimmungen zu Verkehrsdaten.

Diese besondere Betrachtung dieser Daten ist als besonderes Risiko im Sinne von Artikel 27 Absatz 1 anzusehen.

Artikel 27 Absatz 2 der Verordnung enthält eine Liste der Verarbeitungen, die solche Risiken beinhalten können. Diese Liste umfasst unter Buchstabe a „*Verarbeitungen von Daten über Gesundheit und Verarbeitungen von Daten, die Verdächtigungen, Straftaten … betreffen*“ und unter Buchstabe b „*Verarbeitungen, die dazu bestimmt sind, die Persönlichkeit der betroffenen Person zu bewerten, einschließlich ihrer Kompetenz, ihrer Leistung oder ihres Verhaltens*“.

Bei der allgemeinen Überwachung werden die betroffenen Personen nicht direkt bestimmt, jedoch kann, in einer zweiten Phase, die individuelle Überwachung (siehe schrittweiser Ansatz, Punkt 3.2.2.) der Internet-Nutzung, wie in den Strategiedokumenten beschrieben, zu einer Bewertung des Benutzerverhaltens führen (um zu bewerten, ob die Nutzung des Internets in Übereinstimmung mit der Internet-Strategie erfolgt), und eine solche Überwachung kann die Erfassung von Daten bezüglich eines Verdachts auf Straftaten (bei Verdacht auf ungesetzliches Verhalten) sowie von anderen Arten sensibler Daten mit sich bringen. Grundsätzlich müssen solche Überwachungen und damit verbundene Datenverarbeitungen gemäß Artikel 27 Buchstabe a und b der Verordnung einer Vorabkontrolle unterzogen werden.

Eine Vorabkontrolle gemäß Artikel 27 der Verordnung sollte grundsätzlich vor Aufnahme der Verarbeitung durchgeführt werden. Der EDSB bedauert daher sehr, dass in diesem Fall die Meldung nicht vor Aufnahme der Verarbeitung bei ihm eingereicht wurde.

3.1.3. Meldung und Frist für die Stellungnahme des EDSB

Die Meldung ging am 10. Februar 2012 ein. Die Frist, innerhalb deren der EDSB gemäß Artikel 27 Absatz 4 der Verordnung eine Stellungnahme abzugeben hat, wurde für 180 Tage ausgesetzt, um einige ergänzende Informationen einzuholen.

Darüber hinaus verlängerte der EDSB in Übereinstimmung mit Artikel 27 Absatz 4 am 10. Mai 2012 angesichts der Komplexität und des sensiblen Charakters der Angelegenheit und der parallel verlaufenden Ausarbeitung der horizontalen Leitlinien zum Thema elektronische Überwachung durch den EDSB die Frist um weitere zwei Monate.

Die Stellungnahme muss daher spätestens am 10. Dezember 2012 angenommen werden.

3.2. Rechtmäßigkeit der Verarbeitung

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dafür rechtliche Gründe gemäß Artikel 5 der Verordnung vorliegen. Gemäß Artikel 5 Buchstabe a dürfen personenbezogene Daten nur verarbeitet werden, wenn die Verarbeitung *„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 (…)*“.

Bei der Prüfung der Frage, ob Verarbeitungen im Einklang mit Artikel 5 Buchstabe a der Verordnung stehen, sind zwei Elemente zu berücksichtigen: Erstens, ob entweder im Vertrag oder in anderen Rechtsakten die Wahrnehmung einer Aufgabe im öffentlichen Interesse vorgesehen ist, aufgrund deren die Datenverarbeitung stattfindet (*Rechtsgrundlage*), und

zweitens, ob die Verarbeitungen für die Wahrnehmung dieser Aufgabe, also das Erreichen der angestrebten Ziele, tatsächlich erforderlich sind (*Notwendigkeit*).

3.2.1. Rechtsgrundlage

Erstens hält der EDSB fest, dass schon die Verordnung verschiedene Bestimmungen enthält, die für die Bewertung der Rechtmäßigkeit der Überwachung der Internetnutzung durch die ERA erheblich sind. So heißt es insbesondere in Erwägungsgrund 30 der Verordnung: *„Die Überwachung von Computernetzen, die unter Kontrolle eines Organs oder einer Einrichtung der Gemeinschaft betrieben werden, kann zur Verhinderung unbefugter Benutzung erforderlich sein"*. Wie oben dargelegt, besteht einer der von der ERA verfolgten Zwecke bei der Internet-Überwachung darin, zu verhindern, dass diese Instrumente entgegen dem Gesetz, den Strategien der ERA oder in einer anderweitig unzulässigen Weise verwendet werden.

Darüber hinaus legt Artikel 35 der Verordnung fest: *„Die Organe und Einrichtungen der Gemeinschaft treffen geeignete technische und organisatorische Maßnahmen, um die sichere Nutzung der Telekommunikationsnetze und Endgeräte … zu garantieren*". Dies rechtfertigt die Verarbeitung von Telekommunikationsdaten, die für die Gewährleistung der Sicherheit des Telekommunikationssystems erforderlich ist.

Artikel 37 Absatz 2 der Verordnung bietet eine weitere Rechtsgrundlage, die es der ERA gestattet, rechtmäßig eine ganz spezielle Datenverarbeitungstätigkeit vorzunehmen, d. h. die Speicherung von Verkehrsdaten, in diesem Fall von Logdateien. Artikel 37 Absatz 2 legt insbesondere fest, dass Verkehrsdaten für die Verwaltung des Telekommunikationshaushalts und des Datenverkehrs einschließlich der Kontrolle der rechtmäßigen Nutzung des Telekommunikationssystems verarbeitet werden können. Der Begriff der *„Kontrolle der rechtmäßigen Nutzung*" ist hier ganz wichtig, denn er betrifft die mögliche Nutzung der Verkehrsdaten über die Verwaltung des Datenverkehrs und des Telekommunikationshaushalts hinaus. So dürfen Verkehrsdaten insbesondere dafür verwendet werden, die Sicherheit des Systems/der Daten und die Einhaltung des Statuts oder anderer Bestimmungen wie der Internet-Strategie zu gewährleisten.

Zweitens weist der EDSB darauf hin, dass die ERA als Arbeitgeber bestimmte im Arbeitsrecht geregelte Pflichten hat, die als angemessene Rechtsgrundlage angesehen werden können, die eine verhältnismäßige Verarbeitung rechtfertigen könnte. So kann auch die Verpflichtung der ERA, sich vor einer Haftung aufgrund von Aktionen durch Mitarbeiter zu schützen, die Verarbeitung rechtfertigen. Dies kann unter bestimmten Umständen die Verarbeitung sensibler Daten umfassen (siehe Punkt 3.3).

Schließlich hält der EDSB fest, dass die von der ERA herausgegebenen Strategiedokumente ein weiteres Element darstellen, mit dem sich bestimmen lässt, ob eine Rechtsgrundlage im Sinne von Artikel 5 Buchstabe a der Verordnung vorliegt, denn sie legen Regeln für die Überwachung elektronischer Ressourcen fest, und zwar u. a. für die Gewährleistung der Sicherheit und die Überprüfung der rechtmäßigen Nutzung.

3.2.2. Notwendigkeit

Wie bereits dargelegt, besteht einer der für diese Verarbeitung angegebenen Hauptzwecke darin, zu überprüfen, ob die Nutzer bei der ERA die IKT-Dienste gemäß der zulässigen Nutzung einsetzen, wie sie in den internen Strategiedokumenten der ERA angegeben ist. Der EDSB nimmt zur Kenntnis, dass die ERA eine gewisse Überwachung der Nutzung ihrer IKT-Dienste einschließlich der Internet-Systeme für erforderlich hält, um in der Lage zu sein, Verstöße gegen ihre Strategien oder Sicherheitsverstöße zu verhindern oder aufzudecken. Man

kann daher davon ausgehen, dass eine selektive und verhältnismäßige Registrierung von Logdateien sowie ihre Analyse zumindest in gewissem Maß als erforderlich angesehen werden können, um die Aufgabe zu erfüllen, eine Nutzung in Übereinstimmung mit der Internet-Strategie sicherzustellen und somit insgesamt die Sicherheit der IKT-Ressourcen der ERA zu gewährleisten.

Eine gewisse Überwachung wird auch als notwendig erachtet, damit der Arbeitgeber – in diesem Fall die ERA - seinen arbeitsrechtlichen Pflichten und Verpflichtungen nachkommen kann. Die ERA erklärt beispielsweise, dass sie, wäre sie nicht in der Lage, die Internetnutzung einer Person zu überwachen, die eines Verstoßes (beispielsweise Herunterladen von Pornografie) gegen ihre Strategie verdächtigt wird, unter Umständen nicht über die für die Eröffnung eines Disziplinarverfahrens erforderlichen Beweise verfügen würde.

In Anbetracht der obigen Ausführungen nimmt der EDSB zur Kenntnis, dass die gemeldete Überwachung der IKT-Nutzung als für die Erfüllung der beabsichtigten Zwecke der Strategie erforderlich angesehen wird. Der EDSB ist daher der Auffassung, dass die Anforderungen für die Einhaltung von Artikel 5 Buchstabe a der Verordnung grundsätzlich erfüllt sind.

Es sei jedoch darauf hingewiesen, dass eine pauschale oder sehr gründliche Überwachung der Nutzung des Internets durch jede einzelne Person nicht gerechtfertigt ist. Für Fälle, in denen der IT-Sicherheitsbeauftragte einen begründeten Verdacht hat, dass eine Person Missbrauch betreibt, empfiehlt der EDSB die Umsetzung einer Strategie, die in Anbetracht der Umstände in einer *schrittweisen* Verschärfung der Überwachung besteht. Dies stellt sicher, dass es nicht zu einer übertriebenen Überwachung kommt, da nur die Daten verarbeitet würden, die für die beabsichtigten Zwecke erforderlich wären. Wenn das Internet-Protokoll auf einen potenziellen Missbrauch der Internet-Dienste der ERA hinweist, könnte ein erster Schritt darin bestehen, die Mitarbeiter an die eingeführten Regelungen und die Möglichkeit einer Verwaltungsmaßnahme zu erinnern; wenn das Internet-Protokoll einen fortgesetzten Missbrauch derselben Art zeigt, kann die ERA eine Verwaltungsuntersuchung sowie eine selektive Überwachung einleiten, die einer ordnungsgemäß dokumentierten Methodik folgt (siehe auch Punkt 3.4). Somit sollte eine individuelle Überwachung der Internet-Nutzung nur bei einem angemessenen, durch erste Beweise erhärteten Verdacht und im Rahmen einer Verwaltungsuntersuchung stattfinden. Die Anonymität des mutmaßlichen Verdächtigen darf erst aufgehoben werden, wenn seine Vorgesetzten die Einleitung einer Verwaltungsuntersuchung beschlossen haben.

Diesbezüglich ist ein klares Verfahren mit einem solchen schrittweisen Ansatz einzurichten. Bei Auftreten eines Verdachts kann der IT-Manager beispielsweise beschließen, dass dieser dem zuständigen Vorgesetzten (z. B. dem Leiter des Bereichs Humanressourcen) gemeldet wird. Dieser kann dann weitere Untersuchungsmaßnahmen beschließen; so kann er z. B. darüber entscheiden, ob die Anonymität im Rahmen einer Verwaltungsuntersuchung aufgehoben wird oder nicht[7].

Der EDSB erinnert daran, dass die Durchführung einer Verwaltungsuntersuchung in den Bereich einer allgemeinen Verarbeitung fällt, nämlich Verwaltungsuntersuchungen und Disziplinarmaßnahmen[8]. Diese Verarbeitung muss zuvor einer eigenen Vorabkontrolle durch den EDSB unterzogen werden, da mit ihr das Verhalten der betroffenen Person bewertet werden soll (Artikel 27 Absatz 2 Buchstabe b) und sie die Verarbeitung von Daten in Verbindung mit Verdächtigungen (Artikel 27 Absatz 2 Buchstabe a) umfasst. Daher sollte die ERA bei der Überwachung der Internet-Nutzung stets Notwendigkeit und Verhältnismäßigkeit im Einklang mit dem Grundsatz der Datenqualität beachten.

---

[7] Siehe beispielsweise Stellungnahme des EDSB vom 10. November 2008 – Internet-Überwachung durch den Rechnungshof (Fall 2008-284), abrufbar auf der EDSB-Website.

[8] Siehe EDSB-Leitlinien: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-04-23_Guidelines_inquiries_DE.pdf

3.2.3. Logdateien fehlgeschlagener Zugangsversuche zum Netz

Die Internet-Strategie der ERA sieht vor, dass die Logdateien fehlgeschlagener Zugangsversuche zum Netz „*nicht verwendet werden, um das Verhalten Einzelner zu überwachen; ausgenommen hiervon sind die Fälle gemäß Artikel 20 der Datenschutzverordnung*". Artikel 20 der Verordnung erlaubt Ausnahmen und Einschränkungen, u. a. zum Grundsatz der Datenqualität (Artikel 4 der Verordnung), wenn derartige Ausnahmen und Einschränkungen notwendig sind, um u. a. strafrechtliche Ermittlungen oder Kontroll-, Überwachungs- und Ordnungsaufgaben durchzuführen, selbst wenn diese nur zeitweise mit der Ausübung öffentlicher Gewalt verbunden sind.

Wie schon in einer früheren Stellungnahme[9] unterstrichen, ist der EDSB der Auffassung, dass Filtertechnologien eher der Prävention des Missbrauchs des Internets als der Aufdeckung oder Sanktionierung dienen. Wird der Zugang zu einer verbotenen Website gesperrt, würde nach Auffassung des EDSB die Überwachung und Bestrafung allein des Versuchs, auf diese Website zuzugreifen, über das hinausgehen, was für den angestrebten Zweck erforderlich ist. Ist es dem einzelnen Nutzer nicht gelungen, Zugang zu einer bestimmten gesperrten Website zu bekommen und ihren Inhalt anzusehen, besteht auch kein berechtigter Grund für eine Verarbeitung eines solchen Fehlversuchs.

Im Verlauf des Verfahrens erklärte die ERA, dass Zugangsversuche zu gesperrten Websites nicht zu Bestrafungs-/Überwachungszwecken protokolliert werden. Alleiniger Zweck ist nämlich die Bewertung der Genauigkeit der Filter (d. h., wenn keine Protokolle gesperrter Zugänge nach Kategorie aufbewahrt werden, kann nicht festgestellt werden, ob der Filter funktioniert oder nicht) sowie die Gewährung des Zugangs zu falsch eingestuften Seiten, die fälschlicherweise gesperrt sind.

Sofern dies die einzigen Zwecke sind, würde der EDSB empfehlen, aus der Internet-Strategie die Ausnahme bezüglich der Überwachung fehlgeschlagener Versuche in den in Artikel 20 Absatz 1 der Verordnung angegebenen Fällen zu streichen.

3.3. Verarbeitung besonderer Datenkategorien

Bei der Überwachung der Internet-Nutzung können „sensible" personenbezogene Daten enthüllt werden. Dabei handelt es sich gemäß Verordnung um personenbezogene Daten, „*aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen*", sowie um „*Daten über Gesundheit oder Sexualleben*" (Artikel 10). So kann beispielsweise in Zugangsprotokollen die Mitgliedschaft in einer Gewerkschaft enthüllt werden, wenn dort deutlich wird, dass sich ein Beamter routinemäßig in die Website einer bestimmten Gewerkschaft einloggt. Die Verarbeitung sensibler Daten ist im Prinzip untersagt, sofern nicht eine der Ausnahmen aus Artikel 10 der Verordnung gilt.

Artikel 10 Absatz 2 Buchstabe b besagt, dass die Untersagung aufgehoben werden kann, wenn die Verarbeitung „*erforderlich ist, um den spezifischen Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund der Verträge oder anderer aufgrund der Verträge erlassenen Rechtsakte zulässig ist*". Eine gewisse Überwachung der Internet-Nutzung mag für die ERA erforderlich scheinen, um die Sicherheit von System/Daten sowie die Einhaltung des Statuts und anderer Vorschriften

[9] Siehe Stellungnahme 2008-284, S. 8f.

sicherzustellen. Dazu gehört eine Erfüllung der im Arbeitsrecht geregelten Pflichten und Verpflichtungen, beispielsweise das Recht der ERA, das Anschauen sexuell anstößiger Informationen am Arbeitsplatz zu verhindern, was wiederum die Verarbeitung sensibler Daten wie der aufgesuchten URL rechtfertigen würde, die ans Tageslicht bringen könnte, dass ein Beschäftigter derartigen Tätigkeiten nachgeht. In manchen Fällen kann eine Überwachung sensibler Daten auch gerechtfertigt sein, um den Arbeitgeber in die Lage zu versetzen, seine Rechte als Arbeitgeber auszuüben, wie das Recht auf Einleitung von Disziplinarverfahren einschließlich der Entlassung von Beschäftigten, die ungesetzlichen Aktivitäten nachgehen.

3.4. Datenqualität

3.4.1. Entsprechung, Erheblichkeit und Verhältnismäßigkeit

Gemäß Artikel 4 Absatz 1 Buchstabe c der Verordnung (EG) Nr. 45/2001 dürfen personenbezogene Daten nur den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, müssen dafür erheblich sein und dürfen nicht darüber hinausgehen. Dies wird als Grundsatz der Datenqualität bezeichnet.

Als Zweck der Internet-Überwachung wird angegeben, dass damit sichergestellt werden soll, dass die Internet-Systeme und –Dienste der Agentur für Zwecke eingesetzt werden, die dem Aufgabenbereich der Agentur entsprechen (Überprüfung der rechtmäßigen Nutzung), und dass Störungen und Missbrauch der Internet-Systeme verhindert werden (Überwachung der Sicherheit). Wie bereits dargelegt, ist der EDSB der Auffassung, dass eine gewisse Überwachung der Internet-Nutzung für das Erreichen dieser Ziele erforderlich ist. Allerdings darf die Verarbeitung personenbezogener Daten in diesem Zusammenhang nicht überzogen, sondern muss in Bezug auf die verfolgten Ziele angemessen und verhältnismäßig sein.

Bei der Beurteilung der Verhältnismäßigkeit sollte dem besonderen Charakter der verarbeiteten Daten im Zusammenhang mit der Internet-Überwachung Rechnung getragen werden. Logdateien zeichnen sehr detailliert die Internet-Nutzung der einzelnen Nutzer auf, darunter die aufgesuchten Websites, die Anzahl der Aufrufe, die Verbindungsdauer, die Verweilzeit auf den einzelnen Websites usw. Daher ist von einem Organ/einer Agentur/einer Einrichtung der EU bei der Konzeption der Internet-Strategien und bei deren Umsetzung in die Praxis ein besonders umsichtiges Vorgehen gefordert.

Diesbezüglich sollte ein klares Verfahren für die Einführung des unter Punkt 3.2.2 erläuterten schrittweisen Ansatzes eingerichtet werden.

3.4.2. Verarbeitung nach Treu und Glauben und auf rechtmäßige Weise

Gemäß Artikel 4 Absatz 1 Buchstabe a der Verordnung dürfen personenbezogene Daten nur nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden. Der Aspekt der Rechtmäßigkeit wurde bereits oben behandelt (siehe Punkt 3.2). Der Aspekt der Verarbeitung nach Treu und Glauben hängt eng mit den Informationen zusammen, die den betroffenen Personen zur Verfügung gestellt werden; auf ihn wird in Punkt 3.8. näher eingegangen.

3.4.3. Sachliche Richtigkeit

Nach Artikel 4 Absatz 1 Buchstabe d der Verordnung müssen personenbezogene Daten „*sachlich richtig sein und, wenn nötig, auf den neuesten Stand gebracht werden*“, und es „*sind*

alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, unrichtige oder unvollständige Daten berichtigt oder gelöscht werden". Im vorliegenden Fall umfassen die Daten im Wesentlichen Logdateien. Die ERA muss alle angemessenen Maßnahmen ergreifen, um sicherzustellen, dass die Daten auf dem neuesten Stand und erheblich sind. Siehe hierzu auch Punkt 3.8.

3.5. Datenaufbewahrung

Gemäß Artikel 4 Absatz 1 Buchstabe e der Verordnung dürfen personenbezogene Daten 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.

Laut der Meldung und der Internet-Strategie werden Logdateien nach ihrer Aufzeichnung für eine Dauer von 90 Tagen aufbewahrt. Diese zeitliche Regelung entspricht Artikel 37 der Verordnung, der spezielle Maßnahmen bezüglich der Aufbewahrung von Daten für die Verkehrsabwicklung und Gebührenabrechnung vorschreibt, und Logdateien fallen unter diese Definition. Artikel 37 Absatz 2 der Verordnung (EG) Nr. 45/2001 besagt, dass Verkehrsdaten für die Verwaltung des Telekommunikationshaushalts und des Datenverkehrs einschließlich der Kontrolle der rechtmäßigen Nutzung des Telekommunikationssystems verarbeitet werden können. Allerdings sind sie so schnell wie möglich zu löschen oder zu anonymisieren und dürfen in keinem Fall länger als sechs Monate nach ihrer Erfassung aufbewahrt werden, es sei denn, ihre weitere Aufbewahrung ist für die Feststellung, Ausübung oder Verteidigung eines Rechtsanspruchs im Rahmen eines anhängigen gerichtlichen Verfahrens erforderlich.

Veranlasst die Überwachung der Logdateien oder der Verkehrsdaten die ERA zu dem Verdacht, dass eine Person gegen die Internet-Strategie verstoßen hat, ist es der ERA gestattet, die belastenden Logdateien aufzubewahren. In diesem Zusammenhang ist Artikel 20 der Verordnung insofern relevant, als er mögliche Einschränkungen des Grundsatzes der sofortigen Löschung der Daten gemäß Artikel 37 Absatz 1 vorsieht, und zwar insbesondere, wenn eine solche Einschränkung zur „*Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten*" notwendig ist. Der EDSB hat diese Bestimmung so ausgelegt, dass sie nicht nur strafrechtliche Ermittlungen, sondern auch Disziplinarverfahren abdeckt[10].

Somit dürfen Logdateien gegebenenfalls im Rahmen einer Verwaltungsuntersuchung verarbeitet werden, und zwar unabhängig davon, ob ein strafrechtliches oder ein disziplinarisches Vergehen vorliegt. Es sei darauf hingewiesen, dass eine solche Maßnahme nur fallweise ergriffen werden darf, wenn der berechtigte Verdacht besteht, dass eine Person gegen die ISP oder das Statut verstoßen und die ERA eine Verwaltungsuntersuchung eingeleitet hat. Nach Ablauf der ersten sechs Monate ist zu beurteilen, ob die erfassten Daten und die durchgeführte Überprüfung eine Fortführung der Untersuchung oder die Einleitung eines Disziplinarverfahrens rechtfertigen. Nur wenn eine solche Beurteilung zu einem positiven Ergebnis führt, dürfen Verkehrsdaten länger als sechs Monate aufbewahrt werden.

3.6. Datenübermittlungen

In Artikel 7, 8 und 9 der Verordnung sind bestimmte Pflichten geregelt, die Anwendung finden, wenn die für die Verarbeitung Verantwortlichen personenbezogene Daten an Dritte

[10] Siehe beispielsweise Stellungnahme des EDSB vom 22. Dezember 2005 – Interne Verwaltungsuntersuchungen bei der Europäischen Zentralbank (Fall 2005-0290).

übermitteln. Für Übermittlungen an i) Organe/Agenturen/Einrichtungen der EU (Artikel 7), ii) Empfänger, die der Richtlinie 95/46/EG unterworfen sind (Artikel 8), oder iii) sonstige Empfänger (Artikel 9) gelten unterschiedliche Vorschriften.

Der EDSB weist nachdrücklich darauf hin, dass gemäß Artikel 7 der Verordnung personenbezogene Daten übermittelt werden dürfen, „*wenn die Daten für die rechtmäßige Erfüllung der Aufgaben erforderlich sind, die in den Zuständigkeitsbereich des Empfängers fallen*". Zur Einhaltung dieser Vorschrift hat der für die Verarbeitung Verantwortliche bei der Übermittlung personenbezogener Daten zu gewährleisten, dass *i)* der Empfänger die entsprechende Zuständigkeit hat und *ii)* die Übermittlung erforderlich ist.

Im vorliegenden Fall scheinen der ITFM-Leiter, der Systemadministrator und der IKT-Sicherheitsbeauftragte die Personen zu sein, die für die interne Verwaltung der Überwachung der Internet-Nutzung verantwortlich sind. Auf der anderen Seite ist der Leiter der Verwaltung der Verantwortliche für die Verarbeitungen im Zusammenhang mit Verwaltungsuntersuchungen und Disziplinarmaßnahmen. Die ERA muss daher der Frage nachgehen, ob Übermittlungen vom IKT-Sicherheitsbeauftragten, Systemadministrator und ITFM-Leiter an die im Sachverhalt beschriebene Liste von Empfängern im Einklang mit Artikel 7 stehen. Die Notwendigkeit derartiger Übermittlungen muss angesichts des oben erläuterten schrittweisen Ansatzes untersucht werden.

Der EDSB empfiehlt der ERA, die Empfängerliste unter Berücksichtigung der vorstehenden Ausführungen zu überarbeiten und fallweise zu bewerten, ob die Bedingungen von Artikel 7 erfüllt sind. Gemäß Artikel 7 dürften insbesondere nur die Personen zuständig sein, die darüber zu entscheiden haben, ob eine Verwaltungsuntersuchung einzuleiten und die Anonymität der Daten aufzuheben ist.

Zu einem späteren Zeitpunkt dürfen die Daten unter besonderen Umständen vorübergehend an die nachstehend genannten Empfängerkategorien innerhalb der Organe/Agenturen/Einrichtungen der EU weitergeleitet werden:

- an OLAF und/oder IDOC (Untersuchungs- und Disziplinaramt) im Rahmen ihrer Untersuchungen,
- an den Bürgerbeauftragten auf dessen Antrag,
- an den Europäischen Datenschutzbeauftragten auf dessen Antrag,
- auf Antrag an die Richter des Europäischen Gerichtshofs.

Nach Auffassung des EDSB werden die Übermittlungen von Informationen an OLAF und/oder IDOC, den Europäischen Gerichtshof, den Bürgerbeauftragten oder den EDSB zur Erfüllung ihrer offiziellen Aufgaben diesen Anforderungen gerecht. Die Empfänger sind grundsätzlich für die Erfüllung der Aufgabe zuständig, für die die Daten übermittelt werden. Die Beurteilung der Notwendigkeit ist fallweise von dem für die Verarbeitung Verantwortlichen vorzunehmen.

Die Übermittlung von Daten an die Staatsanwaltschaft wird im Rahmen der Stellungnahme zur Vorabkontrolle zu Verwaltungsuntersuchungen und Disziplinarverfahren behandelt. Eine derartige Übermittlung erfolgt nämlich nur, wenn die Verwaltungsuntersuchung zu dem Schluss kommt, dass ein Mitarbeiter eventuell eine Straftat begangen hat.

Laut Meldung sind keine Übermittlungen in Drittländer oder an internationale Organisationen vorgesehen.

3.7. Auskunfts- und Berichtigungsrecht

Gemäß Artikel 13 der Verordnung hat die betroffene Person das Recht, jederzeit frei und ungehindert innerhalb von drei Monaten nach Eingang eines entsprechenden Antrags von dem

für die Verarbeitung Verantwortlichen eine Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten zu erhalten.

Der EDSB erinnert daran, dass das Recht auf Auskunft verbindlich ist, sofern keine Ausnahme zum Tragen kommt, und dass die ERA die Verfahren einzurichten hat, die eine Ausübung dieses Rechts ermöglichen. Das Recht auf Auskunft impliziert u. a. das Recht auf Information und den Erhalt einer verständlichen Kopie der Daten, die zu einer Person verarbeitet werden. Im vorliegenden Fall wird die Anonymität der betroffenen Person nur aufgehoben, wenn die ERA auf der Grundlage der durch die Überwachung der Internet-Nutzung erhobenen Daten beschließt, eine Verwaltungsuntersuchung einzuleiten. Daher kann in der Praxis das Auskunfts- und Berichtigungsrecht nicht vor der Einleitung einer Verwaltungsuntersuchung ausgeübt werden.

3.8. Informationspflicht gegenüber der betroffenen Person

Gemäß Artikel 11 und 12 der Verordnung sind die für die Erhebung personenbezogener Daten Verantwortlichen 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 ihre Rechte als betroffene Personen unterrichtet zu werden.

Um die Einhaltung der Artikel 11 und 12 zu gewährleisten, hat die ERA folgende Schritte unternommen:

- IKT-Nutzer wurden offiziell durch eine Mitteilung an die Belegschaft zum „Use of ERA's ICT owned resources" (Nutzung der ERA-eigenen IKT-Ressourcen) informiert;
- darüber hinaus muss jeder Nutzer binnen 30 Tagen nach dem Inkrafttreten der ICT das „ERA User acknowledgement Form" (ERA-Benutzervereinbarungsformular) („Formular") unterzeichnen. Neue Nutzer müssen das Formular ebenfalls unterzeichnen, bevor sie Zugang zu den IKT-Ressourcen der ERA erhalten. Das Formular enthält eine Bestätigung, dass der Nutzer die ICT gelesen und verstanden hat und ihr zustimmt;
- alle Strategiedokumente stehen auf der ITFM-Intranet-Seite unter dem Punkt „DRAFT Policies–ERA Consultation" zur Verfügung;
- in den kommenden Monaten wird vom IT-Sicherheitsbeauftragten ein spezielles Programm zur Bewusstseinsschaffung durchgeführt, das Teil des Programms zur Sicherheit elektronischer Informationen ist;
- schließlich werden Nutzer, die versucht haben, auf eine gesperrte Website zuzugreifen, über die Zugangsverweigerung informiert und über die Gründe für die Verweigerung in Kenntnis gesetzt (die Website gehört zu einer unerwünschten Kategorie, ferner wird der Name der Kategorie angegeben). Die Nachricht nennt die Gründe, aus denen der Zugang verweigert wurde.

Wurde der unter Punkt 3.4 beschriebene schrittweise Ansatz durchgeführt und deuten die Internet-Protokolle auf einen möglichen Missbrauch der Internet-Dienste der ERA hin, muss die ERA die Nutzer über die in der Internet-Strategie festgelegten Regeln und die Möglichkeit der Agentur, eine Verwaltungsuntersuchung einzuleiten, informieren.

3.8.1. Informationskanäle

Nach Auffassung des EDSB muss die ERA unbedingt dafür sorgen, dass die für die

Information über die Überwachung gewählten Kanäle den Personen die Möglichkeit geben, den Inhalt wirksam zur Kenntnis zu nehmen. Nach Ansicht des EDSB sind die beiden folgenden Aspekte zu berücksichtigen:

Erstens: Im Sinne einer wirksamen Information sowie der Fairness gegenüber den betroffenen Personen müssen die Nutzer eine direkte Mitteilung über die Verarbeitung ihrer personenbezogenen Daten erhalten. Da der Großteil der Informationen in den Strategiedokumenten enthalten ist, dürfte deren Veröffentlichung im Intranet nicht ausreichen, da nicht alle Nutzer diese von sich aus lesen. Solange dies noch nicht erfolgt ist, fordert der EDSB die ERA daher dringend auf, eine individualisierte Mitteilung an alle Mitarbeiter zu senden, z. B. eine E-Mail-Nachricht mit einem Link zur einschlägigen Datenschutzerklärung und dem entsprechenden Strategiedokument.

Zweitens sind die Informationen auf viele Dokumente verstreut; der Nutzer muss, um Zugang zu den gesetzlich vorgeschriebenen Informationen zu erhalten, mindestens fünf separate Dokumente lesen, nämlich den Vermerk für die Mitarbeiter, die Datenschutzerklärung, die Internet-Strategie sowie ICT und ECP. In manchen Fällen wird der Zusammenhang zwischen den einzelnen Dokumenten nicht recht deutlich.

Nach Ansicht des EDSB sollten die sachdienlichen Informationen einschließlich der in Artikel 11 und 12 der Verordnung (EG) Nr. 45/2001 geforderten Angaben in einem einzigen Dokument (und nicht in verschiedenen Dokumenten) bereitgestellt werden. Um jegliche Verwirrung zu vermeiden und um die Strategie verständlicher zu gestalten, schlägt der EDSB vor, alle Informationen zur Überwachung der Internet-Nutzung in einem einzigen, alle erforderlichen Informationen enthaltenden Dokument zu vereinen (siehe dazu auch Punkt 3.8.2). Dieses Dokument kann mit einer Datenschutzerklärung kombiniert werden, die deutlich darauf verweist.

3.8.2. Inhalt der Strategie

Vorrangiges Ziel der IKT-Strategien ist es, die Nutzer über die zulässige und verbotene Nutzung der IKT zu informieren, die Art der Überwachung der Nutzung darzulegen und die Folgen einer Zweckentfremdung oder eines Missbrauchs aufzuzeigen. Zur Internet-Strategie der ERA merkt der EDSB im Wesentlichen Folgendes an:

- Sowohl ICT als auch die Internet-Strategie besagen, dass die IKT der ERA zu offiziellen Geschäftszwecken zu nutzen ist und dass nur eine begrenzte private Nutzung zulässig ist, sofern diese nicht den Interessen der ERA abträglich ist. Der Begriff der „begrenzten privaten Nutzung“ wird nicht weiter erläutert.
- Die Zwecke für die Einleitung einer Internet-Überwachung scheinen nicht immer deutlich dargelegt. Die Strategie besagt insbesondere ganz klar, dass die Überwachung der Log-Aufzeichnungen durchgeführt werden kann, um die Funktionsfähigkeit und Sicherheit der Systeme zu gewährleisten; hinsichtlich der Überprüfung der Rechtmäßigkeit der Nutzung scheint dies jedoch nicht klar zu sein. Sollte die Überwachung auch auf die Überprüfung der rechtmäßigen Nutzung abzielen, empfiehlt der EDSB, dies explizit zum Ausdruck zu bringen.
- Das Dokument legt keine klare Methodik für die Internet-Überwachung fest. Dies spiegelt die Tatsache wider, dass eine solche Methodik noch nicht entwickelt wurde (siehe weiter oben Punkt 3.4.1.), und zwar im Wesentlichen deshalb, weil die Internet-Überwachung hauptsächlich anonym erfolgt.
- Laut Internet-Strategie fällt das World Wide Web klar in den Geltungsbereich der Strategie, andere Protokolle (wie Instant Messaging, FTP usw.) erwähnt sie hingegen nicht. Der EDSB empfiehlt, deutlich zu machen, dass die Strategie alle Internet-Protokolle umfasst.

Bezüglich der Datenschutzerklärung weist der EDSB darauf hin, dass sie nicht alle in Artikel 11 und 12 geforderten Angaben enthält. So fehlen insbesondere ausreichende Informationen zum (i) Zweck der Verarbeitung, (ii) zu den Empfängern, (iii) zu den Datenkategorien und (iv) zum Bestehen des Auskunftsrechts. Die zusätzlichen Informationen, die angesichts der besonderen Umstände eine Verarbeitung nach Treu und Glauben als erforderlich gelten könnten (z. B. Rechtsgrundlage, Aufbewahrungsfrist, das Recht, sich an den EDSB zu wenden, usw.), fehlen ebenfalls.

Daher fordert der EDSB die ERA auf, diese Mängel zu beheben, damit die Datenschutzerklärung die Anforderungen in Artikel 12 der Verordnung erfüllt.

3.9. Sicherheitsmaßnahmen

Gemäß Artikel 22 und 23 der Verordnung haben der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu treffen, damit ein Schutzniveau gewährleistet ist, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Diese Maßnahmen müssen insbesondere einer unbefugten Weitergabe, einem unbefugten Zugriff sowie einer zufälligen oder unrechtmäßigen Vernichtung, einem zufälligen Verlust oder einer Veränderung sowie jeder anderen Form der unrechtmäßigen Verarbeitung personenbezogener Daten vorbeugen.

Die ERA bestätigte, dass sie die in Artikel 22 der Verordnung geforderten Sicherheitsmaßnahmen ergriffen hat und diese im EISP-Dokument detailliert geschildert werden. Für den EDSB besteht kein Grund zu der Annahme, dass diese technischen und organisatorischen Maßnahmen nicht angemessen sind, um ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.

Allerdings ist der EDSB der Ansicht, dass die Sicherheitsmaßnahmen eventuell zu verstärken sind, da diese Protokolle nicht nur zu reinen Sicherheitszwecken, sondern auch für die Bewertung von Verhalten verwendet werden. Der EDSB empfiehlt insbesondere folgende Maßnahmen:

1. eine regelmäßige Überprüfung der in der EISP beschriebenen Risikobewertungen (dies könnte im Rahmen des in dieser Strategie ebenfalls dargestellten Informationssicherheitsplans erfolgen);
2. sicherstellen, dass die Internet-Protokolle gegen unbefugten Zugriff, Änderung oder Löschung auch durch den IKT-Sicherheitsbeauftragten und den IT-Systemadministratoren geschützt werden;
3. sicherstellen, dass jeder Zugriff auf die Internet-Protokolle zu einer bestimmten Person zurückverfolgt werden kann;
4. sicherstellen, dass alle Zugriffe auf die Internet-Protokolle gerechtfertigt sind und einem ordnungsgemäß dokumentierten Verfahren folgen;
5. Zuständigkeiten für den Umgang mit Sicherheitszwischenfällen, interne Ermittlungen und Untersuchungen sind klar spezifischen Funktionen zuzuweisen und haben ordnungsgemäß dokumentierte Verfahren zu befolgen.

SCHLUSSFOLGERUNGEN

Die gemeldete Verarbeitung kann nur durchgeführt werden, wenn die in dieser Stellungnahme formulierten Empfehlungen in vollem Umfang berücksichtigt werden. Damit die ERA im Einklang mit der Verordnung (EG) Nr. 45/2001 handelt, empfiehlt ihr der EDSB Folgendes:

- Streichung aus der Strategie der Ausnahme bezüglich der Überwachung fehlgeschlagener Versuche in den Fällen, die in Artikel 20 Absatz 1 der Verordnung angegeben sind;
- Umsetzung eines schrittweisen Ansatzes für die Überwachung der individuellen Internet-Nutzung gemäß Punkt 3.2.2. Insbesondere die individuelle Überwachung der Internet-Nutzung sollte nur bei Vorliegen eines begründeten, durch Beweise erhärteten Verdachts im Rahmen einer Verwaltungsuntersuchung und in den Fällen erfolgen, in denen verfügbare, weniger in die Privatsphäre eindringende Mittel bereits ausgeschöpft wurden;
- Sicherstellung, dass Datenübermittlungen nach einer konkreten Bewertung ihrer Notwendigkeit im Einklang mit Artikel 7 der Verordnung erfolgen;
- Aufbewahrung von Verkehrsdaten für einen Zeitraum von mehr als sechs Monaten nur, wenn sie zur „*Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten*“ notwendig sind (in Übereinstimmung mit Punkt 3.7);
- Überarbeitung der Liste der Empfänger gemäß Punkt 3.6. Gemäß Artikel 7 dürften insbesondere nur die Personen zuständig sein, die darüber zu entscheiden haben, ob eine Verwaltungsuntersuchung einzuleiten und die Anonymität der Daten aufzuheben ist;
- Erwägung der Zusammenfassung aller Informationen zur Überwachung der Internet-Nutzung in einem einzigen, alle erforderlichen Informationen enthaltenden Dokument;
- Zusammenführung und/oder Verdeutlichung der Internet-Strategie und der Datenschutzerklärung gemäß den Empfehlungen in Punkt 3.8.2.;
- Verstärkung der Sicherheitsmaßnahmen bezüglich der Logdateien, indem die Rückverfolgbarkeit von Verarbeitungen und die Beschränkung des Zugriffs auf Personen, die unbedingt über diese Informationen verfügen müssen, gewährleistet werden.

Brüssel, den 6. Dezember 2012

(**unterzeichnet**)

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter