Stellungnahme zur Meldung des Datenschutzbeauftragten der Europäischen Eisenbahnagentur (ERA) für eine Vorabkontrolle des E-Mail-Systems und des Back-End E-Mail-Systems der ERA

Brüssel, 6. Dezember 2012 (Fälle 2012-136 und 137)

1. VERFAHREN

Am 10. Februar 2012 erhielt der Europäische Datenschutzbeauftragte („**EDSB**“) zwei Meldungen des Datenschutzbeauftragten („**DSB**“) der Europäischen Eisenbahnagentur („**ERA**“ oder „**Agentur**“) für eine Vorabkontrolle des E-Mail-Systems und des Back-End E-Mail-Systems der ERA. Vor Einreichen der Meldungen konsultierte die ERA den EDSB zur Notwendigkeit der Vorabkontrolle gemäß Artikel 27 Absatz 3 der Verordnung (EG) Nr. 45/2001 („**Verordnung**“). Den Meldungen waren folgende Unterlagen als Entwurf 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**“).

Als Back-End-Teil des E-Mail-Systems wird der Teil bezeichnet, der die Kommunikation zwischen den E-Mail-Servern (z. B Microsoft Exchange) und der Außenwelt/internen Nutzern betrifft (im Gegensatz zum Client-End-Teil, zu dem die Software gehört, die die Nutzer für den Zugang zu ihren E-Mails verwenden, wie beispielsweise Microsoft Outlook, ein Browser für Web-E-Mail usw.). Da kein eindeutiger Unterschied zwischen den Meldungen besteht, behandelt sie der EDSB in einer einzigen Stellungnahme. Beide Meldungen werden in der vorliegenden Stellungnahme als „E-Mail-Policy“ bezeichnet.

[1] Informations- und Kommunikationstechnologie.

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 63
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: +32 (0)2 283 19 00 – Fax: +32 (0)2 283 19 50

Der EDSB forderte die ERA am 2. April, 2. Juli, 7. und 28. September sowie am 26. Oktober 2012 auf, einige ergänzende Informationen vorzulegen. Die Antworten gingen am 4. Mai, 5. und 25. September, 15. und 17. 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.

2. SACHVERHALT

Gegenstand der vorliegenden Stellungnahme für eine Vorabkontrolle sind das in der E-Mail-Policy und der ECP beschriebene E-Mail-System bzw. Back-End E-Mail-System der ERA. Das Referat Verwaltung (Administration Unit) ist der Teil der Organisation der Agentur, der mit der Verarbeitung befasst ist.

Neben den Meldungen 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 E-Mail-Policy lauten wie folgt:

- Darstellung der angemessenen und der unangemessenen Nutzung des E-Mail-Systems;
- Gewährleistung, dass die E-Mail-Systeme der Agentur für Zwecke eingesetzt werden, die dem Aufgabenbereich der Agentur entsprechen;
- Information der Mitarbeiter und Nutzer der Agentur über die Anwendbarkeit der E-Mail-Vorschriften und -Strategien der ERA;
- Vermeidung von Störungen und Missbrauch der E-Mail-Systeme und -Dienste.

2.2. Kategorien betroffener Personen

Die Meldungen erwähnen folgende Kategorien betroffener Personen:

- alle Personen, deren E-Mail-Adresse in den Zeilen „An“, „Von“, „CC“ und/oder „BCC“ in den Kopfzeilen einer E-Mail-Nachricht erscheint, sofern diese Nachrichten von den E-Mail-Servern der ERA verarbeitet wurden;
- bezüglich der Verwaltung des E-Mail-Adressbuchs alle Bediensteten von Organen/Agenturen und Einrichtungen der EU, mit denen ein Übereinkommen gemäß Artikel 7 der Verordnung (EG) Nr. 45/2001 („Datenübermittlung“) abgeschlossen und unterzeichnet wurde;
- dem Statut unterliegende Mitarbeiter der ERA, Beamte und dem Statut unterliegende Mitarbeiter anderer Organe/Agenturen/Einrichtungen der EU, abgeordnete nationale Sachverständige, Praktikanten und Unterauftragnehmer;
- EU-Bürger und Bürger von Drittländern.

[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.

2.3. Erlaubte und nicht erlaubte Nutzung

Nach Angaben der ERA dürfen E-Mail-Dienste nicht für Zwecke genutzt werden, von denen vernünftigerweise angenommen werden kann, dass sie eine übermäßige Belastung elektronischer Kommunikationsressourcen bedeuten oder einen Eingriff in die Nutzung elektronischer Ressourcen durch andere verursachen könnten. In diesem Zusammenhang dürfen E-Mail-Nutzer insbesondere Folgendes nicht tun:

- Kettenbriefe oder Gleichwertiges in andere Dienste senden oder weiterleiten;
- Spam versenden, also elektronische Kommunikationssysteme für Zwecke nutzen, die über ihre beabsichtigte Nutzung hinausgehen, um unerwünschte elektronische Nachrichten weit zu verbreiten;
- so genannte „Brief-Bomben" versenden, also extrem umfangreiche Nachrichten oder mehrfach elektronische Nachrichten an einen oder mehrere Empfänger senden und damit in die Nutzung elektronischer Kommunikationssysteme und -dienste durch die Empfänger eingreifen;
- vorsätzlich sich an Vorgehensweisen wie so genannten „Angriffen, die Dienstleistungsverhinderungen bewirken" beteiligen, die die Verfügbarkeit elektronischer Kommunikationsdienste beeinträchtigen.

Eine gelegentliche private Nutzung ist erlaubt, sofern sie i) keinen Eingriff in den Betrieb elektronischer Kommunikationsressourcen durch die Agentur bedeutet, ii) sich nicht auf das Beschäftigungsverhältnis des Nutzers oder andere Verpflichtungen seinerseits gegenüber der Agentur auswirkt oder iii) für die Agentur erhebliche Zusatzkosten mit sich bringt.

2.4. Überwachung der Nutzung

Die E-Mail-Policy besagt, dass Spam und Viren noch vor Erreichen der Nutzer herausgefiltert werden. In der ICT Policy werden die Nutzer außerdem darüber in Kenntnis gesetzt, dass die Agentur routinemäßig Nutzungsmuster der IKT-Ressourcen überwacht, und dort heißt es, dass dies zur Gewährleistung der Funktionsfähigkeit der Informationssysteme der ERA und zur Verhinderung von Sicherheitsverstößen geschieht. Laut ICT Policy wird der Inhalt von Mitteilungen nicht überwacht.

Die E-Mail-Nutzer der ERA sollen die E-Mail-Dienste nicht für die Übermittlung bestimmter Daten wie Benutzernamen, Passwörter, Sozialversicherungsnummern und Kontonummern über das Internet nutzen. Die Nutzer sollten das E-Mail-System auch nicht für die Übermittlung sensibler Daten verwenden, es sei denn, dies steht im Einklang mit den Datenschutzvorschriften der ERA.

2.5 Zugang zu E-Mails ohne Einwilligung

In Abschnitt IV des Dokuments sind die Vorschriften für Anträge auf Einsichtnahme in E-Mails ohne Einwilligung des Nutzers beschrieben. Es heißt dort, dass die ERA im Allgemeinen keine Einwilligung benötigt, um Einsicht in auf dem Computer einer Person gespeicherte Dateien zu nehmen, da diese Dateien nicht der ECP-Definition einer „Aufzeichnung elektronischer Kommunikation (Electronic Communication Record (ECR)" entsprechen. Bei der Überprüfung solcher Dateien sind die Kollegen allerdings verpflichtet, die Vertraulichkeit privater Mitteilungen zu wahren. Jegliche Überprüfung sollte auf das absolute Mindestmaß beschränkt bleiben.

Nach Auffassung der ERA ist es erforderlich, vor der Einsichtnahme in die E-Mails eines Mitarbeiters gemäß den Vorschriften in Abschnitt V der ECP den Account-Inhaber um seine Einwilligung zu bitten. Ein Zugang zu E-Mails ohne Einwilligung kann nur „*unter sehr begrenzten Umständen*" beantragt werden, wie sie in der ECP und der E-Mail-Policy (Abschnitt IV.B) aufgeführt sind:

- Der Bedienstete ist nicht mehr bei der ERA tätig oder ist verstorben. In diesem Fall ist normalweise ein Zugang ohne offiziellen Antrag auf Zugang ohne Einwilligung erlaubt;
- der Bedienstete ist in Urlaub. Der Leiter des Referats/Bereichs oder der unmittelbare Vorgesetzte („Antragsteller") sollte den betreffenden Bediensteten im Sinne der Kontinuität des Dienstbetriebs vorab um Einwilligung in den Zugang zu dessen E-Mails während seines Urlaubs bitten. Der Bedienstete kann auch während seines Urlaubs um Einwilligung gebeten werden. Ist dies nicht möglich, sollte sich der Antragsteller an die ECP-Verfahren zur Erlangung des Zugangs ohne Einwilligung halten.
- Strafrechtliche Ermittlungen oder sensible Fragen: Hierunter sind Situationen zu verstehen, in denen i) der Bedienstete seine Einwilligung nicht geben kann oder will, ii) der Bedienstete nicht gewarnt werden darf, iii) gegen einen ehemaligen Stelleninhaber strafrechtliche Ermittlungen laufen. In diesem Fall hat der Antragsteller den Sicherheitsbeauftragten der ERA anzusprechen, der sich dann an die Verfahren zur Erlangung des Zugangs ohne Einwilligung zu halten hat.

Möchte jemand Zugang ohne die Einwilligung des Betroffenen erhalten, hat er das so genannte „Formular zur Beantragung des Zugangs ohne Einwilligung" auszufüllen (ausgenommen sind die vorstehend unter dem ersten Anstrich genannten Fälle).

Das Verfahren, nach dem Zugang ohne Einwilligung erhalten werden kann, wird in der ECP näher beschrieben. Der Zugang zu elektronischen Mitteilungen ist vom Exekutivdirektor oder dem Leiter der Verwaltung oder anderen Personen, denen diese Befugnis übertragen wurde, in Absprache mit dem Datenschutzbeauftragten der ERA und dem IT-Sicherheitsbeauftragten der ERA zu genehmigen. Bevor sich die ERA ohne Einwilligung Zugang zu Aufzeichnungen elektronischer Kommunikation verschafft, sollte sie sich stets vom DSB und/oder dem Rechtsdienst der ERA beraten lassen (siehe ECP, S. 14).

Die Genehmigung sollte so formuliert sein, dass zur Lösung des Problems möglichst wenig Einsicht in Inhalte genommen wird und so wenige Maßnahmen wie möglich ergriffen werden. In Notfällen erlaubt die ECP einen sofortigen Zugang ohne Genehmigung, allerdings mit angemessenen Garantien. Die Genehmigung sollte dann unverzüglich eingeholt werden.

2.6. Kategorien personenbezogener Daten

Betroffen sind folgende Datenkategorien:

- Bei der E-Mail-Nachricht: Kopf der Nachricht (Verkehrsdaten) – Betreff, Text der Nachricht (also ihr Inhalt) und Anhänge;
- beim Adressbuch: Vorname, Nachname, Alias (Login-Daten), Büro-Telefonnummer, Referat oder Bereich, E-Mail-Adresse.

2.7. Datenübermittlungen/Empfänger

Potenzielle Empfänger von E-Mails sind alle Personen auf der Welt, die über eine E-Mail-Adresse verfügen, also auch Bedienstete von Organen, Agenturen und Einrichtungen der EU. Zu den Empfängern von Daten aus dem Adressbuch gehören die Bediensteten der ERA, E-

Mail-Dienste der EU-Organe, Bedienstete von Agenturen und Einrichtungen der EU, mit denen die ERA eine bilaterale Vereinbarung abgeschlossen hat.

2.8. Datenaufbewahrung

Die personenbezogenen Daten in E-Mails werden so lange aufbewahrt, wie die betroffene Person ein aktives E-Mail-Account hat, sowie 90 Tage nach dessen Deaktivierung oder 13 Monate nach der Löschung des E-Mail-Accounts in Logs und Back-up-Medien. Die personenbezogenen Daten im Adressbuch werden so lange aufbewahrt, wie die betroffene Person bei der ERA beschäftigt ist.

2.9. Rechte der betroffenen Personen

Betroffene Personen werden mit Hilfe des Vermerks für die Mitarbeiter „Use of ERA's ICT owned resources", ICT, IAM, ECP und E-Mail-Policy informiert.

Bei Aufnahme seiner Tätigkeit wird ein Bediensteter über die Verordnung informiert, in der unter anderem das Recht betroffener Personen auf Auskunft und Berichtigung geregelt ist; demnach kann er von der ERA die unverzügliche Berichtigung unrichtiger oder unvollständiger Daten oder die Löschung von Daten bei unrechtmäßiger Verarbeitung verlangen. Betroffene Personen können ihre Rechte durch Senden einer E-Mail an die ERA ausüben. Anträge auf Berichtigung bearbeitet die ERA binnen eines Monats nach Einreichung des Antrags. Anträge auf Sperrung und Löschung sind innerhalb von drei Monaten zu beantworten. Die betroffenen Personen können sich jederzeit per E-Mail an den DSB wenden.

2.10. Sicherheitsmaßnahmen

Es bestehen mehrere systemspezifische Sicherheitsmaßnahmen, die in der E-Mail-Policy 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;
- zur Virenbekämpfung können bestimmte Arten von Anhängen am E-Mail-Gateway der Agentur durchsucht werden. Die Empfänger werden hierüber per E-Mail in Kenntnis gesetzt. Da Anhänge Viren und andere Malware enthalten können, werden die Nutzer darauf hingewiesen, dass sie Anhänge nur öffnen sollten, wenn diese von einer vertrauenswürdigen Quelle stammen, und dass verdächtige Anhänge an den Service Desk weitergeleitet werden sollten;
- Spam wird am Gateway der Agentur automatisch herausgefiltert. Eindeutig als Spam identifizierte E-Mails werden anhand einer Schwarzen Liste von Domains noch vor ihrer Ankunft am E-Mail-Gateway gelöscht. Verdächtige E-Mails kommen in einen lokalen Junk-E-Mail-Ordner;
- Zugriff auf Log-Dateien haben nur die Administratoren des E-Mail-Systems (laufender Betrieb) und andere zuständige Behörden (z. B. OLAF).

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 Vorabkontrollstellungnahme sind die Strategien der ERA für die E-Mail-Nutzung einschließlich der Datenverarbeitungstätigkeiten zur Überwachung des Nutzerverhaltens. Die Stellungnahme beurteilt also, inwieweit die oben beschriebenen Datenverarbeitungstätigkeiten der zuständigen Akteure der ERA im Einklang mit der Verordnung stehen.

3.1.1. Anwendbarkeit der Verordnung

Die Verordnung (EG) Nr. 45/2001 gilt für die *„ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind“* und findet auf die Verarbeitung „*durch alle Organe und Einrichtungen der Gemeinschaft Anwendung, soweit die Verarbeitung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Gemeinschaftsrechts fallen“*. Aus den nachstehend dargelegten Gründen sind alle Elemente vorhanden, die die Anwendung der Verordnung auslösen.

Erstens bringt die Überwachung der Nutzung des E-Mail-Systems das Erfassen und Weiterverarbeiten *personenbezogener Daten* mit sich, wie sie in Artikel 2 Buchstabe a der Verordnung (EG) Nr. 45/2001 definiert sind. Dies umfasst auch Aufzeichnungen des E-Mail-Verkehrs mit Einzelheiten zur Art und Weise, in der einzelne ERA-Bedienstete das E-Mail-System nutzen (Transaktionsdaten), sowie zum Inhalt der E-Mail-Nachrichten.

Zweitens werden, wie in den Meldungen beschrieben, die erhobenen personenbezogenen Daten einer in Artikel 2 Buchstabe b der Verordnung definierten „*automatisierten Verarbeitung*“ sowie manuellen Verarbeitungsvorgängen unterzogen. Die personenbezogenen Daten werden nämlich zunächst automatisiert erhoben (automatische Speicherung von Log-Dateien) und automatisch vom System bearbeitet (Herausfiltern von Spam und Viren), können dann aber von den zuständigen IT-Mitarbeitern noch einer Analyse unterzogen werden.

Schließlich erfolgt die Verarbeitung durch eine Einrichtung der EU, in diesem Fall durch die Europäische Eisenbahnagentur, 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. 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".

In Anbetracht der Tatsache, dass zum einen die in den vorgelegten Strategiedokumenten beschriebene Überwachung der E-Mail-Nutzung zu einer Bewertung des Verhaltens der Nutzer führen kann (wobei beurteilt wird, ob die Nutzung des E-Mail-Systems der E-Mail-Policy der ERA entspricht oder nicht), und dass zum anderen eine solche Überwachung die Erhebung von Daten über mutmaßliche Straftaten zur Folge haben kann (sofern ein Verdacht auf ungesetzliches Verhalten besteht), sowie aller anderen Arten sensibler Daten, sind eine derartige Überwachung und die entsprechenden Datenverarbeitungen grundsätzlich einer Vorabkontrolle gemäß Artikel 27 Absatz 2 Buchstabe a und b der Verordnung zu unterziehen.

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 Meldungen nicht vor Aufnahme der Verarbeitung bei ihm eingereicht wurden.

3.1.3. Meldung und Frist für die Stellungnahme des EDSB

Die Meldungen gingen am 10. Februar 2012 ein. Die Frist, innerhalb derer der EDSB gemäß Artikel 27 Absatz 4 der Verordnung eine Stellungnahme abzugeben hat, wurde für 178 Tage ausgesetzt, um einige ergänzende Informationen einzuholen.

Darüber hinaus verlängerte der EDSB 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 6. 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. In den Meldungen werden die Verarbeitungsvorgänge mit Artikel 5 Buchstabe a der Verordnung begründet, also als Verarbeitung, die zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse ausgeführt wird. In der E-Mail-Policy ist darüber hinaus mehrfach von der Einwilligung der betroffenen Person die Rede (Artikel 5 Buchstabe d der Verordnung). Diese Rechtsgrundlage wird nachstehend noch näher erörtert (Punkte 3.2.1 und 3.2.2).

Außerdem geht der EDSB auf einige in der ECP und der E-Mail-Policy beschriebene konkrete Verarbeitungstätigkeiten ein, die im Hinblick auf ihre Rechtmäßigkeit einige Bedenken aufwerfen (Punkte 3.2.3 bis 3.2.6).

3.2.1. Artikel 5 Buchstabe a – Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse

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

- *Rechtsgrundlage*

Erstens hält der EDSB fest, dass schon die Verordnung verschiedene Bestimmungen enthält, die für die Bewertung der Rechtmäßigkeit der Überwachung der E-Mail-Nutzung 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 E-Mail-Überwachung darin, zu verhindern, dass dieses Instrument unter Verletzung der Rechtsvorschriften, der internen Strategien der ERA oder in einer anderweitig unbefugten Weise verwendet wird.

Artikel 37 Absatz 2 der Verordnung bietet eine weitere Rechtsgrundlage, die es der ERA gestattet, eine ganz spezielle Datenverarbeitungstätigkeit vorzunehmen, nämlich die Speicherung von Verkehrsdaten, in diesem Fall von Log-Dateien. 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 Verwendung 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 der E-Mail-Policy zu gewährleisten.

Zweitens hat die ERA nach Auffassung des EDSB als Arbeitgeber bestimmte im Arbeitsrecht geregelte Pflichten, 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 besonderer Datenkategorien umfassen (siehe Punkt 3.3).

Schließlich hält der EDSB fest, dass die von der ERA herausgegebenen Strategiedokumente ein weiteres Element darstellen, mit dem sich bestimmten 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.

- *Notwendigkeit*

Wie vorstehend beschrieben, besteht einer der Hauptzwecke der hier zu prüfenden Verarbeitung darin, zu gewährleisten, dass die E-Mail-Systeme der Agentur der E-Mail-Policy entsprechend für Zwecke verwendet werden, die dem Aufgabenbereich der Agentur angemessen sind, und Störungen und Missbrauch der E-Mail-Systeme und -Dienste zu verhindern. Der EDSB nimmt zur Kenntnis, dass die ERA eine gewisse Überwachung der

Nutzung ihrer E-Mail-Dienste für erforderlich hält, um in der Lage zu sein, Verstöße gegen ihre E-Mail-Policy oder Sicherheitsverstöße zu verhindern oder aufzudecken. Man kann daher davon ausgehen, dass eine selektive und rechtmäßige Überwachung von E-Mail-Systemen zumindest in gewissem Maß als erforderlich angesehen werden kann, um die Aufgabe zu erfüllen, eine Nutzung in Übereinstimmung mit der E-Mail-Policy sicherzustellen und somit insgesamt die Sicherheit der IKT-Ressourcen der ERA zu gewährleisten.

Eine gewisse Überwachung wird von der ERA auch als notwendig erachtet, damit sie gegebenenfalls ihre arbeitsrechtlichen Rechte wahrnehmen und ihren arbeitsrechtlichen Pflichten nachkommen kann. Die ERA erklärt beispielsweise, dass sie, wäre sie nicht in der Lage, die E-Mail-Nutzung einer Person zu überwachen, die eines Verstoßes (beispielsweise Weitergabe vertraulicher Unterlagen) 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 Verarbeitung als für die Erfüllung der beabsichtigten Zwecke der Strategie erforderlich angesehen werden kann. Grundsätzlich dürften damit die Anforderungen von Artikel 5 Buchstabe a der Verordnung erfüllt sein. Daher sollte die ERA bei der Überwachung der E-Mail-Nutzung stets Notwendigkeit und Verhältnismäßigkeit im Einklang mit dem in Abschnitt 3.4 diskutierten Grundsatz der Datenqualität beachten.

3.2.2. Artikel 5 Buchstabe d – Einwilligung der betroffenen Person

Der EDSB hält fest, dass die ERA Daten über elektronische Mitteilungen grundsätzlich nur mit Einwilligung des Nutzers untersucht. Damit eine Einwilligung gültig ist, muss sie ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage gegeben worden sein. Der Nutzer soll sich der Verarbeitungsvorgänge bewusst sein, vor allem derer, in die er eingewilligt hat, und zwar auch konkreter Einzelheiten der Verarbeitung einschließlich der Konsequenzen seiner Entscheidungen.

Die Verwendung der Einwilligung stößt auf gewisse Grenzen in Situationen, in denen die betroffene Person in einem Abhängigkeits- oder Unterordnungsverhältnis zu dem für die Verarbeitung Verantwortlichen steht. Dies gilt insbesondere für Beziehungen im Beschäftigungsumfeld.[3] Nach Auffassung des EDSB darf die Einwilligung als stichhaltige Grundlage für die Verarbeitung personenbezogener Daten im Zusammenhang mit elektronischen Mitteilungen nur in wenigen Ausnahmefällen herangezogen werden.

3.2.2.1. Zugang zu E-Mails in Abwesenheit des Nutzers

Ein Fall, in dem die Einwilligung beim Zugang zu elektronischen Mitteilungen ausnahmsweise herangezogen werden könnte, ist gegeben, wenn der Zugang für die Kontinuität des Dienstbetriebs erforderlich ist, wenn also der Nutzer abwesend ist oder nicht länger für die Agentur arbeitet und der Arbeitgeber Zugang zu seinen beruflichen E-Mails benötigt.[4] Auch wenn, wie gesagt, die Einwilligung nicht die Idealvoraussetzung für eine derartige Verarbeitung personenbezogener Daten darstellt, hilft die „Zustimmung“ der betroffenen Person doch, Spannungen am Arbeitsplatz abzubauen.

[3] Siehe z. B. Artikel 29-Datenschutzgruppe, Stellungnahme zur Definition von Einwilligung (WP 187). S. 13ff.
[4] Siehe Stellungnahme vom 18. Januar 2010 – Verfahren des Rechnungshofes für den Zugang zu privaten Festplatten / privaten E-Mails (C 2009-0620).

In diesem Zusammenhang sollte der Nutzer alle erforderlichen Informationen erhalten, vor allem über die Gründe für das Zugangsersuchen, die Dringlichkeit der Angelegenheit, die Art und den Umfang der gesuchten Informationen sowie die anderen in Artikel 11 der Verordnung aufgeführten Angaben. Die ERA hat dem EDSB eine in solchen Fällen zu verwendende Einwilligungserklärung vorgelegt. Dieses Formular enthält Felder zu i) den Gründen für die Zugangsgewährung, ii) dem Umfang des Zugangs, iii) dem Zugangszeitraum und iv) den einzuhaltenden Verpflichtungen bezüglich Verhältnismäßigkeit und Vertraulichkeit. Zum Inhalt dieser Erklärung merkt der EDSB Folgendes an:

- Die Erklärung sollte klar und deutlich besagen, dass die Einwilligung freiwillig erfolgt und jederzeit widerrufen werden kann und dass dem Nutzer im Falle der Verweigerung der Einwilligung keinerlei Nachteile entstehen;
- die Formulierung „alle für die Ausübung der Tätigkeit der Agentur erforderlichen Aufzeichnungen“ ist zu weit gefasst. Der EDSB empfiehlt, sie durch eine präzisere Definition zu ersetzen;
- es sollten die folgenden in Artikel 11 verlangten Angaben hinzugefügt werden: Identität des für die Verarbeitung Verantwortlichen; Empfänger oder Empfängerkategorien; Bestehen des Rechts, Auskunft über alle im Eingriffszeitraum über den Account eingegangene und versandte E-Mails zu bekommen.

Nur wenn es unmöglich ist, die Einwilligung des Nutzers einzuholen (wenn der nicht erreichbar oder nicht in der Lage ist, seine Einwilligung zu erteilen), oder wenn alternative organisatorische oder technische Lösungen (z. B. funktionale Mailbox, siehe weiter unten) nicht durchführbar sind, sollte Artikel 5 Buchstabe a als Rechtsgrundlage herangezogen werden. Nach Auffassung des EDSB kann der Zugang im Zusammenhang mit dem Verfahren nur dann als für das Erreichen der beabsichtigten Ziele erforderlich gelten, wenn die ERA belegen kann, dass der Mitarbeiter klar und umfassend über die Nutzung privater/beruflicher E-Mails und einer private Festplatte aufgeklärt wurde, dass die Dringlichkeit des beantragten Zugangs nachgewiesen werden konnte und dass die Einwilligung des Nutzers nicht eingeholt werden konnte. Diese Aspekte der Notwendigkeit wären in jedem Einzelfall zu belegen. Sofern der Zugang außerdem in Abwesenheit des Nutzers erfolgt, ist dieser jeweils darüber in Kenntnis zu setzen.

Es sei nachdrücklich darauf hingewiesen, dass ein solches Zugangsverfahren nicht als Teil einer Verwaltungsuntersuchung gegen einen Bediensteten zu betrachten ist. Genauer gesagt, darf dieses Verfahren nicht benutzt werden, um die Vorschriften für eine Verwaltungsuntersuchung oder ein Disziplinarverfahren gegen einen Bediensteten zu umgehen. Der DSB der ERA sollte in seiner schriftlichen Stellungnahme nachweisen, dass er diesen Aspekt geprüft hat.

Zusätzlich oder alternativ zu der vorstehend beschriebenen Methode könnte die ERA die Einrichtung gemeinsamer Mailboxen erwägen und die Empfänger auffordern, dienstliche Schreiben als Kopie an diese Mailboxen zu senden. In diesem Fall könnten grundsätzlich alle Mitglieder eines Referats Zugriff auf die gemeinsamen Mailboxen haben. Mit dieser Vorgehensweise könnte es deutlich seltener vorkommen, dass zur Aufrechterhaltung des Betriebs auf einzelne E-Mails zugegriffen werden muss.

Zu den E-Mail-Accounts von Nutzern, die nicht mehr für die Agentur tätig sind, sei angemerkt, dass diese Bediensteten aufgefordert werden sollten, vor ihrem Ausscheiden aus dem Dienst alle privaten E-Mails von ihrem Account zu löschen. Im Sinne eines proaktiven Umgangs mit Zugangsanträgen ehemaliger Bediensteter hält es der EDSB für sinnvoll, eine Kopie des Inhalts

privater E-Mails, die vom Nutzer als solche gekennzeichnet wurden (oder der privaten Festplatte mit solchen E-Mails), auf CD/DVD zur Verfügung zu stellen.

Abschnitt IV B der E-Mail-Policy (wie weiter oben in Punkt 2.5 beschrieben) und die entsprechenden Abschnitt der ECP sollten geändert/geprüft werden, um den vorstehenden Empfehlungen Genüge zu tun.

3.2.2.2. Zugang zu Dateien, die im Computer einer Person gespeichert sind

In der E-Mail-Policy heißt es hierzu: *„Bei der Überprüfung von Dateien auf dem Computer einer Person ist eine Einwilligung in die Einsichtnahme im Allgemeinen nicht erforderlich, da diese Dateien nicht der ECP-Definition einer „Aufzeichnung einer elektronischen Mitteilung" entsprechen"*. Dieser Aussage kann sich der EDSB nicht anschließen, da die Definition einer „Aufzeichnung einer elektronischen Mitteilung" in der ECP lautet: *„Inhalt von elektronischen Mitteilungen, die von einem oder mehreren elektronischen Kommunikationssystemen oder -diensten geschaffen, versendet, weitergeleitet, beantwortet, übermittelt, verteilt, gesendet,* ***gespeichert, aufbewahrt, kopiert, heruntergeladen****, angezeigt, betrachtet, gelesen oder gedruckt werden"* (Hervorhebung durch den EDSB). Die in dem Computer eines Nutzers gespeicherten Dateien einschließlich E-Mails können also sehr wohl personenbezogene Daten enthalten. Nach Auffassung des EDSB sollten die im Computer einer Person gespeicherten Dateien den gleichen Vorschriften unterliegen, wie sie für den Zugang zu E-Mails in Abwesenheit eines Nutzers gelten.

Der EDSB empfiehlt der ERA daher, die für den Zugang zu E-Mails in Abwesenheit des Nutzers geltenden Vorschriften auch auf diese Art des Zugangs auszudehnen (siehe vorstehenden Punkt 3.2.2.1).

3.2.3. Persönliche Webmail-Accounts

Die E-Mail-Policy besagt, sie gelte *„für die Nutzung privater E-Mail-Accounts durch Stelleninhaber, wie unten ausgeführt"*. Im weiteren Schriftwechsel mit dem EDSB führte die ERA aus, dass *„alle Bediensteten der ERA, die die IKT-Infrastruktur der ERA nutzen, einen privaten E-Mail-Account führen dürfen. Auch wenn dieser E-Mail-Account außerhalb des IT-Systems der ERA angesiedelt ist, wird bei seiner Nutzung über das Internet doch deutlich, dass der Zugang über die IP-Adressen der Agentur erfolgt. Es wird daher erwartet, dass sich die Nutzer an die Vorgaben der Strategie halten"*.

Generell kann der Arbeitgeber die Nutzung privater Webmail-Accounts durch seine Mitarbeiter nicht regeln oder beeinflussen, selbst wenn der Zugriff auf diese über Verbindungen der Agentur erfolgt. Private Webmail-Accounts gehören generell nicht in den Einflussbereich des für die Verarbeitung Verantwortlichen; sie sind der Privatsphäre zuzuordnen, und damit hat der Arbeitgeber grundsätzlich kein Eingriffsrecht. Die Tatsache, dass deutlich wird, dass die Nutzung privater E-Mail-Accounts bei der Arbeit über die IP-Adressen der Agentur erfolgt, ist keine plausible Begründung dafür, dass private Webmail-Accounts der E-Mail-Policy der ERA unterliegen sollen. Ein weiterer Beleg hierfür ist die eindeutige Unvereinbarkeit mit einigen Bestimmungen dieser Strategie, wie der Bestimmungen über die Aktivierung/Deaktivierung des E-Mail-Accounts, Beschränkungen, gelegentliche private Nutzung, Zugang ohne Einwilligung usw.

Sofern sie begründet und verhältnismäßig sind, könnte es einige Ausnahmen von dieser allgemeinen Vorschrift geben, wie das Verbot, Dateien herunterzuladen oder sogar auf private E-Mail-Accounts zuzugreifen. Die E-Mail-Policy enthält jedoch keinerlei nähere Angaben zu

den Gegebenheiten, unter denen die E-Mail-Policy auch auf die Nutzung privater Webmail-Accounts Anwendung findet. Eine allgemeine Anwendung dieser Strategie auf private Webmail-Accounts ist nicht gerechtfertigt.

Aus ähnlichen Gründen ist der EDSB der Auffassung, dass die ECP-Bestimmung, der zufolge es *„Bediensteten der ERA untersagt ist, ohne Genehmigung in elektronischen Mitteilungen personenbezogene Daten herauszusuchen, zu verwenden oder weiterzugeben“*, übermäßig in die Privatsphäre eindringt und zu restriktiv ist. Diese Bestimmung ist zu weit gefasst. Sie impliziert, dass es Nutzern bei der ERA nicht gestattet ist, das E-Mail-System für private E-Mails oder berufliche Mitteilungen mit personenbezogenen Daten zu verwenden. Die erste Lesart stünde im Widerspruch zu der Tatsache, dass die ECP eine gelegentliche private Nutzung zulässt, die zweite wäre unrealistisch.

Der EDSB fordert die ERA daher auf, diese Bestimmungen noch einmal zu überdenken und die entsprechenden Teile der E-Mail-Policy umzuformulieren, um diesen Erwägungen Rechnung zu tragen.

3.2.4. Zugang zu öffentlichen Aufzeichnungen

Die ECP enthält eine Definition des Begriffs „Aufzeichnung einer elektronischen Mitteilung der Agentur“ („ECR“). Sie lautet:

„Aufzeichnungen elektronischer Mitteilungen im Zusammenhang mit der Verwaltungstätigkeit der Agentur gelten als öffentliche Aufzeichnungen ***unabhängig davon, ob die Agentur Eigentümerin der Systeme oder Geräte elektronischer Kommunikationsressourcen ist****, mit denen die Mitteilungen geschaffen, gesendet, weitergeleitet, beantwortet, gespeichert, aufbewahrt, kopiert, heruntergeladen, angezeigt, betrachtet, gelesen, gedruckt oder anderweitig aufgezeichnet werden,* ***oder nicht****. Dessen ungeachtet können* ***andere Aufzeichnungen, unabhängig davon, ob sie im Besitz der Agentur sind****, nach EU-Rechtsvorschriften als öffentliche Aufzeichnungen der Öffentlichkeit zugänglich gemacht werden, sofern sie zum Tätigkeitsbereich der Agentur gehören“* (Hervorhebung durch den EDSB).

Die oben genannte Definition von Aufzeichnungen elektronischer Mitteilungen der Agentur weist eindeutig Verbindungen zum Begriff des öffentlichen Dokuments für den Zweck der Verordnung (EG) Nr. 1049/2001 über den Zugang der Öffentlichkeit zu Dokumenten auf. Die Tatsache, dass die ECR der Agentur als öffentliche Aufzeichnungen gelten, könnte die Verpflichtung implizieren, gemäß dieser Verordnung Zugang zu diesen Aufzeichnungen zu gewähren. Die vorstehend erwähnte Definition dürfte jedoch über die EU-Definition eines „öffentlichen Dokuments“ hinausgehen. In diesem Zusammenhang weist der EDSB darauf hin, dass die Verordnung (EG) Nr. 1049/2001 nur für „Dokumente eines Organs“ gilt, das heißt, für „Dokumente aus allen Tätigkeitsbereichen der Union, die von dem Organ erstellt wurden oder bei ihm eingegangen sind und sich in seinem Besitz befinden“. Der EDSB fordert die ERA daher auf, sich Gedanken über diese Definition zu machen, damit sie auch weiterhin im Einklang mit der zitierten Verordnung steht.

In der ECP heißt es ferner: *„Alle Aufzeichnungen elektronischer Mitteilungen auf Kommunikations-, Video-, Audio-Geräten oder Computern im Besitz oder unter der Kontrolle der Agentur gelten für die Zwecke dieser Strategie als Aufzeichnungen elektronischer Mitteilungen der Agentur“. Dazu gehören auch private elektronische Mitteilungen“* (Hervorhebung durch den EDSB). Die Bedeutung dieses letzten Satzes wird zwar nicht recht klar, doch weist der EDSB darauf hin, dass die zitierte Passage möglicherweise nicht ganz

stimmig ist, weil dort besagt wird, dass private elektronische Mitteilungen unter Umständen der Öffentlichkeit zugänglich gemacht werden können. Solange es sich um rein private (also nicht mit der Wahrnehmung der Aufgaben der ERA zusammenhängende) Mitteilungen handelt, fallen sie nicht in den Anwendungsbereich der Verordnung (EG) Nr. 1049/2001. Der EDSB empfiehlt daher der ERA eine Überprüfung und/oder Klarstellung der betreffenden Passage.

3.2.6. Abhören von Telefongesprächen

Gemäß ECP *„werden Audio- oder Video-Telefongespräche nicht ohne entsprechenden Hinweis an die Teilnehmer aufgezeichnet oder überwacht, sofern nicht ein Gericht eine solche Überwachung oder Aufzeichnung ausdrücklich genehmigt hat“*.

In Anbetracht der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte vertritt der EDSB die Auffassung, dass das Abhören elektronischer Kommunikation nur gestützt auf eine hinreichend präzise und konkrete Rechtsgrundlage stattfinden darf.[5] So muss das Abhören insbesondere gesetzlich eindeutig erlaubt sein und sich auf einen konkreten Rechtsakt stützen, im dem die Umstände festgelegt sind, unter denen das Abhören erfolgen darf, sowie angemessene Garantien gegen die Gefahr eines Missbrauchs vorgesehen sind. Ein Verwaltungsakt kann in diesem Fall nicht als ausreichend gelten.

Dem EDSB ist nichts von einem Rechtsakt bekannt, der in dem vorstehend geschilderten Sinn das Abhören elektronischer Kommunikation durch die ERA erlaubt. Die allgemeinen Rechtsgrundlagen für Verwaltungsuntersuchungen und Disziplinarverfahren reichen normalerweise als Rechtsgrundlage für das Abhören von Telefongesprächen nicht aus. Ganz im Gegenteil: Gemäß Erwägungsgrund 19 der Verordnung müsste **sich** die ERA an die zuständigen Behörden in den Mitgliedstaaten **wenden**, wenn sie der Auffassung ist, dass Fernmeldeverbindungen in ihren Telekommunikationsnetzen gemäß den geltenden einzelstaatlichen Rechtsvorschriften überwacht werden sollen.

Nach Auffassung des EDSB verfügt die ERA daher über keine hinreichend präzise und konkrete Rechtsgrundlage für das Abhören elektronischer Kommunikation am Arbeitsplatz. Er empfiehlt der ERA daher die Streichung der entsprechenden Passage aus der ECP.

3.3. Verarbeitung besonderer Datenkategorien

Von der Überwachung der E-Mail-Nutzung können besondere Kategorien personenbezogener Daten betroffen sein. Dabei handelt es sich gemäß Verordnung um personenbezogene Daten, „*aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen hervorgehen*“, sowie um „*Daten über Gesundheit oder Sexualleben*“ (Artikel 10). Vor allem der Inhalt bestimmter E-Mails kann Einblicke in sehr intime Einzelheiten des Privatlebens einer Person geben, wie sexuelle Präferenzen, Gesundheitsdaten oder politische Einstellungen. Selbst bei der Verarbeitung von Verkehrsdaten wie E-Mail-Log-Dateien können gelegentlich besondere Datenkategorien enthüllt werden, wenn beispielsweise E-Mails an „sensible Empfänger“ wie Gewerkschaften, politische Parteien und ähnliche Organisationen gehen.

Die Verarbeitung besonderer Datenkategorien ist im Prinzip untersagt, sofern nicht eine der Ausnahmen aus Artikel 10 der Verordnung greift. 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*

[5] Siehe z. B. EGMR, *Kruslin ./. Frankreich* (11801/85), Urteil vom 24. April 1990, Randnr. 33; EGMR, *Malone*, bereits zitiert, Randnr. 68.

des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund der Verträge oder anderer aufgrund der Verträge erlassenen Rechtsakte zulässig ist". Eine gewisse Überwachung der E-Mail-Nutzung mag für die ERA erforderlich scheinen, um die Sicherheit von System/Daten sowie die Einhaltung des Statuts und anderer Vorschriften sicherzustellen.

Dazu gehört z. B. das Recht der ERA, das Anschauen oder den Austausch von sex-bezogenen Inhalten oder Informationen am Arbeitsplatz zu verhindern. 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 Beschäftigen, die ungesetzlichen Aktivitäten wie dem Anschauen und Herunterladen von Material nachgehen, das dem Verbrechen Vorschub leistet. Der EDSB ist daher der Auffassung, dass die ERA als Arbeitgeber bestimmte im Arbeitsrecht geregelte Rechte und Pflichten hat, die die Verarbeitung sensibler Daten von Nutzern rechtfertigen, wenn dies im Rahmen interner Untersuchungen erforderlich und verhältnismäßig ist.

Bezüglich der Verarbeitung personenbezogener Daten im Rahmen von Verwaltungsuntersuchungen verweist der EDSB die ERA auf die Leitlinien für Verwaltungsuntersuchungen und Disziplinarverfahren.[6]

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.

Erklärtermaßen dient die E-Mail-Policy der ERA folgenden Zwecken:

- Darstellung der angemessenen und der unangemessenen Nutzung des E-Mail-Systems;
- Gewährleistung, dass die E-Mail-Systeme der Agentur für Zwecke eingesetzt werden, die dem Aufgabenbereich der Agentur entsprechen;
- Information der Mitarbeiter und Nutzer der Agentur über die Anwendbarkeit der E-Mail-Vorschriften und -Strategien der ERA;
- Vermeidung von Störungen und Missbrauch der E-Mail-Systeme und -Dienste.

Wie bereits dargestellt, besteht die Verarbeitung von E-Mails zu Sicherheitszwecken im Wesentlichen aus der systematischen automatisierten Kontrolle von E-Mail-Nachrichten, die durch das Telekommunikationsnetzwerk eines Organs gehen, auf Viren oder andere Malware sowie auf Spam. Da dies automatisiert geschieht, werden bei diesem Prozess normalerweise keine personenbezogenen Daten manuell verarbeitet. Zu dieser Vorgehensweise, die in derartigen Fällen üblich ist, hat der EDSB keine besonderen Anmerkungen zu machen.

Er weist jedoch darauf hin, dass im Einzelfall eine Prüfung elektronischer Kommunikationsdaten von E-Mails einschließlich des Inhalts nur erfolgen kann, wenn ein hinreichender Verdacht auf Fehlverhalten vorliegt, der durch konkrete erste Beweise erhärtet wird, und wenn dies im Rahmen einer Verwaltungsuntersuchung geschieht. Der Zugang sollte verhältnismäßig sein und nicht über das den jeweiligen Umständen angemessene Maß

[6] Leitlinien zur Verarbeitung personenbezogener Daten durch europäische Organe und Einrichtungen im Rahmen von Verwaltungsuntersuchungen und Disziplinarverfahren, 23. April 2010, abrufbar auf der Website des EDSB.

hinausgehen und hierzu in einem angemessenen Verhältnis stehen. Diesbezüglich sollte ein klares Verfahren mit einem schrittweisen und verhältnismäßigen Ansatz eingerichtet werden. Bezüglich der Verarbeitung personenbezogener Daten im Rahmen von Verwaltungsuntersuchungen verweist der EDSB die ERA auf die Leitlinien für Verwaltungsuntersuchungen und Disziplinarverfahren.[7]

In der ECP werden folgende Situationen aufgeführt, in denen ein Zugang ohne Einwilligung erlaubt ist: 1) Er ist erforderlich und rechtmäßig; 2) es besteht begründeter Verdacht auf Verstöße gegen das Gesetz oder die Strategie der Agentur; 3) es bestehen „zwingende Gründe", wie im Anhang definiert; 4) es liegen „zeitabhängige, kritische betriebliche Umstände" vor, wie im Anhang definiert. Weiter heißt es dort, dass abgesehen von „Notfällen" derartige Maßnahmen vorab schriftlich vom Exekutivdirektor oder dem Leiter der Verwaltung oder anderen Personen, denen diese Befugnis übertragen wurde, in Absprache mit dem Datenschutzbeauftragten der ERA und dem IT-Sicherheitsbeauftragten der ERA genehmigt werden müssen.

Der EDSB begrüßt, dass vor Einsichtnahme in E-Mails ohne Einwilligung der DSB konsultiert wird. Er unterstreicht jedoch, dass Begriffe wie „zwingende Gründe", „zeitabhängige, kritische betriebliche Umstände" und „Notfälle" trotz Definition zu allgemein sind und sich überschneiden. Er empfiehlt daher der ERA, die Verwendung solcher Begriff in ihren Strategien zu überdenken. Vor allem sollte die ERA die genannten Begriffsbestimmungen näher spezifizieren und klarstellen.

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*". 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.

[7] Bereits zitiert.

Aus den Meldungen und der E-Mail-Policy geht hervor, dass Daten in Logs und Back-up-Medien so lange aufbewahrt werden, wie die betroffene Person einen aktiven E-Mail-Account hat, bis zu 90 Tage nach der Deaktivierung des E-Mail-Accounts und 13 Monate nach der Löschung des E-Mail-Accounts.

Diese Fristen stehen nicht ganz im Einklang mit Artikel 37 der Verordnung, der besondere Bestimmungen für die Aufbewahrung von Verkehrsdaten und Daten für die Gebührenabrechnung enthält. Artikel 37 Absatz 2 der Verordnung besagt, dass Verkehrsdaten so schnell wie möglich zu löschen oder zu anonymisieren sind und in keinem Fall länger als sechs Monate nach ihrer Erfassung aufbewahrt werden dürfen, es sei denn, ihre weitere Aufbewahrung ist für die Feststellung, Ausübung oder Verteidigung eines Rechtsanspruchs im Rahmen eines anhängigen gerichtlichen Verfahrens erforderlich. Die ERA kann daher beschließen, die Logs für höchstens sechs Monate aufzubewahren.

Sollte aufgrund der Überwachung von Log-Dateien oder Verkehrsdaten bei der ERA der Verdacht entstehen, dass jemand gegen die E-Mail-Policy verstoßen hat, darf die ERA die belastenden Log-Dateien *„für die Feststellung, die Ausübung oder die Verteidigung eines Rechtsanspruchs im Rahmen eines anhängigen gerichtlichen Verfahrens“* aufbewahren. 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 dahingehend ausgelegt, dass sie nicht nur strafrechtliche Ermittlungen, sondern auch Disziplinarverfahren abdeckt.[8]

Somit dürfen Log-Dateien 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 E-Mail-Policy oder das Statut verstoßen oder eine Straftat begangen hat 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 (die offiziell eingeleitet worden sein sollte) oder die Einleitung eines Disziplinarverfahrens angemessen rechtfertigen. Nur bei einem positiven Ergebnis dieser Prüfung dürfen Verkehrsdaten länger als sechs Monate aufbewahrt werden; es sei unterstrichen, dass in diesen Fällen nur die erheblichen Teile der Log-Dateien aufbewahrt werden sollten.

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 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.

Den Meldungen ist zu entnehmen, dass intern nur der IT-Sicherheitsbeauftragte und der Leiter der IT-Abteilung auf die Daten zugreifen dürfen. In weiteren Kontakten mit dem EDSB fügte die ERA noch die folgenden internen Empfänger mit dem Hinweis hinzu, dass

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

personenbezogene Daten an sie im Rahmen des „Zwischenfall-Management-Prozesses“ (technische Zwischenfälle, Sicherheitszwischenfälle) übermittelt werden können, wenn also ein Zwischenfall als ernst genug eingestuft wird, um an diese Hierarchieebene weitergeleitet zu werden:

- Exekutivdirektor,
- Datenschutzbeauftragter,
- Leiter des Referats Verwaltung,
- Leiter des betroffenen Referats,
- Leiter des betroffenen Bereichs,
- Leiter des Bereichs Humanressourcen,
- Leiter des Bereichs ITFM,
- IKT-Sicherheitsbeauftragter,
- IT-Systemadministrator,
- IT-Dienstleister.

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 Vorschriften hat die ERA bei der Übermittlung personenbezogener Daten zu gewährleisten, dass *i)* der Empfänger die entsprechende Zuständigkeit hat und *ii)* die Übermittlung erforderlich ist. Die Notwendigkeit der Übermittlung (und der übermittelten Daten) ist von dem für die Verarbeitung Verantwortlichen in jedem Einzelfall zu beurteilen.

Im vorliegenden Fall scheinen der Leiter des Bereichs ITFM, der Systemadministrator und der IKT-Sicherheitsbeauftragte die Personen zu sein, die für die interne Verwaltung der Überwachung der E-Mail-Nutzung verantwortlich sind. Auf der anderen Seite ist der Leiter der Verwaltung der für die Verarbeitungen Verantwortliche im Zusammenhang mit Verwaltungsuntersuchungen und Disziplinarmaßnahmen. Der EDSB empfiehlt der ERA, in Anbetracht dieser Ausführungen die Liste der Empfänger zu überprüfen und fallweise die Frage zu beantworten, ob Übermittlungen durch den IKT-Sicherheitsbeauftragten, den Systemadministrator oder den Leiter des Bereichs ITFM an diese Empfänger im Einklang mit Artikel 7 stehen. Gemäß Artikel 7 dürften nämlich nur die Personen zuständig sein, die darüber zu entscheiden haben, ob eine Verwaltungsuntersuchung einzuleiten ist, und die für die Verwaltung des Systems zuständig sind.

Des Weiteren dürfen die Daten unter besonderen Umständen vorübergehend an die nachstehend genannten Empfängerkategorien innerhalb der Organe und Einrichtungen der EU weitergeleitet werden:

- an OLAF und/oder IDOC 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 tun die Übermittlungen von Informationen an OLAF, IDOC, den Europäischen Gerichtshof, den Bürgerbeauftragten oder den EDSB zur Erfüllung ihrer offiziellen Aufgaben Artikel 7 grundsätzlich Genüge. Die Notwendigkeit ist jedoch fallweise von der ERA zu beurteilen.

Die Meldungen erwähnen auch Datenübermittlungen an die Staatsanwaltschaft. 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.

Gemäß den Meldungen sind keine Übermittlungen in Drittländer oder an internationale Organisationen vorgesehen.

3.7. Recht auf Auskunft und Berichtigung, Sperrung und Löschung

Gemäß Artikel 13 der Verordnung hat die betroffene Person das Recht, jederzeit frei und ungehindert innerhalb von drei Monaten nach Eingang eines entsprechenden Antrags unentgeltlich 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. Die ERA hat mit angemessenen Verfahren zu gewährleisten, dass Nutzer ihr Recht auf Auskunft ausüben können. Der EDSB nimmt mit Zufriedenheit zur Kenntnis, dass betroffene Personen ihre Rechte durch Senden einer E-Mail an eine funktionale Mailbox wahrnehmen können und dass sich die ERA dazu verpflichtet hat, auf das Ersuchen binnen eines Monats zu antworten.

In bestimmten Fällen kann sich der für die Verarbeitung Verantwortliche auf die Ausnahmen in Artikel 20 Absatz 1 der Verordnung berufen, um die Wahrnehmung des Rechts auf Auskunft oder Berichtigung abzulehnen. Im vorliegenden Fall ist dies rechtmäßig, wenn die Einschränkung notwendig ist für *„a) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten“*. Vor einer Entscheidung über die Inanspruchnahme einer Ausnahme muss die ERA in jedem Einzelfall die Umstände der betreffenden Datenverarbeitung bewerten.

Sollte die ERA ausnahmsweise die Auskunft verweigern, sollte sie bedenken, dass ein Grundrecht nicht systematisch eingeschränkt werden darf. Sie muss in jedem Einzelfall prüfen, ob die Bedingungen für die Anwendung einer der Ausnahmen erfüllt sind. Gemäß Artikel 20 der Verordnung muss die Maßnahme außerdem „notwendig“ sein. Das heißt, dass für jeden Fall die „Notwendigkeitsprüfung“ durchgeführt werden muss. Beruft sich die ERA auf eine Ausnahme, hat dies im Einklang mit Artikel 20 Absatz 3 zu geschehen, dem zufolge *„die betroffene Person gemäß dem Gemeinschaftsrecht über die wesentlichen Gründe für diese Einschränkung und darüber zu unterrichten ist, dass sie das Recht hat, sich an den Europäischen Datenschutzbeauftragten zu wenden“*. Die ERA kann sich jedoch auf Artikel 20 Absatz 5 berufen, um die Auskunft, wie in diesem Artikel geregelt, aufzuschieben: *„Die Unterrichtung nach den Absätzen 3 und 4 kann so lange aufgeschoben werden, wie sie die Einschränkung gemäß Absatz 1 ihrer Wirkung beraubt“*.

Gemäß Artikel 14 der Verordnung hat die betroffene Person das Recht auf Berichtigung unrichtiger oder unvollständiger Daten. In Anbetracht der Art der Daten (mit Benutzerkennungen und IP-Adressen verknüpfte Log-Dateien) und der Art ihrer Erhebung (automatische Protokollierung) dürfte eine Berichtigung der Daten eher unwahrscheinlich sein.

Grundsätzlich muss die ERA allerdings das Bestehen eines solchen Rechts anerkennen, das in wenigen Fällen angewandt werden mag, wenn beispielsweise jemand die Benutzerkennung einer anderen Person verwendet. Die funktionale Mailbox kann auch für Anträge auf Löschung und Berichtigung verwendet werden, und eine Antwort hat, so besagen es die Meldungen, binnen drei Kalendermonaten zu erfolgen.

Der EDSB weist die ERA auf das in Artikel 16 und 15 der Verordnung verankerte Recht auf Löschung bzw. Sperrung hin. Die betroffene Person kann das Recht auf Löschung der Daten geltend machen, wenn diese unrechtmäßig verarbeitet wurden. Gemäß Artikel 15 hat die betroffene Person das Recht, von dem für die Verarbeitung Verantwortlichen die Sperrung von Daten zu verlangen, wenn ihre Richtigkeit bestritten wird, und zwar für eine Dauer, die es dem für die Verarbeitung Verantwortlichen ermöglicht, die Richtigkeit zu überprüfen, wenn der für die Verarbeitung Verantwortliche sie für die Erfüllung seiner Aufgaben nicht länger benötigt, sie aber für Beweiszwecke weiter aufbewahrt werden müssen, und wenn die Verarbeitung unrechtmäßig ist, die betroffene Person Einspruch gegen ihre Löschung erhebt und stattdessen ihre Sperrung fordert.

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 (oder wird sie unternehmen):

- IKT-Nutzer werden offiziell durch einen Vermerk für die Mitarbeiter 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-Benutzervereinbarung) („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.

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 tatsächlich zur Kenntnis zu nehmen. Nach Ansicht des EDSB sind die beiden folgenden Aspekte zu berücksichtigen.

Erstens: Im Sinne einer wirksamen Information 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 nachdrücklich 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 sieben separate Dokumente lesen, nämlich den Vermerk für die Mitarbeiter, die Datenschutzerklärung, die Internet-Strategie, die IAM-Strategie, die E-Mail-Policy und die ECP. In manchen Fällen wird der Zusammenhang zwischen den einzelnen Dokumenten nicht recht deutlich.

Nach Ansicht des EDSB wäre es besser gewesen, 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) bereitzustellen. Dies könnte den Grundsätzen von Treu und Glauben und Transparenz mehr Gewicht verschaffen. Um jegliche Verwirrung zu vermeiden und die Strategien verständlicher zu gestalten, schlägt der EDSB vor, alle Informationen zur Überwachung der E-Mail-Nutzung in einem einzigen, alle erforderlichen Informationen enthaltenden Dokument zu vereinen (siehe dazu auch Punkt 3.8.2). Dieses Dokument könnte mit einer Datenschutzerklärung kombiniert werden.

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 E-Mail-Strategie der ERA merkt der EDSB im Wesentlichen Folgendes an:

- Sowohl ICT als auch die E-Mail-Policy 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 der Einleitung einer E-Mail-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/Untersuchungszwecke äußert sie sich hingegen nicht klar. Erfolgt die Überwachung zur Überprüfung der rechtmäßigen Nutzung, muss dies ausdrücklich erwähnt werden.

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 einer 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 die E-Mail-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 E-Mail-Protokolle gegen unbefugten Zugriff, Änderung oder Löschung auch durch den IKT-Sicherheitsbeauftragten und die IT-Systemadministratoren geschützt werden;
3. sicherstellen, dass jeder Zugriff auf die E-Mail-Protokolle zu einer bestimmten Person zurückverfolgt werden kann;
4. sicherstellen, dass alle Zugriffe auf die E-Mail-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.

4. SCHLUSSFOLGERUNGEN

Die gemeldete Verarbeitung kann nur umgesetzt werden, wenn die in dieser Stellungnahme formulierten Empfehlungen in vollem Umfang berücksichtigt werden. Damit die ERA im Einklang mit der Verordnung handelt, empfiehlt ihr der EDSB Folgendes:

- Beschränkung der Nutzung der Einwilligung bei Zugang zu E-Mails des Nutzers zur Wahrung der Kontinuität des Dienstbetriebs nach den in Punkt 3.2.2.1 beschriebenen Verfahren und Bedingungen;
- Ausdehnung der gleichen Vorschriften, wie sie für den Zugang zu E-Mails in Abwesenheit des Nutzers gelten, auf den Zugang zu auf einzelnen Computern gespeicherten Dateien, wie in Punkt 3.2.2.2 dargestellt;
- Überarbeitung des Teils der E-Mail-Policy, in dem es um die Anwendbarkeit dieser Strategie auf private Webmail-Accounts geht (Punkt 3.2.3);

- Überarbeitung der ECP-Bestimmung, der zufolge es *„ERA-Mitarbeitern untersagt ist, ohne Genehmigung personenbezogene Informationen in elektronischen Mitteilungen ausfindig zu machen, zu verwenden oder offenzulegen“* (Punkt 3.2.3);
- Überdenken der Definition von „Aufzeichnung elektronischer Kommunikation der Agentur“ dahingehend, dass sie dem Begriff des öffentlichen Dokuments im Sinne der Verordnung (EG) Nr. 1049/2001 über den Zugang der Öffentlichkeit zu Dokumenten entspricht;
- Streichung oder Klarstellung der Bestimmung der ECP, der zufolge Aufzeichnungen elektronischer Kommunikation der Agentur auch private elektronische Mitteilungen umfassen können (Punkt 3.2.4);
- Streichung der ECP-Bestimmung über das Abhören elektronischer Kommunikation;
- Bereitstellung technischer und verfahrensmäßiger Garantien dafür, dass die Verarbeitung besonderer Datenkategorien bei der Kontrolle oder Überwachung von E-Mails auf ein Mindestmaß beschränkt bleibt und nur erfolgt, wenn sie unumgänglich ist;
- Vornahme individueller Prüfungen elektronischer Kommunikationsdaten von E-Mails einschließlich des Inhalts nur, wenn ein hinreichender Verdacht auf Fehlverhalten vorliegt, der durch konkrete erste Beweise erhärtet wird, und im Rahmen einer Verwaltungsuntersuchung. Eine solche Überwachung sollte erst eingeleitet werden, nachdem weniger in die Privatsphäre eindringende Mittel erwogen oder ausprobiert worden sind. Diesbezüglich sollte ein klares Verfahren mit einem schrittweisen und verhältnismäßigen Ansatz eingerichtet werden;
- im Hinblick auf Zugang ohne Einwilligung nähere Bestimmung und Einengung von Begriffen wie „zwingende Gründe“, „zeitabhängige, kritische betriebliche Umstände“ und „Notfälle“;
- Aufbewahrung von E-Mail-Verkehrsdaten (einschließlich Log-Dateien) gemäß Artikel 37 Absatz 2 der Verordnung für höchstens sechs Monate nach ihrer Erhebung, es sei denn, ihre weitere Aufbewahrung ist für die Feststellung, die Ausübung oder die Verteidigung eines Rechtsanspruchs im Rahmen eine anhängigen gerichtlichen Verfahrens erforderlich;
- Sicherstellung, dass Datenübermittlungen nach einer konkreten Bewertung ihrer Notwendigkeit im Einklang mit Artikel 7 und 8 der Verordnung erfolgen;
- Erwägung der Zusammenfassung aller Informationen zur Verarbeitung von Daten im Zusammenhang mit der E-Mail-Nutzung in einem einzigen, alle erforderlichen Informationen enthaltenden Dokument;
- Zusammenführung und/oder Verdeutlichung der E-Mail-Policy und der Datenschutzerklärung gemäß den Empfehlungen in Punkt 3.8.2.;
- regelmäßige Überprüfung der Analysen zur Festlegung der Kontrollen, die erforderlich sind, um die Risiken auf ein für die Leitung der Agentur annehmbares Niveau zu senken;
- Verstärkung der Sicherheitsmaßnahmen bezüglich der E-Mail-Log-Dateien, indem die Rückverfolgbarkeit von Verarbeitungen und die Beschränkung des Zugriffs auf Personen, die unbedingt über diese Informationen verfügen müssen, gewährleistet werden;
- eindeutige Festlegung der Verantwortlichkeiten derer, die Zugang zu personenbezogenen Daten von Bediensteten gewähren.

Brüssel, den 6. Dezember 2012
(**unterzeichnet**)
Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter