Stellungnahme zu einer Meldung des Datenschutzbeauftragten der Europäischen Kommission für eine Vorabkontrolle des „physischen Zugangskontrollsystems (PACS)“ der Kommission: „PSG Projet de Sécurisation Globale (Projekt „Umfassende Sicherung“)“

Brüssel, den 8. September 2011 (Fall 2010-0427)

1. Verfahren

Am 3. Juni 2010 erhielt der Europäische Datenschutzbeauftragte (**EDSB**) eine Meldung des Datenschutzbeauftragten (**DSB**) der Europäischen Kommission für eine Vorabkontrolle der Verarbeitung personenbezogener Daten im Zusammenhang mit der physischen Zugangskontrolle (PACS) der Kommission.

Darüber hinaus gingen beim EDSB einschlägige Unterlagen in Verbindung mit dieser Meldung ein, die im Intranet der Kommission bereitgestellt wurden, und zwar:

1. Konzeptpapier zum Projekt „Umfassende Sicherung“ (Projet de Sécurisation Globale, PSG)
2. Dokument zur Architektur des PSG
3. Bericht mit technologischen Optionen und Empfehlungen zum PSG
4. Anwendungsfälle des PSG physische Zugangskontrolle und Datenverarbeitungsszenarien
5. Infrastruktur und Anwendungen des PSG
6. Empfänger der Verarbeitung
7. Fristen für die Sperrung/Löschung von Daten
8. Informationen für Besucher
9. Informationen für neue Inhaber eines Dienstausweises

In Rahmen des PSG wurde eine Vorproduktionsstätte für eine ordnungsgemäße Validierung und Feinabstimmung der verschiedenen vorgeschlagenen technologischen Optionen, Systeme und Maßnahmen zur Umsetzung des neuen physischen Zugangskontrollsystems (PACS) bei der Europäischen Kommission für erforderlich erachtet. Im Einklang mit seiner üblichen Vorgehensweise bei der Vorabkontrolle von Pilotprojekten hat der EDSB ein Verfahren für Pilotprojekte/Vorproduktion im Zusammenhang mit neuen technologischen Verarbeitungsvorgängen ausgearbeitet, und die Kommission hat sich an dieses Verfahren gehalten.

Im Rahmen dieses Verfahrens hatte der EDSB die Europäische Kommission aufgefordert, nähere Informationen über die Vorproduktionsphase vorzulegen, und hat die Verarbeitungsvorgänge genau geprüft. In einem Schreiben vom 21. Oktober 2010, also noch

Postanschrift: Rue Wiertz 60 – 1047 Brüssel (Belgien)
Dienststelle: Rue Montoyer 63
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: +32 (02) 283 19 00 – Fax: +32 (02) 283 19 50

vor dem Anlaufen der Vorproduktionsphase, sprach der EDSB Empfehlungen zum Pilotprojekt aus. Ferner formulierte der EDSB Empfehlungen, die beim Vollbetrieb des Systems zu berücksichtigen sind, damit keine Widersprüche zwischen den beiden Phasen (Pilotphase und Vollbetrieb des Systems) auftreten, die sich auf den Schutz personenbezogener Daten auswirken könnten.

Die Vorproduktionsphase lief von November 2010 bis Mai 2011, und die Ergebnisse wurden dem EDSB von dem für die Verarbeitung Verantwortlichen am 1. Juli 2011 übermittelt.

Bei dieser Gelegenheit legte der DSB dem EDSB zwei weitere Dokumente vor, nämlich

- einen Bewertungsbericht über die Vorproduktionsstätte sowie
- die geänderten Anwendungsfälle (Szenarien) für das PSG – physische Zugangskontrolle und Datenverarbeitungsszenarien, in denen die nach dem Abschluss der Vorproduktionsphase beschlossenen Änderungen Berücksichtigung finden.

Die Schlussfolgerungen der Vorproduktionsphase wurden von dem für die Verarbeitung Verantwortlichen folgendermaßen zusammengefasst: „*Insgesamt wurden alle vorgesehenen Optionen und Technologien validiert und, wie geplant und konzipiert, als für den beabsichtigten Zweck und für die Erbringung der geforderten Funktionalitäten geeignet erachtet. Die wichtigsten Änderungen, die vorgenommen werden mussten oder noch erfolgen werden, betrafen den Betrieb oder die Ebene von Betriebsverfahren.*“

Nach dem Ende der Vorproduktionsphase blieb das PACS weiter in dem Gebäude in Betrieb, das als Vorproduktionsstätte genutzt worden war (L-56), wobei die für seinen Einsatz geltenden Bedingungen (Information, Aufbewahrung usw.) eingehalten wurden.

Die vorliegende Stellungnahme im Rahmen der Vorabkontrolle schließt die rechtliche Analyse des PACS ab. Angestrebt wird der umfassende Einsatz des PACS in den Gebäuden der Kommissionsdienststellen in Brüssel Anfang 2012.

Der EDSB stellt fest, dass sich die Europäische Kommission mit der Einbeziehung des EDSB in einer sehr frühen Phase des Meldeverfahrens, durch die Entwicklung einer Pilotphase und durch die Berücksichtigung aller relevanten Datenschutzaspekte in einer frühen Phase ihrer Arbeiten für ein datenschutzfreundliches Konzept bei der Durchführung der Verarbeitungen entschieden hat.

Der Entwurf der Stellungnahme wurde dem DSB am 29. Juli 2011 zur Kommentierung zugesandt; seine Bemerkungen gingen am 6. September 2011 beim EDSB ein.

2. Sachverhalt

Zweck des Systems ist die Umsetzung einer einheitlichen und kohärenten physischen Zugangskontrolle für die gesamte Kommission durch Erbringung aller geforderten physischen Sicherheitsfunktionen. Bei dem System handelt es sich um ein verteiltes PACS, das ausschließlich bei der physischen Zugangskontrolle und den damit verbundenen Sicherheitsfunktionen zum Einsatz kommt.

Im Einzelnen soll die physische Zugangskontrolle automatisiert und Verfahren und Sicherheitsvorkehrungen einheitlich durchgeführt werden. Hierzu werden die folgenden Ziele angestrebt und technologischen Lösungen umgesetzt:

- ein zentrales IT-Zugangskontrollsystem, das alle Funktionen der physischen Zugangskontrolle und Definitionen von Zugangsrechten ausführt und verwaltet und dabei insbesondere Folgendes zulässt:
    - einheitliche und gemeinsame Herstellung von Dienstausweisen und Definitionen von Zugangsrechten;
    - zentrale Definition von Zugangskontrolle, Überwachung und Ermittlung von Eindringlingen;
    - zentrale Überwachung von Eigentum, gestützt auf Standardtechnologien und gemeinsame Maßnahmen;
    - zentrale Verwaltung und Konfiguration der Endgeräte für die Zugangskontrolle.

- ein gemeinsamer Dienstausweis oder eine gemeinsame Identitätskarte mit effizienten und standardisierten Technologien, gestützt auf
    - einen kontaktlosen Proximity-Chip, der die RFID-Technologie nutzt und in vollem Umfang mit der internationalen Norm ISO/IEC 14443 Typ A übereinstimmt;
    - eine biometrische Überprüfung anhand von Fingerabdruckmerkmalen, die ausschließlich im chipinternen Speicher aufbewahrt werden;
    - eine Reihe verteilter physischer Sicherheitsausrüstungen (z. B. Steuereinheiten für Türen und Tore, Systeme für die Entdeckung und Prävention von Eindringlingen, Überwachungsgeräte, Videoüberwachung usw.).

Funktionen und Arbeitsweise des Systems sind im PSG-Konzeptpapier beschrieben; nähere Erläuterungen zu den Anwendungsfällen des Systems und den Datenverarbeitungsszenarien finden sich in dem Dokument „Physical Access Control Use Cases and Data Processing Scenarios“, das am Ende der Vorproduktionsphase aktualisiert wurde.

Wie in der Meldung dargestellt, werden mit den Verarbeitungen folgende **Zwecke** verfolgt:

1. Kontrolle und Schutz von Räumlichkeiten, Daten und Eigentum der Kommission;
2. Sicherheit und Schutz von Personen, die sich in den Räumlichkeiten der Kommission aufhalten;
3. Erfüllung von Sicherheitsanforderungen. Eine möglichst genaue Kenntnis der Zahl der sich noch in den Räumlichkeiten aufhaltenden Personen ist bei Evakuierungen und in anderen Notsituationen unerlässlich;
4. Einhaltung rechtlicher Vorgaben. Verhütung, Aufdeckung, Aufklärung und strafrechtliche Verfolgung von Verstößen gegen Disziplinar- oder Verwaltungsvorschriften oder von Straftaten (die Verarbeitung beruht allein auf der Datenerhebung und der anschließenden Weitergabe solcher Daten an die zuständigen Kommissionsstellen).

Eine **manuelle** Verarbeitung der Daten ist nicht oder nur in geringem Umfang geplant. In gewissem Umfang kann eine manuelle Verarbeitung der Daten erforderlich werden bei gelegentlicher Verwendung von rechtlichen oder ID-Dokumenten durch Mitarbeiter am Empfang und andere Beschäftigte, bei möglichen Ausnahmen, wenn das System nicht verfügbar ist, und wenn ein Eingreifen von Menschen zwingend erforderlich ist.

Laut Meldung bilden folgende Rechtsakte die **Rechtsgrundlage** der Verarbeitungen:

1. Mitteilung der Kommission über das neue System der Zugangskontrolle und Sicherung der Kommissionsgebäude K(2007)797 vom 14. März 2007;
2. Beschluss der Kommission zu den Aufgaben und Zuständigkeiten des Sicherheitsbüros K(94)2129 vom 8. September 1994;

3. Verantwortung der Kommission für den Schutz ihrer Bediensteten (Sicherheit und Gefahrenabwehr) und ihres Eigentums: Beschluss der Kommission über Alarmstufen und Krisenmanagement 2007/65/EG vom 15. Dezember 2006;
4. Sicherheitsbestimmungen der Kommission: Beschluss der Kommission zur Änderung ihrer Geschäftsordnung 2001/844/EG, EGKS, Euratom vom 29. November 2001.

Im Einklang mit den oben dargestellten Zwecken sind **betroffene Personen** alle Personen[1], die Zutritt zu den Räumlichkeiten der Kommission haben oder beantragen.

Betroffene Personen erhalten mindestens einen Dienstausweis einer der beiden folgenden Kategorien: personenbezogener Dienstausweis (mit Zugangsberechtigung) und gegebenenfalls ein Ausweis, der keine Zugangsberechtigung verleiht, aber Auskunft über die Funktion des Inhabers gibt:

1. Ausweis mit Zugangsberechtigung (je nach Kategorie betroffener Personen unterschiedlich gestaltet) – Dienstausweis, der je nach den spezifischen Zugangsrechten der Person zum Zugang berechtigt
2. funktionale Ausweise (je nach Funktion der betroffenen Person unterschiedlich gestaltet) – Ausweis, der nicht zum Zugang berechtigt, der aber Auskunft über bestimmte Funktionen gibt (z. B.: Sicherheitspersonal, Sicherheitsbeauftragte usw.).[2]

Laut Meldung werden (gegebenenfalls) folgende **Datenfelder** verarbeitet:

Vor- und Zuname*; Geburtsdatum*; Lichtbild; Staatsangehörigkeit*; Personalnummer (eindeutige Kennung: Personalnummer für Kommissionsbedienstete und interne DB-Nummer für andere Personen)*; Geschlecht*; Fingerabdruckmerkmale; Art der Verbindung zur Kommission: Beamter, Bediensteter auf Zeit, Auftragnehmer, Besucher, Vertragsbediensteter, Bediensteter im Ruhestand, Familienangehöriger eines Bediensteten usw.*; derzeitiger Beschäftigungsstatus: im aktiven Dienst, abgeordnet, längere Abwesenheit usw.*; Arbeitsstätte*; zuständige GD*; Büro und Tel/Fax-Nummer(n)*; E-Mail*; Vertragsnummer und Datum des Vertragsendes*; Nummer und Daten des Identitätsdokuments; Zugangsrechte; Funktionen in Verbindung mit Systemprivilegien und Aufgaben; Kontaktdaten des Arbeitgebers bei Unterauftragnehmern*; Kfz-Kennzeichen; besondere Daten im Zusammenhang mit Funktionen innerhalb der Kommission: Presse, diplomatische Vertretungen, Sicherheitspersonal, Sicherheitsbeauftragter usw.*; Informationen zum Passieren eines Zugangspunkts: Dienstausweisnummer, Datum, Uhrzeit, Richtung, ggf.

---

[1] Folgende Hauptkategorien werden aufgelistet:
1. Bedienstete der Kommission (Beamte oder gleichwertige Bedienstete);
2. Mitarbeiter externer Organisationen oder Unternehmen, mit denen die Kommission Einzelverträge unterzeichnet hat;
3. abgeordnete nationale Sachverständige (ANS, Sachverständige aus Mitgliedstaaten oder anderen Ländern);
4. Bedienstete anderer Organe oder Einrichtungen der EU;
5. Besucher;
6. Familienmitglieder von Kommissionsbediensteten;
7. Kommissionsbedienstete im Ruhestand;
8. akkreditierte Personen (Pressevertreter und Techniker, Vertreter der Mitgliedstaaten oder andere diplomatische Vertreter, die von den zuständigen Kommissionsdienststellen offiziell akkreditiert wurden);
9. Praktikanten der Kommission;
10. sonstige (alle andere Personen, die in keine der genannten Kategorien fallen und Zutritt zu Räumlichkeiten der Kommission benötigen oder beantragen).

[2] Zugangsrechte werden nach Kategorien betroffener Personen vergeben und der Zugangsbedarf anhand der geltenden Sicherheitsvorschriften der Kommission für den physischen Zugang bestimmt.

Alarmmeldungen und Videoaufnahmen usw.; Daten im Zusammenhang mit Wachleuten und der Durchführung von Patrouillenaufgaben und Vorgängen: Präsenz oder Inspektionen an bestimmten Kontrollpunkten, Bedienung von Sicherheitsausrüstung (z. B. Röntgengeräten) entsprechend den Anforderungen; Videobilder des entsprechenden Videoüberwachungssystems.[3]

Es werden nicht für alle betroffenen Personen alle Datenfelder verarbeitet oder aufbewahrt. Die verarbeiteten oder aufgezeichneten Felder stehen in unmittelbarem Zusammenhang mit der Art der Verbindung zwischen der betroffenen Person und der Kommission oder mit dem Grund für die Anwesenheit in den Räumlichkeiten der Kommission.

Sämtliche vorstehend genannten Daten gehören in die folgenden Hauptdatenkategorien: Identifizierungsdaten, Durchgangsdaten, Ausrüstungsdaten, Sicherheitsprofildaten, Systemdaten und Sperrdaten.

1. Identifizierungsdaten: im Wesentlichen Daten zur Identität der betroffenen Person und ihrer administrativen Situation (einschließlich Name, Personalnummer, Lichtbild, Ausweisnummer, Telefonnummer, Büroadresse, E-Mail-Adresse, Nummer des Personalausweises/Reisepasses, Fingerabdruckmerkmale);
2. Durchgangsdaten: hauptsächlich Daten über Kontrollen beim Zutritt und Ereignisse/Alarmmeldungen, die durch die Nutzung des Systems durch betroffene Personen ausgelöst wurden (einschließlich Ausweisnummer, Datum/Uhrzeit des Passierens der Zugangskontrollposten und der Kontrolle, Systemalarmmeldungen aufgrund von Zwischenfällen bei der Nutzung, in einer bestimmten Zone präsente Ausweise und Videodateien);
3. Ausrüstungsdaten: in der Hauptsache Daten zur eingesetzten Sicherheitsausrüstung (einschließlich Systemnamen, IP-Adressen, Standorten und Softwareversionen);
4. Sicherheitsprofildaten: im Wesentlichen Daten zur Definition und den Mitgliedern von Sicherheitsgruppen, allgemeine und spezifische Zugangsrechte, Standard- und Nichtstandard-Zugangszeiten, erlaubte Zugangszeiten, Sicherheitsfunktionen;
5. Systemdaten: hauptsächlich Daten zum Systemmanagement (einschließlich definierter Systemnutzer und Funktionen, System-Logs, Prüfpfade, ggf. Zugangszeit für interaktive Nutzer);
6. Sperrdaten: Daten zur Identifizierung betroffener Personen, denen der Zutritt zu einigen oder allen Räumlichkeiten der Kommission für eine bestimmte Zeit verwehrt ist. Diese Liste enthält lediglich folgende Datenfelder: Vor- und Zuname der betroffenen Person, Identifizierungsnummer (interne ID-Nummer, Nummer des Personalausweises oder andere verfügbare Nummer), Räumlichkeiten, zu denen die betroffene Person keinen Zutritt hat, Beginn und Ende des Zutrittsverbots.

Die **biometrische Erfassung** erfolgt freiwillig und wird hauptsächlich zur Erleichterung des Zugangs zu Räumlichkeiten außerhalb der normalen Arbeitszeiten und des Zugangs zu sensiblen Bereichen oder Bereichen mit Zutrittsbeschränkungen verwendet (z. B. Computerräume, Kommunikationskonfigurationsräume). Unter genau definierten Umständen aufgrund einer besonderen Sicherheitslage (z. B. hohe Alarmstufen, Zutritt zu Bereichen mit Geheimhaltung usw.) kann eine biometrische Überprüfung vorgeschrieben werden und ist dann fallweise zu bewerten und durchzuführen.

[3] Daten mit (*): Datenquelle ist hier Sysper2/Comref für Kommissionsbedienstete oder gleichwertige Bedienstete, ORIANA für externes Personal und e-Pass für Besucher. Alle anderen Daten werden unmittelbar vom System generiert oder erhoben.

Zur Vermeidung von Ausfällen und aus Gründen der Nutzerfreundlichkeit werden immer Abdrücke von zwei Fingern genommen, nach Möglichkeit einer von jeder Hand. Für die Erfassung wird jeweils der Zeige- oder Mittelfinger vorgeschlagen, doch kann der Nutzer selber entscheiden, von welchen Fingern er Abdrücke nehmen lässt.

Die Überprüfung besteht im Wesentlichen aus einer 1:1-(Ein-zu-eins-)Überprüfung, d. h., die in dem Ausweis der betroffenen Person gespeicherten Merkmale werden mit den gescannten Merkmalen vor Ort von dem biometrischen Lesegerät/Scanner auf Übereinstimmung überprüft. Der Abgleich wird vor Ort von dem biometrischen Lesegerät (*Match on Reader*) vorgenommen.

Die **Empfänger** der verarbeiteten Daten lassen sich in folgenden Hauptkategorien zusammenfassen:
- Systemadministratoren (HR.DS.4[4]);
- Systembetreiber (HR.DS.4);
- Sicherheitsdienste und Sicherheitsbeauftragte (HR.DS.RA, HR.DS.1, HR.DS.2, HR.DS.4, HR.DS.6);
- interne oder externe Untersuchungsstellen (offizielle Untersuchungsstellen: HR.DS.RA, HR.DS.1, HR.IDOC, OLAF, EDSB, EuGH);
- Verwalter von Zugangsrechten und Profilen;
- Validierer (Personen, die das System benutzen, um Zugang zu den Räumlichkeiten der Kommission zu erhalten);[5]
- IT-Anwendung(en) (derzeit SYSPER: Das Lichtbild der betroffenen Person kann auf deren Antrag übertragen werden);
- Stellen, die Anträge validieren (HR.DS.4, HR.DS.6, GD COMM, Chefs d'immeuble);
- örtliche Betreiber (LSO usw.).

Zur **Aufbewahrungsregelung** besagt die Meldung, dass für die genannten Datenkategorien folgende Aufbewahrungsfristen gelten:
1. Identifizierungsdaten: Die Daten werden bis zur Beendigung der Verbindung zwischen der betroffenen Person und der Kommission sowie weitere sechs Monate aufbewahrt; die Frist ist von der Art der Verbindung abhängig (z. B. Bediensteter: Ende des Vertrags plus sechs Monate; Besucher: Ende des Besuchs plus sechs Monate usw.);
2. Durchgangsdaten: Die Aufbewahrungsfrist beträgt sechs Monate (einschließlich Videodaten, damit eine Verknüpfung mit anderen Durchgangsdaten möglich ist);
3. Sicherheitsprofildaten: Hier ist keine Frist festgelegt (die Daten werden so lange aufbewahrt, wie es für das reibungslose Funktionieren des Systems erforderlich ist);[6]

---

[4] Generaldirektion Humanressourcen und Sicherheit, Direktion Sicherheit, Physische Sicherheit.

[5] In der ersten Fassung der Meldung war von „Endnutzern“ als Empfängern die Rede. Der für die Verarbeitung Verantwortliche stellte jedoch klar, dass im Zusammenhang mit der Meldung diese Endnutzer als Nutzer zu gelten haben, die die IT-Schnittstellen des Systems als normale IT-Endnutzer nutzen oder damit interagieren. Dies ist der Fall bei der Validierung oder Visualisierung von Besuchsanträgen durch interne Nutzer. Diese Nutzer haben Zugriff auf Daten, die von den Besuchern über sich selber und ihre Besuche eingegeben wurden; daher wurden sie in Validierer umbenannt.

[6] Sicherheitsprofildaten sind eigentlich keine personenbezogenen Daten. Sie werden im Wesentlichen als Gruppen von Eingängen, Zugangszeiträumen oder Zugangsgenehmigungen beschrieben, die das System zur Verwaltung von Zugangsgenehmigungen und Zeitplänen benötigt. Dies lässt sich mit Zugangsgruppen und entsprechenden Genehmigungen vergleichen, die in IT-Systemen definiert sind, um den Zugriff auf Dateien und Ressourcen zu ermöglichen. Typische Gruppen sind:
   a. ALL-BXL-BUILDINGS-Entrances – eine Gruppe mit allen Haupteingängen in Gebäuden in Brüssel;
   b. ACCESS-24h-7d – eine Gruppe, die jederzeit Zutritt gewährt;
   c. ACCESS-08-20-WeekDays – eine Gruppe, die Zutritt nur während der normalen Arbeitsstunden gewährt;

4. Systemdaten: Die Daten werden ein Jahr lang aufbewahrt;
5. Sperrdaten (Personen auf einer Ausschlussliste): Über die Datenaufbewahrung entscheidet die zuständige Stelle der Kommission, also die Stelle, die den Ausschluss beschlossen hat. Daten in dieser Kategorie werden nach Genehmigung der zuständigen Stelle der Kommission vollständig aus dem System gelöscht.

Daten, bei denen die Aufbewahrungsfristen abgelaufen sind, werden
1. auf ein Ersatzsystem kopiert und dort bei Bedarf anonymisiert und zur statistischen Zwecken aggregiert: Data Warehouse oder
2. aus den operationellen IT-Systemen vollständig gelöscht.

Die Anonymisierung der Daten wird nach folgendem Verfahren vorgenommen:
a. Einmal monatlich verbindet sich das Data Warehouse-System mit der operationellen Datenbank;
b. in dem dann ablaufenden Prozess werden die Datensätze (wie Ausweisproduktion, Durchgangskontrollen, bekannte Personen usw.) ausgewählt, deren Aufbewahrungsfrist abgelaufen ist;
c. es werden anhand der ausgewählten Datensätze die für die Aggregierung erforderlichen Berechnungen durchgeführt (z. B. wie viele Durchgänge, wie viele Durchgänge pro Tag/Stunde/Monat, wie oft wurde der Zutritt verweigert, wie oft wurde die Ausstellung eines Ausweises verweigert, wie viele Ausweise wurden gedruckt usw.);
d. die berechneten Werte werden in die Datenbank des Data Warehouse eingegeben;
e. nach dieser Verarbeitung werden alle ausgewählten Daten, deren Aufbewahrungsfrist abgelaufen war, aus der operationellen Datenbank gelöscht.

Die Fristen und Verfahren für die Datenaufbewahrung gelten für alle Daten über betroffene Personen, die Zutritt zu den unter das System fallenden Räumlichkeiten der Kommission haben oder sich zu diesem Zweck registrieren lassen.

Sonderfälle:
1. Daten, die in den örtlichen Steuereinheiten für Türen aufbewahrt werden, werden vor ihrer Übermittlung an das Zentralsystem weniger als eine Woche gespeichert oder im Round-Robin-Modus überschrieben;
2. an den Erfassungsgeräten werden Bilder und Fingerabdruckmerkmale im Hauptspeicher oder im Swap-Space zwischengespeichert. Der Zwischenspeicherplatz wird beim Hochfahren geleert;
3. Fingerabdruckmerkmale (falls verwendet) werden auf dem in den Ausweis der betroffenen Person eingebauten RFID-Chip gespeichert, und zwar für die gesamte Gültigkeitsdauer des Ausweises (geplant sind zehn Jahre).

Zu den **Rechten** der betroffenen Person besagt die Meldung, dass betroffene Personen über ihre Rechte, verfügbare Ansprechpartner, Kommunikationskanäle und bestehende Verfahren unterrichtet werden, wie sie in den oben genannten Unterlagen und Informationsquellen beschrieben werden.

---

d. Specific-Zone-ClassII – eine Gruppe mit allen Hauptzugängen (Eingängen) zu dem besonderen Bereich;
e. usw.

Es handelt sich um permanente Systemdaten, daher wurde auch keine Aufbewahrungsfrist festgelegt. Diese Gruppen werden nach ihrer Schaffung so lange aufbewahrt, wie es erforderlich ist (fast für immer). Wenn zu diesen Gruppen Ausweise (Kennungen) gehören, gilt für die entsprechenden Ausweisdaten und Daten der betroffenen Person die übliche Aufbewahrungsfrist; gehören keine Ausweise dazu (leere Gruppe), besteht auch keine Verknüpfung mit personenbezogenen Daten.

Auf der Ausschlussliste stehende Personen (Sperrdaten) werden von der für den Ausschluss zuständigen Stelle der Kommission (Direktion Sicherheit, IDOC oder Ärztlicher Dienst) informiert. Hierbei verfügt der für die Verarbeitung der Zugangskontrolle Verantwortliche über keinerlei Informationen zu den Gründen oder der Dauer des Ausschlusses betroffener Personen und ist bei der Verarbeitung dieser Daten im Namen der betreffenden Kommissionsdienststelle tätig. Auf Ersuchen des Direktors der Direktion Sicherheit aktualisiert er die Liste und aktiviert oder deaktiviert die Ausschlüsse wie gewünscht. Der EDSB weist darauf hin, dass dieser Ausschluss nicht Bestandteil der hier analysierten Meldung ist.

Der **Informationspflicht** wird mit folgenden Unterlagen Genüge getan:
- eine Informationsbroschüre (oder Gleichwertiges) wendet sich an neue Ausweisinhaber und wird bei der Aushändigung des Ausweises überreicht („Information for New Badge Holder“);
- eine Informationsbroschüre (oder Gleichwertiges) wendet sich an Besucher und wird am Empfang der Gebäude überreicht („Information to Visitors“);
- fest angebrachte Informationstafeln zur Aufklärung in den RFID-Lesezonen, im Wesentlichen in den Eingangsbereichen der Gebäude (inhaltlich ist hier die Information vorgesehen, die in Anhang II des „PSG Technological Options and Recommendations Report“ enthalten ist);
- fest angebrachte Informationstafeln in Videoaufnahmezonen, im Wesentlichen in den Eingangsbereichen der Gebäude;
- auf den Intranetseiten der Direktion Sicherheit Informationen, die denen in der vorstehend genannten Broschüre entsprechen;
- auf der Europa-Website und bei Bereitstellung weltweiter Internetregistrierungsformulare Informationen, die denen in der vorstehend beschriebenen Broschüre für Besucher entsprechen;
- angemessene Informationen und Beratung zu den Anforderungen an die Verarbeitung personenbezogener Daten auf der Homepage oder den einschlägigen Websites der Webschnittstellen der Nutzer/Betreiber der jeweiligen eingesetzten Systeme;
- bei Untersuchungen, die einen Zugriff auf Daten der physischen Zugangskontrollsysteme erfordern, wird die Person stets nach den für die Untersuchungen geltenden Regeln und durch die für die Untersuchung zuständige Dienststelle informiert.

Zur **Datenspeicherung** besagt die Meldung Folgendes:

Alle operationellen oder aktiven Daten werden auf besonderen geclusterten Servern mit dedizierten Datenspeichern (Platten) aufbewahrt. Die Systeme sind in den Datenzentren der Kommission untergebracht.

Werden personenbezogene Daten aus den Hauptsystemen herausverbracht (z. B. Sicherungen), werden sie vor der Übermittlung verschlüsselt. Die Sicherungen erfolgen in den zentralen Bandsystemen der Datenzentren der Kommission.

Aus Gründen der Notfallplanung (Business Continuity Planning) und zur Bewältigung eventueller Ausfälle von Zentralservern wird ein verschlüsselter Datensatz auf dedizierte Server im Computerraum der Direktion Sicherheit kopiert.

Die Zwischenspeicherung von Daten durch Infrastrukturserver ist mit Blick auf Anforderungen an Übermittlung oder Zwischenverarbeitung vorgesehen; dies betrifft hauptsächlich E-Mail-Übermittlungen (Server-Hopping), Daten, die vor Übermittlungen von externen Website erhoben wurden, Daten, die von betroffenen Personen an automatisierten

Registrierungs- und Ausweisausgabegeräten eingegeben wurden, optisches Lesen von ID-Dokumenten usw.

Jede örtliche Sicherheitsausrüstung (Steuereinheiten für Türen, Schlüsselkästen, IP-Kameras, Monitoring-PCs oder PCs für den Empfang usw.), die für die Zugangskontrolle zuständig ist oder zur Überwachung eingesetzt wird, enthält eine in ihrem örtlichen Speicher gespeicherte Kopie der erforderlichen Zugangsgenehmigungen. Diese Ausrüstungen sind physisch getrennt und der Öffentlichkeit nicht zugänglich. Zugriff auf die gespeicherten Daten haben nur befugte Personen.

Fingerabdruckmerkmale werden nach der Erfassung ausschließlich auf dem Chip im Ausweis der betroffenen Person gespeichert; die Erfassung erfolgt mithilfe eines eigenständigen Systems. Werden für die Zugangskontrolle Fingerabdrücke verwendet, erfolgt am Ausweislesegerät eine (1:1-)Überprüfung durch einen Vergleich des Ausweisinhalts mit dem gerade gelesenen Fingerabdruck; eine lokale oder zentrale Speicherung findet nicht statt.

Die Meldung sieht verschiedene **Sicherheitsmaßnahmen** vor:

[...]

3. Rechtliche Analyse

3.1. Vorabkontrolle

Anwendbarkeit der Verordnung (EG) Nr. 45/2001 („Verordnung"): Gegenstand dieser Stellungnahme zur Vorabkontrolle ist die Verarbeitung personenbezogener Daten durch die Europäische Kommission, insbesondere die Direktion Sicherheit.

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 Anwendung auf die Verarbeitung personenbezogener Daten *„durch alle Organe und Einrichtungen der Gemeinschaft […], soweit die Verarbeitung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Gemeinschaftsrechts fallen"*[7]. Aus den nachstehend dargelegten Gründen sind alle Elemente vorhanden, die die Anwendung der Verordnung auslösen.

Erstens werden *personenbezogene Daten* gemäß der Begriffsbestimmung in Artikel 2 Buchstabe a der Verordnung (EG) Nr. 45/2001 erhoben und weiter verarbeitet. Zweitens werden die erhobenen personenbezogenen Daten einer in Artikel 2 Buchstabe b der Verordnung (EG) Nr. 45/2001 definierten *„automatisierten"* Verarbeitung sowie manuellen Verarbeitungsvorgängen unterzogen. Es werden nämlich personenbezogene Daten wie persönliche Identifizierungsdaten einschließlich Fingerabdrücke erhoben und einer „automatisierten" Verarbeitung unterzogen, beispielsweise wenn der Informationsdienst Fingerabdruckvorlagen abnimmt. Schließlich wird die Verarbeitung von einem Organ, im vorliegenden Fall von der Europäischen Kommission, im Rahmen von Tätigkeiten vorgenommen, die in den Anwendungsbereich des EU-Rechts fallen (Artikel 3 Absatz 1 der Verordnung).

[7] Siehe Artikel 3 Absatz 2 und Absatz 1 der Verordnung (EG) Nr. 45/2001.

Begründung der Vorabkontrolle: In Artikel 27 Absatz 1 der Verordnung (EG) Nr. 45/2001 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. Der EDSB ist der Ansicht[8], dass das Vorhandensein und die Verarbeitung einiger biometrischer Daten über Lichtbilder hinaus (wie im vorliegenden Fall, in dem biometrische Fingerabdrücke genommen werden) besondere Risiken für die Rechte und Freiheiten betroffener Personen darstellen. Seine Ansicht stützt sich im Wesentlichen auf die aufgrund einiger diesen Daten innewohnenden Merkmale höchst heikle Natur biometrischer Daten. So verändern beispielsweise biometrische Daten die Beziehung zwischen Körper und Identität unwiderruflich, da sie die Merkmale des menschlichen Körpers „maschinenlesbar“ und einer weiteren Nutzung zugänglich machen. Diese Risiken rechtfertigen eine Vorabkontrolle der Datenverarbeitung durch den EDSB, der die Einhaltung strenger Sicherheitsvorkehrungen zu überprüfen hat.

Darüber hinaus bringt nach Ansicht des EDSB in einigen besonderen Fällen die Aufnahme der RFID-Technologie (der in den Ausweis eingebaute RFID-Chip) in ein Zugangskontrollsystem besondere Risiken mit sich. Daher fällt die vorliegende Vorabkontrolle unter Artikel 27 Absatz 1 der Verordnung.

Wie bereits erwähnt, gehören nach Ansicht der EDSB das Verfahren bei Ermittlungen sowie Ausschlüsse nicht zum Gegenstand dieser Meldung zur Vorabkontrolle.

Fristen: Da die Vorabkontrolle dazu dient, sich mit Situationen zu befassen, die gewisse Risiken beinhalten können, sollte der EDSB seine Stellungnahme vor Aufnahme der Verarbeitungen abgeben. In der vorliegenden Stellungnahme geht es um eine **Vorabkontrolle**. Mit der Verarbeitung sollte also erst begonnen werden, wenn der EDSB offiziell seine Zustimmung erteilt hat.

Die Meldung ging am 3. Juni 2010 ein. Gemäß Artikel 27 Absatz 4 der Verordnung (EG) Nr. 45/2001 wurde der Zeitraum von zwei Monaten, innerhalb dessen der EDSB seine Stellungnahme abzugeben hat, für insgesamt 355 Tage, um zusätzliche Auskünfte einzuholen, sowie während der Vorproduktionsphase ausgesetzt; darüber hinaus wurden 39 Tage für Kommentare zum Entwurf der Stellungnahme eingeräumt. Die Stellungnahme muss daher spätestens am 13. September 2011 angenommen werden.

3.2. Rechtmäßigkeit der Verarbeitung

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dafür rechtliche Gründe nach Artikel 5 der Verordnung (EG) Nr. 45/2001 vorliegen.

In Artikel 5 der Verordnung (EG) Nr. 45/2001 werden verschiedene Gründe aufgeführt; die im vorliegenden Fall zur Vorabkontrolle gemeldete Verarbeitung fällt unter Artikel 5 Buchstabe a, dem zufolge Daten verarbeitet werden dürfen, 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*“. In Auslegung von Artikel 5 Buchstabe a heißt es in Erwägungsgrund 27: „*Die Verarbeitung personenbezogener Daten […] zur Wahrnehmung einer Aufgabe im öffentlichen Interesse schließt die Verarbeitung personenbezogener Daten*

[8] Siehe die Fälle 2007-635 vom 7. April 2008 und 2008-223 vom 30. Juni 2008, abzurufen von der Website des EDSB.

ein, die für die Verwaltung und das Funktionieren dieser Organe und Einrichtungen erforderlich ist."

Bei der Prüfung der Frage, ob Verarbeitungen im Einklang mit Artikel 5 Buchstabe a der Verordnung (EG) Nr. 45/2001 stehen, sind drei Elemente zu berücksichtigen. Es geht darum, ob erstens der Vertrag oder andere Rechtsinstrumente die Datenverarbeitungen vorsehen, zweitens die Verarbeitungen im öffentlichen Interesse liegen und drittens die Verarbeitungen für die Wahrnehmung dieser Aufgabe tatsächlich erforderlich sind (Erforderlichkeitstest). Diese drei Anforderungen sind natürlich eng miteinander verknüpft.

* Als **Rechtsgrundlage** für die Verarbeitung gelten:

  - Mitteilung der Kommission über das neue System der Zugangskontrolle und Sicherung der Kommissionsgebäude K(2007)797 vom 14. März 2007;
  - Beschluss der Kommission zu den Aufgaben und Zuständigkeiten des Sicherheitsbüros K(94)2129 vom 8. September 1994;
  - Verantwortung der Kommission für den Schutz ihrer Bediensteten (Sicherheit und Gefahrenabwehr) und ihre Eigentums: Beschluss der Kommission über Alarmstufen und Krisenmanagement 2007/65/EG vom 15. Dezember 2006;
  - Sicherheitsbestimmungen der Kommission: Beschluss der Kommission zur Änderung ihrer Geschäftsordnung 2001/844/EG, EGKS, Euratom vom 29. November 2001.

* Die Verarbeitungen werden **in legitimer Ausübung öffentlicher Gewalt** durchgeführt. Der EDSB stellt fest, dass die Kommission die Verarbeitung in legitimer Ausübung ihrer öffentlichen Gewalt vornimmt, gestützt auf die vorstehend genannten Rechtsakte, die auf der Grundlage des Beamtenstatuts erlassen wurden.

* Zur Erforderlichkeit der Verarbeitung (**Erforderlichkeitstest**) bestimmt Artikel 5 Buchstabe a der Verordnung (EG) Nr. 45/2001, wie bereits ausgeführt, dass die Verarbeitung „*für die Wahrnehmung einer Aufgabe erforderlich*" sein muss. Hierzu heißt es in Erwägungsgrund 27 der Verordnung (EG) Nr. 45/2001: „*Die Verarbeitung personenbezogener Daten […] zur Wahrnehmung einer Aufgabe im öffentlichen Interesse schließt die Verarbeitung personenbezogener Daten ein, die für die Verwaltung und das Funktionieren dieser Organe und Einrichtungen erforderlich ist.*"

Zweck der Verarbeitungen sind der physische Schutz der Bediensteten der Kommission, ihrer Daten und ihres Eigentums, die Sicherheitsbedingungen für die Beschäftigten (auch für Evakuierungen und Notfälle) und für Besucher sowie die Zugangskontrolle zum Eigentum der Kommission.

In Anbetracht der Relevanz dieser Interessen könnte die Europäische Kommission es durchaus für erforderlich halten, besondere Sicherheitsvorkehrungen einschließlich des Aufbaus strenger Zugangskontrollsysteme zu treffen und die Untersuchung von Sicherheitszwischenfällen durch IDOC und OLAF zuzulassen.

Daher kann nach Auffassung des EDSB die Umsetzung strenger Zugangskontrollsysteme, die die Verarbeitung personenbezogener Daten nach sich zieht, im vorliegenden Fall vernünftigerweise als notwendige interne Kontrollmaßnahme zum Schutz von Daten und anderer Interessen der EU gelten.

3.3. Datenqualität

Zweckentsprechung, 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, dafür erheblich sein und nicht darüber hinausgehen. Dies wird als Grundsatz der Datenqualität bezeichnet.

Der EDSB hat die gegebenenfalls zu verarbeitenden Datenfelder analysiert und ist zu dem Schluss gekommen, dass die derzeitige Liste von Datenfeldern der Verordnung (EG) Nr. 45/2001 entspricht. Ferner wurde ausgeführt, dass nicht für alle betroffenen Personen alle Datenfelder verarbeitet oder aufbewahrt werden. Die verarbeiteten oder aufgezeichneten Felder stehen in unmittelbarem Zusammenhang mit der Art der Verbindung zwischen der betroffenen Person und der Kommission oder mit dem Grund für die Anwesenheit in den Räumlichkeiten der Kommission.

Zu biometrischen Daten merkt der EDSB an, dass nur Personen mit besonderen Zugangsrechten im System erfasst und nur ihnen Fingerabdrücke abgenommen werden. Zur Vermeidung von Ausfällen und aus Gründen der Nutzerfreundlichkeit werden immer Abdrücke von zwei Fingern genommen, nach Möglichkeit einer von jeder Hand. Für die Erfassung wird jeweils der Zeige- oder Mittelfinger vorgeschlagen, doch kann der Nutzer selber entscheiden, von welchen Fingern er Abdrücke nehmen lässt. Die Art der erhobenen Daten, bei denen es sich im Wesentlichen um Fingerabdruckvorlagen von zwei Fingern und die dazu gehörenden Identifizierungsdaten handelt, entspricht den Daten, die für ein auf der Verarbeitung biometrischer Daten beruhendes Zugangskontrollsystem erforderlich sind. Damit entsprechen nach Ansicht des EDSB die erhobenen Daten den Zwecken der Verarbeitung und sind dafür erheblich.

Die Verwendung von Fingerabdruckmerkmalen als biometrische Validierungsmethode kann als zweckentsprechend gelten.

Die Überprüfung besteht im Wesentlichen aus einer 1:1-(Ein-zu-eins-)Überprüfung, d. h., die in dem Ausweis der betroffenen Person gespeicherten Merkmale werden mit den gescannten Merkmalen vor Ort von dem biometrischen Lesegerät/Scanner auf Übereinstimmung überprüft. Der Abgleich wird vor Ort von dem biometrischen Lesegerät (*Match on Reader*) vorgenommen. Nach Meinung des EDSB bedeutet diese Überprüfung einen geringeren Eingriff in die Privatsphäre, als es ein Vergleich mit Referenzmaterial in einer Datenbank wäre.

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. Die Frage der Rechtmäßigkeit wurde bereits behandelt (siehe Abschnitt 2.2.2). Der Aspekt der Verarbeitung nach Treu und Glauben hängt eng damit zusammen, welche Informationen den betroffenen Personen zur Verfügung gestellt werden (siehe hierzu Näheres in Abschnitt 2.2.9).

Sachliche Richtigkeit: Nach Artikel 4 Absatz 1 Buchstabe d der Verordnung müssen personenbezogene Daten *„sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht*“ sein, 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 personenbezogenen Daten biometrische Daten, die zu Zugangskontrollzwecken verwendet werden. Einige Schlüsselmerkmale biometrischer Systeme wirken sich unmittelbar auf das Ausmaß der sachlichen Richtigkeit der entweder in der Erfassungs- oder der Identifizierungsphase eines solchen Systems generierten Daten aus. Je nach der Ausformung des biometrischen Systems (mit diesen Schlüsselelementen oder ohne sie) ist die sachliche Richtigkeit der Daten betroffen oder nicht. Der EDSB hat sich in früheren Stellungnahmen zu Zugangskontrollen mit den Regeln für den Einsatz biometrischer Systeme befasst.[9] Im Folgenden sollen diese Schlüsselelemente kurz beschrieben und der Frage nachgegangen werden, inwieweit sie in dem zu prüfenden biometrischen IT-Zugangskontrollsystem berücksichtigt wurden.

Erstens muss in der Erfassungsphase nach alternativen Möglichkeiten für die Identifizierung von Personen gesucht werden, die z. B. wegen beschädigter Fingerkuppen für eine Erfassung nicht infrage kommen. Dies wird üblicherweise als ***„Ausweichverfahren“*** bezeichnet.[10]

Zur eigentlichen Erfassungsphase beschloss der für die Verarbeitung Verantwortliche nach der Vorproduktionsphase, in das Erfassungsverfahren eine Überprüfung der jeweils erfassten Fingerabdrücke vor der Fertigstellung und Aushändigung der Ausweise aufzunehmen, um die Wahrscheinlichkeit späterer Ablehnungen (*Falschrückweisungen*) möglichst gering zu halten. Nach Aussage der Kommission schafft diese Überprüfung in Verbindung mit der Fingerkuppenscanning-Qualitätsmetrik, die jede professionelle Erfassungssoftware bietet, die Voraussetzungen, um spätere Rückweisungen auf ein Mindestmaß zu reduzieren.

Stehen ferner nach der Vorproduktionsphase keine biometrischen Daten zur Verfügung oder ist eine biometrische Überprüfung zu einer besonderen Überprüfungszeit nicht möglich, stehen je nach den Gegebenheiten des Einzelfalls und den spezifischen Zugangskontrollüberprüfungsbedingungen folgende *Ausweichlösungen* zur Verfügung:

1. Gesichtserkennung des Ausweisinhabers durch eine vertrauenswürdige Person (z. B. Kontrollraummitarbeiter, Sicherheitspersonal, Zonen-/Bereichsverantwortlicher usw.) aus der Ferne oder vor Ort und mit der Befugnis, Zutritt zu erteilen;
2. für den Zutritt zu weniger sensiblen Bereichen kann ein besonderer geheimer PIN-Code statt der Überprüfung biometrischer Fingerabdruckmerkmale vorgeschlagen werden.

Nach Ansicht des EDSB sind diese Ausweichverfahren zufriedenstellend, doch erinnert er die Kommission daran, dass bei diesen Maßnahmen das Sicherheitsniveaurisiko des Gebäudes zu berücksichtigen ist und außerdem die Rechte der betroffenen Person(en) zu wahren sind.

Darüber hinaus schlägt der EDSB vor, dass die Kommission im Hinblick auf Falschrückweisungen ein Verfahren entwickelt, mit dem das Problem ohne eine allzu große Belastung der Personen gelöst wird. Mit anderen Worten: Das Alternativverfahren sollte hinreichend einfache Lösungen für das Problem der Fehlidentifizierung und Zurückweisung bieten. In diesem Zusammenhang würde es der EDSB begrüßen, wenn die Kommission die Erfassung in regelmäßigen Abständen erneuern würde, um ein hohes Maß an Datenqualität aufrechtzuerhalten. Die Festlegung eines Zeitraums, nach dem die Erfassung erneuert wird, ist durchaus gerechtfertigt, da sich biometrische Merkmale und hier vor allem Fingerabdrücke im Laufe des Lebens einer betroffenen Person durchaus verändern können. Weitere Gründe

[9] Siehe beispielsweise die Fälle 2007-0635 und 2008-0223 zur (physikalischen und logischen) Zugangskontrolle bei OLAF.

[10] Eine Darstellung der Datenschutzgrundsätze, die für Ausweichverfahren gelten, findet sich in der Stellungnahme vom 13. Oktober 2006 zu dem Entwurf einer Verordnung (EG) des Rates zur Festlegung der Form der Ausweise für die Mitglieder und Bediensteten der Organe, ABl. C 313 vom 20.12.2006, S. 36.

wären mögliche Veränderungen in der Hautstruktur des betreffenden Fingers des Nutzers im Zeitverlauf sowie die Qualität der erfassten Fingerabdruckvorlage. Dieser Zeitraum für die erneute Erfassung könnte nach zwei Jahren des Betriebs des neuen Systems und gestützt auf die bis dahin von der Kommission mit dem System gesammelten Erfahrungen festgelegt und umgesetzt werden.

Schließlich werden die Merkmale nur, wie ursprünglich angekündigt, im internen Speicherchip gespeichert, und die Überprüfung – Übereinstimmung der Merkmale, 1:1-Überprüfung – erfolgt lokal mithilfe des biometrischen Lesegeräts. Der EDSB begrüßt dieses System, mit dem sich weitere unrechtmäßige Verwendungen und Phishing-Vorgänge vermeiden lassen, die häufig beim Einsatz von Datenbanken auftreten.[11]

3.4. Datenaufbewahrung

Gemäß Artikel 4 Absatz 1 Buchstabe e der Verordnung (EG) Nr. 45/2001 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. Dies wird im Allgemeinen als „Grundsatz der Aufbewahrung“ bezeichnet.

Nach Angaben der Kommission werden Identifizierungsdaten sechs Monate und Systemdaten ein Jahr lang aufbewahrt.

- Zu den Identifizierungsdaten merkt der EDSB an, dass die gemäß Artikel 4 der Verordnung (EG) Nr. 45/2001 festgelegten Fristen sowie die Aufbewahrungsfristen für die verschiedenen Datenkategorien als angemessen gelten können.

- Im Hinblick auf die Aufbewahrung von Systemdaten geht der EDSB davon aus, dass es sich bei diesen Daten um Zugangsprotokolle handelt. Der EDSB vertritt hier die Auffassung, dass die Europäische Kommission nach einem Jahr des Systembetriebs die Notwendigkeit einer Aufbewahrung der Daten über diesen Zeitraum bewerten und bei Bedarf diese Frist anpassen sollte. In anderen geprüften Fällen[12] vertrat der EDSB die Ansicht, dass eine Aufbewahrungsfrist von drei Monaten als angemessen gelten könnte.

Außerdem werden Fingerabdruckmerkmale (falls verwendet) dauerhaft auf dem in den Ausweis der betroffenen Person eingebauten RFID-Chip gespeichert, und zwar für die gesamte Gültigkeitsdauer des Ausweises (geplant sind zehn Jahre). Mit dieser Aufbewahrungsfrist ist der EDSB einverstanden.

3.5. Datenübermittlung

Die Meldung und das Dokument „Empfänger der Verarbeitung“ besagen, dass verschiedene Empfänger innerhalb der GD HR DS Zugriff auf die Daten haben können. Im Verlauf ihrer Untersuchungen können sowohl interne Dienststellen der GD HR DS als auch externe Stellen (IDOC, OLAF, EDPS, EuGH) auf die Daten zugreifen.

---

[11] Siehe Stellungnahme zu einer Meldung des Datenschutzbeauftragten der Europäischen Zentralbank zur Vorabkontrolle der Erweiterung eines bereits bestehenden Zugangskontrollsystems durch eine Iris-Scan-Technologie für Hochsicherheitsbereiche, 14. Februar 2008 (2007-501), abzurufen von der Website des EDSB.

[12] Siehe die weiter oben genannten OLAF-Fälle.

Der EDSB erinnert daran, dass nach Artikel 7 Absatz 1 der Verordnung (EG) Nr. 45/2001 personenbezogene Daten nur übermittelt werden, wenn sie „*für die rechtmäßige Erfüllung der Aufgaben erforderlich sind, die in den Zuständigkeitsbereich des Empfängers fallen*". Zur Einhaltung dieser Vorschriften hat HR DS bei der Übermittlung personenbezogener Daten zu gewährleisten, dass 1) der Empfänger die entsprechende Zuständigkeit hat und 2) die Übermittlung notwendig ist. Nach Auffassung des EDSB trifft dies bei der Meldung von Sicherheitszwischenfällen im vorliegenden Fall zu. Ob eine Übermittlung diese Anforderungen erfüllt, wird jedoch fallweise zu prüfen sein. Außerdem ist gemäß Artikel 7 der Verordnung (EG) Nr. 45/2001 dem Empfänger ein Vermerk zuzusenden, in dem er darüber in Kenntnis gesetzt wird, dass personenbezogene Daten nur für die Zwecke verarbeitet werden dürfen, für die sie übermittelt wurden.

Weitere Datenübermittlungen nach Artikel 8 oder 9 sind nicht vorgesehen. Es besteht jedoch die Möglichkeit, dass Daten zur Verhütung von Straftaten oder zu Ermittlungen an nationale Strafverfolgungsbehörden weitergegeben werden. Für diesen Fall unterstreicht der EDSB, dass Artikel 8 der Verordnung (EG) Nr. 45/2001 besagt, dass personenbezogene Daten nur übermittelt werden, „*a) wenn der Empfänger nachweist, dass die Daten für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder zur Ausübung der öffentlichen Gewalt gehört, erforderlich sind[,] oder b) wenn der Empfänger die Notwendigkeit der Datenübermittlung nachweist und kein Grund zu der Annahme besteht, dass die berechtigten Interessen der betroffenen Person beeinträchtigt werden*".

Der EDSB erinnert die Kommission daran, dass eine solche Prüfung fallweise vorzunehmen ist.

Nach den vorliegenden Informationen werden keine Daten an Drittstaaten übermittelt.

3.6. Verarbeitung von Personalnummer oder eindeutiger Kennung

Artikel 10 Absatz 6 der Verordnung besagt: „*Der Europäische Datenschutzbeauftragte bestimmt, unter welchen Voraussetzungen eine Personalnummer oder ein anderes Kennzeichen allgemeiner Bedeutung von einem Organ oder einer Einrichtung der Gemeinschaft verarbeitet werden darf.*" In dieser Stellungnahme sollen nicht die allgemeinen Bedingungen für eine solche Verwendung einer Personalnummer festgelegt, sondern die im Zusammenhang mit dem PACS erforderlichen spezifischen Maßnahmen betrachtet werden.

Der EDSB hat bereits in einer früheren Stellungnahme zur Vorabkontrolle[13] den Status der Nummer eines in einen Ausweis eingebauten RFID-Chips geklärt. Die an den RFID-Chip geknüpfte Identifizierungsnummer gehört zu den unter die Verordnung (EG) Nr. 45/2001 fallenden personenbezogenen Daten. Wenn also diese Identifizierungsnummer zur Aufzeichnung des Verhaltens eines Bediensteten verwendet und mit der Personalnummer (die, wie im vorliegenden Fall, wiederum mit dem Namen einer Person verknüpft ist) in Verbindung gebracht wird, dann stellt dies eine Verarbeitung personenbezogener Daten dar, bei der die Grundsätze des Datenschutzes einzuhalten sind.

Die Verwendung der Personalnummer ist notwendig, da die Karten-ID dem Zugangskontrollsystem mitgeteilt wird. Im hier zu prüfenden Fall ist die Verwendung der Personalnummer zur Überprüfung der Daten über Zugangsrechte im System sinnvoll, da diese

[13] Siehe Stellungnahme zu einer Meldung des Datenschutzbeauftragten der Europäischen Kommission zur Vorabkontrolle von „Umsetzung der für die GD INFSO spezifischen flexiblen Arbeitszeit", 19. Oktober 2007 (2007-218).

Nummer ja auch zur Identifizierung der Person im System verwendet und damit sichergestellt wird, dass die Daten sachlich richtig sind.

3.7. Auskunftsrecht und Berichtigung

Gemäß Artikel 13 der Verordnung (EG) Nr. 45/2001 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. Artikel 14 der Verordnung gewährt der betroffenen Person das Recht, unrichtige oder unvollständige Daten berichtigen zu lassen.

Die Meldung besagt, dass betroffene Personen über ihre Rechte, verfügbare Ansprechpartner, Kommunikationskanäle und bestehende Verfahren unterrichtet werden, wie sie in den oben genannten Unterlagen und Informationsquellen beschrieben werden (siehe Punkt 2 Sachverhalt). Die vorliegenden Informationen deuten ferner darauf hin, dass die Europäische Kommission die Rechte der betroffenen Personen gemäß der Verordnung (EG) Nr. 45/2001 ordnungsgemäß wahrt.

Der für die Verarbeitung Verantwortliche übermittelte dem EDSB ferner das Dokument mit den PSG-Fristen für die Sperrung/Löschung von Daten und den definierten Datenkategorien. In diesem Dokument werden die vorgesehenen Datenkategorien dargestellt und nähere Auskünfte zur Sperrung/Löschung von Daten auf begründeten Antrag der betroffenen Personen gegeben.

Sollte Artikel 20 angewandt werden (z. B. bei Ermittlungen), erinnert der EDSB die Kommission daran, dass dies nur restriktiv und fallweise geschehen sollte.

Zusammenfassend ist der EDSB der Ansicht, dass die Bedingungen von Artikel 13 und 14 der Verordnung unter der Voraussetzung erfüllt sind, dass sie fallweise angewandt werden.

3.8. Informationspflicht gegenüber der betroffenen Person

Gemäß Artikel 11 und 12 der Verordnung (EG) Nr. 45/2001 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.

Die Europäische Kommission hat dem EDSB die Datenschutzerklärung für betroffene Personen vorgelegt, die das PACS nutzen werden. Diese Datenschutzerklärung kann im Intranet abgerufen werden und wird an die Inhaber neuer Ausweise verteilt.

Der EDSB überprüfte ferner die in der Datenschutzerklärung enthaltenen Informationen darauf, ob sie inhaltlich den Anforderungen von Artikel 11 und 12 der Verordnung (EG) Nr. 45/2001 entsprechen.

Nach Auffassung des EDSB enthält die Datenschutzerklärung alle in Artikel 11 und 12 der Verordnung (EG) Nr. 45/2001 aufgeführten Elemente.

3.9. Sicherheitsmaßnahmen

Gemäß Artikel 22 der Verordnung hat der für die Verarbeitung Verantwortliche technische und organisatorische Maßnahmen zu treffen, die geeignet sind, ein Schutzniveau zu gewährleisten, 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.

[...]

Laut Meldung sollen ferner eine umfassende IT-Risikobewertung vorgenommen und angemessene Sicherheitskontroll- und Abhilfemaßnahmen ergriffen werden. Darüber hinaus soll jedes Restrisiko dokumentiert und von dem für die Verarbeitung Verantwortlichen und vom Auftragsverarbeiter formal akzeptiert werden. Der EDSB erwartet, über die durchgeführten Risikobewertungen informiert zu werden.

Gestützt auf die ihm vorliegenden Informationen sieht der EDSB keinen Anlass zu der Annahme, dass die Europäische Kommission die in Artikel 22 der Verordnung geforderten Sicherheitsmaßnahmen nicht ergriffen hat, fordert sie jedoch auf, ihm die vorstehend genannten Unterlagen zukommen zu lassen.

4. Schlussfolgerungen

Es besteht kein Anlass zu der Annahme, dass die Europäische Kommission gegen die Verordnung (EG) Nr. 45/2001 verstößt; allerdings sollte sie

- die Aufbewahrungsfrist für Systemdaten neu bewerten und nach einem Betriebsjahr des PACS die Aufbewahrungsfrist anpassen;

- dem EDSB Einsicht in die Ergebnisse der IT-Risikobewertung und in die Liste der umgesetzten Sicherheitskontroll- und Abhilfemaßnahmen gewähren;

- dem EDSB die Unterlagen zu dem Verfahren bei Sicherheitszwischenfällen zukommen lassen.

Brüssel, den 8. September 2011

(**unterzeichnet**)

Giovanni Buttarelli
Stellvertretender Europäischer Datenschutzbeauftragter