Stellungnahme zur Meldung des Datenschutzbeauftragten des Europäischen Parlaments für eine Vorabkontrolle über den Fall „Biometrische Kontrolleinrichtung“

1. Verfahren

Am 9. Oktober 2013 erhielt der Europäische Datenschutzbeauftragte (**EDSB**) eine Meldung des Datenschutzbeauftragten (**DSB**) des Europäischen Parlaments (**Parlament**) für eine Vorabkontrolle über die Verarbeitung personenbezogener Daten im Zusammenhang mit der biometrischen Kontrolleinrichtung des Parlaments.

Der EDSB erhielt zudem verschiedene Dokumente, die mit dieser Meldung in Verbindung stehen. Dies sind:

1. Beschluss des Präsidiums des Parlaments zum globalen Sicherheitskonzept;
2. Beschluss des Präsidiums zur Internalisierung der Sicherheit des Parlaments;
3. Vertraulichkeitserklärung bezüglich der biometrischen Kontrolleinrichtung.

Der EDSB erhielt am 21. Oktober 2013 zudem zusätzliche technische Informationen über das vom Parlament gewählte biometrische System sowie Antworten auf eine Reihe von technischen Fragen, die gestellt worden waren. Die Frist für die Abgabe der Stellungnahme des EDSB wurde anschließend am 9. Dezember 2013 aufgrund der Kompliziertheit des Sachverhalts in Übereinstimmung mit Artikel 27 Absatz 4 der Verordnung um zwei Monate verlängert. Am 10. Januar 2014 wurde die Frist in Erwartung eines Treffens mit dem Parlament ausgesetzt. Dieses Treffen fand am 30. Januar 2014 statt. Im Anschluss an dieses Treffen wurde dem Parlament eine Reihe weiterer Fragen übermittelt. Das Parlament hat diese Fragen am 26. März 2014 beantwortet.

Die Meldung wurde unter Anwendung von Artikel 27 Absatz 1 der Verordnung (EG) Nr. 45/2001 („die Verordnung“) einer Vorabkontrolle unterzogen.

2. Sachverhalt

Infolge des Beschlusses zur Internalisierung seiner Sicherheitstätigkeiten beschloss das Parlament, eine bestehende biometrische Kontrolleinrichtung wiederzuverwenden, um zu gewährleisten, dass die Sicherheitsposten ausschließlich von den entsprechend befugten Präventions- und Überwachungsbediensteten und dem entsprechend befugten Sicherheitspersonal besetzt sind.

Dieses biometrische System wird gegenwärtig von dem für die Sicherheit des Parlaments zuständigen externen Unternehmen (Securitas) genutzt. Der Beschluss zur Internalisierung hat zur Folge, dass das Parlament zukünftig Präventions- und Überwachungsbedienstete einsetzen wird, die direkt seiner Verantwortung unterstellt sind, und für spezifische Aufgaben auf Wachpersonal eines externen Dienstleisters zurückgreifen wird [...]. Gemäß der Meldung entspricht die gewählte Lösung dem geplanten globalen Sicherheitskonzept, das von dem Organ beschlossen wurde. Die Direktion Ressourcen bzw. deren Dienststellen für Planung und Dispatching tragen die praktische Verantwortung für die Umsetzung der Verarbeitung.

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 30
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

Die Registrierung der Bediensteten im System erfolgt bei Bediensteten des Parlaments über die Dienststelle Planung und bei Mitarbeitern von Securitas über Securitas […].

Die Einführung einer solchen Einrichtung wurde vom Parlament als unverzichtbar für die Erfüllung seiner Sicherheitserfordernisse eingestuft. Diese Sicherheitserfordernisse betreffen insbesondere die Verwaltung der Präventions- und Überwachungsbediensteten, die für die zahlreichen physischen Zugänge zum Parlament zuständig sind. Das Parlament muss in der Lage sein, die Identität der Bediensteten an ihrem Posten zu überprüfen, um eine unbefugte Einnahme von Posten zu verhindern. Es muss insbesondere:
- verhindert werden, dass interne Präventions- und Überwachungsbedienstete des Parlaments ihre Posten mit Wachpersonal des externen Dienstleisters tauschen und umgekehrt; dies ist aus Sicherheits- und Haftungsgründen erforderlich, insbesondere im Fall von Unfällen;
- verhindert werden, dass bestimmte Bedienstete in Absprache mit anderen (dem zuvor oder anschließend am gleichen Posten eingesetzten Bediensteten) von ihren Arbeitszeiten abweichen und so das Sicherheitsrisiko erhöhen;
- sichergestellt werden, dass die Bediensteten tatsächlich den Posten besetzen, **zu dessen Besetzung sie befugt sind**. In diesem Zusammenhang sollen folgende Beispiele genannt werden: i) Bedienstete, die in vom Parlament betriebenen Kindertagesstätten eingesetzt werden und die eine besondere Schulung absolviert und ein erweitertes Führungszeugnis/eine erweiterte Strafregisterbescheinigung vorlegen müssen; ii) Posten, an denen Personen- und Warenkontrolleinrichtungen (Röntgensysteme) bedient werden, wozu ebenfalls eine besondere Schulung erforderlich ist; iii) […]; iv) Posten an Einfahrten von Parkhäusern und Parkplätzen, für die besondere Ausrüstungsgegenstände benötigt werden und v) individuelle medizinische Einschränkungen, die berücksichtigt werden müssen.

Dem Parlament zufolge ist es vor diesem Hintergrund erforderlich, dass die für die Planung zuständige Dienststelle über die Einnahme von Posten informiert werden und diese Einnahme auf effiziente und zuverlässige Weise kontrollieren kann, um im Falle der Abwesenheit oder einer unbefugten Einnahme von Posten, die zu einem unbefugten Zugriff auf die Sicherheitsanweisungen des Organs (zum Beispiel [...]) führen kann, reagieren zu können.

Die Funktionsweise des Systems beruht darauf, dass das biometrische Lesegerät ein dreidimensionales Bild der Hand erfasst. Nach dieser Erfassung wandelt das Lesegerät das Bild in ein elektronisches Modell um. Dieses Modell sowie die Identifizierungsnummer des jeweiligen Nutzers werden in Datenbanken gespeichert, die im Falle [...].

Im Rahmen des im Parlament vorgesehenen Verfahrens legt die für die Planung zuständige Dienststelle die Verteilung der Bediensteten fest. Bei der Einnahme/dem Verlassen des Postens muss der Bedienstete seinen Ausweis und seine Hand vorzeigen, um sich zu identifizieren. Der Nutzer verwendet ein in das biometrische Lesegerät integriertes Ausweislesegerät, um seine Identifizierungsnummer zu erfassen. Das biometrische Lesegerät fordert den Nutzer anschließend dazu auf, seine Hand aufzulegen. Das Lesegerät vergleicht dann die aufgelegte Hand mit dem gespeicherten eindeutigen Modell [...].

Somit werden einerseits die biometrischen Merkmale und die Identifizierungsnummer (Ausweis) ([...]) und andererseits die Identifizierungsnummer, die Personalnummer und der Vor- und Nachname des Bediensteten [...] miteinander abgeglichen.

Bei den **betroffenen Personen** handelt es sich um das Sicherheitspersonal des Parlaments und von Securitas. Für das Registrierungsverfahren ist das Führungspersonal verantwortlich.

Die im Rahmen dieser Verarbeitung **erhobenen Daten** umfassen:
- Vor- und Nachname;
- biometrisches Modell (gemäß einer Norm/einer festgelegten Verschlüsselung in ein digitales Format umgewandelte biometrische Merkmale) und keine biometrischen Rohdaten;
- Identifizierungsnummer (Ausweis) des Bediensteten;
- Personalnummer;
- Daten über die geplante Uhrzeit der Einnahme und des Verlassens des Postens.

Bezüglich der **Empfänger der verarbeiteten Daten** ist zu sagen, dass die Daten über die Ableistung der Arbeitszeit an die zuständigen Dienststellen der GD PERS übermittelt werden (Übermittlung von der Datenbank Planning zur Datenbank Streamline):

- individuelle Rechte und Bezüge;
- Personal- und Laufbahnverwaltung (Auswirkungen von Langzeiturlaub auf die Laufbahn);

Es wurde außerdem angegeben, dass die Daten gegebenenfalls an die für die Erfassung krankheitsbedingter Fehlzeiten zuständige Dienststelle übermittelt werden.

[…].

Bezüglich der biometrischen Daten ist zu sagen, [...]. Diese biometrischen Daten werden nicht an die für die Planung zuständige Dienststelle übermittelt. Diese erhält lediglich die Daten über die Identifizierungsnummer des Bediensteten und die geplanten Uhrzeiten der Einnahme und des Verlassens des Postens, die sie prüft und bestätigt.

Bezüglich der **Rechte der betroffenen Personen** ist zu sagen, dass gemäß der Meldung vorgesehen ist, dass die betroffenen Personen ihre Auskunfts-, Berichtigungs-, Sperrungs-, Löschungs- und Widerspruchsrechte jederzeit ausüben können, indem sie einen entsprechenden Antrag an die Dienststelle Planung richten. […].

Hinsichtlich der Rechte der betroffenen Personen ist außerdem darauf hinzuweisen, dass der für die Verarbeitung Verantwortliche innerhalb einer Frist von 15 Werktagen ab Erhalt des Antrags auf Sperrung eine Entscheidung mitteilen muss. Wird dem Antrag stattgegeben, muss diesem innerhalb einer Frist von 30 Werktagen nachgekommen werden und die betroffene Person wird entsprechend informiert. Wird der Antrag auf Sperrung abgewiesen, muss der für die Verarbeitung Verantwortliche die betroffene Person innerhalb einer Frist von 15 Werktagen in einem Schreiben und unter Angabe von Gründen entsprechend informieren.

Ebenso muss der für die Verarbeitung Verantwortliche innerhalb einer Frist von 15 Werktagen ab Erhalt des Antrags auf Löschung eine Antwort übermitteln. Wird dem Antrag stattgegeben, muss diesem unverzüglich nachgekommen werden. Ist der für die Verarbeitung Verantwortliche der Auffassung, dass der Antrag nicht gerechtfertigt ist, muss er die betroffene Person innerhalb einer Frist von 15 Werktagen in einem Schreiben und unter Angabe von Gründen entsprechend informieren.

Gemäß der Meldung wird die **Informationspflicht** gegenüber den betroffenen Personen mithilfe folgender Maßnahmen erfüllt:
- einer Schulung neu eingestellter Bediensteter, an der der Datenschutzbeauftragte des Parlaments teilnimmt;
- einer Datenschutzerklärung, in der alle Merkmale der entsprechenden Verarbeitung, wie in Artikel 11 und 12 der Verordnung gefordert, aufgeführt sind. Das Parlament hat einen Entwurf einer Vertraulichkeitserklärung vorgelegt.

Bezüglich der **Datenaufbewahrung** sieht die Meldung vor, [...].

Bezüglich der **Aufbewahrungsfrist** gestaltet sich das gegenwärtig vorgesehene Verfahren wie folgt:
Die Daten über die Identität der Bediensteten, die Identifizierungsnummer (Ausweis) und die biometrischen Merkmale werden [...] so lange aufbewahrt, wie der Bedienstete die Funktionen eines Präventions- und Überwachungsbediensteten/Sicherheitsaufgaben und -funktionen ausüben soll.

Bezüglich der **technischen und sicherheitsrelevanten Merkmale** des biometrischen Systems hat der für die Verarbeitung Verantwortliche zusätzliche Informationen über die Architektur und die Beschreibung des gewählten Systems bereitgestellt:

Diese umfassen im Wesentlichen Folgendes: […]

3. Rechtliche Prüfung

3.1. Vorabkontrolle

Anwendbarkeit der Verordnung: Die vorliegende Stellungnahme über eine Vorabkontrolle betrifft die Verarbeitung personenbezogener Daten durch das Europäische Parlament.

Die Verordnung gilt für die *„ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen“* 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 nachfolgend beschriebenen Gründen liegen sämtliche Voraussetzungen für die Anwendung der Verordnung vor.

Zunächst werden *personenbezogene Daten*, wie sie in Artikel 2 Buchstabe a der Verordnung definiert sind, erhoben und zu einem späteren Zeitpunkt verarbeitet. Anschließend werden die erhobenen personenbezogenen Daten einer *„automatisierten Verarbeitung“* im Sinne von Artikel 2 Buchstabe b der Verordnung unterzogen. So werden personenbezogene Daten, etwa persönliche Identifizierungsdaten wie Handabdrücke, erhoben und einer „automatisierten Verarbeitung“ unterzogen, beispielsweise wenn der Dienst Abdrücke nimmt. Schließlich erfolgt die Verarbeitung durch ein Organ, im vorliegenden Fall das Parlament, im Rahmen von Tätigkeiten, die in den Anwendungsbereich des EU-Rechts fallen (Artikel 3 Absatz 1 der Verordnung).

Begründung der Vorabkontrolle: Gemäß Artikel 27 Absatz 1 der Verordnung werden *“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. Der EDSB ist der Auffassung[1], dass das Vorliegen und die Verarbeitung biometrischer Daten, bei denen es sich nicht um Fotografien handelt, wie dies im vorliegenden Sachverhalt der Fall ist, in dem biometrische Handabdrücke erhoben werden, besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können. Diese Schlussfolgerung stützt sich aufgrund der

[1] Siehe dazu auch die Fälle 2010-0427 vom 8. September 2011, 2007-635 vom 7. April 2008 und 2008-223 vom 30. Juni 2008, die auf der Website des EDSB abgerufen werden können.

inhärenten Merkmale dieses Datentyps im Wesentlichen auf den Charakter der biometrischen Daten. So machen die biometrischen Daten beispielsweise die Merkmale des menschlichen Körpers „maschinenlesbar“ und zu einem wahrscheinlichen Gegenstand einer späteren Nutzung. Diese Risiken können einen Grund für die Notwendigkeit darstellen, die Verarbeitung der Daten auf Grundlage von Artikel 27 Absatz 1 der Verordnung einer Vorabkontrolle des EDSB zu unterziehen, um sicherzustellen, dass die strengen Garantien umgesetzt wurden.

Darüber hinaus ist der EDSB der Auffassung, dass die Integration der RFID-Technologie (RFID-Chipkarte im Ausweis) in bestimmten Fällen spezifische Risiken bergen kann. Im vorliegenden Fall ist die Nutzung der RFID-Technologie lediglich für den Ausweis vorgesehen, der gegenwärtig keine biometrischen Daten enthält. Gemäß den vorgelegten Informationen plant das Parlament jedoch [...]. Für diesen Fall möchte der EDSB darauf hinweisen, dass dies zu einer Veränderung der Risiken der Verarbeitung führen könnte.

Fristen: Da die Vorabkontrolle darauf abzielt, Situationen aufzuzeigen, die möglicherweise besondere Risiken beinhalten, muss die Stellungnahme des EDSB gemäß Artikel 27 der Verordnung vor Beginn der Verarbeitung abgegeben werden. Somit sollte die Verarbeitung nicht erfolgen, solange der EDSB noch nicht seine förmliche Zustimmung erteilt hat.

Die Meldung ging am 9. Oktober 2013 ein. Gemäß Artikel 27 Absatz 4 der Verordnung wurde die Frist von zwei Monaten, in der der EDSB seine Stellungnahme abgeben muss, um einen weiteren Zeitraum von zwei Monaten verlängert (im vorliegenden Fall wurde das Verfahren insgesamt um 75 Tage ausgesetzt, um weitere Auskünfte einzuholen, wozu weitere 20 Tage für die Ausarbeitung von Bemerkungen zu dem Entwurf der Stellungnahme hinzukommen). Die vorliegende Stellungnahme muss demnach spätestens am 15. Mai 2014 angenommen werden.

3.2. Rechtmäßigkeit der Verarbeitung

Die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn sie Artikel 5 der Verordnung entspricht. Von den verschiedenen in Artikel 5 der Verordnung aufgeführten Gründen scheint bei der gemeldeten Verarbeitung Artikel 5 Buchstabe a Anwendung zu finden. Gemäß diesem dürfen personenbezogene Daten nur verarbeitet werden, wenn dies *„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 […] übertragen wurde“*.

Um zu ermitteln, ob die Verarbeitung Artikel 5 Buchstabe a der Verordnung entspricht, müssen drei Punkte berücksichtigt werden: 1.) ob die Verträge oder andere Rechtsakte die durchgeführte Verarbeitung vorsehen, 2.) ob die Verarbeitung im öffentlichen Interesse erfolgt und 3.) ob die Verarbeitung für die Wahrnehmung dieser Aufgabe tatsächlich erforderlich ist (Prüfung der Erforderlichkeit). Diese drei Voraussetzungen sind eng miteinander verbunden.

* Die für die betroffene Verarbeitung geltende **Rechtsgrundlage** ist in den folgenden Rechtsakten beschrieben:

- Beschluss des Präsidiums vom 6. Juli 2011 zum globalen Sicherheitskonzept;
- Beschluss des Präsidiums vom 11. Juni 2012 zur Internalisierung der Sicherheit des Parlaments.

Diese Beschlüsse sehen die Entwicklung eines „globalen Sicherheitskonzepts“ innerhalb des Parlaments sowie die schrittweise Internalisierung der Sicherheit des Parlaments vor.

Die Beschlüsse des Präsidiums des Parlaments beruhen auf der Geschäftsordnung des Parlaments, die auf Grundlage von Artikel 232 des Vertrags über die Arbeitsweise der Europäischen Union beschlossen wurde.

Die Verarbeitung erfolgt im Rahmen der **legitimen Ausübung öffentlicher Gewalt**. Der EDSB stellt fest, dass das Parlament die Verarbeitungstätigkeiten im Rahmen einer Aufgabe vornimmt, die in legitimer Ausübung seiner öffentlichen Gewalt und auf Grundlage der vorstehend genannten Rechtsakte, die auf Grundlage des Statuts der Beamten beschlossen wurden, ausgeführt wird. Das Parlament hat ein globales Sicherheitskonzept beschlossen, das die gemeldete Verarbeitung beinhaltet.

Bezüglich der Erforderlichkeit der Verarbeitung **(Prüfung der Erforderlichkeit)** ist zu sagen, dass gemäß Artikel 5 Buchstabe a der Verordnung die Verarbeitung für *„die Wahrnehmung einer Aufgabe erforderlich“* sein muss, wie dies weiter oben bereits aufgeführt wurde. Diesbezüglich wird in Erwägungsgrund 27 Folgendes festgelegt: *„Die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft 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.“*

Die Erforderlichkeit der Nutzung eines biometrischen Kontrollsystems beruht gemäß den Ausführungen des Parlaments auf den allgemeinen Sicherheitserfordernissen, die auch eine spezifische Verwaltung des Sicherheitspersonals umfassen (Ausgleich etwaiger Pflichtverletzungen seitens des Personals wie etwa die unbefugte Einnahme von Posten). Der EDSB darf dabei jedoch nicht unberücksichtigt lassen, dass die Wahl der spezifischen technischen Lösung (einschließlich der biometrischen Handerkennung) auch damit zusammenhängt, dass diese Lösung aktuell von dem externen, vom Parlament beauftragten Wachunternehmen genutzt wird (Securitas). Dieser Aspekt darf im Rahmen der gegenwärtigen Prüfung nicht ausgespart werden, auch wenn er nicht der Hauptbeweggrund für die endgültige Entscheidung zur Nutzung dieser Lösung war.

Es gestaltet sich somit schwierig, die absolute Erforderlichkeit der Nutzung des spezifischen, vom Parlament gewählten biometrischen Systems anstelle eines anderen Systems nachzuweisen. Dabei gilt es zu berücksichtigen, dass „Erforderlichkeit“ nicht bedeutet, dass das Vorgehen unvermeidbar ist, sondern dass es im spezifischen Rahmen der Erreichung des angestrebten Ziels nach vernünftigem Ermessen als erforderlich angesehen werden kann. Im begrenzten Rahmen der Verwaltung des Präventions- und Überwachungspersonals – die direkte Auswirkungen auf die allgemeine Sicherheit des Parlaments hat – scheint die Verarbeitung nach vernünftigem Ermessen als erforderlich angesehen werden zu können. Es ist daran zu erinnern, dass das endgültige Ziel der Verarbeitung der physische Schutz des Personals, der Informationen und der Sachgüter des Organs ist.

Angesichts der umfassenden Bedeutung dieser Interessen kann das Parlament es tatsächlich als erforderlich erachten, besondere Sicherheitsmaßnahmen wie die Nutzung strenger Identitätskontrollsysteme für das Sicherheitspersonal zu beschließen, die die im vorliegenden Fall betrachtete Verarbeitung personenbezogener Daten einschließt.

Die Nutzung dieses spezifischen biometrischen Systems sowie [...] erscheinen als angemessene Maßnahmen zur Vermeidung einer unbefugten Einnahme von Posten.

Dennoch möchte der EDSB anmerken, dass das gegenwärtige Prüfverfahren im Wesentlichen aus einem Prüfprozess besteht [...].

Der EDSB ist der Ansicht, dass dieses System die Privatsphäre weniger schützt als ein System, dessen Prüfverfahren aus einem 1:1-Prüfprozess des Ausweises (eins zu eins) besteht, bei dem die Minutien in der Karte des Inhabers integriert sind und vor Ort mithilfe des Lesegeräts/Scanners für biometrische Daten mit den gescannten Minutien (zu Kontrollzwecken) abgeglichen werden. Der Abgleich/die Kontrolle würde dabei lokal über das Lesegerät für biometrische Daten erfolgen, [...]. Der EDSB befürwortet ein solches System, bei dem eine spätere unzulässige Nutzung und Phishing-Angriffe, die sich allgemein aus der Nutzung von Datenbanken ergeben können[2], verhindert werden.

In Übereinstimmung mit seinem konsequenten Ansatz in Bezug auf biometrische Daten[3] kann der EDSB den vom Parlament beschlossenen Ansatz nicht vollständig unterstützen, sofern das gegenwärtig genutzte System in der bestehenden Form weiterverwendet wird. Zwar hat das Parlament angekündigt, das aktuelle System auf das beschriebene zweite System mit 1:1-Kontrolle umstellen zu wollen, doch gegenwärtig besteht kein genauer Zeitplan für eine solche Umstellung. Der EDSB fordert das Parlament somit auf, alle notwendigen Maßnahmen zu ergreifen, um diese Umstellung gemäß einem genauen, noch mitzuteilenden Zeitplan durchzuführen.

3.3. Datenqualität

Zweckentsprechung, Erheblichkeit und Verhältnismäßigkeit: Gemäß Artikel 4 Absatz 1 Buchstabe c der Verordnung müssen die personenbezogenen Daten den Zwecken entsprechen, für die sie erhoben und weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen. Dabei handelt es sich um den Grundsatz der Datenqualität.

Bezüglich der biometrischen Daten stellt der EDSB fest, dass das System auf einem biometrischen Modell des Handumrisses basiert.

Die Art der erhobenen Daten – die biometrischen Merkmale der Hand und zugehörige Identifizierungsinformationen – entspricht den Daten, die für den Betrieb des Systems auf Grundlage biometrischer Daten benötigt werden. Der EDSB betont, dass die erhobenen Daten unter diesem Gesichtspunkt als den Verarbeitungszwecken entsprechend und für diese erheblich angesehen werden könnten.

Verarbeitung nach Treu und Glauben und Rechtmäßigkeit: Artikel 4 Absatz 1 Buchstabe a der Verordnung schreibt vor, dass die Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden müssen. Die Frage nach der Rechtmäßigkeit wurde bereits weiter oben analysiert (siehe Punkt 3.2). Der Aspekt der Verarbeitung nach Treu und Glauben ist eng mit der Informationspflicht gegenüber den betroffenen Personen verbunden, die nachstehend unter Punkt 3.9 behandelt wird.

Sachliche Richtigkeit: Gemäß Artikel 4 Absatz 1 Buchstabe d der Verordnung dürfen personenbezogene Daten nur verwendet werden, wenn sie *„sachlich richtig und, wenn nötig,*

[2] Siehe Stellungnahme vom 14. Februar 2008 zur Meldung des Datenschutzbeauftragten der Europäischen Zentralbank für eine Vorabkontrolle über die Erweiterung des bestehenden Zugangskontrollsystems um Iriserkennung für den Hochsicherheitsbereich der EZB (2007-501), die auf der Website des EDSB abgerufen werden kann.

[3] Siehe Fußnote auf Seite 1.

auf den neuesten Stand gebracht sind; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, unrichtige oder unvollständige Daten gelöscht oder berichtigt werden".

Im vorliegenden Fall umfassen die von der Verarbeitung betroffenen personenbezogenen Daten biometrische Daten, die zu Zwecken der Identitätskontrolle genutzt werden. Bestimmte zentrale Merkmale biometrischer Systeme haben direkte Auswirkungen auf den Grad der sachlichen Richtigkeit der Daten, die im Rahmen der bei diesem Systemtyp stets durchlaufenen Registrierungs- oder Identifizierungsphasen erzeugt werden. Je nachdem, ob das biometrische System so ausgelegt wird, dass diese zentralen Merkmale einbezogen werden, oder nicht, stellt die sachliche Richtigkeit der Daten einen Faktor dar, der berücksichtigt oder nicht berücksichtigt werden muss.

Der EDSB hat in früheren Stellungnahmen zu Zugangskontrollen die Vorgaben analysiert, die bei der Nutzung biometrischer Systeme zu beachten sind. Die nachfolgende Analyse beschreibt diese zentralen Merkmale und bewertet, inwieweit diese in der biometrischen Kontrolleinrichtung des Parlaments Berücksichtigung gefunden haben.

Zunächst müssen für die Registrierungsphase alternative Mittel zur Identifizierung von Personen vorgesehen sein, die – wenn auch nur temporär – nicht für das Registrierungsverfahren in Frage kommen, beispielsweise weil ihr Handabdruck beschädigt ist. Ein solches Verfahren wird im Allgemeinen als ***„Notfallverfahren"***[4] bezeichnet. Im Rahmen der Registrierung bestätigt das Gerät die Registrierung oder lehnt sie ab, wobei diese Ablehnung etwa im Falle einer schlechten Qualität der Registrierung erfolgt.

Auch in der anschließenden Phase der Nutzung der Technologie besteht die Möglichkeit, dass die biometrische Kontrolle nicht durchgeführt werden kann. Der EDSB stellt fest, dass für den Fall, dass die biometrische Kontrolle nicht durchgeführt werden kann (in der Meldung wird dafür die Bezeichnung „Systemfehler" verwendet), die Einführung einer solchen Notfalllösung vorgesehen ist. In einem solchen Fall [...].

Der EDSB stellt außerdem fest, dass von der genutzten Technologie eine weitere Maßnahme zur Gewährleistung der sachlichen Richtigkeit der Daten angewandt wird. Falls eine Person die Geräte nicht regelmäßig nutzt, entsprechen die zum Zeitpunkt der Kontrolle erhobenen Daten nicht mehr den gespeicherten Daten. Dies ist dadurch begründet, dass die menschliche Hand natürlichen Veränderungen unterworfen ist (Verlust oder Zunahme von Gewicht, altersbedingte Gelenkveränderungen usw.). Um dieses Problem zu vermeiden, wird bei jeder Messung/Kontrolle automatisch ein Durchschnitt der Messwerte gebildet und als aktualisierter Datensatz im Gerät gespeichert; die vorherigen Daten werden durch die neuen, aktualisierten Daten ersetzt.

Der EDSB erachtet diese Notfallverfahren im Hinblick auf Artikel 4 Absatz 1 Buchstabe a für zufriedenstellend.

3.4. 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

[4] Siehe Stellungnahme des Europäischen Datenschutzbeauftragten 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 für eine Beschreibung der im Rahmen von Notfallverfahren anwendbaren Datenschutzgrundsätze.

werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht.

Bezüglich der gegenwärtig vorgesehenen Dauer der Aufbewahrung [...] stellt der EDSB fest, dass die festgelegte Dauer für die verschiedenen Kategorien von Daten, die mit der Identifizierung und den biometrischen Merkmalen in Verbindung stehen, als gerechtfertigt angesehen werden könnte.

Dennoch muss die Aufbewahrungsdauer [...] angesichts der bereits angeführten Bemerkungen [...] erneut geprüft werden, um eine angemessene Aufbewahrungsdauer festzulegen [...].

3.5. Datenübermittlung

Es ist eine Übermittlung gemäß Artikel 7 der Verordnung vorgesehen. Der EDSB erinnert daran, dass laut Artikel 7 der Verordnung die Übermittlung personenbezogener Daten zulässig ist, *„wenn die Daten für die rechtmäßige Erfüllung der Aufgaben erforderlich sind, die in den Zuständigkeitsbereich des Empfängers fallen"*. Um dieser Bestimmung gerecht zu werden, muss der für die Verarbeitung Verantwortliche bei der Übermittlung personenbezogener Daten sicherstellen, dass i) der Empfänger über die geeignete Zuständigkeit verfügt und dass ii) die Übermittlung erforderlich ist. Der EDSB ist der Auffassung, dass diese Bedingungen im vorliegenden Fall erfüllt sind.

Die Daten über die Ableistung der Arbeitszeit werden an die Dienststelle Planung und die anderen zuständigen Dienststellen der GD PERS, die Dienststelle „Individuelle Rechte und Bezüge" und das Referat „Personal- und Laufbahnverwaltung", übermittelt. Die Übermittlung erfolgt von der Datenbank Planning zur Datenbank Streamline. Bei Bedarf werden die Daten zudem an die für die Erfassung krankheitsbedingter Fehlzeiten zuständige Dienststelle übermittelt. Diese Empfänger dürfen die personenbezogenen Daten in Übereinstimmung mit Artikel 7 der Verordnung nur für die Zwecke verarbeiten, für die sie übermittelt wurden.

3.6. Verarbeitung der Personalnummer oder des eindeutigen Kennzeichens

Artikel 10 Absatz 6 der Verordnung legt fest, dass *„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 der vorliegenden Stellungnahme werden keine allgemeinen Bedingungen für die Nutzung der Personalnummer festgelegt, sondern besondere Maßnahmen erwogen, die im Rahmen der biometrischen Prüfung innerhalb des Parlaments erforderlich sind.

Der EDSB hat sich bereits in einer früheren Stellungnahme zu einer Vorabkontrolle[5] bezüglich des Status einer in eine Karte integrierten Chipkartennummer geäußert. Die mit der RFID-Chipkarte verbundene Identifizierungsnummer zählt zu den durch die Verordnung Nr. 45/2001 geregelten personenbezogenen Daten. Wird diese Identifizierungsnummer genutzt, um das Verhalten eines Angestellten zu bewerten, und wird sie mit der Personalnummer (mit dem Namen einer Person, wie dies im vorliegenden Fall zutrifft) verknüpft, so stellt dies eine Verarbeitung personenbezogener Daten dar, die somit die Beachtung der Datenschutzgrundsätze erfordert.

[5] Siehe Stellungnahme vom 19. Oktober 2007 zur Meldung des Datenschutzbeauftragten der Europäischen Kommission für eine Vorabkontrolle über die „Einführung von Flexitime speziell für die GD INFSO" (2007-218).

Die Nutzung der Personalnummer ist erforderlich, da das Kennzeichen der Karte an das biometrische Kontrollsystem übermittelt wird. Im vorliegenden Fall ist die Nutzung der Personalnummer der Angestellten zu Zwecken der Kontrolle der Zugangsdaten im System angemessen, wenn man berücksichtigt, dass diese Nummer verwendet wird, um die Person im System zu identifizieren, und diese so die sachliche Richtigkeit der Daten gewährleistet. Für eine Festlegung weiterer Bedingungen besteht im vorliegenden Fall kein Anlass.

3.7. Auskunftsrecht und Berichtigung

Gemäß Artikel 13 der Verordnung gilt Folgendes: *„Die betroffene Person hat das Recht, jederzeit frei und ungehindert innerhalb von drei Monaten nach Eingang eines entsprechenden Antrags unentgeltlich von dem für die Verarbeitung Verantwortlichen folgende Auskünfte zu erhalten: [...] eine Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten."* Artikel 14 sichert den betroffenen Personen das Recht zu, unrichtige oder unvollständige Daten berichtigen zu lassen.

Die Meldung und die Vertraulichkeitserklärung enthalten diese Informationen (siehe Punkt 2 „Sachverhalt" oben). Die Meldung sieht außerdem ein Vorgehen zur Sperrung/Löschung der Daten auf rechtmäßigen und begründeten Antrag der betroffenen Person vor.

In Fällen, in denen Artikel 20 Anwendung finden könnte (beispielsweise im Fall von Untersuchungen), betont der EDSB gegenüber dem Parlament, dass dieser auf restriktive Weise und auf Einzelfallbasis anzuwenden ist.

Der EDSB ist somit der Ansicht, dass die durch Artikel 13 und 14 der Verordnung vorgesehenen Bedingungen erfüllt sind, wobei im Rahmen der Anwendung von Artikel 20 der Verordnung die Anwendung auf Einzelfallbasis zu erfolgen hat.

3.8. Informationspflicht gegenüber den betroffenen Personen

Gemäß Artikel 11 und 12 der Verordnung müssen die für die Erhebung der personenbezogenen Daten Verantwortlichen die betroffenen Personen über die Erhebung ihrer Daten informieren. Zudem verfügen diese Personen über das Recht, Informationen, insbesondere über die Zwecke der Verarbeitung, die Empfänger der Daten und ihre besonderen Rechte als betroffene Personen, zu erhalten.

Das Parlament hat dem EDSB einen Entwurf einer Vertraulichkeitserklärung für die betroffenen Personen (die Bediensteten), die das biometrische Kontrollsystem nutzen werden, übermittelt. Das Parlament hat jedoch nicht angegeben, wann und wie diese Erklärung den betroffenen Personen zur Verfügung gestellt wird.

Die Informationspflicht wird außerdem mithilfe einer Schulung neu eingestellter Bediensteter erfüllt, an der der DSB des Parlaments teilnimmt.

Bezüglich der Vertraulichkeitserklärung hat der EDSB auch den Inhalt der bereitgestellten Informationen geprüft, um festzustellen, ob dieser den Anforderungen von Artikel 11 und 12 der Verordnung genügt. Der EDSB stellt fest, dass die Daten über die Ableistung der Arbeitszeit und krankheitsbedingte Fehlzeiten an die Dienststelle „Individuelle Rechte und Bezüge", das Referat „Personal- und Laufbahnverwaltung" und ggf. die für die Erfassung krankheitsbedingter Fehlzeiten zuständige Dienststelle übermittelt werden (siehe Punkt 3.5). Diese drei Dienststellen sind somit die Empfänger der Daten, die als solche die entsprechende

Verantwortung gegenüber den betroffenen Personen tragen. Um eine Verarbeitung nach Treu und Glauben zu gewährleisten, muss die Vertraulichkeitserklärung Informationen darüber beinhalten, welche Daten welcher Dienststelle zu welchen Zwecken übermittelt werden.

Daraus folgt, dass diese Information über die Herkunft der Daten, die im Rahmen der oben genannten zugehörigen Verarbeitungen verarbeitet werden, auch in den entsprechenden Vertraulichkeitserklärungen (Leistungsverwaltung, Urlaubsverwaltung, Erfassung krankheitsbedingter Fehlzeiten usw.) enthalten sein muss. Die entsprechenden Mitteilungen sind gegebenenfalls zu aktualisieren.

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.

Im vorliegenden Fall steht die Wahl der spezifischen Lösung wie bereits erwähnt auch damit in Zusammenhang, dass diese Lösung aktuell von dem externen, vom Parlament beauftragten Wachunternehmen genutzt wird. In Anbetracht der veränderten Verantwortlichkeiten wäre es zweckdienlich, wenn das Parlament die Risikoanalyse nochmals prüfen würde, um zu ermitteln, welche Kontrollmaßnahmen getroffen werden sollten, um die Risiken auf ein für das Parlament annehmbares Niveau zu senken.

[…]

Zudem macht der EDSB das Parlament auf die folgenden technischen Erwägungen aufmerksam, [...]:
[…]

Schlussfolgerungen

Die vorgeschlagene Verarbeitung scheint keine Verletzungen der Bestimmungen der Verordnung (EG) Nr. 45/2001 nach sich zu ziehen, sofern die vorstehend geäußerten Empfehlungen berücksichtigt werden. In diesem Zusammenhang muss das Parlament insbesondere:

- alle notwendigen Maßnahmen ergreifen, um Änderungen des gegenwärtigen Systems durchzuführen [...] und um dem EDSB einen Zeitplan für diese Änderungen vorzulegen;
- das betroffene Personal auf verständliche Weise über die Empfänger der verschiedenen Kategorien personenbezogener Daten informieren und die Informationen aktualisieren, die den betroffenen Personen im Rahmen der zugehörigen Verarbeitungen bereitgestellt werden (siehe Punkt 3.8);
- den EDSB über die Art und Weise und den Zeitpunkt der Bereitstellung der Vertraulichkeitserklärung an die betroffenen Personen informieren.

Bezüglich der Sicherheitsaspekte der Lösung schlägt der EDSB zudem vor, dass das Parlament Folgendes unternimmt:

- […]

Bezüglich der Übermittlung von Daten an Securitas empfiehlt der EDSB dem Parlament abschließend Folgendes:

- […]

Brüssel, den 15. Mai 2014