Stellungnahme des EDSB zur Nutzung eines computergestützten Systems durch das Europäische Parlament für die Digitalisierung der Plenartagungen und der zentralen Anwesenheitslisten mittels biometrischer Technologie
(Verbundene Fälle 2020-0921 und 2021-0355)

1. HINTERGRUND

Diese Stellungnahme befasst sich mit einem aktualisierten System zur Bescheinigung der Anwesenheit von Mitgliedern des Europäischen Parlaments (MdEP). Mit dem System soll das zentrale Anwesenheitsregister (Central Attendance Register, CAR) des Europäischen Parlaments für MdEP digitalisiert werden, indem das bestehende papiergestützte Signatursystem durch eine Lösung ersetzt wird, die auf einem optischen Fingerabdruckscanner beruht. Das System wird verwendet, um die Anwesenheit der MdEP gemäß Artikel 12 der DBAS[1] zu bescheinigen und ihnen die entsprechenden Tagegelder gemäß Artikel 24 DBAS zu zahlen.

Der Europäische Datenschutzbeauftragte (EDSB) wurde erstmals informell am 18. Juni 2018 vom Datenschutzbeauftragten (DSB) des Europäischen Parlaments um Beratung zu diesem Projekt gebeten.[2] Damals stellte der EDSB fest, dass die Notwendigkeit des Einsatzes eines biometrischen Systems für die Überwachung von MdEP nicht nachgewiesen war und die geplante Verarbeitung personenbezogener Daten daher gegen Artikel 5 der Verordnung (EG) Nr. 45/2001 verstoßen würde.[3] Der EDSB war insbesondere der Ansicht, derselbe Zweck könne mit weniger einschneidenden Mitteln erreicht werden, wie z. B.:

- einen PIN-Code;
- Stempelsysteme mit Magnetbändern;
- Zwei-Faktor-Authentifizierung durch Kombination mehrerer der vorstehend genannten Lösungen;
- stichprobenartige und regelmäßige Überprüfung der Unterschriften/Anwesenheit durch Menschen.

Der EDSB stellte ferner fest, dass, selbst wenn die Notwendigkeit des Projekts festgestellt worden wäre, die Verarbeitung biometrischer Daten weiterhin dem Ergebnis einer Datenschutz-Folgenabschätzung (DSFA) hätte folgen und sie hätte berücksichtigen müssen.

Im Anschluss an ein Treffen zwischen dem Europäischen Parlament und dem EDSB am 26. Juni 2018 beschloss das Europäische Parlament, intern alternative und weniger einschneidende Systeme für die Registrierung der Anwesenheit der Mitglieder zu prüfen.

[1] Durchführungsbestimmungen zum Abgeordnetenstatut des Europäischen Parlaments, Beschluss des Präsidiums vom 19. Mai und 9. Juli 2008, geändert durch den Beschluss des Präsidiums des Europäischen Parlaments vom 17. Juni 2019, *PE422.536/BUR*.
[2] EDSB-Fall 2018-0553.
[3] Die Verordnung (EG) Nr. 45/2001 wurde inzwischen durch die Verordnung (EU) 2018/1725 ersetzt.

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 30 – 1000 Brüssel, Belgien
E- Mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: +32 2 283 19 00 – Fax: +32 2 283 19 50

Am 7. Oktober 2020 wiesen MdEP den EDSB darauf hin, dass das Europäische Parlament nun die Modernisierung seiner zentralen Anwesenheitsliste vorantreibt, indem es biometrische Daten der MdEP verarbeitet. Um zu überprüfen, ob seine früheren Bedenken ausgeräumt wurden, beschloss der EDSB, das Parlament um weitere Informationen zu dieser Angelegenheit zu ersuchen.

Am 16. Oktober 2020 übermittelte der EDSB ein Informationsersuchen an das Europäische Parlament. Am 11. November 2020 erhielt der EDSB die Antwort des Europäischen Parlaments, die sowohl ein Schreiben zu den spezifischen Fragen des EDSB als auch acht Anhänge umfasste.[4]

Vor diesem Hintergrund hat der EDSB beschlossen, diese Initiativstellungnahme auf der Grundlage von Artikel 57 Absatz 1 Buchstabe g der Verordnung (EU) 2018/1725 (im Folgenden „Verordnung")[5] abzugeben.

2. BESCHREIBUNG DER VORGESCHLAGENEN VERARBEITUNG

Das Europäische Parlament hat dem EDSB eine Datenschutz-Folgenabschätzung zur aktualisierten Fassung des Anwesenheitskontrollsystems vorgelegt. Laut der Datenschutz-Folgenabschätzung[6] bestätigen die MdEP ihre Anwesenheit nunmehr digital, indem sie ihren Fingerabdruck auf dem Fingerabdruckleser scannen, der ihre Anwesenheit im System mittels eines Zeitstempels protokolliert. Dieses System ersetzt das derzeitige System der Anwesenheitskontrolle, bei dem eine Unterschrift geleistet wird (d. h. es wird die Signaturpflicht nicht digitalisieren), und es stützt sich nicht auf andere Informationen wie z. B. ein Passwort.[7]

Das Verfahren beginnt mit der Erfassung der verschlüsselten Fingerabdruck-Vorlagen der MdEP in der zentralen Datenbank des Systems und in jedem der in den Räumlichkeiten des Europäischen Parlaments installierten Lesegeräte. Jedes Mal, wenn ein MdEP seinen Finger

---

[4] Einen Hauptanhang, in dem die Struktur der verschiedenen Dokumente dargelegt wird;
Anhang 1.1/1.2.: Artikel 20 des Abgeordnetenstatuts des Europäischen Parlaments (2005/684/EG, Euratom) / Artikel 12 Absatz 1 der Durchführungsbestimmungen zum Abgeordnetenstatut des Europäischen Parlaments (Beschluss des Präsidiums vom 19. Mai und 9. Juli 2008);
Anhang 2: Protokoll der Sitzung des Präsidiums vom 11. Juni 2018;
Anhang 3: Protokoll der Sitzung des Präsidiums vom 17. Juni 2019;
Anhang 4: Datenschutz-Folgenabschätzung „Digitalisierung der zentralen Anwesenheitsliste mit Hilfe der Technologie der verschlüsselten Biometriedaten-Vorlagen" (Version 1.6) einschließlich ihrer Anhänge (im Folgenden „DSFA-Anhänge");
Anhang 5: Stellungnahme des Datenschutzbeauftragten des Parlaments zur Version 1.5 der Datenschutz-Folgenabschätzung „Digitalisierung der zentralen Anwesenheitsliste mit Hilfe der Technologie der verschlüsselten Biometriedaten-Vorlagen";
Anhang 6.1/6.2: Informationen über die technische Lösung und die Infrastruktur des vorgeschlagenen biometrischen Systems;
Anhang 7: Rechtliches Memorandum zur Übereinstimmung von TBS-biometrischen Lösungen mit der Verordnung (EU) 2016/679.

[5] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABl. L 295 vom 21.11.2018, S. 39.

[6] Insbesondere auf den Seiten 10 und 11.

[7] Dennoch sieht das Europäische Parlament vor, die Unterschrift auf Papier als Verfahren für den Notfall beizubehalten, wie auf S. 50 der Datenschutz-Folgenabschätzung (Anhang 4) erwähnt. „Möglichkeit, auf manuelle Unterschriften auf Papier zurückzugreifen (z. B. bei Problemen mit der Stromversorgung, die länger als zwei Stunden dauern)".

auf ein lokales Fingerabdrucklesegerät legt, scannt dieses Gerät den Fingerabdruck, um die erforderlichen Elemente zu extrahieren und eine neue biometrische Vorlage erstellen zu können. Diese Vorlage wird dann mit den biometrischen Vorlagen abgeglichen, die entweder in der zentralen Datenbank oder in der lokalen Datenbank des Lesegeräts gespeichert sind. Mit ihrer Speicherung nicht nur auf den beiden zentralen Servern des Parlaments, sondern auch in jedem lokalen Fingerabdruck-Lesegerät soll vermieden werden, dass wegen eines Netzausfalls die MdEP ihre Anwesenheit nicht bestätigen können. Wenn das System eine passende Vorlage findet, leuchtet auf dem Lesegerät ein grünes Licht auf, speichert es den Zeitstempel, und das System könnte so programmiert werden, dass es eine E-Mail-Benachrichtigung an den Abgeordneten versendet; wenn nicht, leuchtet ein rotes Licht auf.

Neben biometrischen Informationen erfordert die Verarbeitung auch **allgemeine, die Tätigkeit betreffende personenbezogene Angaben**: Name, Funktion, Anfangs- und Enddatum des Mandats, E-Mail-Adresse und persID-Nummer. Alle diese personenbezogenen Informationen stammen aus dem Abgeordnetenregister des Parlaments (CODICT). Sie werden dann sowohl in einer speziellen Datenbank zusammen mit den Daten über die Anwesenheit der MdEP (einschließlich der erhaltenen Zeitstempel) als auch in den lokalen Fingerabdruck-Lesegeräten und zentralen biometrischen Datenbanken gespeichert.

Bestimmte Anwesenheitsdaten (einschließlich Namen und Zeitstempel) können von den Bediensteten des Parlaments direkt abgefragt werden, um die Anwesenheit zu überprüfen. Bestimmte Nutzer (Bedienstete) der GD FINS[8] und der GD PERS (für Daten über die Plenartagungen des Parlaments) fungieren als Erheber und Empfänger personenbezogener Daten. Diese Nutzer erhalten Zugang zu den aus der CODICT-Datenbank und den Datenbanken mit den biometrischen Vorlagen der MdEP importierten Informationen ausschließlich nach dem Grundsatz „Kenntnis nur, wenn nötig".

Bezüglich der **Integration mit der Zahlungssoftware** besagt die Datenschutz-Folgenabschätzung, dass das System einmal täglich automatisch zwei XML-Dateien generiert und die persIDs aller Mitglieder auflistet, deren Anwesenheit erfolgreich registriert wurde. Diese XML-Dateien werden an einem vom Integrated Travel Expense Management System (iTEMS)[9] gescannten Netzstandort platziert, auf den befugte Bedienstete der GD FINS auf der Grundlage „Kenntnis nur, wenn nötig" zugreifen können. iTEMS importiert automatisch die Dateien und aktualisiert die Anwesenheitszeiten der Mitglieder, was die Zahlung von Tagegeldern auslöst, ohne dass es menschlichen Zutuns bedarf.

3. RECHTLICHE UND TECHNISCHE BEMERKUNGEN

3.1. Rechtmäßigkeit der Verarbeitung und Rechtsgrundlage (Artikel 5 der Verordnung)

Angesichts der Vorteile der vorgeschlagenen Lösung gegenüber dem derzeitigen CAR-System oder einer auf Zugangsausweisen basierenden Lösung geht der EDSB davon aus, dass der **Hauptgrund für die Entscheidung für die biometrische Lösung** des vorgeschlagenen Systems die **Verhinderung finanziellen Betrugs** ist (es soll also vermieden werden, dass das manuelle oder elektronische Anwesenheitsregister von einer anderen Person im Namen des MdEP unterzeichnet wird).[10] Eng mit diesem Zweck verknüpft dürfte nach Auffassung des

[8] Referat Reisekosten und Tagegelder der Mitglieder und Referat Informationstechnologie und E-Portal.

[9] Das Integrated Travel Expense Management System wird im Laufe des Jahres die derzeitige Reiseabrechnungssoftware des Parlaments ersetzen.

[10] Ein weiterer Grund ist die Möglichkeit für Mitglieder, ihre Anwesenheit zu belegen, wenn sie ihren Zugangsausweis vergessen und auch kein anderes Identitätsdokument bei sich haben.

EDSB der Wunsch stehen, dass die Abgeordneten als Vertreter der Unionsbürger[11] mit gutem Beispiel vorangehen und sich bei der Wahrnehmung ihrer Aufgaben von den allgemeinen Grundsätzen der Integrität, der Ehrlichkeit, der Rechenschaftspflicht und der Achtung des Ansehens des Europäischen Parlaments leiten lassen sollten.[12]

Wie bei jedem von einer EU-Einrichtung eingeleiteten Verarbeitungsvorgang muss das vorgeschlagene biometrische Registrierungssystem auf einem rechtmäßigen Grund gemäß Artikel 5 der Verordnung beruhen. Nach Ansicht des Europäischen Parlaments ist als **Grund für die Rechtmäßigkeit** des Verarbeitungsvorgangs, d. h. die Verarbeitung personenbezogener Daten über ein digitales System zur Bescheinigung der Anwesenheit von MdEP, Artikel 5 Absatz 1 Buchstabe b der Verordnung vorzuschlagen (was bedeutet, dass die Verarbeitung für die Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt).

Nach Auffassung des EDSB findet Artikel 5 Absatz 1 Buchstabe b nur auf Fälle Anwendung, in denen EU-Einrichtungen aufgrund einer rechtlichen Verpflichtung personenbezogene Daten verarbeiten müssen, ohne dass sie bei der Anwendung über Spielraum verfügen. Das bedeutet, dass die Verpflichtung selbst hinreichend konkret sein muss, was die von ihr vorgeschriebene Verarbeitung personenbezogener Daten betrifft. Da im vorliegenden Fall keine spezifische Verpflichtung des Europäischen Parlaments zur Verarbeitung biometrischer Daten besteht, sollte es den Verarbeitungsvorgang nicht auf Artikel 5 Absatz 1 Buchstabe b der Verordnung als Grundlage für die Rechtmäßigkeit stützen.

Folglich sollte das Europäische Parlament prüfen, ob **eine andere Grundlage** geltend gemacht werden kann, nämlich **Artikel 5 Absatz 1 Buchstabe a der Verordnung** – vorausgesetzt, die Verarbeitung personenbezogener Daten **ist notwendig und steht in einem angemessenen Verhältnis** zur Wahrnehmung einer Aufgabe, die das EU-Organ im öffentlichen Interesse wahrnimmt (Erforderlichkeit und Verhältnismäßigkeit, siehe Abschnitt 3.3).

Hinsichtlich der **Rechtsgrundlage** für die von ihm geplante Verarbeitung verweist das Europäische Parlament auf Artikel 156 der Geschäftsordnung des Europäischen Parlaments[13] sowie auf Artikel 12 Absatz 1 und Artikel 24 der DBAS[14].

Artikel 156 der Geschäftsordnung lautet:

In jeder Sitzung wird eine Anwesenheitsliste zur Unterzeichnung durch die Mitglieder ausgelegt. 2. Die Namen der Mitglieder, die in der Liste als anwesend eingetragen sind, werden im Protokoll der jeweiligen Sitzung als „anwesend" vermerkt. Die Namen der Mitglieder,

---

[11] Artikel 14 Absatz 2 EUV.

[12] Artikel 1 des Verhaltenskodex für die Mitglieder des Europäischen Parlaments in Bezug auf finanzielle Interessen und Interessenkonflikte (https://www.europarl.europa.eu/doceo/document/RULES-9-2019-07-02-ANN-01_EN.html).
Siehe auch Artikel 3 des Kodex für angemessenes Verhalten für die Mitglieder des Europäischen Parlaments im Rahmen ihres Mandats (https://www.europarl.europa.eu/doceo/document/RULES-9-2019-07-02-ANN-02_EN.html): „*Die Mitglieder dürfen das Personal nicht durch ihre Handlungen dazu verleiten oder ermutigen, die geltenden Rechtsvorschriften, internen Regelungen des Parlaments oder diesen Kodex zu missachten, zu umgehen oder dagegen zu verstoßen, oder ein derartiges Verhalten von Mitarbeitern, die unter ihrer Verantwortung stehen, zu dulden*."

[13] Geschäftsordnung – 9. Wahlperiode – Juli 2019, ABl. L 302 vom 22.11.2019, S. 1.

[14] Durchführungsbestimmungen zum Abgeordnetenstatut des Europäischen Parlaments, Beschluss des Präsidiums vom 19. Mai und 9. Juli 2008; PE422.536/BUR.

deren Abwesenheit durch den Präsidenten entschuldigt ist, werden im Protokoll der jeweiligen Sitzung als „entschuldigt" vermerkt.

Derweilen besagen die DBAS Folgendes:

Artikel 12
Anwesenheitsnachweis
1. Die Anwesenheit der Abgeordneten wird durch die persönliche Unterzeichnung der innerhalb des Plenarsaals oder in dem Sitzungssaal ausliegenden Anwesenheitsliste oder durch die persönliche Unterzeichnung der zentralen Anwesenheitsliste während der vom Präsidium festgelegten Öffnungszeiten bescheinigt. ***Ein elektronischer Nachweis für die Anwesenheit der Abgeordneten kann anstatt der persönlichen Unterzeichnung verwendet werden****.*[15]

Artikel 24
Tagegeld
1. Die Abgeordneten haben Anspruch auf ein Tagegeld für jeden Tag ihrer Anwesenheit:
(a) an einem Arbeits- oder Sitzungsort, bescheinigt gemäß Artikel 12, wenn sie sich auf einer Reise befinden, für die ihnen eine Erstattung im Rahmen der normalen Reisekosten gezahlt wird;
[...]

Diese Artikel sowie die Gesamtheit der DBAS und der Geschäftsordnung dienen der Umsetzung von Artikel 223 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (vormals Artikel 190 Absatz 5 des Vertrags zur Gründung der Europäischen Gemeinschaft), wonach das Europäische Parlament die Regelungen und allgemeinen Bedingungen für die Wahrnehmung der Aufgaben seiner Mitglieder festlegt.

Bereits in seinen ersten Bemerkungen im Jahr 2018 äußerte der EDSB Zweifel an der Entscheidung, die Verarbeitung biometrischer Daten[16] auf eine Bestimmung zu stützen, die es dem Europäischen Parlament erlaubt, eine „elektronische Bescheinigung" zu verwenden, die jedoch keinen spezifischen Verweis auf biometrische Daten enthält.

Damit die internen Vorschriften des Europäischen Parlaments als Rechtsgrundlage für den geplanten Verarbeitungsvorgang dienen können, und sofern es keine weniger einschneidenden Mittel zur Erreichung des verfolgten Ziels (in erster Linie Betrugsbekämpfung) gibt, ist der EDSB der Auffassung, dass diese Vorschriften angepasst werden und klar und konkret darauf hinweisen sollten, dass biometrische Daten (und nicht nur „elektronische Bescheinigungen") in der Regel[17] zum Nachweis der Anwesenheit verwendet werden (und nicht „verwendet werden können").

[15] Hervorhebung durch uns.

[16] Die Definition des Begriffs „biometrische Daten" umfasst keine handschriftlichen Unterschriften (Artikel 4 Absatz 14 der Verordnung: „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten".

[17] Handschriftliche Unterschriften auf Papier könnten eine Ausweichlösung bei einer Stromunterbrechung von mehr als zwei Stunden sein (siehe S. 50 der Datenschutz-Folgenabschätzung).

Empfehlung 1

Der EDSB ist der Auffassung, dass Artikel 5 Absatz 1 Buchstabe a der Verordnung als **Grund für die Rechtmäßigkeit** dieses Projekts herangezogen werden sollte, sofern die Verarbeitung für die Wahrnehmung einer Aufgabe im öffentlichen Interesse notwendig und verhältnismäßig ist und ihre Grundlage im Unionsrecht verankert ist.

Was Letzteres anbelangt, so ist der EDSB der Auffassung, dass der derzeitige Wortlaut der internen Vorschriften des Europäischen Parlaments **als Rechtsgrundlage** für die Verarbeitung *biometrischer* Daten als *wichtigstes Mittel* zur Bescheinigung der Anwesenheit nicht hinreichend klar ist, und empfiehlt dem Europäischen Parlament, diese Regelung entsprechend zu ändern.

Hinsichtlich spezifischer Aspekte im Zusammenhang mit **automatisierter Entscheidungsfindung** gemäß Artikel 24 der Verordnung verweist der EDSB auf Abschnitt 3.4.

3.2. Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 10 der Verordnung)

Wie in der Datenschutz-Folgenabschätzung auf Seite 12 hervorgehoben, sind sowohl Fingerabdruckbilder als auch extrahierte biometrische Vorlagen besondere Kategorien personenbezogener Daten im Sinne von Artikel 10 der Verordnung. Ihre Verarbeitung ist durch die Verordnung grundsätzlich verboten, mit Ausnahme einiger der in Artikel 10 Absatz 2 der Verordnung genannten Fälle.

Der Grund, warum die Verarbeitung besonderer Datenkategorien so stark eingeschränkt ist, ist auf ihre Auswirkungen auf die Grundrechte der betroffenen Personen und insbesondere auf das in Artikel 8 der Charta der Grundrechte der Europäischen Union verankerte Recht auf Datenschutz zurückzuführen. Biometrische Daten können nicht oder zumindest nicht leicht geändert werden. Im Falle eines Verstoßes gegen die Vertraulichkeit können die Fingerabdrücke der MdEP nicht zurückgesetzt oder aktualisiert werden. Wenn die Fingerabdrücke eines bestimmten Mitglieds nicht vom System erkannt werden, ist es nicht möglich, ihm neue Fingerabdrücke zu beschaffen.

Die Verarbeitung von Fingerabdrücken birgt spezifische Risiken, die gemindert oder vermieden werden müssen. So haben beispielsweise wissenschaftliche Untersuchungen gezeigt, dass gespeicherte Fingerabdruckvorlagen die teilweise Wiederherstellung des ursprünglichen Fingerabdrucks ermöglichen.[18] Eine solche partielle Wiederherstellung ist mitunter so genau, dass ein anderes biometrisches System den Abdruck als den ursprünglichen Abdruck erkennt.

In der Datenschutz-Folgenabschätzung wird vorgeschlagen, das System solle sich bei der Verarbeitung biometrischer Informationen auf die Ausnahme gemäß Artikel 10 Absatz 2 Buchstabe d der Verordnung stützen, doch wird diese Wahl nicht eindeutig begründet. Darüber hinaus soll mit dieser Bestimmung eine Rechtsgrundlage geschaffen werden, damit z. B. Gewerkschaften und religiöse Organisationen, die in die EU-Institutionen integriert sind, ihren Tätigkeiten nachkommen können (bei denen es standardmäßig um sensible Informationen

[18] Cappelli, Raffaele & Maio, Dario & Lumini, Alessandra & Maltoni, Davide. (2007). Fingerprint Image Reconstruction from Standard Templates. IEEE Trans. Pattern Anal. Mach. Intell. 29. 1489-1503. 10.1109/TPAMI.2007.1087.

geht). Der EDSB ist daher der Auffassung, dass diese Bestimmung nicht auf die Verarbeitung biometrischer Daten der MdEP zur Bescheinigung ihrer Anwesenheit an Arbeitsorten und Sitzungen angewandt werden sollte. Das Europäische Parlament könnte **Artikel 10 Absatz 2 Buchstabe g** prüfen, wonach besondere Kategorien von Daten verarbeitet werden dürfen, sofern dies „aus Gründen eines **erheblichen öffentlichen Interesses erforderlich** ist, und zwar auf der Grundlage des Unionsrechts, das **in angemessenem Verhältnis** zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und **angemessene und spezifische Maßnahmen** zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht.[19]

Das Europäische Parlament sollte berücksichtigen, dass möglicherweise Verletzungen, Unfälle, Gesundheitszustand (z. B. Lähmung) oder andere Umstände vorübergehend oder dauerhaft einige MdEP davon abhalten könnten, das System zu nutzen. In der Datenschutz-Folgenabschätzung wird zwar *die Möglichkeit erwähnt, auf handschriftliche Unterschriften auf Papier zurückzugreifen (z. B. bei einem Ausfall der Stromversorgung, der länger als zwei Stunden dauert)*[20], es ist aber nicht vorgesehen, dass das System für bestimmte MdEP nicht geeignet sein könnte.

Empfehlung 2:
Da Artikel 10 Absatz 2 Buchstabe d der Verordnung auf den Verarbeitungsvorgang nicht anwendbar ist, sollte das Europäische Parlament klarstellen, auf welche andere Ausnahme es bei der Verarbeitung **besonderer Kategorien personenbezogener Daten** gemäß Artikel 10 der Verordnung zurückgreifen würde, wie etwa Artikel 10 Absatz 2 Buchstabe g, und **ausführlicher begründen**, warum diese Ausnahme Anwendung finden würde.

Empfehlung 3:
Sollte das Europäische Parlament letztendlich das biometrische System zum Nachweis der Anwesenheit einführen, empfiehlt der EDSB dem Europäischen Parlament, ein alternatives Verfahren für die Anwesenheitsbescheinigung einzuführen, um sicherzustellen, dass die MdEP, deren Fingerabdrücke nicht erkannt werden, ihre Anwesenheit trotzdem nachweisen können.

3.3. Notwendigkeit und Verhältnismäßigkeit der Verarbeitung im Hinblick auf das verfolgte Ziel

Die Verhinderung von Finanzbetrug, einschließlich der Tatsache, dass demokratisch gewählte Personen mit gutem Beispiel vorangehen müssen, kann als ein **Grund für ein wesentliches öffentliches Interesse** betrachtet werden, der die Verarbeitung biometrischer Daten gemäß Artikel 10 Absatz 2 Buchstabe g der Verordnung[21] rechtfertigen kann, sofern insbesondere die Verwendung biometrischer Daten erforderlich ist und in einem angemessenen Verhältnis zu diesem Ziel steht.[22]

---

[19] Hervorhebung durch uns. Mit dieser Bestimmung werden die Anforderungen von Artikel 52 der Charta der Grundrechte für jede Einschränkung der Ausübung der in der Charta anerkannten Grundrechte, einschließlich des Rechts auf Datenschutz, erfüllt.

[20] Siehe Seite 50 von Anhang 4 (Datenschutz-Folgenabschätzung).

[21] Zur Verwendung biometrischer Daten zur Verhinderung von Identitätsbetrug siehe Stellungnahme des EDSB vom 15. Mai 2014 zur Verwendung biometrischer Kontrolleinrichtungen durch Sicherheitsbedienstete im Europäischen Parlament: 14-05-15_pc_ep_biometric_data_en.pdf (europa.eu)

[22] Nach Kenntnis des EDSB kann ein neuer Ausweis innerhalb von Minuten ausgestellt werden. Der zweite Vorteil der Nutzung biometrischer Daten, den das Europäische Parlament vorgebracht hat, scheint weder stichhaltig noch notwendig/verhältnismäßig zu sein.

Wie bereits in den Hintergrundinformationen erwähnt, hat der EDSB schon früher betont, wie wichtig eine gründliche Prüfung der **Erforderlichkeit und Verhältnismäßigkeit** für dieses Projekt ist.

„Erforderlichkeit" impliziert das Erfordernis einer kombinierten, faktengestützten Bewertung der Wirksamkeit der Maßnahme mit Blick auf das angestrebte Ziel und auf die Frage, ob sie im Vergleich zu anderen Optionen für das Erreichen desselben Ziels weniger eingreifend ist. Sollte sich die Maßnahme als erforderlich erweisen, muss die Maßnahme nach wie vor darauf geprüft werden, welche Garantien mit einer Maßnahme einhergehen sollten, um die Risiken, die mit der geplanten Maßnahme für die Grundrechte und Grundfreiheiten der betroffenen Personen verbunden sind, auf ein akzeptables/angemessenes Maß zu reduzieren. Ein weiterer Faktor, der bei der Prüfung der Verhältnismäßigkeit einer vorgeschlagenen Maßnahme zu berücksichtigen ist, ist die Effektivität der vorhandenen Maßnahmen gegenüber der geplanten. Liegen bereits Maßnahmen für einen ähnlichen oder den gleichen Zweck vor, sollte deren Effektivität im Rahmen der Beurteilung der Verhältnismäßigkeit systematisch bewertet werden.[23]

In diesem Zusammenhang begrüßt der EDSB Abschnitt 6 der Datenschutz-Folgenabschätzung, der sich ausschließlich mit der Notwendigkeit und Verhältnismäßigkeit der biometrischen Registrierung befasst. Um diese Ausführungen weiter zu untermauern, stellt das Europäische Parlament einen Vergleich zwischen dem System und zwei früheren Systemen an, die es getestet oder verwendet hat:

- eine zentrale physische Anwesenheitsliste, also das derzeit verwendete System;
- ein computergestütztes System, bei dem die Mitglieder ihren persönlichen Zugangsausweis von Ausweislesegeräten lesen lassen, die im Anschluss an frühere Bemerkungen des EDSB getestet wurde.

Im Rahmen der Konsultation des Europäischen Parlaments im Jahr 2018 legte der EDSB einige Alternativen fest, die in Betracht gezogen werden könnten, um die Verarbeitung biometrischer Daten zu vermeiden. Von diesen scheint nur eine erwogen worden zu sein, nämlich die Verwendung von Zugangsausweisen.

Der EDSB hält fest, dass sowohl für das derzeitige papiergestützte System als auch für das Zugangsausweissystem eine Folgenabschätzungstabelle erstellt wurde, in der unter anderem die verschiedenen Risiken, ihre Wahrscheinlichkeit und ihre Auswirkungen sowie mögliche Strategien zur Minderung oder Duldung der Risiken aufgeführt sind. Daraus ergab sich, dass „die Umsetzung beider Lösungen mehrere hohe und kritische Risiken mit Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen, den Ruf und die Finanzen des Organs oder die Sicherheit der verarbeiteten Daten [offenbart]".

Bei näherer Betrachtung der Bewertung sind einige wichtige Elemente nach wie vor nicht ausreichend spezifiziert und wurden nicht erläutert. Der EDSB stellt beispielsweise fest, dass es keine Hinweise auf eine Leitlinie oder Strategie gibt, aus der hervorgeht, wie zwischen „unwahrscheinlich" und „möglich" unterschieden wird. Dies scheint jedoch von

[23] Siehe die Leitlinien des EDSB zur Notwendigkeit und Verhältnismäßigkeit legislativer Maßnahmen, die *mutatis mutandis* auf alle Maßnahmen angewandt werden können, die darauf abzielen, das in Artikel 8 der Charta der Grundrechte verankerte Recht auf Datenschutz einzuschränken:
- 17-04-11 Toolkit zur Beurteilung der Erforderlichkeit von Maßnahmen;
- 19-12-19 Leitlinien zur Verhältnismäßigkeit.

entscheidender Bedeutung zu sein, da die unbestimmte „mögliche“ Häufigkeit mit allen als hoch eingestuften Risiken einhergeht.

Darüber hinaus sind die meisten Nachteile, die den Zugangsausweissystemen zugeschrieben werden, unklar oder nicht ausreichend nachgewiesen, wie z. B.:

- „*Es besteht keine Kontrolle über den Schutz personenbezogener Daten: Die verarbeiteten Ausweisnummern werden auf den Ausweis aufgedruckt*“. Nach Kenntnis des EDSB werden die Zugangsausweisnummern (neben anderen personenbezogenen Daten wie dem vollständigen Namen und dem Foto) auf allen Zugangsausweisen des Parlaments aufgedruckt. Nicht klar wird, warum in der Abschätzung davon ausgegangen wird, dass dies nur für MdEP ein schwerwiegendes Datenschutzproblem darstellt. Unklar ist auch, wie die Kenntnis der Nummer eines MdEP-Zugangsausweises es Dritten ermöglichen würde, die Anwesenheit des MdEP in einem der drei Systeme zu bescheinigen.
- „*Die Bestätigung der Anwesenheit in Echtzeit ist für eine gewisse Zeit (sogar einen Tag lang) beeinträchtigt, wenn der Zugangsausweis der Mitglieder von der GD SAFE neu ausgestellt wird (Unwirksamkeit und Ineffizienz)*.“ Soweit der EDSB weiß, dauert die Neuausstellung eines Zugangsausweises nur Minuten. Darüber hinaus ist eine der wichtigsten Kontrollen, die laut Datenschutz-Folgenabschätzung zur Gewährleistung der vorgeschlagenen Systemverfügbarkeit in Betracht gezogen werden, die „Möglichkeit, auf handschriftliche Unterschriften auf Papier zurückzugreifen (z. B. bei Unterbrechungen der Stromversorgung, die länger als zwei Stunden dauern)“. Es ist uns nicht klar, warum dieser Nachteil relevant ist, wenn dieselbe Ausweichlösung genutzt werden könnte, um ihn zu beheben.
- „*Mitglieder können mehrere (auch abgelaufene) Zugangsausweise besitzen, sie verwenden und somit die Datenbank belasten (Ineffizienz)*.“ Wenn die automatische Tür im Parlament einen abgelaufenen Zugangsausweis erkennen kann, ist uns nicht klar, warum das Anwesenheitssystem dies nicht auch tun und die Verwendung abgelaufener Zugangsausweise verhindern könnte.
- „*Aufgrund der Ähnlichkeit mit dem Zugangssystem der GD SAFE verwenden die Mitglieder möglicherweise die falschen Lesegeräte (Unwirksamkeit)*.“ Unabhängig von der implementierten Lösung würden eine klare äußere Kennzeichnung oder unterschiedliche Farben auf der Benutzeroberfläche dieses Problem lösen.

Bei der weiteren Analyse des auf Zugangsausweisen basierenden Systems hat das Europäische Parlament zwei Risiken als „hoch“ eingestuft:

- Risiko des Identitätsbetrugs, wenn z. B. ein MdEP (auch) für ein abwesendes MdEP unterzeichnen kann;
- Risiko des Zugriffs auf personenbezogene Daten (Nummer des Zugangsausweises) für Unbefugte.

Es ist unklar, ob dem Europäischen Parlament Daten über die Zahl der Fälle von Identitätsbetrug vorliegen, die möglicherweise während des Tests des Zugangsausweissystems (an dem mehr als 270 Mitglieder teilgenommen haben) aufgetreten sind. Liegen solche Daten nicht vor, sollte erläutert werden, warum das Szenario höher als „unwahrscheinlich“ eingestuft wird, warum das Europäische Parlament also der Ansicht ist, dass dies mehr ist als eine Randerscheinung. Stehen keine Daten zur Verfügung und kann keine Schätzung vorgenommen werden, sollte dies insbesondere deshalb erwähnt werden, weil die Verhinderung von Betrug oder Identitätsbetrug der Hauptzweck für den Übergang zum biometrischen System ist. Da Verhinderung von Betrug das wichtigste Ziel der Verarbeitung biometrischer Daten ist, **muss**

das Europäische Parlament seine Einschätzung der Betrugswahrscheinlichkeit weiter begründen und dokumentieren.

In Bezug auf das Risiko des unbefugten Zugangs zu einer auf dem Zugangsausweis aufgedruckten Ausweisnummer stellt der EDSB zunächst ein ähnliches Problem fest, da die Risikowahrscheinlichkeit mit „möglich" bewertet wird (was zu einer hohen Punktzahl führt). Darüber hinaus ist dem EDSB nicht klar, warum die einzige vorgeschlagene Risikominderungsstrategie darin besteht, „**ein alternatives computergestütztes System einzuführen, das nicht auf der Verwendung von Zugangsausweisen beruht**", anstatt die Nummern nicht sichtbar aufzudrucken, sondern (ausschließlich) RFID-Ausweise zu verwenden.

Schließlich nimmt der EDSB zur Kenntnis, dass die **auf Zugangsausweisen basierende Lösung** die einzige Alternative war, die vom Europäischen Parlament geprüft wurde. Im Hinblick auf das Erreichen der oben genannten Zwecke gibt es jedoch möglicherweise **andere Lösungen**, die ein akzeptables Maß an Sicherheit und Betrugsprävention bieten könnten, ohne biometrische Daten zu verarbeiten. Ein Beispiel könnte ein einmaliges Passwort oder ein ähnliches Bestätigungsmerkmal (z. B. NFC- oder Bluetooth-basierte Authentifizierung) sein, das auf den Telefonen der MdEP generiert wird, wenn sie ihre Anwesenheit bestätigen. Hier wird die als „leicht" empfundene Weitergabe des Zugangsausweises durch die mangelnde Bereitschaft gemindert, das Mobiltelefon mit Assistenten oder anderen MdEP zu teilen. Auch die Wahrscheinlichkeit, dass die Mitglieder ihr Telefon vergessen oder verlieren, ist möglicherweise geringer. Dies sind nämlich zwei weitere vom Europäischen Parlament identifizierte Risiken.

Empfehlung 4:

Zwar lehnt der EDSB nicht grundsätzlich eine bestimmte Technologie ab oder verlangt keine bestimmte Technologie, doch sollten die Verantwortlichen sicherstellen, dass eine Prüfung der Notwendigkeit und Verhältnismäßigkeit eine **gründliche Bewertung der verfügbaren, weniger einschneidenden Alternativen vorsieht**. Daher empfiehlt der EDSB dem Europäischen Parlament, **die Durchführbarkeit anderer verfügbarer Alternativen**, die nicht die Verwendung sensibler Daten erfordern würden, **zu dokumentieren**, alle Optionen zu vergleichen und seine Schlussfolgerungen zu dokumentieren.

3.4. Automatisierte Einzelentscheidungen (Artikel 24 der Verordnung)

Der EDSB geht davon aus, dass die geplante Verarbeitung kein menschliches Eingreifen[24] erfordert, was die Anwendung von Artikel 24 der Verordnung auf **Entscheidungen** auslöst, **die ausschließlich auf einer automatisierten Verarbeitung beruhen**, die **rechtliche Wirkung** gegenüber der betroffenen Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Entscheidungen, die „ausschließlich auf einer automatisierter Verarbeitung beruhen", beinhalten keine menschliche Beteiligung an der Entscheidungsfindung. Wie in den Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling[25] betont wird: „*Der Verantwortliche kann die Bestimmungen des Artikels 22* [~ Artikel 24 der Verordnung] *nicht*

[24] Siehe weiter oben Punkt 2. Beschreibung der Verarbeitung.

[25] Vgl. S. 22 der Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, (WP251rev.01), zuletzt überarbeitet und angenommen am 6. Februar 2018 (gebilligt vom EDSA).

umgehen, indem er eine Person in die Entscheidung einbezieht. Wenn jemand beispielsweise routinemäßig automatisch erstellte Profile auf Personen anwendet, die keinen tatsächlichen Einfluss auf das Ergebnis haben, wäre dies dennoch eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung. Um für eine direkte Einbeziehung einer Person zu sorgen, muss der Verantwortliche gewährleisten, dass es sich nicht nur um eine symbolische Geste handelt, sondern dass die Entscheidung einer echten Aufsicht unterliegt. Daher sollte die Entscheidung von einer Person getroffen werden, die zur Änderung derselben befugt und befähigt ist."

Sofern das Verfahren nicht irgendwann mit der sinnvollen Einbeziehung einer Person verbunden ist, gilt Artikel 24 der Verordnung für die geplante Verarbeitung, die rechtliche Wirkung gegenüber den Mitgliedern entfaltet, nämlich die (Nicht-)Auszahlung ihrer Tagegelder.

Artikel 24 Absatz 1 enthält ein **allgemeines Verbot** von Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung beruhen. Artikel 24 Absatz 2 der Verordnung regelt drei Ausnahmen, die ausschließlich automatisierte individuelle Entscheidungen ermöglichen:

(i) Die Entscheidung muss für den Abschluss eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich sein;
(ii) sie muss aufgrund von Rechtsvorschriften […] zulässig sein und diese Rechtsvorschriften müssen angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
(iii) sie muss mit ausdrücklicher Einwilligung der betroffenen Person erfolgen.

Darüber hinaus ist eine automatisierte Entscheidung, die auf besonderen Kategorien personenbezogener Daten beruht, nur zulässig, wenn **Artikel 10 Absatz 2 Buchstabe** a oder **g** der Verordnung gilt (Artikel 2$ Absatz 4 der Verordnung).

(i) Erhebliches öffentliches Interesse steht auf dem Spiel

Wie bereits erwähnt[26], können die Verhinderung von Betrug sowie die Achtung der allgemeinen Grundsätze der Integrität, der Ehrlichkeit, der Rechenschaftspflicht und der Achtung des Ansehens des Europäischen Parlaments durch die Mitglieder als Vertreter der Unionsbürgerinnen und Unionsbürger als **Grund eines wesentlichen öffentlichen Interesses** angesehen werden, das in den Anwendungsbereich von Artikel 10 Absatz 2 Buchstabe g der Verordnung fällt.

(ii) Das Konzept „Rechtsvorschriften der Union"

Anwendbare Rechtsgrundlage muss **eine Rechtsvorschrift der Union sein, aufgrund derer eine automatisierte Entscheidung zulässig ist** (Artikel 24 Absatz 2 Buchstabe b der Verordnung).[27] Nach Ansicht des EDSB bezeichnet der Ausdruck „Rechtsvorschrift der Union" grundsätzlich einen Gesetzgebungsakt (d. h. eine Verordnung) oder zumindest einen Durchführungsrechtsakt, der auf einem Gesetzgebungsakt beruht. In Anbetracht der Tatsache, dass es sich bei dem Organ, um das es hier geht, um ein Parlament handelt, und dass das Primärrecht dem Europäischen Parlament die Befugnis verleiht, seine eigenen Vorschriften zu

[26] Abschnitt 3.2. Siehe auch S. 26 der Leitlinien für automatisierte Einzelentscheidungen, wonach automatisierte Entscheidungen zur Betrugsbekämpfung genutzt werden können.

[27] Erwägungsgrund 43 sieht vor, dass die automatisierte Entscheidungsfindung nur erlaubt sein sollte, wenn dies nach dem Unionsrecht ausdrücklich zulässig ist.

erlassen[28], räumt der EDSB in diesem speziellen Fall ein, dass interne Vorschriften einen automatisierten Entscheidungsprozess wie den geplanten vorsehen können. Wie bereits weiter oben empfohlen (Abschnitt 3.2.) sollten diese interne Vorschriften jedoch ausdrücklich vorsehen, dass die Anwesenheit der Mitglieder im Wesentlichen mit Hilfe biometrischer Technologie bescheinigt wird.

(iii) Angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person

Artikel 24 Absatz 2 Buchstabe b schreibt vor, dass **in diesen Vorschriften** nicht nur die automatisierte Verarbeitung als solche, **sondern auch angemessene Maßnahmen** zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der Mitglieder **festgelegt werden**.[29] Wie in Erwägungsgrund 43 erwähnt, sollen diese angemessenen Garantien die spezifische Unterrichtung der betroffenen Person (siehe weiter unten Abschnitt 3.6.) und den Anspruch auf direktes Eingreifen einer Person, auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf Anfechtung der Entscheidung umfassen.

Empfehlung 5:
Soweit die geplante Verarbeitung kein sinnvolles Eingreifen einer Person erfordert, empfiehlt der EDSB dem Europäischen Parlament, **seine internen Vorschriften** über die Verwendung biometrischer Daten zur Bescheinigung der Anwesenheit der Mitglieder durch Aufnahme **angemessener Maßnahmen** zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person **zu ergänzen** (Artikel 24 Absatz 2 Buchstabe b der Verordnung).

3.5. Datenminimierung

Als Maßnahme zur möglichst geringen Verwendung (biometrischer) Daten hebt das Europäische Parlament hervor, dass anstelle von Rohbildern der Fingerabdrücke biometrische Vorlagen für die Verarbeitung verwendet werden. Es sei darauf hingewiesen, dass die Verwendung biometrischer Vorlagen, Signaturen oder Muster ein Standardverfahren für die biometrische Identifizierung ist. Diese Muster erfassen zahlenmäßig die physischen Merkmale, die es Algorithmen ermöglichen, Menschen zu identifizieren und voneinander zu unterscheiden. Die Verwendung biometrischer Vorlagen an sich sollte daher nicht als Maßnahme zur Minimierung personenbezogener Daten betrachtet werden.

Im Gegensatz dazu geht aus Anhang 6.1. (insbesondere aus den Antworten 2.C.6 und 2.C.9) hervor, dass anscheinend der Auftragnehmer einen proprietären Algorithmus und ein Vorlagenformat verwenden würde, in dem im Vergleich zu einer ISO-Standardvorlage deutlich mehr Daten gespeichert würden – zusätzlich beispielsweise Informationen über Poren und die Häufigkeit von Fingererhebungen. In der Begründung dieses proprietären Modells heißt es: „*ISO-Vorlagen sind aufgrund der begrenzten Menge und Art der Daten nicht geeignet, größere Gruppen (mehr als 100 Personen) zu identifizieren*“, und „*diese zusätzlichen Daten ermöglichen eine zuverlässige Identifizierung von Datenbanken mit Tausenden von Nutzern*“.[30]

[28] Artikel 223 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union.

[29] Artikel 10 Absatz 2 Buchstabe g und Artikel 24 Absatz 4 sehen ebenfalls angemessene Maßnahmen vor, doch verlangt Artikel 24 Absatz 2 Buchstabe b, dass diese Garantien in den Vorschriften enthalten sein müssen, die die automatisierte Entscheidung erlauben.

[30] Anhang 6.1 Technologische Lösung und Infrastruktur.

Der EDSB hält fest, dass in einem NIST-Bericht[31] verschiedene Vorlagen anhand der Fingerabdruckvorlage von INCITS 378 auf Datensätze Tausender Fingerabdrücke getestet wurden. Auch wenn die Verwendung bestimmter proprietärer Formate gegenüber internationalen Standards derzeit einen Vorteil im Hinblick auf die Genauigkeit bieten könnte, sollte das Europäische Parlament prüfen, ob der Anstieg der Genauigkeit die verringerte Datenübertragbarkeit wert ist. Im vorliegenden Fall würde die Zahl der Nutzer weniger als tausend betragen, was die Notwendigkeit der Erfassung dieser zusätzlichen Daten in Frage stellen würde. Ferner hegt der EDSB Bedenken, dass sich das Europäische Parlament mit einer Entscheidung für eine proprietäre Lösung an den Auftragnehmer „binden" könnte, da er keine vollständige Garantie dafür bietet, dass seine Vorlage in ein ISO-Format exportiert werden könnte. Dies kann dazu führen, dass MdEP ihre Fingerabdrücke erneut registrieren müssen, wenn das Europäische Parlament entweder freiwillig oder gezwungenermaßen den Auftragnehmer wechseln müsste.

Empfehlung 6:
Der EDSB empfiehlt dem Europäischen Parlament, weiter zu prüfen, ob in Anbetracht des registrierten Personenkreises das vorgeschlagene System mit allen zusätzlichen biometrischen personenbezogenen Daten eingerichtet werden muss.

Wenn das System mit weniger zusätzlichen Informationen angemessen eingerichtet werden könnte, fordert der EDSB das Europäische Parlament auf, seinen Auftragnehmer zu beauftragen, **die Menge der** verwendeten **personenbezogenen Daten** wirksam **zu minimieren**.

3.6. Informationspflicht gegenüber den betroffenen Personen

Gemäß den Artikeln 14 bis 16 der Verordnung sollte das Europäische Parlament den Datenschutzhinweis über die Anwesenheitsliste aktualisieren und sicherstellen, dass die Mitglieder vor Beginn der Verarbeitung **konkret** über das neue System und alle damit verbundenen Modalitäten **informiert** werden.

Soweit die Verarbeitung eine automatisierte Entscheidungsfindung beinhaltet, sollten die Unterrichtung der Mitglieder spezifische Informationen umfassen, d. h. aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für sie (Artikel 15 Absatz 2 Buchstabe f und Artikel 16 Absatz 2 Buchstabe f der Verordnung).

Empfehlung 7:
Im Einklang mit den Artikeln 14 bis 16 der Verordnung empfiehlt der EDSB dem Europäischen Parlament, den Datenschutzhinweis über die Anwesenheitsliste zu aktualisieren und sicherzustellen, dass die Mitglieder vor Beginn der Verarbeitung **konkret** über das neue System und alle damit verbundenen Modalitäten **informiert** werden.

Beinhaltet die Verarbeitung eine automatisierte Entscheidungsfindung, sollte diese Unterrichtung aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der Verarbeitung umfassen (Artikel 15 Absatz 2 Buchstabe f und Artikel 16 Absatz 2 Buchstabe f der Verordnung).

[31] Vgl. MINEX Performance and Interoperability of the INCITS 378 Fingerprint Template | NIST.

4. SCHLUSSFOLGERUNG

Der EDSB begrüßt die erheblichen Anstrengungen des Europäischen Parlaments bei der Analyse der Auswirkungen des Übergangs zu einem biometrischen System zur Bescheinigung der Anwesenheit der Mitglieder auf den Datenschutz.

Die vorstehende Analyse hat jedoch einige kritische Bedenken deutlich gemacht, die ausgeräumt werden müssen. Der EDSB hat daher in dieser Stellungnahme mehrere Empfehlungen ausgesprochen, damit der Verordnung Genüge getan werden kann.

Das Europäische Parlament sollte insbesondere:

1) sich auf Artikel 5 Absatz 1 Buchstabe a (und nicht Artikel 5 Absatz 1 Buchstabe b) der Verordnung als **Grund für die Rechtmäßigkeit** stützen, sofern die Verarbeitung für die Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich ist und ihre Grundlage auf dem Unionsrecht beruht, und es sollte seine internen Vorschriften dahingehend ändern, dass sie als **Rechtsgrundlage** für die Verarbeitung *biometrischer* Informationen als *vorrangiges Mittel* zur Bescheinigung der Anwesenheit herangezogen werden können, und es wird dem Europäischen Parlament empfohlen, diese Vorschriften entsprechend zu ändern;

2) die Ausnahme klarstellen, auf die sich das Europäische Parlament bei der Verarbeitung **besonderer Kategorien personenbezogener Daten** gemäß Artikel 10 der Verordnung stützen würde, wie etwa Artikel 10 Absatz 2 Buchstabe g; ferner sollte es ausführlicher begründen, warum diese Ausnahme zur Anwendung kommen würde;

3) ein alternatives Verfahren für den Nachweis der Anwesenheit einrichten, um sicherzustellen, dass MdEP, deren Fingerabdrücke nicht erkannt werden, ihre Anwesenheit trotzdem bestätigen können;

4) die Durchführbarkeit **anderer verfügbarer Alternativen** dokumentieren, die nicht die Verwendung sensibler Daten erfordern würden, alle Optionen vergleichen und seine Schlussfolgerungen dokumentieren;

5) soweit die geplante Verarbeitung kein sinnvolles Eingreifen einer Person erfordert, **seine internen Vorschriften** über die Verwendung biometrischer Daten zur Bescheinigung der Anwesenheit der Mitglieder durch Aufnahme **angemessener Maßnahmen** zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person ergänzen (Artikel 24 Absatz 2 Buchstabe b der Verordnung);

6) weiter prüfen, ob in Anbetracht des registrierten Personenkreises das vorgeschlagene System mit allen zusätzlichen biometrischen personenbezogenen Daten eingerichtet werden muss; wenn das System mit weniger zusätzlichen Informationen angemessen eingerichtet werden könnte, sollte es seinen Auftragnehmer beauftragen, die Menge der verwendeten personenbezogenen Daten wirksam zu **minimieren**;

7) den Datenschutzhinweis über die Anwesenheitsliste aktualisieren und sicherstellen, dass die Mitglieder vor Beginn der Verarbeitung **konkret** über das neue System und alle damit verbundenen Modalitäten **informiert** werden. Beinhaltet die Verarbeitung eine automatisierte Entscheidungsfindung, sollten aussagekräftige Informationen über die

involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der Verarbeitung aufgenommen werden.

Der EDSB erwartet, dass das Europäische Parlament **die oben genannten Empfehlungen umsetzt und** innerhalb von **drei Monaten** nach Ergehen dieser Stellungnahme **Belege** für diese Umsetzung **vorlegt**.

Brüssel, 29. März 2021

[elektronisch unterzeichnet]

Wojciech Rafał WIEWIÓROWSKI