EDPS Opinion on the use of a computerised system by the European Parliament for the digitalisation of the Plenary and central attendance registers through biometric technology
(Joint cases 2020-0921 & 2021-0355)

1. BACKGROUND

This Opinion concerns an updated system for the attestation of the presence of Members of the European Parliament (MEPs). The system seeks to digitalise the European Parliament's Central Attendance Register (CAR) for MEPs by replacing the existing paper-based signing system with a solution based on an optical fingerprint scanner. The system will be used in order to attest MEPs' attendance under Article 12 of the IMMS[1] and to pay them the corresponding daily allowances under Article 24 of the IMMS.

The European Data Protection Supervisor (EDPS) was first informally asked to provide advice on this project on 18 June 2018, by the European Parliament's Data Protection Officer (DPO).[2] At that stage, the EDPS noted that the use of a biometric based system for the monitoring of MEPs was not demonstrated to be necessary and, therefore, the envisaged processing of personal data would be in breach of Article 5 of Regulation (EC) 45/2001.[3] In particular, the EDPS was of the opinion that the same purpose could be achieved by less intrusive means, such as:

- a PIN code;
- clocking-in systems via magnetic bands;
- two-factor authentication, by the combination of more than one of the abovementioned solutions;
- random and periodic checks of the signatures/presences by human monitoring.

The EDPS further noted that, even if the necessity of the project had been established, the processing of biometric data would still need to follow and take into account the outcome of a data protection risk assessment (DPIA).

Following a meeting on 26 June 2018 between the European Parliament and the EDPS, the European Parliament resolved to internally assess alternative and less intrusive systems for the MEPs' presence registration.

On 7 October 2020, MEPs brought to the attention of the EDPS that the European Parliament was now moving forward with an update of its central attendance registry by processing MEPs' biometric data. In order to verify whether its earlier concerns had been addressed, the EDPS decided to request from the Parliament further information on the matter.

---

1 Implementing Measures for the statute of Members of the European Parliament, Bureau Decision of 19 May and 9 July 2008, as amended by the EP Bureau Decision of 17 June 2019, *PE422.536/BUR*.

2 EDPS case number 2018-0553.

3 Regulation (EC) 45/2001 has since been replaced with Regulation (EU) 2018/1725.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: +32 2-283 19 00 - Fax: +32 2-283 19 50

On 16 October 2020, the EDPS sent a request for information to the European Parliament. On 11 November 2020, the EDPS received the response of the European Parliament, which comprised both of a letter addressing the specific questions of the EDPS as well as eight Annexes[4].

In view of the above, the EDPS has decided to issue this own-initiative Opinion based on Article 57(1)(g) of Regulation EU) 2018/1725 (the Regulation)[5].

2. DESCRIPTION OF THE PROPOSED PROCESSING

The European Parliament provided the EDPS with a DPIA regarding the attendance control system update. According to the DPIA[6], MEPs will attest their attendances digitally by scanning their fingerprint onto the fingerprint reader, which will log their presence in the system by means of a timestamp. This system will completely replace the current attendance control system, which involves signing in using a signature (i.e. it will not digitalise the signing requirement) and will not rely on any other piece of information such as a password.[7]

The process will start by the enrolment of MEP's encrypted fingerprint templates in the system's central database and in each of the readers installed in the European Parliament premises. Each time an MEP places his/her finger on a Local Fingerprint Reader, that reader will scan the fingerprint to extract the necessary elements in order to create a new biometric template. This template will then be compared with the biometric templates stored in either the central database or the reader's local database. The reason why these are stored in each Local Fingerprint Reader in addition to the two central Parliament servers is to avoid that a network failure prevents MEPs from attesting their attendance. If the system finds a matching template, the reader displays a green light, logs the time stamp, and the system could be programmed to send an email notification to the Member; if not, the reader displays a red light.

---

4 A main annex outlining the structure of the different documents;
Annex 1.1/1.2.: Article 20 of the Statute for Members of the European Parliament (2005/684/EC, Euratom) / Article 12 (1) of the Implementing Measures for the Statute for Members of the European Parliament (Bureau Decision of 19 May and 9 July 2008);
Annex 2: Minutes of the Bureau meeting of 11 June 2018;
Annex 3: Minutes of the Bureau meeting of 17 June 2019;
Annex 4: Data Protection Impact Assessment "Digitalisation of the central attendance register through encrypted biometric templates technology" (version 1.6) including its annexes (in the following "DPIA annexes");
Annex 5: Comments of the Data Protection Officer of Parliament on version 1.5 of the Data Protection Impact Assessment "Digitalisation of the central attendance register through encrypted biometric templates technology";
Annex 6.1/6.2: Information on the technical solution and infrastructure of the proposed biometric system;
Annex 7: Legal memorandum on the compliance of TBS Biometric Solutions with Regulation (EU) 2016/679.

5 Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ, L 295, 21.11.2018, pp. 39-98.

6 In particular on pages 10 and 11.

7 Nevertheless, the European Parliament foresees to keep the paper signature as a fall back procedure, as mentioned on page 50 of the DPIA (Annex 4)."Possibility to fall back to manual signatures on paper (e.g. in case of power supply issue that would last more than two hours)."

In addition to biometric information, the processing operation requires **general work-related personal information** to operate: name, role, start and end date of mandate, email address and persID number. All these pieces of personal information are extracted from the Parliament's register of Members (CODICT). They are then both stored in a dedicated database together with the data on MEP's attendance (including the obtained timestamps), as well as in the Local Fingeprint Reader's and central biometric databases.

Certain attendance data (including names and timestamps) can be consulted by Parliament staff by direct search in order to verify attendance. Specific users (staff) of DG FINS[8] and DG PERS (for data concerning Parliament's plenaries) will be working as collectors and recipients of personal data. These users will be granted acce**ss** to the information imported from the CODICT database and the MEPs' biometric templates databases, on a 'need-to-know basis' only.

As regards the **integration with payments software**, the DPIA specifies that the system will automatically generate two XML files once a day, listing the persIDs of all Members whose attendance has been successfully registered. These XML files will be placed on a network location scanned by the Integrated Travel Expense Management System (iTEMS)[9], accessible by authorised staff of DG FINS, on a need-to-know basis. iTEMS will automatically import the files and update the attendances of the Members which will trigger the payments of daily allowances, without the need for any human intervention.

3. LEGAL AND TECHNICAL REMARKS

3.1. Lawfulness of the processing and legal basis (Article 5 of the Regulation)

From the listed benefits of the proposed solution over the current CAR system or a badge-based solution, the EDPS understands that **a main driver for the choice of biometric purpose** of the proposed system is **financial fraud prevention** (i.e. to avoid the manual or electronic attendance register being signed by another person on behalf of the MEP)[10]. As a closely related purpose, the EDPS underlines that the Members, as representatives of the Union's citizens[11] should lead by example and be guided in exercising their duties by the general principles of integrity, honesty, accountability and respect of the European Parliament's reputation[12].

As with each processing operation started by an EUI, the proposed biometric registration system must be based on a lawful ground under Article 5 of the Regulation. According to the European Parliament, the proposed **ground for the lawfulness** of the processing operation, i.e.

---

8 Members' Travel and Subsistence Expenses Unit and the Information Technology and e-Portal Unit.

9 The Integrated Travel Expense Management System will replace the current Parliament's travel-related software in the course of 2021.

10 Another reason is the possibility for Members to attest their presence if they have forgotten either their badge or other identifying documents.

11 Article 14(2) TEU.

12 Article 1 of the Code of Conduct for Members of the European Parliament with respect to financial interests and conflicts of interest (https://www.europarl.europa.eu/doceo/document/RULES-9-2019-07-02-ANN-01_EN.html).
See also Article 3 of the Code of Appropriate Behaviour for the Members of the European Parliament in exercising their duties (https://www.europarl.europa.eu/doceo/document/RULES-9-2019-07-02-ANN-02_EN.html): '*Members may not, by their actions, incite or encourage staff to violate, circumvent or ignore the legislation in force, Parliament's internal rules or this Code, or tolerate such behaviour by staff under their responsibility.*'.

the processing of personal data through a digital system for the attestation of attendance of MEPs, is Article 5(1)(b) of the Regulation (meaning that the processing would be necessary for compliance with a legal obligation to which the controller is subject).

The EDPS considers that Article 5(1)(b) applies only in cases where a legal obligation requires EU institutions to process personal data without any leeway in its implementation. This implies that the obligation itself must be sufficiently specific as to the processing of personal data it requires. As in the present case, there is no specific obligation requiring the European Parliament to process biometric information, it should not base the processing operation on Article 5(1)(b) of the Regulation as a ground for lawfulness.

Consequently, the European Parliament should examine whether **another ground** can be relied on, i.e. **Article 5(1)(a) of the Regulation** - provided that the processing of personal data is **necessary and proportionate** to the performance of a task carried out in the public interest by the EU institution (on necessity and proportionality, see Section 3.3).

As regards the **legal basis** for the processing it wants to do, the European Parliament points to Rule 156 of the European Parliament Rules of Procedure[13], as well as Article 12(1) and Article 24 of the IMMS[14].

Article 156 of the Rules of Procedure reads as follows:

An attendance register shall be open for signature by Members at each sitting. 2. The names of the Members recorded as being present in the attendance register shall be indicated in the minutes of each sitting as "present". The names of the Members excused by the President shall be indicated in the minutes of each sitting as "excused".

Meanwhile, the IMMS indicate the following:

Article 12
Attestation of attendance
1. A Member's attendance shall be attested by his or her signature in the record of attendance available in the Chamber or meeting room or by his or her signature in the central attendance register entered during its opening hours as laid down by the Bureau. ***An electronic attestation of a Member's attendance may be used instead of his or her signature****.*[15]

Article 24
Subsistence allowance
1. Members shall be entitled to a subsistence allowance for each day's attendance:
(a) in a place of work or at a meeting venue, duly attested in accordance with Article 12, involving travel covered by the provisions governing reimbursement of ordinary travel expenses;
[...]

These Articles, and indeed the entirety of the IMMS and the Rules of Procedure, serve to implement Article 223(2) of the Treaty on the Functioning of the European Union (former

[13] Rules of Procedure — 9th parliamentary term — July 2019, OJ L 302, 22.11.2019, p. 1–128.
[14] Implementing Measures for the statute of Members of the European Parliament, Bureau Decision of 19 May and 9 July 2008; PE422.536/BUR.
[15] We underline.

Article 190(5) of the Treaty establishing the European Community), which states that the European Parliament shall lay down the regulations and general conditions governing the performance of the duties of its Members.

Already during its first comments in 2018, the EDPS expressed doubts on the decision to ground the processing of biometric information[16] on a provision allowing the European Parliament to use an 'electronic attestation', but which does not contain any specific reference to biometrics.

In order to serve as a legal basis for the envisaged processing operation and provided that there is no less intrusive means for achieving the pursued goal (mainly fraud prevention), the EDPS believes that the internal rules of the European Parliament should be adapted to clearly and specifically indicate that biometric registration (and not only 'electronic attestation') shall be used (and not 'may be used') as a rule[17] to attest attendance.

Recommendation 1

The EDPS considers that Article 5(1)(a) of the Regulation should be relied on as a **ground for lawfulness** of this project provided that the processing is necessary and proportionate for the performance of a task in the public interest and its basis is laid down on Union law.

As to the latter, the EDPS believes that the current wording of the European Parliament's internal rules is insufficiently clear as a **legal basis** for the processing of *biometric* information as the *primary means* for attesting attendance and recommends that the European Parliament amend these rules accordingly.

As regards specific aspects related to **automated decision-making** under Article 24 of the Regulation, the EDPS refers to Section 3.4.

3.2. Processing of special categories of personal data (Article 10 of the Regulation)

As highlighted by the DPIA on page 12, both fingerprint images and extracted biometric templates are special categories of personal data in the sense of Article 10 of the Regulation. Their processing is forbidden by the Regulation as a rule, with the exception of a few cases mentioned under Article 10(2) thereof.

The reason why processing of special categories of data is so severely limited is due to its impact for the fundamental rights of the data subjects and in particular the right to data protection enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (CFR). Biometric data cannot be changed, or at least not easily. In case of a confidentiality breach, MEPs fingerprints cannot be reset or updated. If the fingerprints of a specific MEP are not recognized by the system, it is not possible to provide him or her with new fingerprints.

[16] The definition of 'biometric data' does not include handwritten signatures (Art. 3(14) of the Regulation: 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'.

[17] Manual signatures on paper could be a fall back solution in case of power supply issue that would last more than two hours (cf. p. 50 of the DPIA).

Processing of fingerprints comes with specific risks that need to be mitigated or avoided. For example, scientific research has demonstrated that stored fingerprint templates allow the partial reconstruction of the original fingerprint.[18] Such partial reconstruction sometimes has sufficient accuracy for another biometric system to recognise it as the original one.

The DPIA suggests that the system would rely on the exception of Article 10(2)(d) of the Regulation to process biometric information, however it does not clearly substantiate this choice. Furthermore, this provision aims to provide a legal basis to e.g. unions and religious organisations integrated in EUIs to fulfil their activities (which by default include sensitive information). The EDPS therefore does not consider this provision applicable to the processing of MEP's biometric information to attest their attendance to work places and meetings. The European Parliament could look into **Article 10(2)(g)**, which allows to process special categories of data provided that it is '**necessary** for reasons of **substantial public interest**, on the basis of Union law which shall be **proportionate** to the aim pursued, respect the essence of the right to data protection and provide for **suitable and specific measures** to safeguard the fundamental rights and the interests of the data subject'[19].

The European Parliament should consider that it is possible that injuries, accidents, health conditions (such as paralysis) or some other conditions could temporarily or permanently prevent some MEPs from using the system. While the DPIA foresees the '*Possibility to fall back to manual signatures on paper (e.g. in case of power supply issue that would last more than two hours)*',[20] it does not foresee the risk of the system not being suitable for specific MEPs.

Recommendation 2:
As Article 10(2)(d) of the Regulation is not applicable to the processing operation, the European Parliament should clarify which other exception it would rely on for its processing of **special categories of personal data** under Article 10 of the Regulation, such as Article 10(2)(g), and to **provide a more detailed substantiation** of why this exception would be applicable.

Recommendation 3:
In case the European Parliament finally implements the biometric attendance system, the EDPS recommends the European Parliament to set up an alternative attendance attestation procedure to ensure that the MEPs whose fingerprints are not recognised can still attest their attendance.

3.3. Necessity and proportionality of the processing in view of the objective pursued

Financial fraud prevention including the necessity for democratically elected individuals to lead by example, can be considered as a **reason for substantial public interest** that may justify

[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.

[19] We underline. This provision applies the requirements of Article 52 CFR for any limitation on the exercise of fundamental rights recognised by the CFR, including the right to data protection.

[20] See page 50 of Annex 4 (DPIA)

the processing of biometric data under Article 10(2)(g) of the Regulation[21], provided notably that the use of biometric data is necessary and proportionate to this objective.[22]

As mentioned in the background section, the EDPS has previously emphasised the importance of a thorough **necessity and proportionality** assessment for this project.

'Necessity' implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal. If proved necessary, the measure must still pass the test, which involves assessing what safeguards should accompany a measure in order to reduce the risks, posed by the envisaged measure to the fundamental rights and freedoms of the individuals concerned, to an acceptable/proportionate level. Another factor to be considered in the assessment of proportionality is the effectiveness of existing measures over and above the proposed one. If measures for a similar or the same purpose already exist, their effectiveness should be systematically assessed as part of the proportionality assessment.[23]

In this respect, the EDPS welcomes section 6 of the DPIA, which focuses entirely on the necessity and proportionality of biometric registration. In order to further substantiate these points, the European Parliament contrasts the system with two previous systems it has tested or used, being:

- a physical central attendance register, *i.e.* the system being used currently;
- a computerised system based on Members using their personal access badge at badge readers, which was tested out following the EDPS' previous comments.

During the European Parliament's consultation of 2018, the EDPS specified some of the alternatives that could be considered to avoid processing biometric data. Only one of them seems to have been considered: the use of access badges.

The EDPS notes that for both the current paper based and the access badge systems, an impact assessment table was drawn up listing *inter alia* the different risks, their likelihood and impact, as well as possible strategies to mitigate or accept the risks. The conclusion of this exercise was that "the implementation of both solutions reveal several high and critical risks with impact to the rights and freedoms of the data subjects, to the reputation and finances of the institution or to the security of processed data".

When looking at the assessment in further detail, several important elements remain underspecified or unexplained. The EDPS notes for instance that there is no indication of an evaluation guideline or policy, which indicates how a differentiation is made between

---

[21] As to the use of biometric data to prevent identity fraud, see Prior checking Opinion of the EDPS of 15 May 2014 on the use of biometric verification device for security officers at the European Parliament: 14-05-15_pc_ep_biometric_data_en.pdf (europa.eu)

[22] To the EDPS knowledge, a new badge can be issued in minutes. The second benefit of the use of biometric data put forward by the European Parliament does not seem either valid or necessary/proportionate.

[23] See the Guidelines issued by the EDPS on necessity and proportionality of legislative measures, which can be applied, *mutatis mutandis*, to any measure that aims to restrict the right to data protection enshrined in Article 8 CFR:
- 17-04-11 Necessity toolkit;
- 19-12-19 Proportionality guidelines.

'unlikely' and 'possible'. This seems to be crucial, as the unspecified 'possible' frequency is associated with all risks evaluated as high.

Furthermore, most disadvantages attributed to the badge systems are unclear or not sufficiently demonstrated, such as:

- "*protection of personal data is out of control: processed badge numbers are printed on the badge itself*". To the EDPS' knowledge, badge numbers (along with other personal data such as the full name and photo) are printed on all Parliament badges. It is unclear why the assessment considers this a severe data protection issue only for MEPs. It is also unclear how knowing an MEP badge number would allow a third party to attest the MEP's attendance in any of the three systems.
- "*real-time attestation of attendance is, for a while (even 1 day), compromised when Members' badge is reissued by DG SAFE (ineffectiveness and inefficiency),*". To the EDPS knowledge, reissuing a badge takes minutes. Moreover, one of the main controls considered in the DPIA to ensure the proposed system availability is the "possibility to fall back to manual signatures on paper (e.g. in case of power supply issue that would last more than two hours)". It is unclear to us why this disadvantage is relevant when the same fall-back solution could be used to resolve it.
- "*Members may hold multiple badges (including expired ones), can use them and, hence, pollute the database* (*inefficiency*)". If the automatic door at the Parliament can detect an expired badge, it is unclear to us why the attendance system could not do so and prevent the use of expired badges.
- "*due to similarity with DG SAFE access system, Members may use the wrong reading machines* (*ineffectiveness)*".Whichever is the implemented solution, adding a clear external marking or different colours in the user interface would easily solve this issue.

Further analysing the badge-based system, the European Parliament has evaluated two risks as 'High':

- risk of impersonation, such as when an MEP can (also) sign for an absent MEP; and
- risk of access to personal data (badge number) to unauthorised persons.

It is unclear if the European Parliament has any data on the amount of impersonations that may have occurred during the badge-based test (to which more than 270 Members participated). Without such data, an explanation should be provided as to why the scenario scores above 'unlikely'- i.e. why the European Parliament believes that this is more than a fringe occurrence. If no data is available, and no estimation can be made, then this should be mentioned, in particular because fraud or impersonation prevention is the key purpose driving the move towards biometrics. Being the main driver for processing biometric data the objective of preventing fraud, **it is necessary for the European Parliament to further justify and document the fraud likelihood assessment**.

For the risk of unauthorised access to a badge number printed on the badge, the EDPS first notes a similar issue with the risk likelihood being rated at 'possible' (leading to a score of high). Furthermore, it is unclear to the EDPS why the only proposed mitigation strategy for this risk is to '*implement an alternative computerised system not based on using badges*', rather than not printing the numbers visibly but using (solely) RFID badges.

Finally, the EDPS takes note that the **badge-based solution** was the only alternative which has been analysed by the European Parliament. In light of achieving the purposes above, there may, however, be **other solutions** that could provide an acceptable level of security and fraud

prevention, while not processing biometric information. One example could be, for instance, to have one-time passwords or a similar confirmation feature (e.g. NFC or Bluetooth based authentication) generated on MEPs' phones when they note their attendance. Here, the perceived 'ease' of sharing one's badge is mitigated by the unwillingness to share one's mobile phone with assistants or other MEPs. MEPs may also be less likely to forget their phone or lose it, which are two other risks identified by the European Parliament.

Recommendation 4:

While the EDPS does not in principle oppose or require any particular technology, controllers should ensure that a necessity and proportionality assessment provides a **thorough assessment of less intrusive alternative options that are available**. Therefore, the EDPS recommends that the European Parliament **document the feasibility of other available alternative options** that would not require the use of sensitive data, compare all options and document its conclusions.

3.4. Automated individual decision-making (Article 24 of the Regulation)

The EDPS understands that the envisaged processing does not to require any human intervention[24], which triggers the application of Article 24 of the Regulation on **decisions based solely on automated processing**, which produce **legal effects** concerning the data subject or similarly significantly affects him or her.

Decisions based 'solely on automated processing' include no human involvement in the decision process. As underlined by the Guidelines on Automated individual decision-making and profiling[25]: '*The controller cannot avoid the provisions of Article 22* [~ Article 24 of the Regulation] *by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated decision. To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competences to change the decision.*'

Unless the process involves meaningful human intervention at some point, Article 24 of the Regulation applies to the envisaged processing, which produces legal effects concerning the Members, being the (non-)payment of their subsistence allowances.

Article 24(1) establishes a **general prohibition** for decision-making based solely on automated processing. Article 24(2) of the Regulation states three exceptions that allow solely automated individual decision-making process:

(i) it is necessary for entering into a contract between the data subject and the controller
(ii) it is authorised by Union Law, which also lays down **suitable measures** to safeguard the data subject's rights and freedoms and legitimate interests;
(iii) it is based on the data subject's explicit consent.

[24] See above Section 2. Description of the processing.
[25] See pp. 20-21 of the Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679 (wp251rev.01), as last revised and adopted on 6 Feb 2018 (endorsed by EDPB).

In addition, automated decision-making involving special categories of personal data is only allowed if point (a) or **(g) of Article 10(2)** of the Regulation applies (Article 24(4) of the Regulation).

(i) Substantial public interest is at stake

As indicated above[26], the prevention of fraud as well the respect by the Members, as representatives of the Union's citizens, of the general principles of integrity, honesty, accountability and respect of the European Parliament's reputation, can be considered as a **reason of substantial public interest** that fall within the scope of Article 10(2)(g) of the Regulation.

(ii) Concept of 'Union law'

The applicable legal basis must be **a Union Law authorising automated decision-making** (Article 24(2)(b) of the Regulation[27]). In the EDPS view, 'Union law' means in principle an act of legislative nature (i.e. a Regulation), or at least an executive act grounded in a legislative act. Nevertheless, in this specific case, considering the parliamentary nature of the institution at stake and given that the primary law gives the European Parliament the power to adopt its own rules[28], the EDPS acknowledges that internal rules may provide for an automated decision-making process such as the one envisaged. However, as recommended above (Section 3.2.) these internal rules should provide expressly that the attendance of the Members is attested using biometric technology as primary means.

(iii) Suitable measures to safeguard the data subject's rights and freedoms and legitimate interests

Article 24(2)(b) require that **these rules lay down** not only the automated processing as such but **also suitable measures** to safeguard the Members' rights and freedoms and legitimate interests[29]. As mentioned in Recital 43 of the Regulation, these suitable safeguards should include specific information to the data subjects (see below section 3.6.) and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.

Recommendation 5:
To the extent that the envisaged processing does not involve any meaningful human intervention, the EDPS recommend that the European Parliament **complements its internal rules** on the use of biometrics to attest Members' attendance, by adding **suitable measures** to safeguard the data subject's rights and freedoms and legitimate interests (Article 24(2)(b) of the Regulation).

[26] Section 3.2. See also p. 24 of the Guidelines on Automated individual decision-making that automated decision-making can be used to prevent fraud.

[27] Recital 43 provides that the automated decision-making should be allowed where expressly authorised by Union law.

[28] Article 223 paragraph 2 of the Treaty on the Functioning of the European Union.

[29] Article 10(2)(g) and Article 24(4) also provide for suitable measures but Article 24(2)(b) require that these safeguards be in the rules that authorise the automated decision-making processing.

3.5. Data minimisation

As a measure to ensure (biometric) data minimisation, the European Parliament highlights that biometric templates will be used for processing instead of raw images of the fingerprints. It should be noted that the use of biometric templates, signatures or patterns is standard procedure in biometric identification. These patterns numerically record the physical characteristics making it possible for algorithms to identify and differentiate people. The use of biometric templates itself should therefore not be considered as a measure minimising personal data.

Conversely, from Annex 6.1. (in particular answers 2.C.6 and 2.C.9) it appears that the contractor would use a proprietary algorithm and template format, which would store significantly more data compared to a standard ISO template - additionally storing for instance information on pores and ridge frequency. The justification for this proprietary model states that: '*ISO templates are not suitable for identification of larger groups (100+ persons) because of limited amount and type of data*' and '*these additional data allow reliable identification of databases with thousands of users*'.[30] The EDPS notes that a NIST report[31] tested different templates against the INCITS 378 Fingerprint Template standard on datasets of thousands of fingerprints. While there might currently exist an accuracy advantage on using specific proprietary formats over international standards, the European Parliament should assess if the accuracy increase is worth the decreased data portability. In this case the number of users would stand at less than a thousand, which would question the necessity of capturing such additional data in the first place. By opting for a proprietary solution, the EDPS has also some concerns that the European Parliament may become 'locked-in' with the contractor, as they do not provide a full guarantee that their template could be exported into an ISO format. This may lead to MEPs having to register their fingerprints again, if the European Parliament would either choose or be forced to switch contractors.

Recommendation 6:
The EDPS recommends that the European Parliament further look into whether it is necessary for the proposed system to be established with all additional biometric personal data, taking into account the population size that will be enrolled.

If the system could be adequately established with less additional information, then the EDPS asks the European Parliament to engage its contractor in order to effectively **minimise the amount of personal data** used.

3.6. Information of data subjects

In accordance with Articles 14-16 of the Regulation, the European Parliament should update the data protection notice on attendance registration and ensure that the Members are **specifically informed** about the new system and all its modalities before starting the processing.

To the extent that the processing involves an automated decision-making, the information of the Members should include specific information, i.e. meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for them (Article 15(2)(f) and 16(2)(f) of the Regulation).

[30] Annex 6.1 Technological solution and infrastructure.

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

Recommendation 7:
In accordance with Articles 14-16 of the Regulation, the EDPS recommends that the European Parliament update the data protection notice on attendance registration and ensure that the Members are **specifically informed** about the new system and all its modalitiesbefore starting the processing.

If the processing involves automated decision-making, this information should include meaningful information on the logic involved as well as the significance and the envisaged consequences of the processing (Article 15(2)(f) and 16(2)(f) of the Regulation.

4. CONCLUSION

The EDPS welcomes the substantial effort made by the European Parliament in analysing the data protection ramifications of moving to a biometric system for the attestation of Members' presence.

However the analysis above has shown some critical concerns that need to be addressed. Therefore, the EDPS has made several recommendations to ensure compliance of the processing with the Regulation.

In particular, the European Parliament should:

1) rely on Article 5(1)(a) (and not on Article 5(1)(b)) of the Regulation as a **ground for lawfulness** provided that the processing is necessary for the performance of a task in the public interest and its basis is laid down on Union law and amend its internal rules to be able to rely on them as **legal basis** for the processing of *biometric* information as the *primary means* for attesting attendance and recommends that the European Parliament amend these rules accordingly.

2) clarify the exception the European Parliament would rely on for its processing of **special categories of personal data** under Article 10 of the Regulation, such as Article 10(2)(g); provide a more detailed substantiation of why this exception would be applicable.

3) set up an alternative attendance attestation procedure to ensure that the MEPs whose fingerprints are not recognised can still attest their attendance.

4) document the feasibility of **other available alternative options** that would not require the use of sensitive data, compare all options and document its conclusions.

5) to the extent that the envisaged processing does not involved any meaningful human intervention, complement its **internal rules** on the use of biometrics to attest Members' attendance, by adding **suitable measures** to safeguard the data subject's rights and freedoms and legitimate interests (Article 24(2)(b) of the Regulation).

6) further look into whether it is necessary for the proposed system to be established with all additional biometric personal data, taking into account the population size that will be

enrolled; If the system could be adequately established with less additional information, engage its contractor in order to effectively **minimise** the amount of personal data used.

7) update the data protection notice on attendance registration and ensure that the Members are **specifically informed** about the new system and all its modalities before starting the processing. If the processing involves automated decision-making, include meaningful information on the logic involved as well as the significance and the envisaged consequences of the processing.

The EDPS expects that European Parliament **implements the above-mentioned recommendations and provides documentary evidence** of this implementation within **three months** of this Opinion.

Done at Brussels, 29 March 2021

[e-signed]

Wojciech Rafał WIEWIÓROWSKI