



Европейски парламент Parlamento Europeo Evropský parlament Europa-Parlamentet Europäisches Parlament
Euroopa Parlament Ευρωπαϊκό Κοινοβούλιο European Parliament Parlement européen Parlaimint na hEorpa
Europski parlament Parlamento europeo Eiropas Parlaments Europos Parlamentas Európai Parlament
Parlament Ewropew Europees Parlement Parlament Europejski Parlamento Europeu Parlamentul European
Evropský parlament Evropski parlament Euroopan parlamentti Europaparlamentet

Livia Járóka

Vice-President of the European Parliament

SENT BY E-MAIL
WITH ACKNOWLEDGMENT OF RECEIPT

Mr Patrick Breyer MEP
ASP 08G108
European Parliament
Rue Wiertz 60,
1047 - Bruxelles
Belgium

e-mail: patrick.breyer@europarl.europa.eu

Subject: Your confirmatory application for public access to documents
Our ref: **A(2020)11855C** (to be quoted in future correspondence)

Dear Mr Breyer,

On 23 October 2020, the European Parliament registered your application seeking public access, under Regulation (EC) No 1049/2001¹ laying down the terms and conditions for public access to the documents of the European Union institutions, to "*all documents regarding plans to establish or test an electronic attendance register for MEPs, including Impact Assessments*".

Parliament understood your application as requesting access to all documents pertaining to the planning and testing phase leading to the decision of the Bureau adopted on its meeting of 17 June 2019 to proceed with a computerised system for the digitalisation of the central attendance register through biometric technology (hereinafter referred to as "*the Bureau decision of 17 June 2019*").

At the initial stage, Parliament identified the following sixteen documents as falling within the scope of your application:

¹ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p.43).

1) Legal memorandum of 23 April 2018 on the compliance of biometric solutions with Regulation (EU) 2016/679 (General Data Protection Regulation);

2) Note from the Secretary-General to the Members of the Bureau of 31 May 2018 entitled "*Facilitating digital signing of the central attendance register*" and its annexes:

2.1) Annex I - Financial statement;

2.2) Annex II - Amendment of Article 12 of the Implementing Measures for the Statute for Members of the European Parliament (IMSM);

2.3) Annex III - Frequently asked questions;

3) Minutes of the Bureau's meeting of 11 June 2018;

4) Comments of the Parliament's Data Protection Officer (DPO) dated 10 May 2019 on the draft Data Protection Impact Assessment entitled "*Digitalisation of the central attendance register through encrypted biometric templates technology*";

5) Note from the Secretary-General to the Members of the Bureau of 4 June 2019 entitled "*Facilitating the signing in the central attendance register through digitalisation: results of the voluntary test phase and follow-up proposal*" and its annexes:

5.1) Annex I - Financial statement;

5.2) Annex II - Evaluation report on the test phase;

5.3) Annex III - Data Protection Impact Assessment (DPIA) dated 24 May 2019 entitled "*Digitalisation of the central attendance register through encrypted biometric templates technology*" and its annexes:

5.3.1) Annex I of the DPIA - Data flow diagram of the process;

5.3.2) Annex II of the DPIA - Evaluation of two systems in relation with the registration of Member's attendances;

5.3.3) Annex III of the DPIA - Risks to the right and freedoms of data subjects;

5.3.4) Annex IV of the DPIA - Data protection notice;

6) Minutes of the Bureau's meeting of 17 June 2019.

By letter of 7 December 2020, Parliament communicated to you its decision to grant access to two of these sixteen documents, i.e. the minutes of the two Bureau meetings held in 2018 and 2019 (documents 3 and 6), and to refuse access to the remaining documents on the grounds of the exception of the first indent of point (a) of Article 4(1) of Regulation (EC) No 1049/2001 relating to the protection of public security, the exception of the second indent of Article 4(2) of Regulation (EC) No 1049/2001 relating to the protection of legal advice and the exception of the second subparagraph of Article 4(3) of Regulation (EC) No 1049/2001 relating to the protection of Parliament's decision-making process (hereinafter referred to as "*the initial decision*").

Following this decision, you submitted a confirmatory application on 21 December 2020 asking Parliament to review its initial position.

Pursuant to Rule 122(5) of the Rules of Procedure of the European Parliament, and Article 15 of the Decision of the Bureau of the European Parliament of 28 November 2001², on rules governing public access to European Parliament documents, as Vice-President responsible for matters relating to access to documents, I am responding to your confirmatory application on behalf and under the authority of the Bureau.

² Rules governing public access to European Parliament documents, Bureau decision of 28 November 2001 (OJ C 216 of 22.7.2011, p. 19).

Your confirmatory application

In your confirmatory application, you put forward the following arguments for Parliament to reconsider its position.

You suggest that the public security exception is not applicable since a system that registers the attendance of MEPs for paying their allowances is not relevant to public security. In your opinion, this exception does not cover the security of personal (private) data and, if the documents concerned should reveal risks regarding the security of personal data, there would be a public interest in exposing such a system.

You state that the disclosure of the documents in question would not undermine the protection of legal advice. You point out that the legal advice in question relates to an administrative Bureau decision, that the procedure leading up to it is already completed, and you suggest that it results from the case-law of the Court of Justice that legal opinions delivered in the context of an administrative procedure generally need to be made public once the administrative process has ended. In your opinion, the Legal Service would not be harmed by the publication of these documents.

You also claim that disclosure of the documents at stake would not undermine Parliament's decision-making process, since Parliament has not given any specific reasons to that effect. In addition, you bring forward that, since the minutes of the Bureau meeting and thus of the internal deliberations of the Bureau have been disclosed, the documents at issue, which are merely preparatory, could all the more be released without a negative impact on the Bureau's decision-making process. Moreover, you argue that the protection of the decision-making process does not extend to the implementation of a decision.

Finally, you claim that there is an overriding public interest in disclosure of the documents in question. In your view, there is a public interest in the disclosure of violations of the law and of fundamental rights. You claim that the European Data Protection Supervisor (EDPS) has concluded in other cases that there is no need to process biometric data to register attendance, because badge-based systems work sufficiently well without processing such sensitive data. Further, you argue that this case could set a precedent in terms of the registration of working hours. You also state that the system comes at a considerable cost, and that, in times of pandemic when many citizens suffer economically, such expenditure is of public concern. There is also a risk in your opinion that taxpayer money will be wasted on a system that must not be used in the end. In addition, you claim that there has already been a media report on the issue and that the media are interested in finding out more.

Scope of your application

As indicated in the initial decision, Parliament understands your application as covering all the documents pertaining to the planning and testing phase leading to the Bureau decision of 17 June 2019, by which it decided to proceed with a computerised system for the digitalisation of the central attendance register through biometric technology. In your confirmatory application, you have not challenged this understanding.

In the context of the examination of your confirmatory application, Parliament has determined that the legal memorandum of 23 April 2018 on the compliance of biometric solutions with Regulation (EU) 2016/679 (General Data Protection Regulation) (document 1) does not in fact fall within the scope of your application.

Indeed, while the date indicated on that memorandum is prior to the date of the adoption of the Bureau decision of 17 June 2019, Parliament did not hold that memorandum before the adoption of that decision. Indeed, this memorandum was not commissioned by Parliament, but by a private company, which submitted it to Parliament during a public tendering procedure that took place after 17 June 2019.

Taking into account that documents 3) and 6) are publicly available and that document 1) does not fall within the scope of the application, Parliament focused its confirmatory examination on the documents 2), 4) and 5), as listed above.

Assessment of your confirmatory application

Parliament has assessed your confirmatory application in the light of Regulation (EC) No 1049/2001 and Regulation (EU) 2018/1725 on the processing of personal data³.

Since your application concerns documents about the attendance register for MEPs, it should be noted from the outset, that, for the time being, the traditional system of this register, which is based on manual signature (hereinafter referred to as "*signature-based system*"), is still in place and that Parliament has not yet set up the system based on the fingerprints of MEPs (hereinafter referred to as "*fingerprint-based system*"). It should also be mentioned that, during a voluntary test phase, which took place between 21 January and 12 April 2019, Parliament used a system based on the personal access badges of MEPs (hereinafter referred to as "*badge-based system*").

Further, I would like to point out that, as the supervisory authority for the processing of personal data by the Union institutions, the EDPS opened an investigation based on point (g) of Article 57(1) of Regulation (EU) 2018/1725 concerning Parliament's project to update its central attendance register. On 15 October 2020, Parliament received a request for information from the EDPS concerning this project, to which it replied by the end of last year. This investigation is still ongoing and the EDPS has not provided Parliament with his findings yet.

Moreover, it should also be noted that, while the fingerprint-based system will be used for the calculation of the daily allowance of MEPs, this is not its only function. Indeed, it will also be used to attest the presence of MEPs in the Plenary or in other meetings at Parliament's places of work and to guarantee their safety while on Parliament's premises.

For every document identified under points 2), 4) and 5) of the initial decision, Parliament has assessed again, in the light of your arguments: (i) whether they fall within the scope of one of the exceptions provided for by Article 4 of Regulation (EC) No 1049/2001, (ii) whether the disclosure of these documents would specifically and actually undermine the protected interest, (iii) whether there is an overriding public interest in disclosure, with regard to the exceptions provided for in Article 4(2) and (3) of that regulation, and (iv) whether the need for protection applies to the whole document.

Please note that, in order to improve the readability of the present reply, the parts of the documents that fall within the scope of an exception as well as the reasons why they fall within this scope are indicated in the Annex to this letter. This Annex constitutes an integral part of the reasoning of the present confirmatory decision.

³ Regulation (EU) 2018/1725 of the European Parliament and of 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, p. 39.

A) Note from the Secretary-General to the Members of the Bureau of 4 June 2019 entitled "Facilitating the signing in the central attendance register through digitalisation: results of the voluntary test phase and follow-up proposal" and its annexes (document 5)

This note, which is document 5), has three annexes:

- 5.1) Annex I - Financial statement;
- 5.2) Annex II - Evaluation report on the test phase;
- 5.3) Annex III - Data Protection Impact Assessment (DPIA) dated 24 May 2019 entitled "Digitalisation of the central attendance register through encrypted biometric templates technology" and its annexes:
 - . 5.3.1) Annex I of the DPIA - Data flow diagram of the process;
 - . 5.3.2) Annex II of the DPIA - Evaluation of two systems in relation with the registration of Member's attendances;
 - . 5.3.3) Annex III of the DPIA - Risks to the right and freedoms of data subjects;
 - . 5.3.4) Annex IV of the DPIA - Data protection notice.

After re-examination, Parliament considers that the documents 5), 5.1) and 5.2) shall be disclosed with some content edited out, which are covered by exceptions to the right of public access to documents. On the other hand, public access to document 5.3) and its four annexes shall be refused since the meaningful content thereof is entirely covered by exceptions. The exceptions to the right of public access apply to the eight documents comprised under point 5) as further laid down in this section.

1) The exception relating to the protection of the purpose of investigations (third indent of Article 4(2) of Regulation (EC) No 1049/2001)

The DPIA that Parliament has conducted concerning the project of an updated attendance register for MEPs is at the heart of the above-mentioned ongoing EDPS investigation. Parliament submitted it to the EDPS following the supervisor's information request. Therefore, Annex III of the note from the Secretary-General of 4 June 2019, which contains the DPIA dated 24 May 2019 and its four annexes (documents 5.3 and 5.3.1 to 5.3.4), are covered by the scope of the EDPS investigation.

Parliament considers that a public disclosure of these documents would undermine the protection of the purpose of the ongoing EDPS investigation.

Indeed, according to Regulation (EU) 2018/1725, one of the tasks of the EDPS as supervisory authority for the processing of personal data by EU institutions is to monitor and enforce the application of data protection rules by Parliament. In this function, the EDPS can advise Parliament on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data, on his own initiative or on request.

The purpose of an EDPS investigation is to ensure that the institution concerned complies with data protection rules. To that end, the EDPS conducts a dialogue with the institution concerned about the data protection issues that are covered by its investigation. In order to be fully effective, this dialogue has to be open, which requires that it be conducted in a climate of mutual trust.

As to the procedural rules governing the conduct of the EDPS investigation, Parliament observes that, in accordance with the last sentence of the first subparagraph of Article 16(2) TFEU, Article 8(3) of the Charter of Fundamental Rights and Article 55(1) and (2) of Regulation (EU) 2018/1725, the EDPS shall act with complete independence and shall remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody. Further, under Article 56 of that Regulation, the EDPS shall be subject to a duty of professional secrecy. It should also be noted that, pursuant to Article 13 and Article 16(5) of the Decision of the EDPS of 15 May 2020⁴ adopting its rules of procedure, where appropriate, the EDPS shall facilitate amicable settlements of complaints.

With a view to these tasks and constraints of the EDPS, the purpose of his investigations and the procedural rules governing their conduct, Parliament considers that these investigations have to be conducted in an atmosphere of serenity and confidentiality. Public disclosure of the documents at stake, which are at the heart of the ongoing EDPS investigation, would jeopardize the climate of mutual trust that is necessary to ensure an open dialogue between the EDPS and Parliament and would therefore undermine the effectiveness of that investigation. It would also entail the risk of external pressure on the EDPS, although, in accordance with the provisions mentioned above, he should remain free from external influence, whether direct or indirect.

I would also like to inform you that, in her decision of 19 October 2020 in case 684/2020/MIG⁵, the European Ombudsman confirmed that the exception relating to the protection of the purpose of investigations applied to DPIAs subject to EDPS investigations and that the public disclosure of a DPIA subject to an EDPS investigation would undermine the purpose of such an investigation.

After careful examination of the arguments you have developed in your confirmatory application, Parliament confirms its view that there is no overriding public interest in the public disclosure of the documents at stake.

At the outset, it has to be recalled that the documents in question concern an administrative issue and that, under the relevant case-law, administrative activities do not require the same breadth of access to documents as that required by the legislative activities of a Union institution.⁶

In your confirmatory application, you allege that there is a public interest in the disclosure of the violation of the law and fundamental rights. In this respect, you bring forward that there would be no need to use biometric data for the updated attendance register. Parliament considers that this argument does not demonstrate that there is an overriding interest in public scrutiny of the compatibility of the project of an updated attendance register with data protection rules. Indeed, the data protection issues concerning this project, which Parliament examined in the light of existing EDPS guidance, have been analysed by Parliament's DPO, who was consulted during the drafting of the DPIA. Further, in his role as supervisory authority of the processing of personal data by Parliament, the EDPS is currently investigating the project.

As an argument aiming at showing the existence of an overriding public interest in disclosure, you added that the registration system comes at considerable cost, that in these pandemic times *"when many citizens suffer economically such expenditure is of public concern"*, and that *"there is also a risk that taxpayers money is wasted on a system that must not be used in*

⁴ Decision of the European Data Protection Supervisor of 15 May 2020 adopting the Rules of Procedure of the EDPS (OJ L 204, 26.6.2020, p. 49).

⁵ <https://www.ombudsman.europa.eu/en/decision/en/133942>

⁶ Judgment of 6 February 2020, *Compañía de Tranvías de la Coruña v Commission*, T-485/18, EU:T:2020:35, para. 35 and the case-law cited.

the end". In this regard, Parliament points out that access is granted to the financial information contained in Annex I to the Secretary-General's Note (document 5.1). But it also draws your attention to its internal control mechanisms, which ensure that the relevant rules are complied with without having to depend on the action of third parties. Indeed, Parliament has thorough internal controls carried out by its financial services, the Internal Auditor and the parliamentary committee on budgetary control. There are as well external controls in place such as the Court of Auditors and OLAF, in the event of alleged fraud, that allow identifying any lack of compliance with the relevant rules.

You also claim that there is a public interest in the disclosure of the documents because the updated attendance register for MEPs could set a precedent with regard to employees whose working hours are registered. However, the attendance register for MEPs is designed to suit Parliament's specific requirements as a public legislative body and cannot be equated to a system for registering working hours.

In any event, Parliament is of the opinion that, in the present case, the interest in the protection of the purpose of the EDPS investigation would override the other interests at stake. Indeed, since the purpose of an EDPS investigation is to ensure that Parliament complies with data protection rules, the interests of compliance with those rules and avoidance of unnecessary costs you bring forward in your confirmatory application are best served if, during the ongoing EDPS investigation, the atmosphere of serenity and confidentiality and the climate of mutual trust that are necessary to ensure the full effectiveness of the EDPS investigation are not disturbed by the public disclosure of the documents in question.

Accordingly, Parliament concludes that the Annex III of the note from the Secretary-General of 4 June 2019, which contains the DPIA dated 24 May 2019, and its four annexes (documents 5.3 and 5.3.1 to 5.3.4) shall not be disclosed on the grounds of the exception of the third indent of Article 4(2) of Regulation (EC) No 1049/2001 relating to the protection of the purpose of investigations.

2) The exception relating to the protection of the public security (first indent of point (a) of Article 4(1) of Regulation (EC) No 1049/2001)

The Secretary-General's note of 4 June 2019, its Annex II, its Annex III (the DPIA) and the four Annexes to the DPIA (documents 5, 5.2, 5.3 and 5.3.1 to 5.3.4) contain detailed information about the components, the structure, the functioning, the weaknesses and the protective elements of the signature-, badge-, and fingerprint-based attendance register systems. The relevant parts of the documents in question and the reasons why they contain such information are indicated in sections VI.1, VIII.1, IX.2, X.2, XI.2, XII.2 and XIII.2 of the Annex to the present decision.

Parliament considers that the public disclosure of such information would undermine the protection of the public interest as regards public security, since it would facilitate the identification of weaknesses of these systems and make it easier to exploit them. This would entail a number of unacceptable security risks for Parliament and its Members, such as, but not limited to the disruption of the attendance register system, unauthorised interception, disclosure or modification of data concerning MEPs, the impersonation of MEPs, as well as the intrusion in Parliament's communications and IT systems.

These risks affect the functioning of Parliament as a public legislative body and, hence, public security in the sense of the first indent of point (a) of Article 4(1) of Regulation (EC) No 1049/2001. The concrete and non-hypothetical nature of these risks is evidenced by cases of hacks and/or hack attempts on Parliament and on its counterparts in the Member States.

Parliament would also like to point out that a public security risk would not only be caused by the public disclosure of information with regard to the signature-based system, which is currently in place, or the projected fingerprint-based system, but also of information concerning the badge-based system. Admittedly, the latter system has only been used during the test phase from 21 January to 12 April 2019. However, in the light of the ongoing EDPS investigation, it is possible that, in order to comply with the EDPS' findings, Parliament will have to use elements of the badge-based system for its project of an updated attendance register.

As it is clear from the wording of point (a) of Article 4(1) of Regulation (EC) No 1049/2001, refusal of access is mandatory where the disclosure of a document would undermine the interests protected by that provision, without the need to balance those interests against other public interests.

Therefore, Parliament refuses access to the parts of the documents in question that are mentioned above and specified further in the Annex to this reply on the grounds of the exception relating to the protection of the public security.

3) The exception relating to the protection of Parliament's decision-making process (second subparagraph of Article 4(3) of Regulation (EC) No 1049/2001)

The note from the Secretary-General of 4 June 2019, its Annex II, its Annex III (the DPIA) and Annex 2 and 3 to the DPIA (documents 5, 5.2, 5.3, 5.3.2 and 5.3.3) contain opinions for internal use as part of deliberations and preliminary consultations within Parliament. The parts of the documents in question and the reasons why they contain such opinions are indicated in Sections VI.2, VIII.2, IX.3, XI.3, and XII.3 of the Annex to the present letter.

The disclosure of these opinions would seriously undermine Parliament's decision-making process.

It is the Secretary-General's role to assist the Bureau in the performance of its tasks by providing decision proposals based on frank and open advice. However, if opinions for internal use contained in a note from the Secretary-General to the Bureau on sensitive and contentious issues, such as on the technology discussed in the note, were publicly disclosed, there would be a reasonably foreseeable and non-hypothetical risk that the Secretary-General and Parliament's services involved would refrain from setting out their views in an frank and open way out of concern that they could be used to challenge the decisions to be taken. Such self-censorship would deprive the Bureau from receiving the kind of useful advice, which enables it to effectively exercise its prerogatives in the interest of Parliament and would therefore seriously undermine its ability to take informed decisions.

Further, in the present case, a public disclosure of the opinions at stake also risks to seriously undermine the future decision-making process concerning the update of the attendance register. As long as the EDPS investigation is ongoing and before it has provided Parliament with its findings, it cannot be reasonably ruled out that, in order to comply with the EDPS' findings, Parliament might have to adopt a new decision.

Parliament considers that there is no overriding public interest in the public disclosure of the opinions at stake. In this respect, Parliament refers to the considerations developed under point A.1), which apply *mutatis mutandis* to the present exception. In particular, Parliament considers that, in the present case, which concerns a particularly sensitive issue of contentious nature, the Bureau's interest in receiving decision proposals based on frank and open advice overrides the interest in public scrutiny.

Therefore, Parliament refuses access to the parts of the documents in question that are indicated above on the grounds of the exception relating to the protection of Parliament's decision-making process.

4) The exception relating to the protection of the privacy and the integrity of the individual (point (b) of Article 4(1) of Regulation (EC) No 1049/2001)

The note from the Secretary-General of 4 June 2019 and its Annexes (documents 5, 5.1 to 5.3 and 5.3.1. to 5.3.4) are partially covered by the exception relating to the protection of the privacy and the integrity of the individual (point (b) of Article 4(1) of Regulation (EC) No 1049/2001).

When processing an application filed under Regulation (EC) No 1049/2001 for public access to documents that contain personal data, in accordance with point (b) of Article 4(1) of Regulation (EC) No 1049/2001⁷ and the relevant case-law⁸, Parliament also has to apply Regulation (EU) 2018/1725.

Annex I and III to the note from the Secretary's General (documents 5.1 and 5.3) contain personal data in the sense of Article 3(1) of Regulation (EU) 2018/1725. Annex I is a financial statement presented by the competent service in order to allow the Bureau to have an overview of all the financial elements involved in the fingerprint-based system adoption project and contains the names of the officials involved in the genesis of this statement and the handwritten signature of one of these officials. Annex III is the DPIA and contains the names of all officials involved in the genesis of this document (page 1 and footer in each page).

Pursuant to point (b) of Article 9(1) of Regulation (EU) 2018/1725, personal data shall only be transmitted to recipients established in the Union other than EU institutions and bodies if "*the recipient establishes that it is necessary to have the data transmitted for a specific purpose in the public interest and the controller, where there is any reason to assume that the data subject's legitimate interests might be prejudiced, establishes that it is proportionate to transmit the personal data for that specific purpose after having demonstrably weighed the various competing interests*".

Accordingly, first, it is for the recipient (yourself in this case) to demonstrate the necessity of the transmission of the personal data for a specific purpose in the public interest by providing express and legitimate justification or any convincing argument, and then, for the controller (Parliament in this case), to establish that it is proportionate to transmit the personal data after having demonstrably weighed the various competing interests.

Parliament is of the opinion that you have not demonstrated that the transmission of the personal data at stake is necessary to achieve a specific purpose in the public interest. Indeed, none of your arguments exposes the reasons why the public disclosure of the names and handwritten signature of the officials involved in the genesis of the documents at stake would be a necessary (or even an appropriate) measure to pursue the public interests you have mentioned in your confirmatory application.

Therefore, Parliament refuses access to the names and the handwritten signature in the Annexes I and III to the note from the Secretary-General of 4 June 2019 on the grounds of the protection of the privacy and the integrity of the individual concerned pursuant to point (b) of Article 4(1) of Regulation (EC) No 1049/2001 in connection with point (b) of Article 9(1) of Regulation (EU) 2018/1725.

⁷ Point (b) of Article 4(1) of Regulation (EC) No 1049/2001 states that "the institutions shall refuse access to a document where disclosure would undermine the protection of [...] privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data".

⁸ Judgment of 23 September 2020, *Basaglia v Commission*, T-727/19, EU:T:2020:446, para.64.

Further, as is apparent from the wording of point (b) of Article 4(1) of Regulation (EC) No 1049/2001, the scope of the exception relating to the protection of the privacy and the integrity of the individual is not limited to the cases where a document contains personal data in the sense of Article 3(1) of Regulation (EU) 2018/1725. Indeed, under this exception, access to a document shall be refused where disclosure would undermine the protection of privacy and the integrity of the individual, in particular in accordance with Union legislation regarding the protection of personal data. It follows from the use of the words 'in particular' that this exception applies also to other cases where the protection of privacy and the integrity of the individual would be undermined by the public disclosure of the document in question.

Hence, Parliament considers that this exception also applies to the parts of the documents in question that contain information whose public disclosure would entail a reasonably foreseeable and not purely hypothetical risk that the privacy and the integrity of an individual would be undermined. As has been exposed under point A.2) above, if the detailed information about the components, the structure, the functioning, the weaknesses and the protective elements of the signature-, badge-, and fingerprint-based systems were exposed, this would facilitate the identification of weaknesses of such systems and make it easier to exploit them, and would entail a reasonably concrete and not purely hypothetical risk of unauthorised interception, disclosure or modification of personal data concerning MEPs.

As it is clear from the wording of point (b) of Article 4(1) of Regulation (EC) No 1049/2001, refusal of access is mandatory where the disclosure of the document would undermine the interests protected by that provision, without the need to balance those interests against other public interests.

Therefore, Parliament refuses access to the parts of the note from the Secretary-General of 4 June 2019 and its Annexes (documents 5, 5.1 to 5.3 and 5.3.1. to 5.3.4) mentioned in sections VI.3, VII.1, VIII.3, IX.4, X.3, XI.4, XII.4 and XIII.3 of the Annex to the present letter on the grounds of the exception of point (b) of Article 4(1) of Regulation (EC) No 1049/2001 relating to the protection of the privacy and the integrity of the individual.

5) Partial access

Parliament has considered the possibility of granting partial access, in accordance with Article 4(6) of Regulation (EC) No 1049/2001.

With regard to the Secretary-General's note and its Annexes I and II (documents 5, 5.1 and 5.2), Parliament grants access to the parts of the documents that are not covered by the exceptions mentioned in points A.2) to A.4).

With regard to Annex III of the note (the DPIA proper) and the annexes to the DPIA (documents 5.3, as well as 5.3.1 to 5.3.4), Parliament has reached the conclusion that granting partial access is not possible. As has been exposed under point A.1), these documents are entirely covered by the exception relating to the protection of the purpose of investigations. In any event, partial access to documents 5.3 and 5.3.1 to 5.3.3 could not be granted, since Annex I of the DPIA (document 5.3.1) is entirely covered by the exceptions relating to the protection of the public security and to the protection of the privacy and the integrity of the individual, while partial access to the DPIA proper and its Annexes 2 and 3 (documents 5.3, 5.3.2, 5.3) would be deprived of any useful effect, as the overwhelming part of these documents is covered by the exceptions mentioned in points A.2) to A.4).⁹

⁹ See, by analogy, judgment of 25 September 2020, *Psara v Parliament*, T-639/15, EU:T:2018:602, para. 126.

B) Comments of Parliament's Data Protection Officer (DPO) dated 10 May 2019 on the draft DPIA entitled "Digitalisation of the central attendance register through encrypted biometric templates technology" (document 4)

This document contains the comments of Parliament's DPO on the DPIA. It was issued after he was consulted on the matter in accordance with Article 4(4) of the Decision of the Bureau of the European Parliament of 17 June 2019¹⁰ on the implementing rules relating to Regulation (EU) 2018/1725.

After re-examination of the document, Parliament confirms that public access thereto shall be refused as it is covered by the following exceptions:

1) The exception relating to the protection of the purpose of investigations (third indent of Article 4(2) of Regulation (EC) No 1049/2001)

The DPO's comments concern the DPIA, which is at the heart of the above-mentioned, ongoing EDPS investigation. They were communicated to the EDPS in reply to his information request. For these reasons, Parliament considers that, with respect to the exception relating to the protection of the purpose of investigations, these comments must be treated in the same way as the DPIA. Therefore, in line with the reasoning and the arguments developed under point A.1) above, access to the whole document has to be refused on the grounds of the exception of the third indent of Article 4(2) of Regulation (EC) No 1049/2001.

2) The exception relating to the protection of Parliament's decision-making process (second sub-paragraph of Article 4(3) of Regulation (EC) No 1049/2001)

The DPO's comments contain opinions for internal use as part of deliberations and preliminary consultations within Parliament. The relevant parts of this document and the reasons why they contain such opinions are indicated in section V.2 of the Annex to this letter.

The disclosure of these opinions would seriously undermine Parliament's decision-making process. The DPO's comments concern a DPIA about the use of biometric technology, a particularly sensitive issue of a contentious nature.

As to the DPO's role, it should be pointed out that, in accordance with Article 43(3) and points (a), (b) and (e) of Article 45(1) of Regulation 2018/1725, the DPO, who has expert knowledge of data protection law and practices, has the task to inform and advise Parliament on data protection issues, particularly with respect to DPIAs. If the DPO's comments concerning sensitive issues of a contentious nature were publicly disclosed, there would be a reasonably foreseeable and non-hypothetical risk that Parliament's ability to seek thorough and straightforward advice from its DPO on DPIAs would be seriously undermined.

First, there is a foreseeable risk that Parliament's services would refrain from asking the DPO for thorough advice on DPIAs dealing with sensitive issues in order to avoid that, after public disclosure, the DPO's observations be used in legal disputes concerning this assessment. Second, there would be a reasonably foreseeable and not purely hypothetical risk that the DPO would refrain from setting out his views in a frank and open way, out of concern that they could be used to challenge the DPIA. Such self-censorship would deprive Parliament from useful advice from the DPO.

¹⁰ Decision of the Bureau of the European Parliament of 17 June 2019 on the implementing rules relating to Regulation (EU) 2018/1725 of the European Parliament and of the Council 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 C 259, 2.8.2019, p. 2).

Parliament would also like to point out that the DPO's consultation often occurs in a short timeframe and that, if the DPO had to anticipate public disclosure of his comments, his ability to advise in a short time frame would be seriously undermined.¹¹

Further, as has been set out under point A.3), public disclosure of the DPO's comments would also seriously undermine an eventual decision-making process following the EDPS' findings, a possibility that cannot be excluded while the EDPS investigation is still ongoing.

Parliament considers that, in line with the reasoning and the arguments developed under point A.3) above, there is no overriding public interest in the public disclosure of the opinions contained in the DPO's comments. Quite to the contrary, as results from the provisions of Regulation (EU) 2018/1725, it is in the public interest that Parliament receives thorough and straightforward advice from its DPO. In the present case, this latter interest and the protection of the institutional role of the DPO, which would be seriously undermined by the public disclosure of the DPO's opinions, overrides the other interests at stake.

Therefore, Parliament refuses access to the above-mentioned parts of the DPO's comments on the grounds of the exception relating to the protection of Parliament's decision-making process.

3) The exception relating to the protection of the public security (first indent of point (a) of Article 4(1) of Regulation (EC) No 1049/2001)

The DPO's comments contain detailed information about the components, the structure, the functioning, the weaknesses and the protective elements of the projected fingerprint-based system. The relevant parts of the comments and the reasons why they contain such information are indicated in Section V.3 of the Annex to the present letter. In line with the reasoning and the arguments developed under point A.2) above, Parliament refuses access to these parts on the grounds of the exception relating to the protection of the public security.

4) The exception relating to the protection of the privacy and the integrity of the individual (point (b) of Article 4(1) of Regulation (EC) No 1049/2001)

Parts of the DPO's comments are covered by the exception relating to the protection of the privacy and the integrity of the individual (point (b) of Article 4(1) of Regulation (EC) No 1049/2001).

This document contains two names (page 9), which are personal data. In line with the reasoning and the arguments developed under point A.4) above, access to these names is refused on the grounds of the protection of the privacy and the integrity of the individual concerned pursuant to point (b) of Article 4(1) of Regulation (EC) No 1049/2001 in connection with point (b) of Article 9(1) of Regulation (EU) 2018/1725.

The DPO's comments that are mentioned in point B.3) contain detailed information about the components, the structure, the functioning, the weaknesses and the protective elements of the different systems of attendance register. Parliament considers that these parts are also covered by the exception relating to the protection of the privacy and the integrity of the individual pursuant to point (b) of Article 4(1) of Regulation (EC) No 1049/2001, in line with the reasoning and the arguments developed under point A.4) above.

Therefore, Parliament refuses access to the parts of the DPO's comments mentioned in Section V.4 of the Annex to this letter on the grounds of the exception relating to the protection of the privacy and the integrity of the individual.

¹¹ See, by analogy, judgment of 7 February 2018, *Access Info Europe v Commission*, T-851/16, EU:T:2018:69, para. 94.

5) Partial access

Parliament has considered the possibility of granting partial access to the DPO's comments on the DPIA, in accordance with Article 4(6) of Regulation (EC) No 1049/2001, but has reached the conclusion that granting such partial access is not possible. Indeed, as has been exposed under point B.1), this document is entirely covered by the exception relating to the protection of the purpose of investigations. In any event, a partial access to this document could not have been granted even if this exception was not applicable, since access to the widest part of this document would at any rate have to be refused on the grounds of the exceptions mentioned in points B.2) to B.4), so that partial access to the document would be deprived of any useful effect.¹²

C) Note from the Secretary-General to the Members of the Bureau of 31 May 2018 entitled "Facilitating digital signing of the central attendance register" and its annexes (document 2)

This note, which is document 2), has three annexes:

- 2.1) Annex I - Financial statement;
- 2.2) Annex II - Amendment of Article 12 of the Implementing Measures for the Statute for Members of the European Parliament (IMSM);
- 2.3) Annex III - Frequently asked questions.

After assessing those documents anew, Parliament considered that public access to them shall be granted with the content falling under exceptions edited out as follows:

- 1) *The exception relating to the protection of the public security (first indent of point (a) of Article 4(1) of Regulation (EC) No 1049/2001)*

The Secretary-General's note of 31 May 2018 and its Annex III (documents 2 and 2.3) contain detailed information about the components, the structure, the functioning, the weaknesses and the protective elements of the different systems of attendance register. The relevant parts of these documents and the reasons why they contain such information are indicated in sections I.1 and IV.1 of the Annex to the present letter. Parliament considers that these parts are also covered by the exception relating to the protection of the public security and refuses access to these parts, in line with the reasoning and the arguments developed under point A.2) above.

- 2) *The exception relating to the protection of Parliament's decision-making process (second subparagraph of Article 4(3) of Regulation (EC) No 1049/2001)*

The note from the Secretary-General of 31 May 2018 and its Annex II (documents 2 and 2.2) contain opinions for internal use as part of deliberations and preliminary consultations within Parliament. The relevant parts of the documents in question and the reasons why they contain such opinions are indicated in sections I.2, and III.1 of the Annex to the present letter. In line with the reasoning and the arguments developed under point A.3) above, Parliament refuses access to these parts on the grounds of the exception relating to the protection of Parliament's decision-making process.

¹² See, to that effect, judgment of 25 September 2020, *Psara v Parliament*, T-639/15, EU:T:2018:602, para. 126.

3) The exception relating to the protection of the privacy and the integrity of the individual (point (b) of Article 4(1) of Regulation (EC) No 1049/2001)

Parts of the note from the Secretary-General of 31 May 2018, its Annex I and its Annex III (documents 2, 2.1 and 2.3) are covered by the exception relating to the protection of the privacy and the integrity of the individual (point (b) of Article 4(1) of Regulation (EC) No 1049/2001).

Annex I, which is a financial statement presented by the competent service in order to allow the Bureau to have an overview of all financial elements relating to the project for the adoption of the fingerprint-based system, contains the names of the officials involved in the genesis of this statement and the handwritten signature of one of these officials. Access to those names and this signature is refused on the grounds of the protection of the privacy and the integrity of the individual concerned pursuant to point (b) of Article 4(1) of Regulation (EC) No 1049/2001 in connection with point (b) of Article 9(1) of Regulation (EU) 2018/1725, in line with the reasoning and the arguments developed under point A.4) above.

With regard to the parts of the note from the Secretary-General of 31 May 2018 and its Annex III, which are mentioned under point C.1) and contain detailed information about the components, the structure, the functioning, the weaknesses and the protective elements of the signature-, badge-, and fingerprint-based systems, Parliament considers, in line with the reasoning and the arguments developed under point A.4) above, that they are also covered by the exception relating to the protection of the privacy and the integrity of the individual pursuant to point (b) of Article 4(1) of Regulation (EC) No 1049/2001.

Therefore, Parliament refuses access to the parts of these documents that are indicated in sections I.3, II.1 and IV.2 of the Annex to this letter on the grounds of the exception relating to the protection of the privacy and the integrity of the individual.

4) Partial access

With regard to the note from the Secretary-General of 31 May 2018 and its Annexes (documents 2 and 2.1 to 2.3), Parliament has considered the possibility of granting partial access, in accordance with Article 4(6) of Regulation (EC) No 1049/2001. After having erased all the parts that are covered by the exceptions mentioned in Points C.1) to C.3) above, Parliament hereby grants partial access to these documents.

Conclusion

As a consequence of the above, I hereby refuse access to the parts of the documents 2, 2.1 to 2.3, 5, 5.1 and 5.2 covered by the above-mentioned exceptions and grant public access to the remaining parts of those documents (see section 1 below) with the exception of documents 4, 5.3 and 5.3.1 to 5.3.4, to which access is refused (see section 2 below):

Section 1) Partial Access

- 2) Note from the Secretary-General to the Members of the Bureau of 31 May 2018 entitled "Facilitating digital signing of the central attendance register" and its three annexes:

. 2.1) Annex I - Financial statement;

. 2.2) Annex II - Amendment of Article 12 of the Implementing Measures for the Statute for Members of the European Parliament (IMSM);

. 2.3) Annex III - Frequently asked questions;

- Document 5) Note from the Secretary-General to the Members of the Bureau of 4 June 2019 entitled "Facilitating the signing in the central attendance register through digitalisation: results of the voluntary test phase and follow-up proposal" and the following annexes:

. 5.1) Annex I - Financial statement;

. 5.2) Annex II - Evaluation report on the test phase.

Section 2) Refusal of access

- 4) Comments of the Parliament's Data Protection Officer (DPO) dated 10 May 2019 on the draft Data Protection Impact Assessment (DPIA) entitled "Digitalisation of the central attendance register through encrypted biometric templates technology";

- 5.3) Annex III of the Note from the Secretary-General to the Members of the Bureau of 04 June 2019 - Data Protection Impact Assessment (DPIA) dated 24 May 2019 entitled "Digitalisation of the central attendance register through encrypted biometric templates technology" and its annexes and its annexes:

. 5.3.1) Annex I of the DPIA - Data flow diagram of the process;

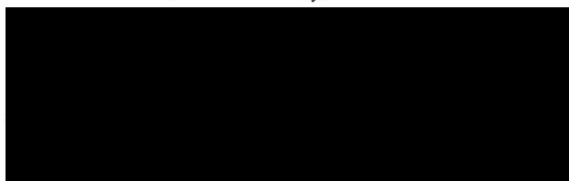
. 5.3.2) Annex II of the DPIA - Evaluation of two systems in relation with the registration of Member's attendances;

. 5.3.3) Annex III of the DPIA - Risks to the right and freedoms of data subjects;

. 5.3.4) Annex IV of the DPIA - Data protection notice.

Finally, I would like to draw your attention to the means of redress against this decision in accordance with Article 8 of Regulation (EC) No 1049/2001. You may either bring proceedings before the General Court or file a complaint with the European Ombudsman under the conditions specified respectively in the Treaty on the Functioning of the European Union.

Yours sincerely,



Lívia JÁRÓKA

- Annex with tables;
- Documents to which partial access is granted.

Annex

Section I	
Document 2- Note from the Secretary-General to the Members of the Bureau of 31 May 2018	
<i>Parts covered by exception</i>	<i>Commentary</i>
1. Public security	
Section II and footnote no. 2 (page 2)	Contains details of the current arrangements for managing the central attendance register
A part of the first paragraph of section III (page 2)	Gives details concerning the fingerprint-based system
The third and fifth indents of section III (page 3)	Contain technical details regarding the setup of the fingerprint-based system
2. Decision-making process	
The first paragraph of the summary (page 1)	Gives an opinion assessing the adequacy of the human resources involved
The whole section II (page 2)	Gives opinions assessing the current arrangements for managing the central attendance register
The second paragraph and first sentence of the third paragraph of section III (page 3)	Give opinions and advice on technologies
The first and fourth indents of section III (page 3)	Give opinions on the fingerprint-based system
3. Privacy and the integrity of the individual	
The parts mentioned under Point 1	Risk of unauthorised interception, disclosure or modification of personal data concerning MEPs

Section II	
Document 2.1 - Annex I to the Note from the Secretary-General to the Members of the Bureau of 31 May 2018	
<i>Parts covered by exception</i>	<i>Commentary</i>
1. Privacy and the integrity of the individual	
Names and the handwritten signature	Personal data

Section III	
Document 2.2 - Annex II to the Note from the Secretary-General to the Members of the Bureau of 31 May 2018	
<i>Parts covered by exception</i>	<i>Commentary</i>
1. Decision-making process	
The third column	Assesses the adequacy of the human resources involved

Section IV	
Document 2.3 - Annex III to the Note from the Secretary-General to the Members of the Bureau of 31 May 2018	
<i>Parts covered by the exception</i>	<i>Commentary</i>
1. Public security	
All the parts that are redacted	Contain technical details regarding the setup of the fingerprint-based system
2. Privacy and the integrity of the individual	
The parts mentioned under Point 1	Risk of unauthorised interception, disclosure or modification of personal data concerning MEPs

Section V	
Document 4 - Comments of the Parliament's Data Protection Officer (DPO) dated 10 May 2019 on the draft Data Protection Impact Assessment (DPIA) entitled "Digitalisation of the central attendance register through encrypted biometric templates technology"	
<i>Parts covered by exception</i>	<i>Commentary</i>
1. Purpose of investigations	
The whole document	Would undermine purpose of EDPS investigation
2. Decision-making process	
The second paragraph of the section "Comments and recommendations regarding point 3: reasons for carrying out the DPIA" (page 1)	Contains an opinion assessing how the DPIA should include technical and organisational measures
The last two paragraphs of the section "Comments and recommendations regarding point 3: reasons for carrying out the DPIA" (page 2)	Contain advice on the different outcomes depending on what legal basis of Article 5 Regulation (EU) 2018/1725 is used and on the indications about the tasks of the services involved
The first paragraph of the section "Comments and recommendations regarding point 5.2 of the proposed solution" concerning p.8 of the DPIA (page 2)	Contains advice on the data subject's signature categorisation under Article 10 of Regulation (EU) 2018/1725 concerning special categories of personal data
The last paragraph of the section "Comments and recommendations regarding point 5.2 of the proposed solution" concerning p.9 of the DPIA (page 2)	Contains advice on how an inconsistency within the text should be dealt with
The first paragraph of the section "Comments and recommendations regarding point 5.2.1 personal data processed" concerning p.9 of the DPIA (page 2)	Contains advice on Article 3 of Regulation (EU) 2018/1725 on the definition of 'processing'

The second paragraph of the section “Comments and recommendations regarding point 5.2.1 personal data processed” concerning p.10 of the DPIA (page 3)	Contains advice on Article 3 of Regulation (EU) 2018/1725 on the definition of ‘personal data’
The four paragraphs of the section “Comments and recommendations regarding point 5.2.2 operational modules and data flow” (page 3)	Contain opinions on how to deal with specific technological issues
The five paragraphs of the section “Comments and recommendations regarding point 5.3 description of the supporting infrastructure” (page 4)	Contain opinions on how to deal with specific functional and technological issues
A part of the paragraph of the section “B) Respect of data protection principles” (page 4)	Gives recommendations on how to improve annex 3 of the DPIA and where to place it in the text
All paragraphs of the section “Comments and recommendations regarding point 6.1.1 necessity of the envisaged processing operations” (pages 4 and 5)	Contain an opinion on how to improve analysis in the DPIA
All content of the section “Comments and recommendations regarding point 6.1.2 objectives of the proposed solution” (page 5)	Refers to a part of the DPIA that the DPO considers unclear
All content of the section “Comments and recommendations regarding point 6.1.5 intrusiveness of the proposed solution”, (page 5)	Contain an opinion on point 6.1.5 of the DPIA and a recommendation on how to deal with this
The paragraph of the section “Comments and recommendations regarding point 6.2.1 benefits of the proposed solution” (page 5)	Contains a recommendation on how to better assess effectiveness of the technology
The three indents of the section “Comments and recommendations regarding point 6.2.2 effectiveness and efficiency of the solution” (page 5)	Contains in opinion of the DPO what further risks should be added in the text of the DPIA
The whole content of the section “Comments and recommendations regarding point 6.2.2.2 interference with and impact on fundamental rights”, with the exception of the table (pages 6 and 7)	Gives opinions on possible inaccuracies in the text concerning the definition of processing activity, on the margin of error of the system, on the importance to be given to IT risk assessment and on the proportionality test
The two paragraphs of the section “Comments and recommendations regarding point 7 analysis of risks and establishment of controls/safeguards”, (page 7)	Address cybersecurity safeguards
The paragraph of the section “Comments and recommendations regarding point 7.1 risks to the rights and freedoms of data subjects” (page 7)	Gives the opinion of the DPO on some drafting in point 7.1 of the DPIA

A part of the second paragraph of the section “III. Risk treatment/mitigation” (page 8)	Addresses the storage of biometric templates
The three paragraphs of the section “IV. General remarks” (pages 8 and 9)	Contain opinions on how the draft of the DPIA can be generally improved
3. Public security	
Two citations of the text of the DPIA concerning (p.9) and (p.10) both reproduced in the section “Comments and recommendations regarding point 5.2.1 personal data processed” (pages 2 and 3)	These parts have been redacted in the DPIA for public security reasons and therefore are also redacted in the present document
The second paragraph of the section “Comments and recommendations regarding point 5.2.1 personal data processed” (page 3)	Contains detailed information on the functioning of the fingerprint-based system
The first paragraph of the section “Comments and recommendations regarding point 5.2.2 operational modules and data flow” (page 3)	Contains detailed information on the functioning of the fingerprint-based system
4. Privacy and the integrity of the individual	
Two names (page 9)	Personal data
The parts mentioned under Point 3	Risk of unauthorised interception, disclosure or modification of personal data concerning MEPs

Section VI	
Document 5 - Note from the Secretary-General to the Members of the Bureau of 4 June 2019	
<i>Parts covered by exception</i>	<i>Commentary</i>
1. Public security	
A part of the third paragraph of the summary (page 1)	Contains technical details regarding the setup of the badge-based test system
The second sentence of the third paragraph of part II. The test phase (page 2)	Contains technical details regarding the setup of the badge-based test system
The final sentence of the third paragraph of part II. The test phase (page 2)	Contains operational details of the test of the badge-based system
2. Decision-making process	
The first paragraph of the summary (page 1)	Contains an appraisal of the current management of the central attendance register
The first paragraph of part I. Introduction (page 2)	Contains an appraisal of the current management of the central attendance register
The first paragraph of part III. Results of the test phase (page 3)	Contains an assessment of MEP's participation in the test phase

The second and third paragraph of part III. Results of the test phase (page 3)	Contain an appraisal of the outcome of the test phase
3. Privacy and the integrity of the individual	
The parts mentioned under Point 1	Risk of unauthorised interception, disclosure or modification of personal data concerning MEPs
The handwritten signature	Personal data

Section VII	
Document 5.1 - Annex I to the Note from the Secretary-General to the Members of the Bureau of 4 June 2019	
<i>Parts covered by exception</i>	<i>Commentary</i>
1. Privacy and the integrity of the individual	
Names and the handwritten signature	Personal data

Section VIII	
Document 5.2 - Annex II to the Note from the Secretary-General to the Members of the Bureau of 4 June 2019	
<i>Parts covered by exception</i>	<i>Commentary</i>
1. Public security	
The second sentence of the second paragraph (page 1)	Lays down information on the setting up and locations of the badge-reading devices
The table laid down on section 2 (page 2)	Summarises and evaluates the risks linked to the implementation of the badge-based system with a stress on operational and security view-points
The section 3 (page 3)	Deals with the conclusions of the evaluation report discusses possible risk mitigation strategies and give an appraisal of those risk mitigations strategies with a view to advising Parliament
2. Decision-making process	
The table laid down on section 2 (page 2)	Gives opinions assessing the risks stemming from the possible use of a badge-based system and how to respond to them
The section 3 dealing with the conclusions of the evaluation report (page 3)	Contains opinions on whether the badge-based system has a degree of reliability enough in order to reach an acceptable level of risk
3. Privacy and the integrity of the individual	
The parts mentioned under Point 1	Risk of unauthorised interception, disclosure or modification of personal data concerning MEPs

Section IX	
Document 5.3 - Annex III to the Note from the Secretary-General to the Members of the Bureau of 4 June 2019	
<i>Parts covered by exception</i>	<i>Commentary</i>
1. Purpose of investigations	
The whole document	Would undermine purpose of EDPS investigation
2. Public security	
A part of the second sentence and the third sentence of the third paragraph of chapter 2, Executive summary (page 4)	Contains technical details regarding the extraction of fingerprints
Footnotes 7 to 10 (page 6)	Contain details of Parliament's internal organisation
Second subparagraph of the third paragraph of chapter 5.2, the proposed solution (page 8)	Contains technical details of possible fingerprint reading technologies
Paragraphs 4 to 7 of section 5.2, the proposed solution (page 8 and 9)	Contain technical and operational details, as well as the risks involved, of the proposed fingerprint-reading solution
Second subparagraph of the second paragraph of section 5.2.1, Personal data processed (page 10)	Contains technical details of the proposed fingerprint-reading solution
A part of the final sentence of the third paragraph of section 5.2.1, Personal data processed and footnote 16 (page 10)	Contains details of the persons who are granted access to the relevant databases
The first sentence of the first paragraph of point (i) of section 5.2.1, Fingerprints and biometric templates (page 10)	Contains operational details regarding the fingerprint-based solution
Paragraphs 4, 5 and 6 of point (i) of section 5.2.1, Fingerprints and biometric templates, (page 10 and 11)	Contains technical and operational details regarding the fingerprint-based solution
Footnotes 17 and 18 (page 11)	Contain operational details regarding the fingerprint-based solution
The second paragraph of point (ii) of section 5.2.1, Name, start and end date of mandate, email address and persID (page 11 and 12)	Contains operational details regarding the fingerprint-based solution
The second and third paragraph of point (iii) of section 5.2.1, Timestamp of the attestation of attendance (page 12)	Contains technical and operational details regarding fingerprint-based solution
Points (a) to (h) of section 5.2.2, operational modules & data flow, with the exception of the first sentence of point (d), Member's account deletion (page 12 to 15)	Contain technical and operational details regarding the fingerprint-based solution
Section 5.3, description of the supporting infrastructure (for each data location) (page 15 to 17)	Contains technical and operational details regarding the fingerprint-based solution
Final sentence of the first paragraph and the second paragraph of section 6.1.1, Necessity of the envisaged processing operations (page 18)	Contain operation details regarding the fingerprint-based solution

Fourth sentence of point (i) of section 6.1.3, Physical central attendance register (CAR) (p. 19)	Contains operational details of the signature-based system
The first paragraph of point (ii) of section 6.1.3, Badge recognition-based computerised system with the exception of the first sentence (page 20)	Contains operational details of the badge-based digitalisation option
The first paragraph, the first and the second sentence of the second paragraph, a part of the first sentence of the third paragraph and the first two sentences of the fourth paragraph of section 6.1.4, Intrusiveness of the proposed solution (page 20 and 21)	Contain operational details regarding the processing involved in the fingerprint-based system
Footnote 28 and the first two paragraphs of section 6.2.2, Interference with and impact on fundamental rights ('costs') (page 23 and 24)	Contain an appraisal of the operational risks associated with the fingerprint-based solution
The first four and the second to last bullet point of the second subparagraph of the second paragraph of section 6.2.2.2, Extent and intensity of the intrusiveness (page 24 and 25)	Contain technical and operational details regarding the fingerprint-based system
The final paragraph of section 6.2.3, proportionality analysis (page 26)	Contains technical and operational details of the proposed solution
The second subparagraph of the third paragraph of section 7.1, Risks to the rights and freedoms of data subjects (incl. risk treatment) (page 28)	Contains technical details of the proposed solution
Parts of the third, fifth and sixth indent of the second subparagraph of the first paragraph of section 7.2, Risks to the compliance of Parliament with data protection rules (page 28)	Contain technical details of the planned implementation of the proposed solution
Parts of the second and third indent of the second subparagraph of the second paragraph of section 7.2, risks to the compliance of Parliament with data protection rules (page 29)	Contain technical and operational details of the planned implementation of the fingerprint-based solution
The second, forth, ninth, tenth and eleventh paragraph of section 10, glossary (page 31 and 32)	Contain technical details of the implementation of the fingerprint-based solution
3. Decision-making process	
The final half-sentence of the third paragraph of chapter 2, Executive summary, (page 4)	Contains an appraisal of the intrusiveness of fingerprint-based systems
The sixth paragraph of chapter 5.1, Context (page 7)	Contains an appraisal of the outcome of the test phase
Paragraphs 6 and 7 of section 5.2, The proposed solution (page 9)	Contain an appraisal of the operational advantages and disadvantages of the proposed fingerprint-reading solution
The final sentence of the first paragraph and the second paragraph of section 6.1.1,	Contain an appraisal of the advantages and disadvantages of the proposed solution

Necessity of the envisaged processing operations (page 18)	
The first paragraph of point (i) of section 6.1.3, Physical central attendance register (CAR), with the exception of its first three sentences, which (page 19)	Contains an appraisal of the functioning of the classical CAR system
The first paragraph and the final sentence of the second paragraph of point (ii) of section 6.1.3, Badge recognition-based computerised system, with the exception of its first two sentences (page 20)	Contains an appraisal of the advantages and disadvantages of the badge-based digitalisation option
The first and second paragraph, as well as a part of the first sentence of the third paragraph of section 6.1.4, intrusiveness of the proposed solution, which (page 20 and 21)	Contain an appraisal of the intrusiveness
The second subparagraph of the first paragraph of section 6.1.5, conclusions on intrusiveness (page 22)	Contains an appraisal of the intrusiveness
The first two paragraphs of section 6.2.2, Interference with and impact on fundamental rights ('costs') (page 23 and 24)	Contain an appraisal of the fundamental rights in relation to the proposed solution
The first sentence of section 6.2.2.1, scope of the interference (page 24)	Contains an overall appraisal of the extent of the interference with fundamental rights of the proposed solution
The second subparagraph of the third paragraph, and the final two sentences of the fourth paragraph of section 6.2.2.2, Extent and intensity of the intrusiveness (page 25)	Contain an appraisal of the effects and impact on fundamental rights of the proposed solution
Section 6.2.3, proportionality analysis (page 25 and 26)	Contains an appraisal of the benefits of the proposed solution and their juxtaposition with previously identified 'costs'
The second subparagraph of the second paragraph, and a part of the final sentence of section 7.1, risks to the rights and freedoms of data subjects (incl. risk treatment) (page 27 and 28)	Contain an appraisal of the possibilities to mitigate the risks identified with the proposed solution
4. Privacy and the integrity of the individual	
The parts mentioned under Point 2	Risk of unauthorised interception, disclosure or modification of personal data concerning MEPs
The names of all officials involved in the genesis of this document (page 1 and footer in each page)	Personal data

Section X	
Document 5.3.1 - Annex 1 to Annex III to the Note from the Secretary-General to the Members of the Bureau of 4 June 2019	
<i>Parts covered by exception</i>	<i>Commentary</i>
1. Purpose of investigations	
The whole document	Would undermine purpose of EDPS investigation
2. Public security	
The whole document	Data flows necessitated by the proposed fingerprint-reading solution
3. Privacy and the integrity of the individual	
The whole document	Risk of unauthorised interception, disclosure or modification of personal data concerning MEPs

Section XI	
Document 5.3.2 - Annex 2 to Annex III to the Note from the Secretary-General to the Members of the Bureau of 4 June 2019	
<i>Parts covered by exception</i>	<i>Commentary</i>
1. Purpose of investigations	
The whole document	Would undermine purpose of EDPS investigation
2. Public security	
The last sentence under point 2) i) concerning the evaluation of solution A, which lays down information on the planned setting up and locations of the badge reading devices (page 1)	Security sensitive information
The table under point 2) ii) "Advantages and disadvantages" concerning the evaluation of solution A (page 1)	Summarises and gauges of the risks linked to the implementation of the badge-based system with a stress on operational and security aspects
The table under point 2) iii) "Options for risk treatment" concerning the evaluation of solution A (pages 2 and 3)	Summarises risks and mitigations strategies
The end of the first sentence under point 3) i) concerning the evaluation of solution B (page 4)	Lays down security sensitive information on the locations of the registration points
The second paragraph under point 3) i) concerning the evaluation of solution B (page 4)	Security sensitive information
The table under point 3) ii) "Advantages and disadvantages" concerning the evaluation of solution B (page 4)	Summarises and gauges the risks linked to the classical paper system with a stress on operational and security aspects

The table under point 3) iii) "Options for risk treatment" concerning the evaluation of solution B (pages 5 and 6)	its risks and mitigations strategies
The conclusions at the end of the document (page 7)	Makes reference to the security and operational risks of the solutions analysed
3. Decision-making process	
The tables concerning evaluation of solution A located at the sections "ii. Advantages and disadvantages" and "iii. Options for risk treatment" (pages 1 to 3)	Contain opinions on security sensitive matters as part of deliberations and preliminary consultations within Parliament
The tables concerning evaluation of solution B located at the sections "ii. Advantages and disadvantages" and "iii. Options for risk treatment" (pages 4 to 6)	Contain opinions on security sensitive matters as part of deliberations and preliminary consultations within Parliament
The conclusions at the end of the document, which (page 7)	Summarises the results of the risk assessment in relation to the implementation of both solutions compared and contains opinions
4. Privacy and the integrity of the individual	
The parts mentioned under Point 2	Risk of unauthorised interception, disclosure or modification of personal data concerning MEPs

Section XII	
Document 5.3.3 - Annex 3 to Annex III to the Note from the Secretary-General to the Members of the Bureau of 4 June 2019	
<i>Parts covered by exception</i>	<i>Commentary</i>
1. Purpose of investigations	
The whole document	Would undermine purpose of EDPS investigation
2. Public security	
The table under point A) "Mapping data flow diagram items and 'protection targets'" (page 1)	Gives details on protection targets
The paragraphs of point B) "Risk assessment and risk treatment (controls and safeguards)" (page 2)	Contain details on risks at the level of each operational module
The table under B.1) "Creation of Member's account" (pages 2 to 5)	Gives more details on those risks
The paragraph of point B.2) "Member's attendance registration" (page 6)	Gives detailed information on how the computerised attendance registration works concerning disclosure or modification of data
The table under B.2) "Member's attendance registration" (page 6)	Gives further detailed information
The paragraph of point B.3a) "Member's account update" (page 7)	Provides details for the case when a new biometric template must be collected

The table under B.3a) "Member's account update" (page 7)	Gives further detailed descriptions on additional risks
The table under B.3b) "Member's account/data deletion" (page 8)	Gives further detailed descriptions on risks related to storage and erasure
The paragraph under B.5) "Data consultation" (page 9)	Provides detailed technical information on biometric templates and how they work within the fingerprint-based system
The description of the first to fourth, sixth to eight and last of the terms of the glossary under point C) (pages 9 and 10)	These descriptions touch upon security-sensitive aspects of the technology
3. Decision-making process	
The paragraphs of point B) "Risk assessment and risk treatment (controls and safeguards)" (page 2)	Contain an opinion assessing the risk at the level of each operation module
The table under B.1) "Creation of Member's account" (pages 2 to 5)	Gives more details of such assessment
The paragraph of point B.2) "Member's attendance registration" (page 6)	Gives an opinion on the risk related to disclosure or modification of data
The table under B.2) "Member's attendance registration" (page 6)	Gives more detailed opinions on such risk
The paragraph of point B.3a) "Member's account update" (page 7)	Provides an appraisal on the risk related to the collection of new biometric templates
The table under B.3a) "Member's account update" (page 7)	Gives further detailed opinions on additional risks
The table under B.3b) "Member's account/data deletion" (page 8)	Gives further detailed opinions on risks related to storage and erasure
4. Privacy and the integrity of the individual	
The parts mentioned under Point 2	Risk of unauthorised interception, disclosure or modification of personal data concerning MEPs

Section XIII	
Document 5.3.4 - Annex 4 to Annex III to the Note from the Secretary-General to the Members of the Bureau of 4 June 2019	
<i>Parts covered by exception</i>	<i>Commentary</i>
1. Purpose of investigations	
The whole document	Would undermine purpose of EDPS investigation
2. Public security	
A part of the first indent of the third paragraph (page 1)	Contains a detailed technical explanation of biometric templates and how they are used in the fingerprint-based system
A part of the last sentence of the fifth paragraph, the last sentence of the sixth paragraph (page 1) and the text between brackets of the first sentence of the first paragraph (page 2)	Concern a technical detail that is considered security-sensitive information

3. Privacy and the integrity of the individual	
The parts mentioned under Point 2	Risk of unauthorised interception, disclosure or modification of personal data concerning MEPs



Der Generalsekretär

31.5.2018

D(2017)15113

NOTE TO THE MEMBERS OF THE BUREAU

Subject: Facilitating digital signing of the central attendance register

SUMMARY

Managing the central attendance register (CAR) – which Members sign as proof of attendance

– [REDACTED]

[REDACTED] A new arrangement which would modernise and computerise the CAR is now being proposed.

The members of the Bureau are being asked to:

- note the most recent assessment of the management of the CAR (rules, confidentiality, reliability and resources required) and give their agreement in principle to the launch of a voluntary test phase during which the system based on manual signatures would be supplemented by a computerised system using biometric technology;
- authorise the Secretary-General to present the results of the test phase towards the end of the eighth parliamentary term, so that the Bureau can take a final decision;
- adopt the attached amendment to Article 12 of the IMSM, so that the voluntary test phase can start, and instruct the President to publish the amendment in the Official Journal.

I. INTRODUCTION

Under Article 12¹ of the Implementing Measures for the Statute for Members of the European Parliament (IMSM), Members prove their attendance by signing the record available in the Chamber or meeting room, or by signing the CAR during the opening hours laid down by the Bureau.

Daily allowances are paid on the basis of that attestation of attendance, in accordance with conditions laid down by the Quaestors.

The CAR is open on working days outside part-sessions as established on Parliament's calendar². It is also open on some public holidays and office closing days.

II. CURRENT ARRANGEMENTS FOR MANAGING THE CAR

[REDACTED]

[REDACTED]

III. PROPOSAL TO COMPUTERISE THE MANAGEMENT OF THE CENTRAL ATTENDANCE REGISTER

The aim is to increase efficiency and provide MEPs with a simpler procedure and a processing method that makes it possible to pay daily subsistence allowances even more quickly. In addition, the system needs to offer all the reliability and confidentiality guarantees required to provide reasonable assurance as to MEPs' attendance. The proposal is, therefore, that an electronic attendance attestation system should be introduced for a voluntary test phase. [REDACTED]

[REDACTED]

[REDACTED] It would also provide the highest possible level of confidentiality for the data

¹ **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.

2. By way of exception, attendance may be attested by other documents proving that the Member was present at the meeting venue during normal meeting hours. This option may be used on no more than five occasions per half-parliamentary term.

3. Declarations by the Member or another person shall not be regarded as proof of attendance within the meaning of paragraphs 1 and 2. However, in the cases referred to in Article 10(1), points (b) and (c), and Article 10(2), attendance shall be attested by the Member's declaration.

² [REDACTED]

concerned, which would be used exclusively to certify an MEP's attendance during a certain time period on a certain day.

[REDACTED]

[REDACTED] Personal data will be protected scrupulously and comprehensively, in cooperation with Parliament's Data Protection Officer, who will verify the lawfulness of the system.

The needs of disabled MEPs will be taken into account on a case-by-case basis with a view to identifying workable solutions. This will be done before testing commences.

The benefits of computerisation

Choosing data processing systems that are similar to those already in use at Parliament will obviate any need for additional expenditure on the studies and extensive test phases that are needed when introducing the IT systems required to provide such processing.

A test phase (over the period to the end of the eighth parliamentary term) will enable those Members who wish to do so to use the biometric system rather than signing the CAR. The results of the testing will be submitted to the Bureau for a final decision. Computerisation could then be phased in for plenary, initially, and then possibly for other meetings at Parliament's places of work.

The advantages of computerisation are as follows:

- [REDACTED]
- procedures for paying daily subsistence allowances will be speeded up even more, every day of the week;
- [REDACTED]
- [REDACTED]
- [REDACTED]

IV. AMENDMENT OF THE IMSM

Article 12 of the IMSM will need to be amended in order to simplify attendance verification by bringing in the option of an electronic record.

V. CONCLUSIONS

The members of the Bureau are being asked to:

- note the most recent assessment of the management of the CAR (rules, confidentiality, reliability and resources required) and give their agreement in principle to the launch of a voluntary test phase during which the system based on manual signatures would be supplemented by a computerised system using biometric technology;
- -authorise the Secretary-General to present the results of the test phase towards the end of the eighth parliamentary term, so that the Bureau can take a final decision;
- -adopt the attached amendment to Article 12 of the IMSM, so that the voluntary test phase can start, and instruct the President to publish the amendment in the Official Journal.

Klaus Welle

Annexes:

Annex 1: Financial statement

Annex 2: Amendment to Article 12 of the IMSM

Annex 3: FAQs on the computerisation of the CAR

FINANCIAL STATEMENT

No. 107 /2018

1. Title of activity: AWP DG FINS: Project FINS 5 Automation of Members' attendance register(s)

1.1 Objectives:

Digitalisation and automation of the registration of the presence of Members of Parliament through the central attendance register, while guaranteeing reliability and confidentiality of the process, enabling efficient and timely payment of corresponding daily allowances

1.2

Indicators for monitoring the extent to which the above objectives have been achieved and for assessing the results obtained:

- Redeployment of contractual / interim staff currently assigned to monitor and manipulate the paper version of the central attendance register
- Decrease turnaround time of having final data available
- Increased timeliness of payment of daily allowances

2. Financial impact:

2.1. Calculations:

Item	Quantity	Unit price	Total
Scanner	5	3.100	15.500
Software	1	3.000	3.000
Service and support	1	1.500	1.500
Total			20.000

2.2 Expenditure provided for in the budget:

NO

If the expenditure is not provided for in the budget, why not?

Internal approval of DG FINS intervened after provision of 2018 budget

proposed means of financing?

Extraordinary approval for the test phase - budget lines were provided by DG ITEC

2.3 Breakdown by budget heading for the current financial year (2018)

Budget heading	Appropriations required (€)	Additional appropriations to be made available (€)
2105-20	15.500	
2103-20	4.500	
Total	20000	0

2.4 Estimated financial impact in future financial years

Budget heading	Amounts in € per year (at constant prices)					
	2018 (n)	n+1	n+2	n+3	n+4	n+5
2105-20 Computing and telecommunications _ Investments in projects: FINS decentralized IT projects	15.500					
2103-20 Computing and telecommunications — business-as-usual operations — management of ICT applications: applications of the DG FINS	4.500	1.500	1.500	1.500	1.500	1.500
Total	20.000	1.500	1.500	1.500	1.500	1.500

3. Impact on human resources:

Personnel types	Staff required to run the activity		
	No. of working days per person	Existing staff	Additional staff
Officials or temporary staff	AD		
	AST		
Other resources	Agents contractuels	0	4
Total		0	4

4. Lead DG / department:

DG FINS

Other DG(s) / department(s) consulted:

DG SAFE, DG ITEC

Prepared by:

on: 05/04/2018

Received on:


11/04/2018

Forwarded on: 12/04/2018

DG FINS, Directorate for Budget and Financial Services
Budget Unit

NB! This financial statement in no way constitutes authorisation of expenditure. Having received authorisation from the competent authorities for the operation concerned, the unit responsible for the project should contact the authorising officers for the budget headings concerned to inform them and ensure that there will be a prior commitment of the appropriations required before taking any action on behalf of the institution.

Compendium of Rules - 2.1.1

Current text	Proposed modifications	Justification
<p style="text-align: center;">TITLE I Chapter 4 REIMBURSEMENT OF EXPENSES</p>		
<p style="text-align: center;">Article 12 Attestation of attendance</p>		
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.	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. <i>An electronic attestation of a Member's attendance may replace his or her signature.</i>	
2. By way of exception, attendance may be attested by other documents proving that the Member was present at the meeting venue during normal meeting hours. This option may be used on no more than five occasions per half-parliamentary term.	2. By way of exception, attendance may be attested by other documents proving that the Member was present at the meeting venue during normal meeting hours. This option may be used on no more than five occasions per half-parliamentary term.	
3. Declarations by the Member or another person shall not be regarded as proof of attendance within the meaning of paragraphs 1 and 2. However, in the cases referred to in Article 10(1), points (b) and (c), and Article 10(2), attendance shall be attested by the Member's declaration.	3. Declarations by the Member or another person shall not be regarded as proof of attendance within the meaning of paragraphs 1 and 2. However, in the cases referred to in Article 10(1), points (b) and (c), and Article 10(2), attendance shall be attested by the Member's declaration.	

FREQUENTLY ASKED QUESTIONS

1. What is a biometric reader?

Biometrics are automated methods of recognizing a person based on a physiological or behavioural characteristic. Biometric fingerprint readers use advanced imaging technologies to capture a highly accurate reading of a fingerprint data. Providing a quick, safe, simple and cost effective solution, the recognition devices can be integrated into existing systems, providing reliable biometric time and attendance system.

2. How will the attendance be registered?

When a person is first enrolled in a biometric time and attendance system, the biometric reader records an image [REDACTED]
[REDACTED]
[REDACTED] If there is a match, the attendance is recorded.

3. What are the advantages for MEPs?

The advantages of using a biometric reader are manifold:

- fast and secure identification without a badge or PIN and registration leading to:
 - payment of the daily allowance the same day,
 - highest standards of protection of personal data;
- possibility for Members to register their attendance in [REDACTED] different locations [REDACTED]
- optimisation of human resources [REDACTED]
[REDACTED] leading to their redeployment to higher added-value services for MEPs.

4. How long does it take to scan?

Scanning will be instant.

5. How is data stored?

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

6. Can the image be duplicated?

[REDACTED]
[REDACTED]

7. Are there any health concerns with the use of biometrics?

No. There is no evidence to support that printing technology can impose a negative effect to health. Fingerprint scans are safe and non-intrusive to the users. Biometric identification and verification systems have been in use for over 30 years, with no reported health hazards.

Some people could have hygiene concerns about placing their finger on the reader. Generally speaking, there is no greater health risk involved in using the reader than there would be in using a doorknob that has been touched by other people, handling money, or shaking hands. The readers will be regularly cleaned during the day.

8. Is the biometric reader complying with the law governing personal data collection and processing securing the privacy?

Yes. It complies with the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 and Regulation 45/2001. [REDACTED]

9. In case of a power failure or system crash, what happens?

Biometric readers are equipped with back-up batteries to prepare for any power failure case.

10. Where are the registered templates stored?

[REDACTED]

11. What happens if the MEP scans the finger more than once?

[REDACTED]

12. What happens if a MEP tries to scan the opposite finger?

[REDACTED]

13. What happens if, due to medical reasons, the scanner does not recognize the finger?

[REDACTED]

Article 12(2) of the Implementing Measures for the Members' Statute is of application. The responsible service will handle this exceptional circumstances on a case-by-case basis.

14. Would I be able to log on with an injured /finger?

[REDACTED]

16. Who to contact in case the biometric readers produce errors?

In case of questions concerning the biometric scanners, please contact your MEPs' Portal team:

at your Front desk in Brussels → ASP 3H352

at your Front desk in Strasbourg → LOW T02 050

via e-mail to meps.portal@ep.europa.eu

by phone, inside the EP at 44422

Der Generalsekretär

04 JUIN 2019

D(2019)12215

NOTE FOR THE ATTENTION OF THE MEMBERS OF THE BUREAU

Subject: *Facilitating the signing in the central attendance register through digitalisation: results of the voluntary test phase and follow-up proposal*

SUMMARY

[REDACTED]

Therefore, at its meeting of 11 June 2018, the Bureau decided¹ to launch a voluntary test phase for Members to supplement the CAR based on personal signatures by a computerised system based on biometrics technology. The Bureau also asked the Secretary-General to present the results of the test phase towards the end of the eighth parliamentary term, so that the Bureau could take a final decision on the most appropriate course of action to follow.

The voluntary test phase (21 January 2019 - 12 April 2019) has been based on a system allowing the use of Members' personal access badges at [REDACTED] badge readers specially installed for the attestation of Members' presences.

The Bureau is invited to:

- take note of the evaluation report on the voluntary test phase;
- take note of the annexed data protection impact assessment and its recommendation for the fingerprint reading system;
- decide to proceed with a computerised system for the digitalisation of the central attendance registry through biometric technology;
- authorise the Secretary-General to launch the procedures for the purchasing and implementation of a digital system for the attestation of Members' attendance based on biometric technology, which shall replace the system based on manual signatures by the end of 2019.

¹ PE-8/BUR/PV/2018-07.

I. INTRODUCTION

[REDACTED]

Therefore, at its meeting of 11 June 2018, the Bureau decided to launch a voluntary test phase for Members to supplement the CAR based on personal signatures by a computerised system based on biometric technology. The Bureau requested the Secretary-General to present the results of the test phase towards the end of the eighth parliamentary term, so that the Bureau could take a final decision on the most appropriate course of action to follow.

The present note sets out the results of the test phase and the reasons justifying the proposal to introduce a system of attestation of Members' presences based on biometric technology (e.g. fingerprint reading).

II. THE TEST PHASE

Following the Bureau's decision mentioned above, Parliament services assessed various technical options available in light of the framework of data protection and functionality.

The Data Protection Regulation (EU) 2018/1725² sets a high standard of protection when processing special categories of personal data (such as biometric data for the purpose of uniquely identifying a natural person). Article 39(1) thereof provides that "*when a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*". This Data Protection Impact Assessment (DPIA) must be carried out prior to the processing operation and be approved by the data controller.

Taking into account the advice from Parliament's Data Protection Officer (DPO) to test a badge-based system first, during a test phase (21 January 2019 - 12 April 2019) trials have been carried out of a computerised system with an autonomous network based on badge-reading devices.

[REDACTED]

² Regulation (EU) 2018/1725 of the European Parliament and of 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) 45/2001 and Decision No 1247/2002/EC.

III. RESULTS OF THE TEST PHASE

[REDACTED]

[REDACTED]

[REDACTED]

Therefore, taking account of the limitations and hindrances of a badge-based system, the implementation of a better digital option based on biometric technology is proposed herewith, supported by the results of the approved Data Protection Impact Assessment ("DPIA", see Annex 3) carried out in line with the said new data protection Regulation.

IV. THE PROPOSED FINGERPRINT-READING SYSTEM

In comparison with the other two options already used (manual signature or personal badge), a computerised system based on biometrics technology is the most viable and secure solution.

The DPIA, i.e. the assessment of the impact of the processing operations³ on the protection of personal data of the Members, has been carried out in accordance with the requirements established by Regulation (EU) 2018/1725 (in particular Article 39 thereof). The DPIA methodology used is in line with the European Data Protection Officer's guidelines on analysing and controlling the risks for data subjects in detail through Data Protection Impact Assessments⁴. The positive conclusions of the DPIA have allowed the data protection controller to validate it, after consultation of Parliament's Data Protection Officer.

On account of the above, the responsible Parliament services have prepared a call for tender for the purchasing and implementation of a digital system for the attestation of Members' presences based on biometrics technology (in particular fingerprint reading technology).

V. CONCLUSIONS

The Bureau is invited to:

- take note of the evaluation report on the voluntary test phase;
- take note of the annexed data protection impact assessment and its recommendation for the fingerprint reading system;

³ Collection, recording/structuring, transfer and erasure of digital encryptions in relation with users' scanned fingerprints.

⁴ EDPS, *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation*, available at https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_2_en.pdf.

- decide to proceed with a computerised system for the digitalisation of the central attendance registry through biometric technology;
- authorise the Secretary-General to launch the procedures for the purchasing and implementation of a digital system for the attestation of Members' attendance based on biometric technology, which shall replace the system based on manual signatures by the end of 2019.



Klaus WELLE

Annexes:

- Annex 1: Financial statement
- Annex 2: Evaluation report on the test phase
- Annex 3: Data Protection Impact Assessment

FINANCIAL STATEMENT

No. 51 /2019

1. Title of activity: AWP DG FINS: Project FINS 5 Automation of Members' attendance register(s)

1.1 Objectives:

Digitalisation and automation of the registration of the presence of Members of Parliament through the central attendance register, while guaranteeing reliability and confidentiality of the process, enabling efficient and timely payment of corresponding daily allowances

- 1.2 Indicators for monitoring the extent to which the above objectives have been achieved and for assessing the results obtained:

- Redeployment of contractual / interim staff currently assigned to monitor and manipulate the paper version of the central attendance register
- Decrease turnaround time of having final data available
- Increased timeliness of payment of daily allowances

2. Financial impact:

2.1. Calculations:

Item	Quantity	Unit price	Total
Hardware (e.g. scanning device)(*)	20	3.500	70.000
Software (including installation), transfer of competences and service & support for the first 2 years	1	25.000	25.000
Service and support for years 3&4	1	16.000	16.000
Total			111.000

(*) including costs with any additional hardware which is necessary

- 2.2 Expenditure provided for in the budget: NO

If the expenditure is not provided for in the budget, why not?

Decision to launch a public procurement procedure for purchasing a solution based on biometry was delayed due to EP's data protection officer's intervention and it was resumed after provision of 2019 budget.

proposed means of financing?

launch of production phase - budget lines were provided by DG ITEC

- 2.3 Breakdown by budget heading for the current financial year (2019) :

Budget heading	Appropriations required (€)	Additional appropriations to be made available (€)
2105-20 - Computing and telecommunications — investment in projects: FINS - decentralized IT projects	95.000	0
Total	95.000	0

- 2.4 Estimated financial impact in future financial years :

Budget heading	Amounts in € per year (at constant prices)			
	2020	2021	2022	
2103-20 - Computing and telecommunications — business-as-usual operations — management of ICT applications: applications of the DG FINS	0	8.000	8.000	
Total	0	8.000	8.000	

3. Impact on human resources: NONE

4. Lead DG / department:

DG FINS

Other DG(s) / department(s) consulted:

DG SAFE, DG ITEC

Prepared by:

on: 22/03/2019

Received on:

25/03/2019

Forwarded on: 25/03/2019

UN

DG FINS, Directorate for Budget and Financial Services
Budget Unit

NB! This financial statement in no way constitutes authorisation of expenditure. Having received authorisation from the competent authorities for the operation concerned, the unit responsible for the project should contact the authorising officers for the budget headings concerned to inform them and ensure that there will be a prior commitment of the appropriations required before taking any action on behalf of the institution.

Evaluation report on the test phase - Risk assessment of a badge-based system to register attendance

1. Introduction

Following the decision of the Bureau of 11 June 2018¹ to proceed with a test phase of a computerised system based on biometrics technology, both the European Data Protection Supervisor (EDPS) and Parliament's Data Protection Officer (DPO) advised the competent services to first consider the option of a less intrusive system in terms of data protection.

As a result, the Directorate-General for Finance (DG FINS), with the support of the Directorate-General for Security and Safety (DG SAFE), implemented a computerised system with an autonomous network based on badge-reading devices. In order to attest their presence, Members could use their personal badges at [REDACTED] badge-reading devices [REDACTED]

[REDACTED] The test phase of the badge-based system took place between 21 January and 12 April 2019 and its arrangements were duly communicated by the Quaestors (3/2019²).

¹ PE-8/BUR/PV/2018-07

² PE 626.191/QUEST/CM

2. Risk assessment

Identified risk	Description of risk	Nature of risk	Type of risk	Likelihood	Impact	Classif. of risk	Strategy	Risk response
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>					
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>					<div> <div></div> <div></div> <div></div> </div>
								<div> <div></div> <div></div> </div>
								<div> <div></div> </div>
<div> <div></div> <div></div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> </div>	<div> <div></div> </div>	<div> <div></div> <div></div> </div>					<div> <div></div> <div></div> <div></div> </div>
								<div> <div></div> </div>
								<div> <div></div> </div>
								<div> <div></div> </div>
<div> <div></div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> </div>	<div> <div></div> </div>			<div> <div></div> <div></div> <div></div> </div>
								<div> <div></div> <div></div> </div>
								<div> <div></div> </div>
<div> <div></div> </div>	<div> <div></div> </div>	<div> <div></div> </div>						
<div> <div></div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> </div>							
<div> <div></div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>						<div> <div></div> <div></div> <div></div> </div>
								<div> <div></div> </div>
								<div> <div></div> </div>

3. Conclusions

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]