



## **EDPS Formal comments on the draft Commission Implementing Regulation laying down detailed rules for the application of Regulation (EC) No 767/2008 of the European Parliament and of the Council, as regards the conditions for the operation of the web service and the data protection and security rules applicable to the web service**

### **THE EUROPEAN DATA PROTECTION SUPERVISOR,**

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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 ('EUDPR')<sup>1</sup>, and in particular Article 42(1) thereof,

### **HAS ADOPTED THE FOLLOWING FORMAL COMMENTS:**

#### **1. Introduction and background**

1. On 27 February 2026, the European Commission consulted the EDPS on the draft Commission Implementing Regulation laying down detailed rules for the application of Regulation (EC) No 767/2008 of the European Parliament and of the Council, as regards the conditions for the operation of the web service and the data protection and security rules applicable to the web service ('the draft Implementing Regulation').
2. Regulation (EU) 2023/2667<sup>2</sup> amended, *inter alia*, Regulation (EC) No 767/2008<sup>3</sup> ('VIS Regulation' or 'basic act') to provide for an EU Visa Application Platform ('EU VAP') in the context of the digitalisation of the visa procedure. The amended VIS Regulation distinguishes between, on the one hand, the secure account service and the verification tool linked to that secure account<sup>4</sup>, and, on the other hand, a web service functionality provided for in Article 7h(3) to allow applicants, visa holders and certain third parties to verify limited visa-related information without the secure account service.
3. The objective of the draft Implementing Regulation is to lay down detailed rules on the conditions for the operation of the web service and the data protection and security rules applicable to that web service, in accordance with Article 7h and Article

---

<sup>1</sup> OJ L 295, 21.11.2018, p. 39.

<sup>2</sup> Regulation (EU) 2023/2667 of the European Parliament and of the Council of 22 November 2023 amending Regulations (EC) No 767/2008, (EC) No 810/2009 and (EU) 2017/2226 of the European Parliament and of the Council, Council Regulations (EC) No 693/2003 and (EC) No 694/2003 and Convention implementing the Schengen Agreement, as regards the digitalisation of the visa procedure, OJ L, 2023/2667, 7.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2667/oj>.

<sup>3</sup> Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, OJ L 218, 13.8.2008, pp. 60.

<sup>4</sup> Article 7h(1) of the VIS Regulation.



45(2), point (n), of the VIS Regulation, including detailed rules on unique identifiers for applicants<sup>5</sup>.

4. The draft Implementing Regulation is adopted pursuant to Article 45(2) point (n) of the VIS Regulation.
5. The EDPS previously issued Opinion 13/2022 on the Proposal for a Regulation on the digitalisation of the visa procedure<sup>6</sup>.
6. The present formal comments are issued in response to a consultation by the European Commission pursuant to Article 42(1) EUDPR. The EDPS welcomes the reference to this consultation in Recital 22 of the draft Implementing Regulation.
7. These formal comments do not preclude any additional comments by the EDPS in the future, in particular if further issues are identified or new information becomes available, for example as a result of the adoption of other related Implementing or Delegated acts<sup>7</sup>.
8. Furthermore, these formal comments are without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Article 58 of the EUDPR and are limited to the provisions of the draft Implementing Regulation that are relevant from a data protection perspective.

## 2. Comments

### 2.1. General Comments

9. The EDPS notes that the amended VIS regulation establishes the functional requirement that a web service must exist to permit verification of the status and validity of visas. The amended VIS Regulation does not, however, prescribe the data protection and security rules applicable to the web service. The aim of the draft implementing regulation is to specify these rules.
10. As a preliminary matter, the EDPS recommends further clarifying the relationship between the secure account, the EU VAP and the web service. In particular, the draft Implementing Regulation should further specify the role and technical function of these three different mechanisms. These clarifications are particularly important because the draft Implementing Regulation defines an operational model, many of the

---

<sup>5</sup> See Article 45(2)(n) of the VIS Regulation. Cf. recital 7 of the draft implementing act: This Regulation should lay down detailed rules on the conditions for the operation of the web service, including the means through which visa holders can be uniquely identified and access the web service in a secure manner, the procedure for submitting a query, and the content and format of the reply to be returned by the web service.

<sup>6</sup> [EDPS Opinion 13/2022 on the Proposal for a Regulation on the digitalisation of the visa procedure, issued on 21 June 2022.](#)

<sup>7</sup> In case of other Implementing or Delegated acts with an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data, the EDPS would like to remind that he needs to be consulted on those acts as well. The same applies in case of future amendments that would introduce new or modify existing provisions that directly or indirectly concern the processing of personal data.

elements of which are not laid down in the amended VIS Regulation, including the absence of a secure-account requirement for the web service<sup>8</sup>, the use of email-based interaction, the delegation of access through a link associated with a time-limited token, and the automatic launching of a query when that link is used.

11. The EDPS further notes that the draft Implementing Regulation uses the expression “web service” to cover different access modalities with different levels of trust and different legal contexts, namely self-service access by applicants and visa holders, delegated access by other entities and duly authorised persons, and exceptional fallback access by border authorities. The different assurance levels and role of those different modalities should be reflected more transparently in the text (e.g. further clarification regarding the circumstances in which the different modalities could be used could be provided by way of recital).

## **2.2. Queries to the web service by visa holders and applicants**

12. According to Article 4 of the draft Implementing Regulation, applicants and visa holders may access visa status information through the web service, which is of particular importance both where they cannot use, or do not have, a secure account in the EU VAP<sup>9</sup> and where the EU VAP is not (yet) used by the competent Member State during the transitional period<sup>10</sup>. The access procedure is layered. First, the person must indicate the email address that was provided in the application form. If the email address is recognised, a time-limited link is sent to that address.
13. Secondly, once the person has opened the link, the web service requires the completion of a bot-detection test. This constitutes an important safeguard against automated scraping and brute-force attempts<sup>11</sup>.
14. Thirdly, after opening the link and completing the bot-detection test, the person must query the web service using either the type and number of the travel document together with the three-letter code of the issuing country, or the visa number. Those data cannot be regarded as secret in a strict sense, but they are not easily guessable at scale and therefore provide an additional contextual layer of protection.
15. The EDPS notes that the layered access established by Article 4 combines verification of the email address indicated in the application form, a bot-detection step, and a subsequent query using travel-document data or the visa number. For the avoidance

---

<sup>8</sup> Article 6(5) of the draft Implementing Regulation.

<sup>9</sup> The EU VAP secure account constitutes the primary interface for digital visa applications, but it is not the exclusive channel. Due to the transitional period, mandatory in-person elements, and specific legal exceptions, visas may be issued without the applicant ever using a secure account. The web service therefore plays a crucial complementary role by enabling the verification of such visas independently of the secure account infrastructure.

<sup>10</sup> Recital (36) of Regulation (EU) 2023/2667 provides that, during the 7-year transitional period, if a Member State does not avail itself of the EU VAP, visa holders should still be able to verify the digital visas using the web service of the EU VAP.

<sup>11</sup> In this context, automated scraping should be understood as the systematic use of scripts or bots to submit large numbers of queries in order to harvest visa-status results, build databases, or monitor changes over time. Brute-force attempts, by contrast, involve the repeated trial of many different combinations of input data in order to discover a valid match or gain access by guessing visa-related identifiers.

of doubt (and to rule out the possibility of accessing visa information relating to another person), the draft Implementing Regulation should expressly clarify that the query may return results only where the data used in the query correspond to a visa record linked to the (verified) email address provided in the application form.

16. The EDPS notes that the web service provides only read access to limited visa-status information and does not enable modification of data, the execution of transactions, or broader access to VIS records. From a risk-based perspective, the layered mechanism provided for in Article 4 may therefore be regarded as providing appropriate safeguards.
17. At the same time, the use of the email address indicated in the application form may create practical difficulties where that address contains a mistake, is no longer accessible to the applicant, or was controlled from the outset by an intermediary such as a travel agency. The current drafting of Article 4(5) appears to address only a mismatch by means of an error message and the possibility to enter a valid email address, without clearly providing a recovery or alternative identification mechanism. The EDPS therefore invites the Commission to consider whether the draft Implementing Regulation should provide a fall-back solution allowing the person concerned to regain access, for example through a combination of visa number and travel-document data or through an update mechanism for the email address, subject to appropriate safeguards.
18. The EDPS also considers that the web service should be systematically monitored for anomalies in order to keep the underlying risk analysis up to date. Patterns such as repeated queries concerning the same travel document, repeated attempts linked to the same visa number, or a high volume of queries originating from the same device or network may justify adjustments to the safeguards or to the amount of data returned.

### **2.3. Queries of the web service by other entities and duly authorised persons**

19. Articles 5 and 6 of the draft Implementing Regulation establish a consent-based and tokenised access mechanism for other entities and duly authorised persons. The mechanism enables the third-country national to identify the relevant visa through the self-query flow and then enables a third party to obtain a limited reply by means of a link associated with a time-limited token. In functional terms, the design resembles a bearer-token system, since possession of the operative link or token is what allows the third party to retrieve the reply.
20. The EDPS notes that such a mechanism may constitute a proportionate and user-friendly way of enabling third-country nationals to share limited visa-status information without imposing the burden of account creation on the recipient. However, a possession-based model also entails risks of interception, inadvertent disclosure, onward sharing and unauthorised use. Once the delegation link or token has been generated, the third-country national's effective control over subsequent

access appears limited, in particular because the draft Implementing Regulation does not clearly provide for revocation, tracking by the applicant, or notifications upon use.

21. Against that background, the EDPS considers that the shift from identity-based access control to possession-based access control should be accompanied by strong ex-post safeguards. In particular, the logging of token generation and token use, the monitoring of abnormal patterns, and adequate transparency towards the third-country national would be important complementary measures. It should also be ensured that the amount of data returned to third parties is limited to what is strictly necessary for the specific verification purpose.

#### **2.4. Token mechanism and email service**

22. The EDPS considers that the interaction between Article 5(2), Article 5(5) and Article 5(6) of the draft Implementing Regulation is not sufficiently clear. Article 5(2)(c) provides that the third-country national requests the generation of “a link associated with a time-limited token” and “to provide the token” to the entity or duly authorised person. Article 5(5), by contrast, states that the EU VAP shall allow the link to be sent via the “email service” to the email address of the entity or duly authorised person concerned. Article 5(6) then envisages that the recipient clicks on the link and that the query is launched automatically. Taken together, those provisions suggest that, in practice, the link itself contains, carries or activates the token. If that is the intended design, Article 5(2)(c) should be reformulated to clarify the relationship between the token and the link<sup>12</sup>.
23. The draft Implementing Regulation does not define the expression “email service” referred to in Article 5(5). That omission matters because the level of assurance attached to the transmission depends in part on the nature of that service. At present, the wording could be understood as referring to an external email-sending functionality of the EU VAP, to an internal secure messaging function within the EU VAP, or to another trusted delivery mechanism. However, those options are materially different in terms of security, legal certainty and implementation.
24. In the view of the EDPS, the most coherent reading of the draft Implementing Regulation and of the amended VIS framework is that the “email service” is a functionality of the EU VAP pursuant to Article 2a(6)(f) of the VIS Regulation, enabling the sending of messages to external email addresses without requiring the recipient to hold a secure account in the EU VAP. The draft Implementing Regulation should clarify this expressly. It should also clarify what is meant by the requirement in Article 5(5) that the email containing the link should be “secured”, since the current text does not indicate whether this refers to transport-layer protection, the design of the link itself, tokenisation, or another technical control.

---

<sup>12</sup> The current drafting could be understood as implying that the token would be transmitted separately from the link, which may not be the case. See also paragraph 5(5) of the draft Implementing Decision.

25. The EDPS further notes that Articles 4 to 6 switch repeatedly between “EU VAP” and “web service” without making sufficiently clear whether these terms designate distinct components, distinct interfaces, or simply different functional descriptions of the same system. In particular, the draft Implementing Regulation refers in Article 6(1) to the EU VAP sending the unique identifier, while the following provisions refer to the web service informing the person concerned and requiring the identifier to be entered. The draft Implementing Regulation would therefore benefit from additional clarification, for example in a recital, explaining the relationship between the EU VAP, the secure account service and the web service.
26. In addition, the EDPS considers that Article 6 of the draft Implementing Regulation requires further clarification. When read in isolation, it may suggest that the generation of the token for third-party access depends only on indicating the email address used in the application form, receiving a unique identifier by email, completing a bot-detection test and entering that identifier. Read together with Article 5(2), however, the mechanism may not be understood in the same way. Article 5(2) first requires the third-country national to launch a query under Article 4 and to select the match relating to the visa that is to be verified by the third party. Since Article 4 requires the use of travel-document data or the visa number, the draft Implementing Regulation does not establish a purely email-based route to token generation.
27. The EDPS therefore recommends clarifying expressly in Article 6 that the generation of a token may be requested only after completion of the steps referred to in Article 5(2)(a) and (b), including the Article 4 query and the selection of the relevant visa match. Such a clarification would avoid the incorrect impression that generating a token for third-party verification is easier than self-verification by the applicant or visa holder.
28. The legal and technical function of the “unique identifier” also remains unclear. The amended VIS Regulation refers, in the implementing empowerment, to detailed rules for the web service including “unique identifiers for applicants”, but does not define that notion or explain its characteristics. For example, it does not indicate whether the identifier is intended to be person-specific or transaction-specific, permanent or one-time, embedded in a link or entered separately, or whether its function is primarily authentication, confirmation of consent, or both.
29. The terminology used in Article 6 is capable of creating confusion. The provision first refers to the sending of a “unique identifier” and subsequently states that the person concerned shall be informed that “the link” shall be valid only for a short period of time. To avoid confusion, the EDPS recommends further clarifying the relationship between the link mentioned in Article 4, the identifier mentioned in Article 6 and the link mentioned in Article 5.
30. The EDPS also questions whether the term “unique identifier” is the most appropriate one in this context. In the broader EU digital-identity framework, including eIDAS-

related terminology<sup>13</sup>, unique identifiers are usually associated with the reliable and potentially persistent identification of a natural or legal person. By contrast, the mechanism described in Article 6 appears functionally much closer to a request-specific verification code or one-time PIN. The use of the term “unique identifier” therefore risks suggesting a stable identity attribute where the draft Implementing Regulation in fact seems to envisage a short-lived confirmation code. The EDPS invites the Commission to consider either replacing the term with wording that reflects the actual function of the measure or clarifying explicitly that the identifier is request-specific, time-limited and used solely to confirm the generation of a token for third-party access.

## **2.5. Consent and evidentiary aspects of third-party access**

31. Article 5 is based on the premise that other entities and duly authorised persons may query the web service only after obtaining the prior free and explicit consent of the third-country national. The draft Implementing Regulation operationalises that requirement through the applicant’s or visa holder’s actions within the web service, in particular the selection of the relevant visa and the generation of a delegation link or token. The legal nature of that consent would nevertheless benefit from further clarification.
32. As currently drafted, the act of generating and sharing the delegation link appears to serve as the operative manifestation of consent. The EDPS notes, however, that the draft Implementing Regulation does not require an explicit confirmation statement from the person concerned, does not indicate whether a consent record would be visible to the recipient, and does not describe in detail the audit trail associated with that consent. This may create evidentiary difficulties, both for the third-country national and for the recipient relying on the link as proof that access is authorised.
33. The EDPS therefore invites the Commission to consider whether an additional confirmation step should be introduced before the token or delegation link is generated, making it explicit that the third-country national consents to the named recipient accessing his or her visa status for the relevant purpose. In addition, the corresponding logs should be sufficiently detailed to record who requested the delegation, when it was generated, to which visa it related and when it was used.

## **2.6. Queries by border authorities**

---

<sup>13</sup> Cf. Recital 54 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, pp. 73–114, as amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L, 2024/1183, 30.4.2024, ELI: <http://data.europa.eu/eli/reg/2024/1183/oj>.

34. The EDPS notes that Article 7 of the draft Implementing Regulation introduces a further access modality, under which border authorities may exceptionally query the web service where it is technically impossible to consult the VIS at the external borders. That modality differs fundamentally from the flows laid down in Articles 4 to 6. It is not based on an email address, a delegation token or a consent mechanism, but on the travel document presented at the border and on access by duly authorised users operating on secure devices in a controlled environment.
35. The EDPS recommends acknowledging more clearly in the draft Implementing Regulation that the web service is, in practice, a shared technical interface with multiple access regimes and different levels of assurance. Self-service access by applicants and visa holders, delegated access by third parties, and contingency access by border authorities are not equivalent use cases and do not raise the same risks. A clearer distinction between these regimes would improve the legal clarity of the draft Implementing Regulation and help ensure that the legal and technical safeguards remain proportionate to the specific risk profile of each regime.
36. The EDPS also observes that Article 7 relies on the assignment of access rights and the use of a secure device but does not specify in detail the user-authentication mechanism applicable to border authority access. Although it may be acceptable to leave the detailed authentication method to technical specifications and to the trusted environment in which border authorities operate, the draft should make clearer that border authority access is subject to specific organisational and technical controls that differ from the public web-service interfaces.

## 2.7. Data protection and security requirements

37. The EDPS welcomes that Article 9(3) of the draft Implementing Regulation lays down a number of security principles applicable to the web service. At the same time, the current draft defines most of the legally binding operational obligations by way of reference to cybersecurity terminology. Expressions such as “defence in depth”, “positive security model” and “zero-trust principles” may be useful as technical design principles, but they do not always provide sufficient legal clarity or facilitate ex post assessment of compliance<sup>14</sup>.

---

<sup>14</sup> In contrast, and for illustration purposes, the categories mentioned in Article 9(3) of the draft Implementing Regulation could be translated into functional requirements along the following lines:

3. The web service shall be designed, implemented and operated in a manner that ensures a level of security appropriate to the risks presented by the processing of personal data, in accordance with Article 32 of Regulation (EU) 2016/679.

To that end, the web service shall in particular:

- (a) implement multiple and complementary security measures at network, system and application level, so that the failure of a single measure does not compromise the overall security of the system;
- (b) ensure that access to the web service and to the data it processes is granted only to duly authorised users or systems and limited to what is strictly necessary for the performance of their tasks;

38. The EDPS invites the Commission to consider describing the security requirements also in a functional way, e.g. by making clear which concrete security outcomes are expected. In particular, Article 9(3) should emphasise that authentication measures must be proportionate to the level of risk associated with the relevant category of user, that any session, token or identifier used to access the web service must be time-limited and protected against misuse, and that secure communication, access control, monitoring and logging must operate coherently across the different access regimes supported by the web service, etc.
39. The EDPS underlines that without aligning the content of Article 9 with the rest of the draft Implementing Regulation, in particular the token-based access (Articles 5–6), authority access (Article 7), and logging (Article 11), the draft Implementing Regulation would not be internally consistent.
40. The EDPS recalls that eu-LISA, as the entity responsible for the development and operation of the relevant components of the EU VAP, is already required under the applicable Union data protection and cybersecurity framework to determine appropriate technical and organisational security measures on the basis of a risk-based assessment and to ensure sufficient documentation to enable accountability, audit and oversight. Against that background, the EDPS invites the Commission to ensure that the technical specifications and operational arrangements for the web service clearly reflect that obligation.

## 2.8. Logging

41. The EDPS welcomes that the draft Implementing Regulation includes a dedicated Article on logging. As logging requirements may differ from other logging requirements under the VIS Regulation, Article 11 of the draft Implementing Regulation can provide for specific requirements associated with the web service.

---

(c) require authentication measures proportionate to the level of risk associated with each category of user, including, where appropriate, multi-factor authentication for access by competent authorities;

(d) ensure that, by default, only explicitly authorised actions, inputs and data processing operations are permitted, and that all other actions are denied;

(e) ensure that, in the event of system errors or failures, access to personal data is restricted and no unauthorised disclosure or processing occurs;

(f) ensure that any session, identifier or token used to access the web service is protected against unauthorised use, is time-limited, and is invalidated after use or expiry;

(g) ensure that all data submitted by users are verified for correctness, completeness and conformity with predefined formats before being processed;

(h) ensure that all communications with the web service are protected against interception and tampering through appropriate encryption and secure communication protocols;

(i) ensure that access requests and system interactions are continuously verified and logged, and that abnormal or unauthorised activities are detected and addressed without delay;

(j) ensure that the principles of data protection by design and by default are integrated into all stages of the development and operation of the web service, in accordance with Article 25 of Regulation (EU) 2016/679. This would also take into due account the token logic, thereby providing consistency with Articles 5-6, and would replace ambiguous and vague concepts such as “zero-trust principles” with concrete obligations such as verification, logging and monitoring.

42. The EDPS recommends extending the provision and the logging obligations beyond queries and to cover also access requests, link, token and ‘unique identifier’ generation, in order to have the necessary data basis to monitor for potential misuse or abuse.
43. The EDPS notes that Article 11(1)(f) of the draft Implementing Regulation refers only to the “type of data used for the query”, without making clear whether the logs contain any identifier enabling the query event to be linked to the record concerned. The EDPS considers that, for the purposes of data protection monitoring, misuse detection and ex post verification, the logging framework should include a proportionate reference allowing the queried dataset to be identified reliably. The EDPS therefore invites the Commission to clarify that the logs must contain sufficient information to link a query to the corresponding visa record, while remaining consistent with the principle of data minimisation.
44. The EDPS further notes that the information to be logged does not have a common baseline for the three user groups visa holder, duly authorised person, or border authority. The EDPS does not consider it necessary that the same technical identifier be logged for all categories of users. However, the EDPS considers that the draft should ensure an equivalent level of traceability across access channels and user categories. In that regard, the EDPS invites the Commission to clarify the scope of the “device-specific information and metadata” to be logged for entities and duly authorised persons and, as regards border authorities, to ensure that the combined central and local logging arrangements permit the identification of the individual authorised user involved in a query or fallback operation, while remaining consistent with the principle of data minimisation.

Brussels, 24 April 2026

*(e-signed)*  
Wojciech Rafał WIEWIÓROWSKI