Ref. Ares(2026)8986564 - 23/09/2026

EUROPEAN EXTERNAL ACTION SERVICE

DG Resource Management
The Director-General

Brussels, 23 September 2026

Mr Giacomo Zandonini
by electronic mail

Subject: **Your confirmatory application for access to documents**
EEAS ref: 2026/94 and 2026/115

Dear Mr Zandonini,

I would like to thank you for your e-mail of 13 July 2026, in which you make a confirmatory application, in accordance with Article 7(2) of Regulation (EC) No 1049/2001 regarding public access to documents.[1]

As requested, I have examined the decision of 13 July 2026 of the EEAS service in charge of access to documents (SG.LD.ATD - Transparency), taken after the assessment of the division holding the documents, not to disclose, the list of documents identified as falling within the scope of your two related requests and consequently not to grant access to those documents.

Your requests concerned:

> *"Any document, in all formats, including correspondence and attachments, in which the company Cellebrite, or any of its representatives or products (such as the UFED), are mentioned. Cellebrite is an Israel-headquartered, US-registered global technology company producing top mobile forensics and data analysis tools, used for security and monitoring purposes. The description can include, but is not limited to:*
> - *Internal correspondence;*
> - *Licensing agreements, contracts, procurement notices;*
> - *Market assessments;*
> - *Minutes of meetings;*
> - *Briefing notes, internal reports, slides, presentations, material received by third parties.*
>
> *The time frame for the request is from September 1, 2022 to April 20, 2026."*

and

[1] Regulation (EC) No 1049/2001 of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (OJ L 145, of 31.5.2001, p. 43, hereafter the "Regulation "), as applied by the EEAS pursuant to Article 11(1) of the Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service (OJ L 201, of 3.8.2010, p. 30).

"All documents, including correspondence and attachments in all formats, produced or held by the EEAS, where the company Cellebrite or any of its products (UFED; Physical Analyzer, Kiosk, Inseyets), are mentioned. The description includes procurement documents and correspondence with the company itself, or with any reseller, with project implementing partners, with any other EU agency and service, and with third countries and governments and any of their branches.
The time frame for the request is from January 1, 2021 to May 19, 2026"

After carefully assessing the arguments put forward in your confirmatory application, I regret to inform you that they did not lead me to reverse the position set out in the initial reply. Indeed, as our services explained therein, whereas the EEAS has identified a limited number of documents falling within the scope of your applications, the mere identification of such documents and consequently their public disclosure would undermine the protection of the public interest as regards public security, as per Article 4(1)(a), first indent, of the Regulation.

In this regard, it should be noted that the protection afforded by that exception is not limited to the substantive content of documents as the information concerning the existence of documents held by an institution may in itself reveal information that is sensitive from the perspective of public security. This interpretation has also been confirmed by the case-law, which acknowledged that an institution ''is not required to identify, in the statement of reasons for the contested act, the sensitive content of the documents at issue that cannot be revealed by the disclosure, where such a step would entail revealing information the protection of which is covered by the exception relied on''.[2]

The mere listing of documents, revealing what type of documents exist (e.g. procurement notices, market assessments, contracts, minutes of meetings, briefing notes or internal reports) would directly or indirectly disclose to the general public information on whether or not Cellebrite is a contractor of the EEAS and a provider of services in a specific domain that is security sensitive. In this respect, we confirm the initial assessment that revealing this information to the general public would jeopardize the security of the EEAS headquarters and of EU delegations throughout the world, thus undermining the protection of the public interest as regards public security. Otherwise, the effectiveness of the exceptions protecting a public interest would be materially weakened since the protected information could be disclosed indirectly through the very description or identification of the documents concerned.

Indeed, it is reasonably foreseeable that disclosing the list of documents would undermine the protection of the public interest as regards public security. Cellebrite is a digital forensics company that provides tools and services to collect, review, analyse and manage digital data, aiding with the recovery, investigation, examination, and analysis of material found in digital devices. By confirming, directly or indirectly through listing the identified documents, whether or not the EEAS uses Cellebrite products or services, the EEAS would be exposing itself to adversarial actors sensitive information about the cyber forensic capabilities of the EEAS. Actors hostile to the EEAS specifically and to the European Union and its institutions in general would exploit knowledge of this sensitive information: in fact, such information would allow them to identify and adopt measures to undermine the security systems deployed by the EEAS.

[2] Judgment of the General Court of 7 February 2018, in case T-851/16, Access Info Europe v European Commission, para. 122, and Judgment of the General Court of 7 February 2018, in case T-852/16, Access Info Europe v European Commission, para. 114.

Therefore, the requested disclosure would have the direct effect of enabling such hostile actors to counteract and undermine the relevant capabilities of the EEAS, compromising the ability of the EEAS to act in the domain of digital forensics, which is an essential component of the security of the EEAS. The impact of such exposure is real and wide-ranging insofar as it would concern the security of data-management and of the staff of the EEAS.

Hence, providing any information on the type of documents identified could enable third parties to draw conclusions about the EEAS's interactions or contacts with such economic operators that would prejudice the security interests of the EEAS and consequently the public interest as regards public security.

I agree with your argument that it is good administrative practice for EU institutions to provide in their decision on a request for public access an individual assessment of each document identified as falling within the scope of that request,[3] and this is indeed the standard practice of the EEAS in this area. However, I would also like to draw your attention to relevant jurisprudence in that regard. Whereas the institutions should usually conduct an individual assessment of all documents falling within the scope of a request, the General Court of the Court of Justice of the European Union has repeatedly recognised that there are exceptional cases where a specific examination of each individual document is not required.[4] Notably, "since the purpose of the specific, individual examination which the institution must in principle undertake in response to a request for access made under Regulation No 1049/2001 is to enable the institution in question to assess, on the one hand, the extent to which an exception to the right of access is applicable and, on the other, the possibility of partial access, such an examination may not be necessary where, due to the particular circumstances of the individual case, it is obvious that access must be refused".[5]

Moreover, where even the disclosure of type of documents would undermine the protection of a public interest recognised by Article 4(1)(a) of the Regulation, it follows, *a fortiori*, that access to those documents must be refused.

Although I share your view regarding the importance of transparency for the sake of public interest, the protection of the public interest as regards public security must also be preserved. In particular, the public interest exception as regards public security laid down in Article 4(1)(a), first indent, of the Regulation is subject to a particular regime as compared to the other exceptions included in Article 4.

First, the Institution "must be recognised as enjoying a wide discretion for the purpose of determining whether the disclosure of documents relating to the fields covered by those exceptions relating to the public interest provided for in Article 4(1)(a) of the Regulation could undermine the public interest."[6]

Second, once the Institution has come to the conclusion that release would indeed undermine the public interest in this area, it has no choice but to refuse access, because "it is clear from

[3] See European Ombudsman guide on the right of public access to EU documents, 27 January 2025, section 7.2., available at https://www.ombudsman.europa.eu/en/document/en/163353.
[4] Judgements of 13 April 2005, Verein für Konsumenteninformation v. Commission, T-2/03, paragraph 75; of 14 December 2017, Evropaïki Dynamiki, T-136/15, paragraph 38.
[5] Ibid.
[6] Judgments of 1 February 2007, Sison v Council, C-266/05 P, EU:C:2007:75, paragraph 34; of 12 September 2013, Besselink v Council, T-331/11, EU:T:2013:419, paragraph 32; and of 3 October 2012, Jurašinović v Council, T-63/10, EU:T:2012:516, paragraph 32.

the wording of Article 4(1)(a) of the Regulation that, as regards the exceptions to the right of access provided for by that provision, refusal of access by the institution is mandatory where disclosure of a document to the public would undermine the interests which that provision protects, without the need, in such a case and in contrast to the provisions, in particular, of Article 4(2), to balance the requirements connected to the protection of those interests against those which stem from other interests."[7] The same considerations must apply all the more to cases where the Institution has come to the conclusion that merely listing the documents identified as falling within the scope of an access to documents request would, as such, already undermine the interests protected by Article 4(1)(a) of the Regulation.

Therefore, while the EEAS enjoys a wide discretion in assessing the impact of the release of documents, since the exception in Article 4(1)(a) of the Regulation, protecting a public interest such as *public security,* falls under the category of absolute exceptions, the EEAS is barred from balancing these exceptions against an overriding public interest in disclosure.[8]

For all these reasons, I hereby confirm that the EEAS cannot identify the documents requested, as doing so would disclose the existence or non-existence of a commercial relationship with the entity referred to in your application, which disclosure would in turn undermine the protection of the public interest as regards public security, pursuant to Article 4(1)(a), first indent, of the Regulation.

It also follows, for the same reasons, that the possibility of granting partial access under Article 4(6) of the Regulation does not arise in the present case. That possibility has been duly considered as part of the overall assessment. However, where the harm stems already from the identification of documents, there is no meaningful non-sensitive part that could be disclosed without undermining the protected interests. Partial access would therefore not avoid the negative effect identified above and cannot be granted.

You have a right, in accordance with Article 8 of the Regulation, to institute court proceedings against the European External Action Service and/or make a complaint to the Ombudsman, under the conditions laid down in Articles 263 and 228 of the Treaty on the Functioning of the EU respectively.

Yours sincerely,

[e-signed]

Kristin de Peyron
Director-General

[7] Judgments of 7 February 2018, Access Info Europe v Commission, T-851/16, EU:T:2018:69, paragraph 40, and Access Info Europe v Commission, T-852/16, EU:T:2018:71, paragraph 40 and the case-law cited
[8] See Judgment of 7 February 2018, Access Info Europe v Commission, T-851/16, EU:T:2018:69, paragraph 38 and cited case-law

Electronically signed on 22/09/2026 19:45 (UTC+02) in accordance with Article 11 of Commission Decision (EU) 2021/2121