

Dawn raids: personal data must be protected under Article 8 of the Charter, but this does not mean prior judicial authorisation is always required

Opinion of Advocate General Medina of 23 October 2025 (Joined Cases C-258/23, C-259/23, C-260/23 *Imagens Médicas*)

In October 2024, the CJEU (Grand Chamber) ruled that prior judicial or independent authorisation is required to access personal data contained in mobile phones for the purpose of criminal investigations, save in exceptional circumstances: C-548/21 *Landeck*.

To what extent could this prior authorisation requirement apply to personal data contained in work emails, accessed in the course of a competition dawn raid?

The CJEU sought to answer this question by taking the exceptional step of reopening the oral procedure in an ongoing dawn raid case (*Imagens Médicas*)¹ and convening a Grand Chamber to consider the issue. While the Grand Chamber is yet to rule, the Opinion of Advocate General Medina gives an indication of where the Court may go. The Advocate General reconciles the *Landeck* case-law with the existing competition case-law to find that protecting personal data in competition cases does not always require prior judicial authorisation.

The Advocate General distinguishes *Landeck* on the basis that:

- **dawn raids focus on businesses rather than individuals:** seizures carried out by competition authorities relate to business information concerning legal persons and not individuals, who are in principle only affected in an ancillary manner;
- **access to emails of a business (between employees and managers) is different from access to a personal mobile telephone (which stores a vast quantity of data in one place):** work emails are in principle incapable of identifying, with the same “precision and intensity” as a private phone, the habits of everyday life of the data subjects.

Accordingly, and in line with existing competition case-law on the right to privacy², access to emails of employees and managers by competition authorities will be a proportionate interference with data protection rights, provided: (i) certain procedural safeguards are followed during the inspection, in line with the GDPR; and (ii) judicial review is available during and after the investigation procedure.

This means that, in the Advocate General’s view, EU law (Article 8 of the Charter of Fundamental Rights of the EU) only requires, as such, competition authorities to seek prior judicial authorisation to seize emails:

- at an individual’s private residence;³
- in order to incriminate an individual under criminal law.

The Advocate General notes that Member States may take a stricter approach, by requiring prior authorisation in other cases (see e.g. Article 6(3) of the ECN+ Directive 2019/1).

Data protection: which procedural safeguards must be in place during the inspection?

- The procedural safeguards which competition authorities must apply are in line with the obligations laid down in Article 5 GDPR, but are, according to the Opinion, “additional” to GDPR-type obligations.⁴
- All or many of the safeguards referred to by the Advocate General are already applied by the European Commission and national authorities⁵. The Opinion (paras. 32–36) nevertheless sets them out at length, turning them into a ‘**compliance checklist**’ for competition authorities, on which companies under inspection can rely.
 - **Lawfulness:** The inspection decision must (in the usual way) be duly-reasoned, based on reasonable suspicions of an infringement, and sufficiently precise in material and temporal scope.
 - **Purpose limitation and data minimisation:**
 - The decision itself “*should ensure*” that the collection and access of personal data, even if ancillary to the search for business information, is limited to what is strictly necessary for the purpose of the investigation. The Opinion is silent on how the decision should ensure this; perhaps some language will creep into recitals to inspection decisions.
 - If computer investigation software is used, the indexing procedure must be conducted using keywords “*rigorously determined in relation to the pre-defined subject matter of the investigation.*” In the recent *Red Bull* case, *Red Bull* alleged that the Commission refused to provide it with a list of keywords, which would

have enabled it to ensure that only the relevant elements were copied.⁶ The judgment of the GCEU does not specifically address whether this was problematic. Where does the Opinion of the Advocate General in *Imagens* leave things? The Opinion requires that the data protection officer of the Commission must be able to review compliance with the rules (thus presumably by reference to the keywords used). A more open question is whether representatives of the inspected undertaking might legitimately be able to seek knowledge of (or rule out) certain keywords based on personal data concerns – thus going beyond traditional transparency and access principles under the GDPR.

- Personal data contained in documents added definitively to the file, which data is not itself relevant, must be anonymised.
- **Fairness and transparency:**
 - The competition authority must inform individuals of any processing of their personal data and inform them of their rights (unless to do so would compromise the investigation, in which case this must be recorded in the relevant register⁷).
 - The collection and access to data through the selection of relevant documents must be carried out in the presence of representatives of the business, who must be able to review all provisional documents intended to be included in the investigation file. They must be able to determine what personal data is included and to raise objections to those they consider irrelevant, or which are special or sensitive and should receive increased protection.
- **Storage limitation, integrity and confidentiality:**
 - Personal data collected must be stored in a secure environment, only for as long as strictly required for the administrative procedure and legal proceedings.
 - Access to that data must be restricted to as few people as possible, who are subject to confidentiality obligations and are prohibited from using the data for purposes other than the investigation.
 - Secure deletion of personal data must be provided by means of a general cleansing mechanism that prevents its subsequent recovery.
- **Accountability:** the data protection officer of the investigating authority must be able to examine independently whether the rules have been correctly applied.

What if the procedural safeguards are not respected?

- The Opinion (para. 32) makes plain that the interference with data protection rights will be proportionate only if the type of procedural safeguards described above apply.
- The Advocate General observes that **a failure to comply with procedural safeguards** may affect the information gathered during the investigation and **invalidate the procedure in whole or in part**. Interestingly, the Advocate General considers that the risk of this happening will give authorities “sufficient incentive” to comply with the rules (thus ensuring that their actions are proportionate). The Opinion effectively uses this ‘incentive’ (together with the obligation for authorities to provide relief for any “irregular operation”⁸) as a reason why prior authorisation is not necessary and ex post judicial review may be sufficient.
- In a typical dawn raid conducted by the **European Commission**, it is hard to think of a scenario in which personal data rights would be breached to the extent that the procedure would be invalidated in whole or in part. It seems more likely that particular items of evidence might need to be excluded from the file as irrelevant, or that redress should be made for otherwise relevant items which were not granted sufficient protection.
- In **national cases**, competition authorities conducting ‘bulk seizures’ may wish to revisit their procedures, and to ensure that business representatives are involved at a sufficiently early stage of data seizure. If personal data is not sufficiently protected, redress will be a matter of national law, subject to compliance with the GDPR and relevant EU law, such as the principle of effectiveness.⁹

Practical significance – and where might the CJEU go?

- It seems likely that the CJEU will take the same approach as the Advocate General. This means that, if they wish to avoid an EU law requirement to seek prior judicial authorisation, competition authorities must have adequate procedural safeguards in place to protect personal data. Such safeguards must logically apply in similar unannounced inspections, such as under the Foreign Subsidies Regulation (EU) 2022/2560.
- The *Imagens* cases concern business emails. More thorny issues were not considered, such as protocols for accessing personal mobile phones used for work purposes, or work mobile phones containing a mixture of business and personal data.

- Subject to proper safeguards being in place, the Advocate General is sympathetic to the need of competition authorities to seize emails in order to identify anticompetitive practices in the internal market: “no equally effective means which is less restrictive of the right to the protection of personal data appears to me to be available as an alternative” (Opinion, para. 21). This view aligns with the approach taken generally by the EU Courts, especially of late:¹⁰ dawn raids may be necessary to detect unlawful activity, and less restrictive measures such as RFIs will not be sufficiently effective.

Key Contacts



[Claire Simpson, Partner](#)

csimpson@vbb.com

+32 (0)473 28 32 90

1-The Portuguese competition authority conducted three dawn raids in relation to suspected unlawful information exchange, concerted practices and abuse of dominance. Cases C-258/23, C-259/23 and C-260/23 respectively concern healthcare/teleradiology, the negotiation of pricing for Covid-19 test kits, and terms of access to the Multibanco network. Work emails were seized during the inspections, upon the prior authorisation of the public prosecutor’s office. The seizure was challenged before the national courts, which referred to the CJEU the question of whether Article 7 of the Charter of Fundamental Rights of the EU (respect for private life and communications) applied to such work emails and, if so, whether authorisation of the public prosecutor (rather than a court) was sufficient. In her first Opinion of 20 June 2024, Advocate General Medina concludes that Article 7 applies and that the authorisation given was sufficient.

2-See the cases cited at paragraphs 42-44 of the first Opinion of Advocate General Medina in the cases (20 June 2024, EU:C:2024:537), in particular *Les Mousquetaires*, C-682/20 P, EU:C:2023:170, para. 57.

3-As already reflected in Article 7(2) of the ECN+ Directive 2019/1 and Article 21 of Regulation 1/2003.

4-The Advocate General also draws on safeguards (such as confidentiality and purpose limitations) considered by the CJEU (Full Court) in *La Quadrature du Net*, C-470/21, EU:C:2024:370, paras. 113-114, when assessing the degree of seriousness of the interference with privacy rights in the context of copyright infringement.

5-As the Advocate General notes, the European Commission is subject to ‘GDPR equivalent’ rules: see Commission Decision (EU) 2018/1927 and the Commission’s Privacy Statement (available online).

6-Judgment of the GCEU of 15 October 2025 in *Red Bull GmbH v Commission*, T-306/23, EU:T:2025:959, para. 115.

7- In the case of the European Commission, under Article 3(2) of Decision 2018/1927.

8- *Intermarché Casino Achats*, C-693/20 P, EU :C :2023 :172, paras. 45-46.

9-See *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paras. 43-44, referred to at para. 44 of the Opinion.

10-See e.g. judgment of the GCEU of 15 October 2025 in *Red Bull GmbH v Commission*, T-306/23, EU:T:2025:959, paras. 121-126