# ECJ: No Use of Data Retained for Criminal Proceedings in Administrative Proceedings for Corruption

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

**Thomas Wahl**

The ECJ ruled on 7 September 2023, in Case C-162/22, that retained data provided to authorities for the purpose of combating serious crime cannot be used in the context of investigations for a disciplinary offense related to corruption.

**AUTHOR**

**Thomas Wahl**

Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2023, Vol. 18(2) eucrim pp 149 – 150

ISSN: 1862-6947

https://eucrim.eu

## Facts of the case and question referred

The case at issue raised the question as to whether data retained and provided by telecommunication service providers to law enforcement authorities in the context of combating serious crimes can be used in other (disciplinary) proceedings involving the misconduct of office related to acts of corruption. This is foreseen under the Lithuanian law. Concretely, a Lithuanian prosecutor is alleged to have unlawfully provided relevant information to the suspect and his lawyer in the course of investigations conducted by him. Internal investigations by the Prosecutor General's Office of the Republic of Lithuania found misconduct on the part of the prosecutor, dismissed him from his position and removed him from office. The Prosecutor General hereby relied on the information obtained from the court-ordered interception and recording of traffic and location data transmitted via electronic communications networks at the suspect's lawyer and the prosecutor subject to the proceedings of misconduct of office (main proceedings).

The referring Supreme Administrative Court of Lithuania (*Lietuvos vyriausiasis administracinis teismas*) observed that, according to the ECJ's case law on data retention, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with Arts. 7 and 8 CFR in connection with Art. 15(1) of Directive 2002/58. However, the Court has not yet ruled on the impact of the subsequent use of the data concerned on the interference with fundamental rights. The referring court sought guidance as to which extent the data retained and provided for the purpose of combating serious crime can be used in the investigations related to the misconduct in office.

## The ECJ's ruling

The ECJ reiterated its case law as to legislative measures that allow exceptions from the obligation to ensure confidentiality of personal data in accordance with Art. 15(1) of Directive 2002/58 (cf. Joined Cases C-793/19 and C-794/19, *SpaceNet and Telekom Deutschland* → eucrim 3/2022, 188-189). It also clarified that the principles developed in previous cases on data retention (cf. Case C-140/20, *G.D. v The Commissioner of*

*An Garda Síochána* → eucrim 2/2022, 115) also apply *mutatis mutandis* to the subsequent use of traffic and location data retained by providers of electronic communications services, in detail:

- A legislative measure must correspond, genuinely and strictly, to one of the objectives exhaustively listed in Art. 15(1) of Directive 2002/58;
- There is a hierarchy amongst those objectives according to their respective importance and the importance of the objective pursued by a legislative measure must be proportionate to the seriousness of the interference that it entails;
- As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights;
- Access to traffic and location data may, in principle, be justified only by the public interest objective for which those providers were ordered to retain those data.

As a consequence, the ECJ concluded: "…data [that have been once retained and made available to the competent authorities for the purpose of combating serious crime] cannot be transmitted to other authorities and used in order to achieve objectives, such as, in the present case, combating corruption-related misconduct in office, which are of lesser importance in the hierarchy of objectives of public interest than the objective of combating serious crime and preventing serious threats to public security. To authorise, in that situation, access to retained data and the use thereof would be contrary to that hierarchy of public interest objectives."

### Put in focus

The ECJ's ruling in Case C-162/22 shows that there are still open questions as to the limits and conditions for national legislation allowing the retention of telecommunication data and its use for law enforcement purposes within the framework defined by the ECJ, notably in *Quadrature du Net and Others* (Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* → eucrim 3/2020, 184-186). The ECJ (again) emphasises that the storage of traffic and location data involves serious interference with the fundamental rights to respect for private and family life and to the protection of personal data. The clarification of the question on the subsequent use of retained data in the Lithuanian case nonetheless triggers further questions: How is "combating serious crime" defined? How is the criterion of the "hierarchy of objectives" applied in other cases? How about the use of retained data that were at first used to maintain public security and subsequently forwarded to combat a serious crime (and vice versa)?

## About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union