

How to exercise data subject rights under the Law Enforcement Directive (EU) 2016/680?

Summary by Alessandra Calvi (VUB/LSTS) and Juraj Sajfert (VUB/University of Luxembourg)

On 5 March 2021, the Brussels Privacy Hub, in cooperation with the [University of Luxembourg](#) within the framework of the FWO/FNR-funded research project MATIS, and in media partnership with [Privacy Laws & Business](#) organised the third webinar within the series [Enforcing Europe - Webinar Series 1](#).

The webinar, entitled **How to exercise data subject rights under the Law Enforcement Directive (EU) 2016/680?** focused on one of the most revolutionary novelties of the [Law Enforcement Directive \(EU\) 2016/680 \(LED\)](#) compared to the previous regime under the Council 2008 Framework Decision, namely **the rights of the data subject**.

Juraj Sajfert (VUB/University of Luxembourg) and **Laura Drechsler** (VUB/FWO) moderated the discussion. Invited speakers were **Plixavra Vogiatzoglou** (KU Leuven - CiTiP), **Stefano Fantin** (KU Leuven - CiTiP) and **Clara Guerra** (Portuguese Data Protection Authority)

Laura Drechsler pinpointed (some of) the main characteristics -and issues- under the LED. The delays and inconsistencies in its transposition. The scope of application depending on two concepts influenced by national law, namely the notion of 'competent authority' (encompassing both 'traditional' law enforcement authorities (LEA) and other entities fulfilling law enforcement tasks) and the 'law enforcement purposes'. The lack of a formalised cooperation mechanism among Data Protection Authorities (DPAs). The applicability of the LED to both domestic and cross-border processing. The existence of data subjects rights, exercisable directly and indirectly via a DPA, whose restrictions are quite specifically regulated.

Questioned on the current situations of data subjects' rights under the LED, **Plixavra Vogiatzoglou** and **Stefano Fantin** presented the main findings of a [study](#) they conducted with their colleagues of the KU Leuven. By combining desk research with empirical-legal methods, the study investigated the transposition of the LED and the Passenger Name Records (PNR) directive in 11 Member States, as well as the transparency measures and the practices for exercising the right to access under the two legal frameworks. They noted slight differences in the wording and the formulation of the right of access and its limitation; that only two countries establish specific time limits to address the data subjects' requests; that a country (Belgium) foresees only indirect access. When examining the websites of LEAs and their privacy notices, they realised that it may be difficult for a layperson to decipher the formal requirements necessary for the exercise of the right of access in certain countries. Not all countries for instance provide templates for data access requests or interactive forms. Albeit most of them accept electronic requests, others rely exclusively on traditional mail. Certain authorities request proofs of residence (e.g. utility bills). Responses received range from refusing of sharing any information to sharing only some. The time to respond was highly variable. In a case, the request was deemed manifestly abusive without giving the possibility to adjust its scope.

Clara Guerra observed that data subjects' rights under the LED represent a novelty for DPAs, LEA and data subjects themselves. For a long time, in the area of law enforcement, there was very few legal instruments providing for this possibility. So, data subjects' rights remained inconceivable due to the (mis)conception that disclosing any sort of information could jeopardise a criminal investigation. By introducing data subjects rights, the LED has fostered a change in this culture. She called for the EU Commission to actively monitor the LED transpositions and take corrective actions in case of inconsistencies in the national laws. She urged DPAs to provide guidance and proactively control that the law is well applied, without waiting for individual complaints, acknowledging that individuals may

refrain from filing them. She emphasised the role of DPOs in public authorities to implement and consolidate a data protection culture. In Portugal, for example, each LEA has a DPO, but it is a new figure introduced by the GDPR and the LED. She stressed that the LED is not a standalone instrument and data stored in law enforcement databases often come from third countries, international organisations and the other Member States. To ensure the exercise of data subjects rights, coordination with other *ad hoc* systems of exchange of information (e.g. EU large-scale databases, Prüm) that qualify as *lex specialis* is required.

On the possibility to consider private entities with inquisitory powers (e.g. banks for anti-money laundering activities) as competent authorities under the LED, and how to qualify administrative sanctions, the speakers expressed different opinions. Plixavra Vogiatzoglou noted how the scope of the LED may vary depending on the interpretation of 'competent authority' and 'law enforcement' given at the national level. Juraj Sajfert argued that finding entities that comply with the threshold requested in Recital 11 (being entrusted by Member State law to, cumulatively, exercise public authority and public powers) would be difficult. Banks for example would not satisfy the conditions, whereas privatised prison services would. He admitted that at the national level there are differences in the qualification of criminal offenses. Clara Guerra noted how administrative sanctions (as the one issued by DPAs) may be punitive, but the LED expressly refers to criminal offences, adding that banks may be obliged to communicate data for law enforcement purposes, but they transmit data under the GDPR and not under the LED.

On the evolution of data subjects rights under the LED, Stefano Fantin urged public institutions to lead by example and to facilitate the exercise of data subjects' rights, by for example making the information as to how exercising the right to access more easily retrievable. He was concerned that allowing LEAs to introduce additional procedural requirements (e.g. proof of residence) could determine a chilling effect, discouraging the exercise of rights. Plixavra Vogiatzoglou added that from the perspective of a data subject the creation of a unique information or contact point would be useful. To be effective, the right to access should lead to meaningful information, and not just to a list of data categories processed. They called for the development of best practices on a European scale, for example by the EDPB and the EU Commission who should pay particular attention to data subject' rights when the report on the LED implementation will be issued.

Clara Guerra expressed concerns that at the DPA level most resources are allocated for GDPR issues. She noted that since LEAs are bound by the accountability principle, DPOs and DPAs must monitor their practice and make sure that any restrictions to the rights of the data subject, in particular the right of access under Article 14 are duly justified and meet the legal requirements. She emphasised that when data subjects exercise their rights, data controllers shall communicate any changes to sources and recipients of information as in law enforcement context data quality is essential. She concluded by stating lawyers acquainted with data protection law could better protect their clients as breaches of data protection law could make a criminal procedure fall on procedural grounds.