PERSONAL DATA PROTECTION BY LAW ENFORCEMENT AUTHORITIES IN THE EUROPEAN UNION

When does the EU Law Enforcement Directive apply?

The Law Enforcement Directive (LED), also known as the EU Police Directive, is not only applied by the police, nor is it applied by the police in all circumstances.

General Preconditions

- The processing of personal data is conducted, wholly or partly, by automated means, or by non-automated means for personal data which form part of a filing system or are intended to form part of a filing system.

The Directive does not apply to manual processing of data that are not structured, regardless of the fact that they may be physically located in one place.

- Processing falls under the scope of European Union law.

The operations of security and intelligence services and the military remain beyond the scope of the Directive.

- The directive is applied in the EU member states and the members of the Schengen Area (Iceland, Lichtenstein, Norway and Switzerland).

The Directive does not apply to EU institutions and agencies, which are covered by separate regulation.

Special Conditions

The Law Enforcement Directive is applied only by competent authorities and for the following purposes:

- Prevention of criminal offences, including threats to public security;
- Investigation and detection of criminal offences;
- Prosecution of the perpetrators of criminal offences;
- Execution of criminal penalties.

A competent authority is:

a. A public authority responsible for the purposes listed (EXAMPLE: the police, prosecutors, courts, prisons),

b. A legal entity entrusted by member state law to exercise public authority and public powers for the purposes listed (EXAMPLE: private prisons).

Personal Data – any data relating to a natural person who is identified or identifiable, directly or indirectly.

Data Processing – any operation performed in order to, amongst other things, collect, record, organise, structure, store, adapt, alter, detect, transmit, use, copy, disseminate, compare, erase or destroy personal data.

Filing System – any centralised or decentralised set of personal data that is structured so that it can be accessed, searched and organised according to certain criteria.

The directive does not apply to:

- Private investigators and private security companies;
- Telecommunications operators obliged to retain and pass electronic data to competent authorities;
- Banks, insurance companies and exchange offices obliged to inform competent authorities of suspicious transactions;
- Circumstances in which competent authorities process data for other purposes (e.g. HR or financial management);
- Collection of fines by public companies such as transport or parking authorities.

*Instead of the Police Directive, the EU General Data Protection Regulation (GDPR) applies.

Belgrade Centre for Security Policy

BCSP