KOVÁCS RÉTI SZEGHEŐ
ÜGYVÉDI IRODA

Cameras, Compliance, and the Risk of Immediate Notification – What the Court's Ruling Signals to Companies About Body-Worn Cameras

The recent judgment of the Court of Justice of the European Union (CJEU), delivered on 18 December 2025, addresses a seemingly narrow data protection issue affecting transport companies. In reality, it carries a much broader message for any business using surveillance technologies—particularly camera systems—in their operations. The ruling makes clear that the practical interpretation of GDPR information obligations is far stricter than many data controllers have previously assumed, and that "technological neutrality" does not eliminate compliance risks.

At the heart of the case was a Stockholm-based transport company that equipped its ticket inspectors with body-worn cameras to record events during inspections. The national data protection authority imposed a fine, arguing that passengers were not provided with adequate and timely information about the processing of their personal data. The company contended that, because the data recorded by the cameras did not come directly from the data subjects, Article 14 of the GDPR—applying less stringent requirements—rather than Article 13, should apply.

The Court firmly rejected this argument, holding that images captured by body-worn cameras typically constitute direct data collection. It is not necessary for the data subject to actively provide data or consciously participate in the processing. It is sufficient that the controller obtains personal data by observing the individual. This interpretation can effectively extend to any business context where a company "detects" individuals through cameras, sensors, or similar technologies.

One of the most important practical implications of the ruling is that information must be provided immediately in such cases. The Court also accepts a so-called layered information model, which is particularly relevant for organizations operating in high-traffic, dynamic environments. Under this model, the most essential information—such as the fact of data processing, its purpose, and the identity of the controller—can be displayed on a clear, visible notice, while detailed privacy information may be provided through easily accessible channels, such as a QR code, website, or physical leaflet.

From a business perspective, the ruling goes far beyond public transport. It affects security services, retail, logistics, event management, and even workplace environments where body-worn, mobile, or wearable cameras are increasingly deployed. The Court's message is clear: the use of such devices is not merely a technical or operational matter but a central element of data protection governance, with shortcomings creating direct financial and reputational risks.

The decision also signals that authorities and courts are likely to be less lenient in the future with solutions that attempt to "tick the box" on information obligations using purely formal, retrospective, or hard-to-access documentation. Compliance here is not about document production—it is about genuinely considering the rights of data subjects.

Overall, the ruling delivers a clear strategic message to corporate executives and legal advisors. When deploying surveillance technologies, the key question is not whether data protection obligations arise, but whether the controller can integrate them into business processes in an immediate and comprehensible manner. Underestimating this requirement risks not only a GDPR fine but also the loss of consumer trust.