OCTOBER 2025 Gökçe ISSUE: 143

THE FINE PRINT

Answers. Not theories.

VERBİS EXEMPTION FOR DATA CONTROLLERS PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

- €1.5 Million Fine Imposed on IKEA for Privacy Violations Arising from Video Surveillance
- Update to the ISO/IEC 27701 Standard: A New Framework for Privacy Management

VERBİS Exemption for Data Controllers Processing Special Categories of Personal Data

By its Decision dated 4 September 2025 and numbered 2025/1572, the Personal Data Protection Board **(Board)** introduced a new exemption criterion regarding the obligation of data controllers whose main field of activity involves the processing of special categories of personal data to register with the Data Controllers' Registry Information System **(VERBİS)**.

As is known, VERBİS is an electronic registry in which data controllers processing personal data are required to register. Accordingly, data controllers who do not fall within the scope of the exemption criteria announced by the Board remain subject to the registration obligation.

Until now, certain exemption criteria had been established based on the number of employees and annual financial balance sheet totals. However, even if such thresholds were met, data controllers whose main field of activity involved the processing of special categories of personal data were required to register with VERBİS under all circumstances.

With the new decision, data controllers whose principal activity consists of processing special categories of personal data will no longer be required to register with VERBİS if they employ fewer than 10 employees and have an annual financial balance sheet total below TRY 10 million. In other words, the Board has now introduced specific exemption criteria applicable even to data controllers whose primary activity involves the processing of sensitive personal data.

The Board's decision was published in the Official Gazette dated 1 October 2025 and entered into force on the same date. The full text of the decision and the Board's public announcement on the matter can be accessed here and here. *(Available in Turkish only)*

€1.5 Million Fine Imposed on IKEA for Privacy Violations Arising from Video Surveillance

The €1.5 million administrative fine imposed on IKEA for recording customers' PIN entries during card payments through its security cameras has been upheld by the Austrian Federal Administrative Court **(BVwG)**.

The Austrian Data Protection Authority **(DSB)** determined that between March and May 2022, the company operated nine cameras covering both indoor and outdoor areas and that this video surveillance was disproportionate and unlawful. The investigation revealed that the cameras' recording zones included checkout areas where customers entered their payment PINs, resulting in approximately 637 PIN entries being captured.

The DSB found that the surveillance system exceeded its legitimate purpose, violated the principle of data minimization, and was contrary to Articles 5(1)(a), 5(1)(c), and 6(1) of the GDPR. Accordingly, it imposed an administrative fine of €1.5 million and an additional €150,000 in procedural costs.

IKEA appealed the decision, arguing that most of the footage did not contain identifiable personal data, that many customers used payment methods not requiring PIN entry or concealed the keypad while entering their codes, and that the cameras had been installed solely for security purposes. The company also contended that calculating the fine based on the group's overall turnover was disproportionate, and requested that the decision be annulled or, alternatively, reduced to a warning.

The Federal Administrative Court found that the cameras had been activated without ensuring GDPR compliance, that privacy masking had not been properly implemented, and that known deficiencies had not been remedied for an extended period. Considering the duration and scope of the infringement, as well as the company's significant turnover, the Court held that the €1.5 million fine was reasonable and proportionate. It noted that the penalty corresponded to only 0.21% of the company's annual turnover, well below the 4% maximum permitted under Article 83(5) of the GDPR.

Through this judgment, the European judiciary once again underscored that security-based surveillance cannot override the principles of personal data protection and that the tests of necessity and proportionality must always be applied.

In Turkey, the Personal Data Protection Board conducts similar assessments concerning the scope of security camera monitoring and the limitation of surveillance areas. Such decisions serve as a reminder that even when data controllers rely on a "security purpose," they must still adhere to the principles of proportionality, data minimization, and transparency under data protection law.

Update to the ISO/IEC 27701 Standard: A New Framework for Privacy Management

The International Organization for Standardization **(ISO)** and the International Electrotechnical Commission **(IEC)** have updated ISO/

IEC 27701, one of the key international references in the field of privacy management. The first edition, published in 2019, enabled organizations to manage their personal data protection obligations within a systematic framework. The second edition, published in 2025, introduces significant structural changes in line with rising regulatory expectations and corporate compliance requirements.

The Standard Can Now Be Applied Independently

In its previous version, ISO/IEC 27701 was considered an "extension" of the ISO/IEC 27001 Information Security Management System. As such, implementing privacy management processes required the prior establishment of an information security management system. With the new edition, this dependency has been removed, and ISO/IEC 27701 can now be implemented as an independent privacy management system standard.

This change has been positively received, particularly by small and medium-sized enterprises, as it increases accessibility. Organizations that do not hold an ISO/IEC 27001 certification can now adopt an internationally recognized structure for personal data protection. That said, integrated implementation of information security and privacy management systems remains the best practice.

The new edition also expands the control sets separately defined for data controllers and data processors. It updates controls relating to the purposes of processing, the allocation of responsibilities between parties, data retention policies, and cross-border data transfers. The revised standard aims to enhance alignment with international instruments, notably the EU General Data Protection Regulation **(GDPR)**. Furthermore, it clarifies the principles of risk-based management of personal data throughout its lifecycle. The new version is also designed to achieve stronger coordination with ISO/IEC 27001:2022 and ISO/IEC 29100 **(Privacy Framework)**.

Other Key Points

The 2025 edition places greater emphasis on the management system approach. Organizations will need to address privacy management not only on a technical level but also at managerial and strategic levels. Accordingly, the requirements under the headings "Context Determination," "Leadership," "Planning," "Support," "Performance Evaluation," and "Continuous Improvement" have been restructured. This approach requires aligning privacy protection policies with the organization's overall objectives and clearly documenting top management's commitment. It also mandates regular measurement and reporting of privacy performance indicators, such as the number of incidents, complaint resolution times, and awareness levels.

Compliance and Transition for Organizations

Organizations that have already established systems in accordance with ISO/IEC 27701:2019 will need to review their existing processes to meet the new requirements. A gap analysis should be conducted, and existing controls and policies should be adjusted to comply with the 2025 edition.

Certification bodies are expected to announce their transition schedules in the near future. Accordingly, organizations planning audits in 2025 or early 2026 should begin preparing for compliance with the new edition without delay.

Editors

Görkem Gökçe
gorkem.gokce@gokce.av.tr

Tuğçe Beyazkılınç
tugce.beyazkilinc@gokce.av.tr

Yağmur Yollu
yagmur.yollu@gokce.av.tr

About us

Gokce Attorney Partnership is an Istanbul-based law firm offering legal services across a broad range of practice areas including mergers and acquisitions, joint ventures, private equity and venture capital transactions, banking and finance, capital markets, insurance, technology, media, telecoms and internet, e-commerce, data protection, intellectual property, regulatory, debt recovery, real property, and commercial litigation. Please visit our web site at www.gokce.av.tr for further information on our legal staff and expertise.

Please contact us at
info@gokce.av.tr
0 212 352 88 33