APRIL 2019

LAW UPDATES

kavlak

07

ISSUE

Some Crucial Points on the Elevator Operation and Maintenance Regulation

The Elevator Operation and Maintenance Regulation (“Regulation”), issued by the Ministry of Industry and Technology, was published in the Official Gazette dated 06.04.2019 and numbered 30737. The aim of this regulation is to determine the rules that must be complied with regarding the registration, operation, maintenance, guarantee and after-sales services, service inspection and improvement of the existing elevators in order to ensure the use of elevators in a way that does not threaten the safety of human life and property and to protect the environment. A few of the issues that attract attention are as follows:

According to the Regulation,

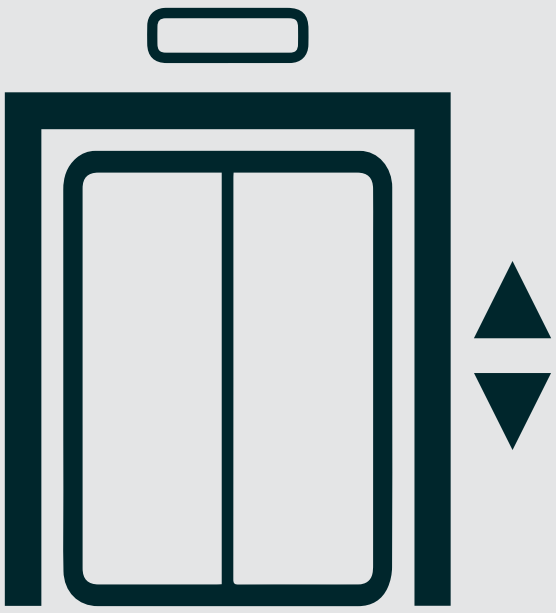
• The elevator, which has not been checked for the first period by the elevator contractor according to the Elevator Periodic Control Regulation before the registration stage and whose green label is not attached, shall not be registered by the relevant administration.

• Maintenance cannot be provided to elevators which have red sticker as a result of periodic control showing that it is unsafe, until it became defective, slightly defective or perfected.

• Managers in the buildings with elevator are obliged to maintain the elevator and pay the maintenance fee. Again, the building manager ensures that the elevator is safely operated continuously for the accessibility of the disabled and is obliged to take the safety precautions by preventing the use of the elevator when it detects problems.

• The professional service insurer undertakes at least 500.000 TL of professional liability insurance to cover the claims and damages to be claimed by the building supervisor and other third parties due to professional errors and / or omissions related to maintenance, repair and service provided by the authorized service itself to the elevator.

• The elevator installers are obliged to provide spare parts and parts for each type and property of the market for at least three years.



The Decision of Constitutional Court Dated 27.02.2019

The General Assembly of the Constitutional Court drew attention to the important points in the context of the right to protection of personal data with decision dated 27.02.2019. The applicant had been successful in the examination for the guardian staff recruiting. Following the examination, the security investigation had been started about the applicant and as a result of the investigation, some criminal records were obtained regarding the applicant committed theft when he was under the age of 18. As a result of the data on the person's criminal record, it was concluded that the applicant did not meet the conditions required for the civil servants and that it would not be appropriate to employ him for that position.

The Court stated that the records relating to the criminal conviction of the person were regulated as sensitive personal data in accordance with Article 6 of the Law on the Protection of Personal Data No. 6698 and these data could only be processed in case prescription by law. In examining the relevant legislative arrangements, the Court has decided that there is no requirement of a statutory basis for the processing of such private data and it has been accepted the existence of an interference to the protected right which is protected under Article 20 of the Constitution.

Amendment On Children's Online Privacy And Protection Act

The Children's Online Privacy and Protection Act (“COPPA”) is one of the United States’ older consumer-facing privacy laws which has passed in 1998. COPPA deals with websites, apps, and other online operators that are collecting data and personal information from kids under the age of 13. Unless an exception applies, an operator subject to COPPA must obtain verifiable parental consent before collecting any personal information from a child. COPPA had been revised in 2012 however due to the development of online tracking and data collection during this period, the act needs to be amended again in order to extend its privacy protections. It’s already prohibited to collect personal data under the age of 13 without explicit parental consent but the new bill amends and adds that, collecting data from children aged between 13 to 15 would only be possible with their own consent. Also if approved, it would create an “eraser button” which is enabling parents to delete online info about their kids. It would also ban targeted advertising to children and ensures that companies and manufacturers will disclose on the packaging for parents detailing how their child’s data would be collected, retained, shared, and protected. Correlatively, devices which do not meet robust cybersecurity standards will be banned from the stores.

Information Technologies and Communication Board's "e-Sim" Decision

The Information Technologies and Communication Board's decision regarding the remotely programmable SIM technologies dated February 12, 2019 and numbered 2019/DK-TED/53 has been published on its website. The Board has determined certain requirements regarding the using of eSIM technologies in Turkey and international roaming.

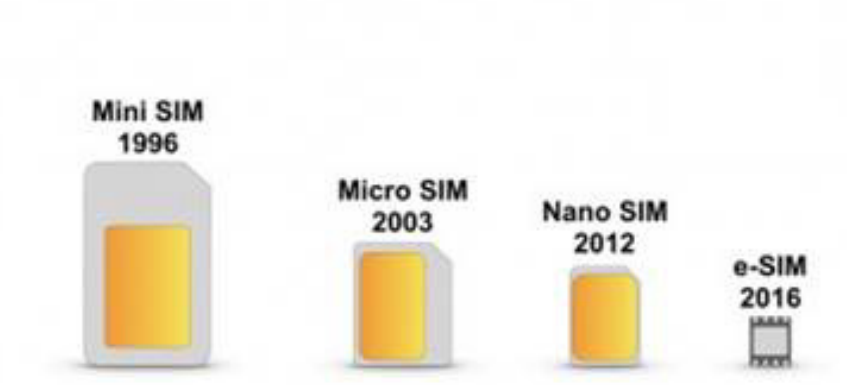
Regarding the remotely programmable SIM Technologies, it is aimed to provide effective competition in information and communication technologies, to minimize potential problems in the process of subscriber exchange, to protect consumer rights and personal data, and to ensure cyber security at the maximum level.

Pursuant to the Decision, if eSIM technologies are used in Turkey, the modules must be programmable in a way that allows Turkish mobile operators to have sole control and only mobile operator profiles in Turkey must be loaded on to the modules. In addition, the SIM profiles of foreign companies are allowed to be loaded outside the customs frontier only when they are abroad.

The Board also requires all structure, system and storage units of eSIM technologies, including the eSIM subscription management, to be established in Turkey by the authorized operators or third parties designated by the authorized operators, on the condition that all liability belongs to the operator. Operators must obtain the "domestic good certificate" until 20.02.2020 for the system components that they will use.

Unless the ITCA determines otherwise, obligation to comply with the relevant legislation regarding the services provided through physical SIMs will also be applicable for the services provided through eSIM technologies.

Finally, the Board has limited the data services offered by mobile operators in Turkey through international roaming to devices manufactured or brought together with passengers or released into the market through import in order to be used in Turkey to 120 days.



Toyota Had Been Victim Through A Cyberattack Caused Data Violation

Today criminals no longer need technical capacity to conduct cyber-crimes as a consequence of the help of opportunities provided by the internet. With the rapid development of the technology, cyber-attack crime continues to increase and the risk of cyber-attack crime is rising rapidly in parallel with the need for information technology. Toyota, one of the major automotive manufacturer, was the last victim of this crime. As a result of the attack on the company's Japan branch, the information of 3.1 million Toyota customers was stolen. This is the second cyber-attack on Toyota in the last five months. The first attack was carried out at Toyota Australia and the second attack was thought to be facilitated by the information captured in this attack. Toyota has launched an investigation into these large data violations and has not yet taken a step to overcome the grievances of its customers. So, what is the data fraud through cyber-attack offense? A data violation occurs when the cybercrime infiltrates the data source and exports sensitive information. This can be achieved by physically accessing a computer or corporate network or by disabling remote access to the corporate network security. The second method is often used in attacks targeting companies. Personal information accessed in this way is leaked and the person or company experiencing data violation.

About Our Firm

Kavlak Law Firm, growing since 2006 with its qualified and dynamic lawyers, is one of the leading law firms of Turkey. With our effective works provided for our client portfolio which includes, by majority, local, international and multinational commercial and financial organizations, we provide distinguished legal support. Kavlak Law Firm, with the lawyers it co-operates in all of the major cities of Turkey, and worldwide, is able to respond immediately to clients' demands, provides a time-efficient service, based on mutual trust, works on long-term cases with each client, and adapts the clients' working principles and provides service accordingly.

Please visit our web site at www.kavlak.com.tr for further information on our legal team and practice areas.

Please contact us at info@kavlak.av.tr, 0212 324 55 00

This document is for informational purposes only and not for the purpose of providing legal advice. You should contact authorized persons for legal consultancy to obtain advice with respect to any particular issue or problem. Use of and access to this document or any of the e-mail links contained within the document do not create an attorney-client relationship between Kavlak Law Firm and the user or browser.

kavlak

LAW FIRM

AVUKATLIK BÜROSU