Dr. Mehmet Bedii KAYA

TURKISH CYBER SECURITY LAW NO. 7545

FULL TRANSLATION

www.mbkaya.com

CYBER SECURITY LAW

THE TURKISH CYBER SECURITY LAW

Law No. 7545 of 12.03.2025

FULL TRANSLATION

TURKISH CYBER SECURITY LAW

TURKISH CYBER SECURITY LAW

UNOFFICIAL TRANSLATION

DISCLAIMER: *This document is an unofficial translation of the full text of Turkish Cyber Security Law No: 7545. The text in this document is not the official translation and is provided for information purposes only.*

ARTICLE INDEX

Chapter One - Initial Provisions

- Article 1 - Objective
- Article 2 - Scope
- Article 3 - Definitions and abbreviations
- Article 4 - Basic Principles

Chapter Two - Duties, Powers, Responsibilities, Audit and Cyber Security Board

- Article 5 - Duties of the Presidency
- Article 6 - Powers
- Article 7 - Responsibilities and Collaboration
- Article 8 - Audit
- Article 9 - Cyber Security Board

Chapter Three - Provisions Regarding Personnel

- Article 10 - Employment of Contracted Expert Personnel
- Article 11 - Transfer of Compulsory Service Obligations
- Article 12 - Prohibited Actions
- Article 13 - Confidentiality Obligation

Chapter Four - Income and Exemptions

- Article 14 - Revenues of the Presidency
- Article 15 - Exemptions

Chapter Five - Criminal Provisions and Implementation of Administrative Fines

- Article 16 - Criminal Provisions and Administrative Fines
- Article 17 - Application of Administrative fines

Chapter Six - Miscellaneous and Final Provisions

- Article 18 - Cyber Security Products and Companies
- Article 19 - Amended and Repealed Provisions
- Provisional Article 1 - Compliance, Transitional Arrangements and Establishment Procedures
- Article 20 - Enforcement
- Article 21 - Execution

CYBER SECURITY LAW

Law No: 7545

Acceptance Date: 12.03.2025

Official Gazette: 19.03.2025/32846

CHAPTER ONE

Initial Provisions

Objective

ARTICLE 1

(1) The purpose of this Law is to identify and eliminate the existing and potential threats directed internally and externally against all elements that constitute the national power of the Republic of Türkiye in cyberspace, to determine the principles to reduce the possible effects of cyber incidents, to make the necessary arrangements for the protection of public institutions and organizations, professional organizations in the nature of public institutions, real and legal persons and organizations without legal personality against cyber attacks, to determine strategies and policies to strengthen the cyber security of the country and to regulate the principles regarding the establishment of the Cyber Security Board.

Scope

ARTICLE 2

(1) This Law covers public institutions and organizations, professional organizations in the nature of public institutions, real and legal persons and organizations without legal personality that exist, operate and provide services in cyberspace.

(2) Intelligence activities conducted pursuant to the Police Duties and Powers Law No. 2559 dated 4/7/1934, the Coast Guard Command Law No. 2692 dated 9/7/1982, the Gendarmerie Organization, Duties and Authorities Law No. 2803 dated 10/3/1983, and the activities carried out in accordance with the Law on the

State Intelligence Services and National Intelligence Organization Law No. 2937 dated 1/11/1983 and the Turkish Armed Forces Internal Service Law No. 211 dated 4/1/1961 are excluded from the scope of this Law.

Definitions and abbreviations

ARTICLE 3

(1) The terms used in this Law shall mean the following:

a) Hosting: The storage of information systems in an external data center,

b) President: The President of Cyber Security,

c) Presidency: Cyber Security Presidency,

ç) Information systems: The hardware, software, systems and all other active or passive components used in the provision of all kinds of services, transactions and data provided through information and communication technologies,

d) Critical infrastructure: Infrastructures that host information systems that could cause loss of life, large-scale economic damage, security vulnerabilities or disruption of public order if the confidentiality, integrity or accessibility of the information/data they process is compromised,

e) Critical public service: A service which is essential for the maintenance of national, social or economic activity and which, if disrupted or impaired, could have a significant impact on national security, the social or economic well-being of the country, public order or health, or the provision of other services, and which is provided by nationwide monopoly or limited substitution,

f) Cyber security: The whole set of activities that includes protecting the information systems that make up cyberspace from attacks, ensuring the confidentiality, integrity and accessibility of the data processed in this environment, detecting attacks and cyber incidents, activating reaction and alarm mechanisms against these detections, and then returning to the situation before the cyber incident,

g) Cyber incident: A breach of the confidentiality, integrity or availability of information systems or data,

ğ) Cyber-attack: Intentional actions directed against persons or information systems anywhere in cyberspace in order to eliminate the confidentiality, integrity or availability of information systems in cyberspace and the data processed by these systems,

h) Cyber threat: Potential dangers that may cause violations of the confidentiality, integrity or accessibility of information systems and, data contained in or processed by these systems,

ı) Cyber threat intelligence: Information gathered, transformed, analyzed, interpreted, or enriched about existing or potential cyber threats and cyber-attacks against assets in cyberspace,

i) Cyberspace: The environment consisting of all information systems that are directly or indirectly connected to the Internet, electronic communication or computer networks and the networks that connect them to each other,

j) SOME (*CERT): Cyber incident response team,

k) Asset: All information and information processing facilities, including data that can be transmitted through communication, in electronic or physical media, personnel using or transporting the data, and physical spaces that house the data,

l) Vulnerability: The weaknesses and security vulnerabilities of assets in cyberspace that can be exploited by any cyber threat,

Basic Principles

ARTICLE 4

(1) The basic principles for ensuring cyber security are as follows:

a) Cyber security is an integral part of national security.

b) The main objective is to protect critical infrastructure and information systems and to create a secure cyber space.

c) Activities related to cyber security are carried out on the basis of institutionalization, continuity and sustainability.

ç) It is essential that cyber security measures are implemented throughout the entire life cycle of services and products.

d) Domestic and national products shall be preferred primarily in activities to ensure cyber security.

e) All public institutions and organizations and real and legal persons are responsible for the implementation of cyber security policies and strategies and for taking the necessary measures to prevent or mitigate cyber-attacks.

f) Accountability is essential in the execution of cyber security processes.

g) Cyber security policy and strategy development activities are carried out with a continuous development approach.

ğ) Efforts to increase the capability and capacity of qualified human resources in the field of cyber security are encouraged.

h) It is aimed to spread the cyber security culture throughout the society.

ı) The principles of the rule of law, fundamental human rights and freedoms and the protection of privacy are considered as fundamental.

CHAPTER TWO

Duties, Powers, Responsibilities, Audit and Cyber Security Board

Duties of the Presidency

ARTICLE 5

(1) The duties of the Presidency are as follows:

a) To perform the duties specified in the relevant legislation.

b) To carry out activities to increase the cyber resilience of critical infrastructures and information systems, to protect them against cyber-attacks, to detect cyber-attacks, to prevent possible attacks and to reduce or eliminate their effects, to conduct or have conducted vulnerability and penetration tests and risk analyses for assets, to combat cyber threats, to obtain, create and share cyber threat intelligence, to carry out malware analysis activities.

c) To identify critical infrastructures and the institutions and locations to which they belong.

ç) To ensure that the inventory of all assets, including the data inventory, of public institutions and organizations and critical infrastructures is kept and risk analysis for assets is carried out, and to take or have security measures taken according to the criticality of the assets owned by public institutions and organizations and critical infrastructures.

d) To establish, have established and supervise CERTs, to conduct studies to determine and increase the maturity levels of CERTs, to measure the cyber incident response capabilities of CERTs by conducting cyber security, to

coordinate with the cyber incident response teams of other countries, to conduct, have conducted and encourage the production and development of all kinds of cyber response tools and national solutions.

e) To regulate the procedures and principles to be followed by those operating in the field of cyber security.

f) To establish, have established, operate, have operated, have operated the necessary infrastructures to ensure the cyber security of public institutions and organizations and critical public services, and to provide or ensure the provision of hosting services to public institutions and organizations over secure systems and infrastructures, and to determine the implementation procedures and principles for these activities.

g) To prepare standards in the field of cyber security, to examine the standards prepared by other persons or organizations, to give opinions on them, to accept them as standards if deemed appropriate, to publish them and to monitor their implementation.

ğ) To carry out testing and certification procedures for software, hardware, products, systems and services related to cyber security, to establish, have established and operate test infrastructures for this purpose, and to carry out certification, authorization and certification procedures for cyber security experts and companies in coordination with relevant institutions.

h) To carry out cyber security audits and imposing sanctions according to the results.

ı) To determine the technical criteria for the cyber security products and services to be used in public institutions and organizations and critical infrastructures and the qualifications to be carried by the enterprises that will provide them, to make legislative arrangements, to audit or have them audited, to determine the qualifications to be carried by the organizations that will carry out the audits, to commission organizations, to temporarily suspend or cancel the commissioning when necessary.

Powers

ARTICLE 6

(1) The Presidency shall use the following powers while fulfilling its duties:

a) To use the powers referred in the relevant legislation.

b) Take or have taken the necessary measures to protect those covered by this Law against cyber-attacks and to provide deterrence against the source of these attacks. In this context, it may ensure the installation and

integration of software and hardware products suitable for information systems, transfer the data and log records generated or collected by these products to the information systems under the management of the Presidency, and use the necessary method and tool for the detection of cyber incidents.

c) Provide on-site or remote cyber incident response support to those who are exposed to cyber incidents within the scope of this Law, follow the traces of attacks through the data, images or log records found or obtained in cyberspace, examine and prove them, share the findings that are considered to constitute a crime with judicial authorities and other relevant parties, and coordinate with stakeholders in Türkiye and abroad.

ç) Receive and evaluate information, documents, data and records from those covered by this Law, limited to the activities it carries out, make use of their archives, electronic data processing centers and communication infrastructure and establish contact with them. The information, documents, data and records obtained within this scope are subject to study for a maximum period of two years and are destroyed after the study period. Those to whom the request is made within this scope cannot refrain from fulfilling the request by citing the provisions of their own legislation.

d) Collect, store and evaluate log records in information systems. It can prepare reports on these and share them with relevant institutions and organizations.

e) In coordination with the Presidency, ministries and other public institutions and organizations, the Presidency may allocate personnel on cyber security issues in case of need.

f) It can carry out relations with international organizations and countries on issues within its field of duty, exchange information, represent our country and ensure coordination, participate in the work of international organizations, follow the implementation of the decisions taken and provide the necessary coordination.

g) It may classify the institutions, organizations and other relevant real and legal persons and entities without legal personality within the scope of this Law, and may establish provisions covering only a certain part of them when necessary while carrying out their activities.

ğ) It may authorize independent auditors and independent audit institutions that perform cyber security audits, and may revoke their authorization for a period of time or indefinitely.

h) Determine the procedures and principles regarding the criteria for software, hardware, products and services that will be used in the information systems of public institutions and organizations and critical infrastructures

and that have an impact on cyber security and the procedures and principles regarding the notifications to be made to the Presidency.

ı) Determine the minimum-security criteria for cyber security software, hardware, products and services. Manages the certification, authorization and certification processes for real and legal persons who will provide or supply them. It may request that cyber security software, hardware, products and services be brought into compliance with the standards to be determined, and may take measures to prevent the use of those that do not comply with this request.

(2) Within the scope of the business and transactions carried out pursuant to this Law; personal data shall be processed in accordance with the law and good faith, provided that it is accurate and up-to-date when necessary, for specific, explicit and legitimate purposes, in connection with the purpose for which it is processed, limited and proportionate, and to be kept for the period required for the purpose for which it is processed. Personal data and trade secrets to be obtained within the framework of the authorizations specified in this Law shall be deleted, destroyed or anonymized ex officio in the event that the reasons requiring access to such data disappear.

(3) The procedures and principles regarding the implementation of this Article shall be determined by a regulation to be issued by the President.

Responsibilities and Collaboration

ARTICLE 7

(1) The duties and responsibilities of those who are covered by this Law and who provide services, collect data, process data and carry out similar activities by using information systems regarding cyber security are as follows:

a) To provide the Presidency with all kinds of data, information, documents, hardware, software and all other contributions requested by the Presidency within the scope of its duties and activities, primarily and in a timely manner.

b) To take the measures stipulated by the legislation for the purposes of national security, public order or the proper execution of public service regarding cyber security, and to notify the Presidency without delay of any vulnerability or cyber incidents detected in the area where they provide services.

c) To procure cyber security products, systems and services to be used in public institutions and organizations and critical infrastructures from cyber security experts, manufacturers or companies authorized and certified by the Presidency.

ç) To obtain the approval of the Presidency within the framework of existing regulations before starting operations by cyber security companies subject to certification, authorization and documentation.

d) To fulfil the issues included in the policies, strategies, action plans developed by the Presidency to increase cyber maturity and other regulatory actions published and to take the necessary measures.

(2) The Presidency shall work in cooperation with public institutions and organizations, real and legal persons and organizations without legal personality in carrying out the activities specified in this Law.

Audit

ARTICLE 8

(1) The Presidency may, when deemed necessary in relation to its duties set forth in this Law, audit all kinds of acts and transactions falling within the scope of the Law, and may conduct or have conducted on-site inspections for this purpose. The audit covers the activities and transactions of the institutions, organizations and other relevant real and legal persons within the scope of this Law in relation to the provisions of this Law. The personnel of the Presidency, authorized and certified independent auditors and independent audit institutions are authorized to audit. This authority shall be exercised by those appointed by the President. Audits in public institutions and organizations and critical infrastructures shall be conducted by or in the presence of the personnel of the Presidency.

(2) The Presidency shall determine the materiality and priority principles for audit activities, the criteria to be taken into account in risk assessments and the implementation principles. Audit activities shall be conducted in accordance with the program to be established within the scope of materiality and priority principles and risk assessments. The President may have extra-program audits conducted on matters deemed necessary to be examined outside the established program.

(3) Local authorities, law enforcement officers and supervisors and officials of other public institutions shall be obliged to provide all kinds of convenience and assistance to those assigned with inspection or audit.

(4) Those assigned to audit are authorized to examine the data, documents, electronic infrastructure, devices, systems, software and hardware in electronic media, to take copies, digital copies or samples thereof, to request written or oral explanations on the subject, to prepare necessary minutes, to examine the facilities and their operation limited to the audit activities they carry out. Those subject to inspection are obliged to keep the relevant devices, systems, software and hardware open for inspection within the given periods, to provide the necessary infrastructure for inspection and to take the necessary measures to keep them operational.

(5) For the purposes of national security, public order, prevention of crime or cyber-attacks, searches may be conducted in residences, workplaces and closed areas not open to the public upon the decision of a judge or, in cases where delay is deemed inconvenient, upon the written order of the public prosecutor, and copying and seizure may be carried out without interruption and without causing long-term service disruption. A copy of the extracted copy shall be delivered to the person concerned and this matter shall be recorded in a report and signed. Reasonable grounds must be demonstrated for these procedures to be carried out, together with their justifications. The searches and copying and seizure operations carried out without a judge's decision shall be submitted to the approval of the competent judge in charge within twenty-four hours. The judge shall announce his/her decision within forty-eight hours; otherwise, the copies made and the transcripts decoded shall be immediately destroyed and the seizure shall be automatically lifted. The data centers of authorized data center operators may be searched, copied and seized only upon a judge's decision. Ankara criminal judgeship of peace shall be competent and authorized for the requests falling within the scope of this paragraph. However, a judge's decision is not required for public institutions and organizations.

Cyber Security Board

ARTICLE 9

(1) The Cyber Security Council shall consist of the President of the Republic, the Vice President of the Republic, the Minister of Justice, the Minister of Foreign Affairs, the Minister of Interior, the Minister of National Defense, the Minister of Industry and Technology, the Minister of Transport and Infrastructure, the Secretary General of the National Security Council, the President of the National Intelligence Organization, the President of the Defense Industry and the President of Cyber Security. In the absence of the President, the Council shall be chaired by the Vice President.

(2) In addition to the members, relevant ministers and persons may also be invited to the meetings of the Board to obtain information and opinions depending on the nature of the agenda.

(3) The Board may establish commissions and working groups as deemed necessary within the scope of its duties. Commissions and working groups shall carry out technical studies and formulate decision proposals on matters falling within the scope of the Board's duties. Experts in their fields may be invited to the commission and working group meetings to benefit from their opinions.

(4) The duties of the Board are as follows:

a) To take decisions on policies, strategies, action plans and other regulatory actions related to cyber security, and to determine the institutions and organizations to be exempted from all or part of the decisions taken.

b) To take decisions for the implementation of the technology roadmap on cyber security prepared by the Presidency throughout the country.

c) To determine the priority areas to be incentivized in the field of cyber security and to take decisions for the development of human resources in the field of cyber security.

ç) To identify critical infrastructure sectors.

d) To take decisions on disputes that may arise between the Presidency and public institutions and organizations.

(5) Secretariat services of the Board shall be carried out by the Presidency. The working procedures and principles of the Board, commissions and working groups shall be determined by a regulation to be issued by the President.

CHAPTER THREE

Provisions Regarding Personnel

Employment of Contracted Expert Personnel

ARTICLE 10

(1) In order to carry out the duties related to ensuring cyber security in the Presidency, contracted expert personnel whose number will be determined by the President may be employed. The qualifications of these personnel, matters related to their employment such as conditions of appointment, and the net wages including all kinds of payments to be paid to them shall be determined by the Cyber Security Board, taking into consideration the duties to be carried out by the relevant personnel, not exceeding five times the contract wage

ceiling applicable to those employed according to subparagraph (B) of Article 4 of the Civil Servants Law No. 657 dated 14/7/1965. The personnel within the scope of this paragraph shall be deemed to be insured within the scope of subparagraph (a) of the first paragraph of Article 4 of the Social Security and General Health Insurance Law dated 31/5/2006 and numbered 5510. Without prejudice to the special provisions of the laws, the employment in this status does not constitute an acquired right in terms of working in any position, staff or status in public institutions and organizations at the end of the contract.

(2) In the Presidency; security investigation and archive research shall be conducted together for all personnel, including those temporarily assigned, in accordance with the Law on Security Investigation and Archival Research dated 7/4/2021 and numbered 7315.

Transfer of Compulsory Service Obligations

ARTICLE 11

(1) The service periods of the personnel employed in the Presidency who have compulsory service obligation to other public institutions and organizations within the scope of the relevant legislation shall be deducted from the said obligation periods, provided that the consent of the relevant public institution and organization is obtained.

Prohibited Actions

ARTICLE 12

(1) Those who have been dismissed from the Presidency for any reason among those working in the Presidency with permanent or contracted status may not take any other official or private position in the field of cyber security in Türkiye or abroad for two years without obtaining consent from the Presidency, and may not engage in trade in this field, engage in self-employment, and especially may not be a shareholder or manager in a company operating in this sector.

(2) It is prohibited to publish or disclose any information, documents and all kinds of similar data obtained within the scope of the duties and activities of the Presidency through radio, television, internet, social media, newspapers, magazines, books and all other media and all kinds of written, visual, audio and electronic mass media, except in cases authorized by the Presidency.

Confidentiality Obligation

ARTICLE 13

(1) Confidential information, personal data, trade secrets and documents belonging to the public, relevant persons and third parties obtained within the scope of the duties and activities carried out by the Presidency cannot be disclosed to anyone other than the authorities authorized by the legislation, and cannot be used for the benefit of real and legal persons.

CHAPTER FOUR

Income and Exemptions

Revenues of the Presidency

ARTICLE 14

(1) The revenues of the Presidency consist of the following:

a) The Treasury aid to be provided from the general budget,

b) The revenues obtained from the activities of the Presidency,

c) The revenues obtained from administrative fines imposed by the Presidency,

ç) The amounts to be transferred up to 10 percent of the revenues of the funds established or to be established by laws and decrees by the President of the Republic,

d) Other revenues,

Exemptions

ARTICLE 15

(1) All kinds of materials, tools, equipment, machinery, devices and systems to be provided from abroad through import or grant within the scope of the needs of the Presidency, and spare parts, raw materials to be used in their research, development, training, production, modernization and software, construction, maintenance and repairs, and aid materials received from foreign sources free of charge are exempt from customs duties, funds and duties, fees, and the papers issued for these transactions are exempt from stamp tax. This exemption shall also apply to the transactions of final departure, temporary departure, free of charge import and entry for the purpose of repair, modernization, maintenance, return to the origin, exchange abroad on behalf of the Presidency.

(2) Permits and certificates of conformity required to be obtained from public institutions and organizations, real persons and legal entities shall not be required for the import and export of all kinds of materials, tools, equipment, machinery, devices and systems needed by the Presidency during the execution of its duties.

(3) Public institutions and organizations and other institutions and organizations may temporarily allocate or transfer free of charge to the Presidency all kinds of materials, equipment, equipment and devices that are in their use and confiscated in cases where they are needed during the fulfillment of the duties stipulated in this Law, regardless of the regulations of other laws on this matter.

CHAPTER FIVE

Criminal Provisions and Implementation of Administrative Fines

Criminal Provisions and Administrative Fines

ARTICLE 16

(1) Except for public institutions and organizations, those who fail to provide the information, documents, software, data and hardware requested by the authorities authorized by this Law and audit officers within the scope of their duties and powers, or who prevent the receipt thereof, shall be sentenced to imprisonment from one year to three years and to a judicial fine from five hundred days to one thousand five hundred days.

(2) Those who carry out activities without obtaining the necessary approvals, authorizations or permits pursuant to this Law shall be sentenced to imprisonment from two to four years and to a judicial fine from one thousand days to two thousand days.

(3) Those who fail to fulfil their obligation to keep secrets shall be sentenced to imprisonment from four to eight years.

(4) A prison sentence of three to five years shall be imposed on those who, without the permission of individuals or institutions, make available, share or put up for sale, with or without charge, personal data or corporate data within the scope of critical public service, which were previously included in cyberspace due to data leakage.

(5) Those who create false content claiming that there is a data leak related to cyber security in order to create anxiety, fear and panic among the public or to target institutions or individuals, even though they know that there

is no data leak in cyberspace, or those who disseminate such content for this purpose shall be sentenced to imprisonment from two to five years.

(6) Those who commit a cyber-attack against the elements constituting the national power of the Republic of Türkiye in cyberspace or who keep any kind of data obtained as a result of this attack in cyberspace shall be sentenced to imprisonment from eight to twelve years, unless the act constitutes another crime requiring a heavier penalty. Those who disseminate any data obtained as a result of this attack in cyberspace, send it elsewhere or put it up for sale shall be sentenced to imprisonment from ten to fifteen years.

(7) The penalty to be imposed pursuant to the preceding paragraphs shall be increased by one-third if the offense is committed by a public official, by half if it is committed by more than one person and by half to twice as much if it is committed within the framework of the activities of an organization.

(8) Those who violate Article 12 shall be sentenced to imprisonment from three to five years.

(9) Those who abuse their duties and powers arising from this Law or who cause a data breach by acting contrary to the requirements of their duties within the scope of protection of critical infrastructures against cyber-attacks shall be sentenced to imprisonment from one year to three years.

(10) Those who fail to fulfil their duties and responsibilities under subparagraphs (b) and (c) of the first paragraph of Article 7 shall be fined from one million Turkish Liras to ten million Turkish Liras, and those who fail to fulfill their duties and responsibilities under Article 18 shall be fined from ten million Turkish Liras to one hundred million Turkish Liras.

(11) Those who fail to fulfil their obligations under the fourth paragraph of Article 8 shall be imposed an administrative fine ranging from one hundred thousand Turkish Liras to one million Turkish Liras, and if these obligations are not fulfilled by commercial companies, an administrative fine of not less than one hundred thousand Turkish Liras and up to 5 percent of the gross sales revenue in the independently audited annual financial statements.

Application of Administrative fines

ARTICLE 17

(1) Before the imposition of administrative fines, the defense of the relevant person shall be taken. In case the defense is not given within thirty days from the date of notification of the letter requesting defense, it shall be deemed that the person concerned waives his/her right of defense.

(2) If it is determined that one of the misdemeanors defined in this Law has been committed more than once until an administrative sanction decision is issued, a single administrative fine shall be imposed on the relevant natural or legal person and the fine to be imposed shall be increased by not exceeding two times. In the event that a benefit is obtained or damage is caused due to the commission of the misdemeanor, the amount of the administrative fine shall not be less than three times or more than five times the amount of the benefit or damage.

(3) Administrative fines imposed by the Presidency shall be paid within one month from the date of notification. Administrative fines that are not paid within this period and finalized shall be collected by the tax offices upon notification of the Agency in accordance with the provisions of the Law on Collection Procedure of Public Receivables dated 21/7/1953 and numbered 6183.

(4) Fifty percent of the administrative fines collected shall be recorded as revenue in the budget of the Presidency and fifty percent in the general budget. The general budget share allocated from administrative fines collected by the Presidency and the Presidency share allocated from administrative fines collected by the tax office shall be transferred until the end of the month following the collection.

(5) Administrative fines imposed pursuant to this Law may be appealed to the administrative judiciary.

CHAPTER SIX

Miscellaneous and Final Provisions

Cyber Security Products and Companies

ARTICLE 18

(1) The sale of cyber security products, systems, software, hardware and services abroad shall be made in accordance with the procedures and principles to be determined by the Presidency. The approval of the Presidency shall be obtained for the sale abroad of products subject to authorization to be included in these procedures and principles.

(2) Merger, demerger, share transfer or sale transactions of companies producing cyber security products, systems, software, hardware and services shall be notified to the Presidency. Within the scope of these transactions, transactions that provide real or legal persons, individually or jointly, with direct or indirect control rights or decision-making authority over the company are subject to the approval of the Presidency.

(3) Transactions carried out without the approval of the Presidency shall not be legally valid. The Presidency may request information and documents from institutions and organizations regarding the transactions to be carried out under this Article.

(4) The matters regarding the implementation of this Article shall be determined by the procedures and principles to be published by the Presidency.

Amended and Repealed Provisions

ARTICLE 19

(1) The following sentence has been added to the third paragraph of the additional article 34 of the Decree Law dated 27/6/1989 and numbered 375.

"The Head of Cyber Security shall be deemed equivalent to the Undersecretary of the Ministry in terms of financial and social rights and benefits and retirement rights within the framework of the procedures and principles specified in this paragraph."

(2) The following line has been added to the "B) Other Administrations with Special Budgets" section of the Schedule (II) annexed to the Public Financial Management and Control Law No. 5018 dated 10/12/2003.

"46) Cyber Security Presidency"

(3) The sixth paragraph of Article 10 of the Law No. 5651 dated 4/5/2007 on the Regulation of Publications on the Internet and Combating Crimes Committed through Such Publications is amended as follows.

"(6) Within the scope of its duties, the Authority coordinates with content, hosting and access providers and other relevant institutions and organizations, carries out activities to ensure that the necessary measures are taken and conducts the necessary studies."

(4) Law on Electronic Communications dated 5/11/2008 and numbered 5809;

a) Subparagraph (h) of the first paragraph of Article 5 has been repealed and subparagraph (ı) has been amended as follows.

" ı) To establish, have established, operate, have operated, have operated the data centers where the data and systems within the scope of the duties carried out by the Ministry will be hosted and the infrastructures required for the transfer of data, to determine the policies, strategies and objectives for these centers, to prepare action plans, to monitor action plans and to determine the implementation procedures and principles for all these activities, to plan, execute and coordinate the installation, implementation and operation processes."

b) Paragraph (v) of the first paragraph of Article 6 has been amended as follows.

"v) To fulfill the duties assigned by the President and the Ministry regarding internet domain names and the duties of the Authority."

c) The eleventh paragraph of Article 60 and Additional Articles 1 and 2 have been repealed.

Compliance, Transitional Arrangements and Establishment Procedures

PROVISIONAL ARTICLE 1

(1) All kinds of movables, IT infrastructure and systems, vehicles, tools, equipment and materials, all kinds of records and documents in physical and electronic media and all kinds of other assets inventory belonging to the Presidency of the Information and Communication Technologies Authority and the Digital Transformation Office and used exclusively within the scope of national cyber security activities, and all kinds of debts and receivables, rights and obligations arising from the execution of the said activities by the aforementioned Presidency and Office shall be transferred to the Cyber Security Presidency within six months following the publication of this Law.

(2) Personnel working within the scope of national cyber security activities among the staff and positions of the Information and Communication Technologies Authority Presidency and Digital Transformation Office may be assigned to the Presidency if they request and if deemed appropriate by the Cyber Security Presidency. Of these, those who request and are deemed appropriate by the Presidency may be appointed to the appropriate staff or positions in the Presidency within nine months from the publication of this Law, taking into account their current staff or position titles and educational background. The periods spent by the personnel appointed within the scope of this paragraph in their previous institutions or positions shall be deemed to have been spent in their new

institutions or positions. Among the personnel appointed within the scope of this paragraph, the provisions of the provisional Article 10 of the Decree Law No. 375 or other relevant legislation shall continue to be applied to those to whom the provisions of the provisional Article 10 of the Decree Law No. 375 or other relevant legislation are applied regarding their financial rights. The personnel appointed from the Digital Transformation Office within the scope of this paragraph shall not be paid any compensation and annual leave fee according to the labor legislation. Except for the periods for which severance indemnity has been paid in advance, the service periods of these personnel who are entitled to severance indemnity shall be taken into account in the calculation of their retirement bonuses or termination indemnity, depending on their interest. In addition, in the event that additional payments or bonuses were paid to these personnel before their appointment according to this paragraph, the portion of the amounts paid corresponding to the unworked days after the date of appointment shall be taken back.

(3) As of the date of completion of the appointment procedures in the second paragraph, the Presidency shall become a party in the contracts made, lawsuits filed and to be filed and enforcement proceedings related to the national cyber security activities of the Presidency of the Information and Communication Technologies Authority and the Digital Transformation Office, and the existing lawsuit files and files related to enforcement proceedings shall be transferred to the Presidency.

(4) Associations, federations consisting of associations, foundations and commercial companies performing activities in the field of cyber security are obliged to complete certification, authorization and certification procedures within one year following the entry into force of the regulations specified in the sixth paragraph within the framework of the principles and principles determined by the Presidency. In case this obligation is not fulfilled, no activity in the field of cyber security can be carried out. The legal entities of associations, foundations and federations that do not fulfill their obligations at the end of this period shall be terminated by court decision in accordance with the relevant provisions of the Turkish Civil Code dated 22/11/2001 and numbered 4721 upon the request of the Presidency, and the necessary measures shall be taken by the court during the trial process. If commercial companies do not fulfill their obligations within the same period, they shall remove the phrases related to cyber security in their trade names and fields of activity from their company contracts or initiate liquidation processes in order to be abandoned from the trade registry.

(5) The institutions operating under the provisions repealed pursuant to the third and fourth paragraphs of Article 19 shall continue to carry out their duties within the framework of the said provisions until the completion of the organization of the Presidency.

(6) Regulations regarding the implementation of this Law shall be put into force within one year. Until these regulations enter into force, the provisions of the existing regulations that are not contrary to this Law shall continue to be applied.

Enforcement

ARTICLE 20

(1) This Law shall enter into force on the date of its publication.

Execution

ARTICLE 21

(1) The President shall execute the provisions of this Law.