Issue: 475

ELECTRONIC COMMUNICATIONS LAW

(Law no 6/2012, 21/2014, 39/2016, 27/2019 and 31/2019)

By-Law made under Article 84, 85 and 94

The Council of Ministers of the Turkish Republic of Northern Cyprus enacts this By-Law with the power given under Articles 84, 85 and 94 of the Electronic Communications Law:	
Short Title	1. This By-law may be cited as By-law on Processing Personal Data and Maintaining Confidentiality in Electronic Communications Sector.
SECTION ONE **General Rules**	
Interpretation	2. In these By-Law, unless the context requires otherwise; "Subscriber" means any natural or legal entity that is a party in a contract made with an electronic service provider for the provision of an electronic communications service. "Emergency service calls" means calls made for fire department, police, health and similar institutions for emergency situations such as fire, health, natural services and security, which are accepted in national and international regulations. "Anonymization" means matching personal data with other data in a manner that will not enable them in any manner to be associated with a natural person whose identity is definite or that can be defined. "Electronic Communications Service Provider/Communications Service Provider," means the legal entity and the Telecommunications Agency that is the operator of an electronic communications network or provides electronic communications services. "Call that did not materialize" means the call, in which communication was not materialized even though connection was successfully established. "Cell ID" means the ID of the cell in which mobile phone call is initiated or terminated. "IMEI" means international electronic identity of mobile devices. "IMSI" means international mobile subscriber identity of mobile subscribers.

	"Internet Telephone Service" means phone calls made by carrying voice signals through IP. "IP (Internet Protocol)" means the protocol which is used by devices that are connected to a specific network to know and communicate with each other. "Transaction registry" means electronic registries about the transaction done by people accessing personal data which are kept to ensure that it could be completed after the materialized date and which contains the transaction, detail of the transaction, the person that made the transaction, date and time of the transaction and the point where the party of the transaction is connected. "Personal data" means all of the information with regards to a natural person whose identity is definite or whose identity can be defined. "Violation of personal data" means the violation of security in an illegal, unauthorized or involuntary manner which cause personal data to be destroyed, deleted, lost, transferred, changed, stored or saved in another environment, processed, exposed or accessed. "Processing personal data" or "Processing" means application of any, a few or all of the transactions such as all of the data of the person being gathered, saved, processed, stored, deleted, assessed, used, adapted or changed, stopped and terminated, by using any method or tool. "Location data" means a specific data which determines the geographical location of a device of an electronic communication service user and which is processed in the electronic communication network or through electronic communication service. "User" means any kind of real individual or legal entity that uses electronic communications services, whether they are a subscriber or not. "User identity" means single and private definition which is allocated to internet access services or internet communication services during subscription or registration. "Board" means the Information Technologies and Communication Agency Board of Directors. "Agency" means the Information Technologies and Communication Agency. "NAT (Network Address Translation)" means the technology which enables the real IP address pool to be used in an efficient manner by turning the real IP addresses in the IP packages that are carried in the

	network into different IP addresses and ports in local network with different techniques. "Traffic data" means all kind of data which is processed in an electronic communications network for data transfer or billing. "Data" means all of the traffic data, location data or other related data which are used to identify the subscriber or user. "Law" means the Electronic Communications Law. "Time Stamp" means the registry, which is verified by an electronic certificate service provider with electronic signature in order to determine the time when an electronic data is produced, changed, sent, received or registered.
Purpose	3. The purpose of this By-law is to regulate principles and procedures which will be abided by communication service providers that are operated in the electronic communication sector in order for personal data in the electronic communications sector to be processed, stored and their confidentiality to be protected.
Scope	4. (1) Principles and procedures that will be abided by communication service providers that are operated in the electronic communication sector for personal data in the electronic communications sector to be processed, stored and their confidentiality to be protected are within the scope of this By-law. (2) Storing data with regards to the content of communication is not within the scope of this By-law.
SECTION TWO Practice Principles	
Principles on Processing Personal Data	5. Principles and conditions for legal processing which are regulated in Articles (5) and (6) of the Law for Protection of Personal Data shall be taken into consideration in terms of the personal data processing activities that are done within the scope of providing electronic communication services.
Security	6. (1) Communication service providers shall determine their security policies for processing personal data in accordance with the principles that are set forth in Article (5) of this By-law. Electronic communication service providers shall take every necessary technical and administrative precaution that are necessary to protect the security of their own network and services in a level suitable for probable risks in consideration of the

	costs for applying the related security systems and the newest technical possibilities. (2) Communication service providers are obliged to enable personal data to be reached by authorized people only and to ensure the security of systems, in which personal data is kept, and software and hardware that are used for accessing personal data. (3) Communication service providers are obliged to keep the registries of transactions for accessing personal data and systems, in which personal data is processed, with time stamp. (4) The Agency may request communication service providers to provide all of the information and documents on the systems, in which personal data is processed and on security measures taken in these systems when it deems necessary and in addition, may request changes in the subject matter security precautions for the protection of the confidentiality of personal data and their security. (5) Communication service providers are responsible for the confidentiality, security, provision of integrity and usage in accordance with its purpose in the scope of the legislation in force and this By-law. (6) Communication service providers are obliged to give the necessary information in accordance with article (13) of the Law for Protection of Personal Data in case of the person subject of knowledge does not have the necessary information at the information gathering stage. (7) Communication service providers are obliged to publish a confidentiality policy, which contains the elements in clause (6) at minimum, on their web site.
Notifying the Risk and Violation of Personal Data	7. (1) In case of the presence of a certain risk that violate the security of the network or personal data, communication service providers are obliged to inform the Agency and affected subscribers and users on the risk and if it is considered necessary by the Agency, their other subscribers and users on this risk in an effective and quick manner. (2) In case of this risk being out of the scope of the precautions taken by communication service providers, it is enabled to inform the subscribers or users that are likely to be affected from the risk and/or all of the subscribers or users in an effective and quick manner on the scope of the subject matter risk and the methods of eliminating the risk. (3) In case of the presence of personal data violation, communication service providers shall inform the subscribers and/or users in a free manner on the qualification of the violation of personal data, the

	communication points where more information can be received and precautions that can be taken by subscribers or users to decrease negative effects of violation and costs. (4) In case of the presence of personal data violation, communication service providers shall inform the Agency on the details of the information given to the subscribers and/or users on the qualification and conclusions of the subject matter violation and on the precautions taken for eliminating the violation. (5) Communication service providers are obliged to record the information on personal data violations which contain the reasons, effects and precautions on the solution by enabling their confidentiality and integrity.
SECTION THREE Processing and Storing Data	
Confidentiality and Data Protection	8. (1) Confidentiality of electronic communication and the related traffic data is considered as basis and apart from the exception set forth in clause (2) of this article, except for the users that are party of communication gives consent in a manner with the avoidance of doubt, the communication between them cannot be listened, stored, interrupted and followed. (2) Except for the conditions which are given in article 84 of the Law, no one apart from the users that communicate among each other can listen, store or prevent the communication between them without their consent. (3) Electronic communication networks may be used by electronic communication service providers in order to store information in the terminal equipment of subscribers or users or to access information that are kept there on the condition that the related subscribers and/or users are informed on processing their data in a clear and comprehensive manner and their consent is taken. However, any technical storing or access, which are made for materializing or facilitating communication through an electronic communication sector or which are required to provide information community service that is clearly requested by subscriber and/or user are not within this scope.
Processing Traffic Data	9. (1) Traffic data shall be deleted or anonymized when the call is terminated with reservation of the obligations set forth in article 12 of this By-law. Traffic data shall be processed for the settlement of disputes that are determining traffic data, traffic management, interconnection,

	billing, unlawfulness and/or fraud and similar transactions or customer complaints and interconnection and billing disputes in particular, on the condition that they are limited to people who are authorized by the communication service provider and by enabling the confidentiality and integrity until the settlement process of these conflicts are completed. (2) Traffic data, which are required in order for marketing electronic communication services or providing value added electronic communication services, can be processed within the scale and time that are required by the stated activities on the condition that their consent is taken in accordance with Article 13 of the Law for Protection of Personal Data regarding the purpose and period of processing the traffic data of the related subscribers and/or users that will be anonymized or processed and only being limited with the people that are authorized by the electronic communication service provider. (3) Subscriber and/or user may request the process of traffic data which they accepted to be suspended or deleted any time without prejudice to the rules of this By-law and legislation in force. (4) The Agency and the Council of Personal Data Protection may request the electronic communication service providers to provide any information they have so as to inspect the conformity for the rules that are envisaged in clause (1) that is given above. In case of obtaining another information on the subject after providing the requested information, electronic communication service provider is obliged to give this information to the Agency as well. (5) Electronic communication service providers shall enable the subscribers or users to withdraw the consent, which they had given with short message, call centres, internet or similar methods, with the same method or with a simple method and for free of charge at any time.
Processing Location Data	10. (1) (A) In cases when location data can be processed and apart from traffic data of electronic communication networks or electronic communication service users or subscribers, these data can only be processed after they are anonymized or with the consent of users or subscribers in the scale and time that are required for a value added service to be provided. (B) The related communication service provider shall inform the users or subscribers before taking their consent on the type, purpose of processing and period for the location data that will be processed and whether the data will be delivered to a third party for providing the value added service except for the traffic data.

	(C) Users or subscribers can prevent location data to be processed at any time they want except for the traffic data. (2) In case of receiving approval from users or subscribers for processing location data except for traffic data, user or subscriber shall continue to have the opportunity to temporarily reject these data to be processed for every connection to the network or for every transmission of communication with a simple manner and for free of charge. (3) Processing location data except for traffic data in accordance with the rules of this article, shall be limited with people that are acting with the authority of the electronic communications network or institution that provides electronic communications service or the third party that provides value added services and it shall be restricted with the scale that is required to provide value added service. (4) Electronic communication service providers shall enable subscribers and/or users to withdraw the consent they gave through short message, call centres, internet and similar methods for their location data to be processed with the same method or with a simple method at any time and for free of charge.
Transferring Traffic and Location Data to Other Countries	11. (1) With reservation of the related provisions of the Law for Protection of Personal Data, traffic and location data and the data that are set forth in article (12) of this By-law may be transferred abroad on the condition that the Agency is notified. The Agency may request the subject matter data to be terminated to be transferred abroad temporarily or constantly for national security and public order. (2) In accordance with article (12) of this By-law, an up-to-date copy of these data, which is foreseen by electronic communication service providers to be kept and which is updated real time shall always be kept domestically. (3) Information on international calls and information on mobile telephone number that is required for providing some electronic communication services (MSISDN) may be taken abroad in the scope of technical obligation without requiring the Agency to be notified.
Categories of Data That Will Be Stored	12. (1) Data in the following categories shall be stored by electronic communication service providers in the scope of this By-law. (A) For subscriber, according to the type of service, for billing and objecting the invoice for interconnection payments or for following a payment: Subscriber station identification number; addresses and type of station of

	the subscriber; total number of units that will be billed for the accounting period; number of the called subscriber; type of the calls, time of originating and call time or the volume of the transmitted data; time for initiating access for the internet service, its period and volume of the transmitted data; date of call or service; and payments in advance, payments in instalments, other information such as disconnection and warnings. (B) For following communication and defining its source: (a) Regarding fixed and mobile telephone services; information on phone number of the line in which communication is initiated including the calls that did not materialize, as well as the name and address of the subscriber and the date when the line is allocated to which subscriber. (b) Regarding access to internet media and internet telephone service; identity of the allocated user and/or their telephone number, internet protocol address of the moment when communication is materialized, name and address of the subscriber/user. (C) In order to determine the point where communication will be terminated: (a) Regarding fixed and mobile telephone services; number or numbers in which communication is terminated and/or will be terminated and name and address of the subscriber in intra-network terminations, in case of the presence of additional services such as call transmitting and call transfer in the network, the number or numbers the call is diverted as well as the name and address of the subscribers. (b) Regarding internet telephone service; identity or telephone number of the receivers that are called through internet call service, name and address of the receivers of internet telephone. (c) Regarding access to internet service; the IP address for each point where communication is terminated. (Ç) In order to determine date, time and period of communication: (a) Regarding fixed and mobile telephone services; date and time for the communication to begin and terminate. (b) Regarding internet access and internet telephone; login with regards to internet access, date and time for logout, dynamic and static IP address that is allocated, port information along with IP address in networks in which NAT is used as well as identity of subscriber/user or login and logout date and time for internet telephone.

	(D) In order to determine the type of communication: (a) Used electronic communication service regarding fixed and mobile telephone services. (b) Used internet service regarding internet telephone. (c) Regarding internet service; type of the used service. (E) In order to determine the devices or their equipment of communication devices that are used: (a) Telephone numbers of which communication is initiated or terminated regarding fixed telephone service. (b) Regarding mobile telephone service; telephone numbers of which communication is initiated and terminated, IMSI and IMEI numbers of the party in which communication is initiated and/or the party of the terminated call if they are the subscriber of the communication service provider; in case of the presence of calling card service that doesn't have subscriber registration, the date and time when the service became active and the cell identity in which the service is activated. (c) Regarding access to internet environment and internet telephone; number of calling telephone for dial-up networking access, digital subscriber line number or the other point where communication is resourced. (F) In order to determine the location of mobile communication device which is envisaged by the related legislation; cell identity where the communication is initiated, data that define geographical locations of cells with regards to cell identities in the time when communication data is kept, cell address and dates of the cell identity to be appointed for and eliminated from that address. (2) Regarding internet telephone within the scope of this By-law, obligations on storing data shall be limited with services which are provided only by electronic communication service providers. (3) Subscriber information on natural person or legal entities in sending bulk short messages by electronic communication service providers shall be stored.
Time of Storing Data By Electronic Communication	13. (1) The data that are set forth in sub-clause (A) of clause (1) of article 12 of this By-law shall be stored until the end of the legal period which is envisaged for legal obligations. (2) With reservation of the provisions for legal prescription that is stated

Service Providers	in the respective legislation, data categories which are defined within the scope of article 12 of this By-law shall be stored for at least 2 (two) years as of the date of communication and the registries on calls that were not materialized shall be stored for 6 (six) months. (3) Personal data that are subject to investigation, review, supervision or conflict shall be kept as of the date when they are notified, until the related process is completed. (4) Transaction registries of personal data and systems in which personal data are processed shall be stored for two years. (5) The registries which show the consent of subscribers/users for processing personal data shall be kept during the term of subscription at minimum.
Protection and Security of Stored Data	14. (1) Electronic communication service providers are obliged to the following at minimum for data that are foreseen to be stored in the scope of this By-law; (A) For the stored data and other data in the network to be subject to the same quality, security and protection characteristics, (B) Suitable technical and administrative measures to be taken for the stored data to be accessed, destroyed, lost, deleted, changed, stored, processed and exposed in an unauthorized or unwilling manner, (C) Suitable technical and administrative measures to be taken for the data to be accessed only by authorized people, (Ç) For enabling the processed and kept data to be irrevocably deleted or anonymized in at least one month as of the date of expiry for keeping the data and for recording these transactions with time stamp with a minutes or in the electronic environment. (2) Electronic communication service providers are obliged to provide the integrity, confidentiality and accessibility of the data they obtain in the scope of the services they offer at every stage. This obligation shall include the transactions that are done by parties that are authorized by electronic communication service providers. (3) In case of being requested by authorities that are authorized by laws, electronic communication service providers are obliged to provide the kept data and all of the information thereof without any delay.
SECTION FOUR	

Offered Opportunities	
Hiding Number (Blocking Number for Being Displayed)	15. (1) In cases when electronic communication service provider enables the calling number to be displayed; it is obliged to (A) Enable the calling user to hide its number with a simple method and for free of charge, (B) Enable the dialled number to prevent the calling number to be displayed in incoming calls with a simple method and for free of charge, (C) Enable the incoming calls to be rejected by the subscriber/user depending on the will of the dialled subscriber/user and for free of charge in case of the calling person hide their number. (2) In case of enabling the connected number to be displayed, electronic communication service provider is obliged to offer the opportunity to the subscriber that is connected to prevent the connected number to be shown to the calling user with a simple method and for free of charge. (3) Electronic communication service provider is obliged to inform its subscribers/users on the services that are stated in clause one and two of this article with short message, internet, press and media organs, mail or with similar tools for free of charge. (4) The opportunity for hiding the calling number shall not be valid for emergency call services.
Confidentiality in Detailed Invoices	16. In case of the request of the subscribers, which are sent detailed invoices, electronic communication service providers enable some numbers of telephone numbers to be concealed in the detail of invoice.
Other Rights of the Subscriber	17. The rights of Subscribers and Users that are in article 14, 15, 16 and 17 of the Law for Protection of Personal Data shall remain.
SECTION FIVE **Various and Final Rules**	
Temporary Article Security	1. Electronic communication service providers are obliged to fulfil all of the technical and administrative measures, which are stated in article 6 of this By-law and which are required for security systems, in 18 (eighteen) months as of this By-law enters into force.
Administrative Fines and Other Sanctions	18. The Agency shall apply administrative fines and other sanctions to electronic communication service providers if they do not fulfil their obligations that are determined with this By-law in accordance with the related articles of the Law.

Executive Authorization	19. This By-law is executed by the Ministry responsible for electronic communications.
Entry Into Force	20. This By-law enters into force as of the date it is published in the Official Gazette.