



Regulation on Processing and Privacy of Personal Data in Electronic Communications Sector

Authors: Gönenç Gürkaynak, Esq., Ceren Yıldız, Yasemin Doğan and Devlet Çağla Nizam, ELIG Gürkaynak Attorneys-at-Law

The Regulation on Processing and Privacy of Personal Data in Electronic Communications Sector (“Regulation”) has been published on the Official Gazette of December 4, 2020. The Regulation will enter into force within six (6) months following its publication date (i.e. June 4, 2020). The Regulation revokes the Regulation on Processing and Privacy of Personal Data in Electronic Communications Sector which was published on the Official Gazette of July 24, 2012.

I. Scope of the Regulation

Regulation provides rules and principles applicable to processing and privacy of personal data in electronic communications sector. The rules and principles enacted under the Regulation are applicable to personal data obtained during provision of services by operators which are operating in electronic communications sector, including for legal entity subscribers.

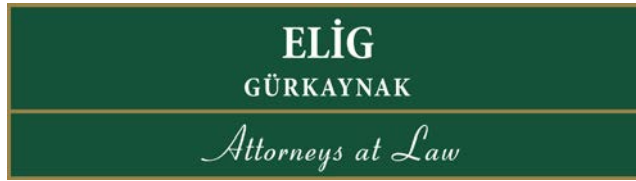
II. Obligations Set Out by the Regulation

(i) Principles

According to the Regulation, personal data must be (i) processed lawfully and fairly, (ii) accurate and where necessary kept up to date, (iii) processed for specified, explicit and legitimate purposes, (iv) relevant, limited and not excessive in relation to the purposes for which they are processed, (v) kept for as long as it is foreseen by relevant legislation or it is necessary for the purposes of processing.

(ii) Obligation to Take Measures

Operators must take technical and administrative measures in line with the Law No. 6698 on Protection of Personal data (“Law No. 6698”), per national and international standards for the security of personal data. These measures must at least contain the following: drafting security policies for processing of personal data, protection of personal data in case of data breaches, ensuring security of applications used for access to personal data. Information Communications and Technologies Authority (“ICTA”) might request information and documents with regards to the security measures, and request modification on them.



(iii) Data Retention Obligation

Operators must retain the records with regards to accesses made to personal data and other related systems for two (2) years.

Besides, for national security purposes, traffic and location data cannot be transferred abroad, in principle (*please see section (v) for particular requirements for transfer*)

(iv) Obligation to Notify Risks and Breaches

Operators must notify the relevant subscribers and users of any potential security risks. Besides, operators must notify Personal Data Protection Authority and relevant subscribers/users in line with the Law No. 6698 of data breaches.

(v) Obligation to Inform and Explicit Consent

Operators must comply with the following in case they are required to obtain explicit consents of subscribers and users:

- Explicit consent must be specific to a subject and obtained prior to the relevant transaction
- Explicit consent must be freely given
- Subscribers/users must be informed of the personal data type to be processed, traffic and location data types, scope, processing purposes and periods.
- Consent of the subscriber/user must be obtained in written or electronic media.
- Records of the consents must be kept at least for the periods set forth under the relevant legislation and in any case during the subscription period.

In line with the data protection legislation, explicit consent cannot be a precondition for establishment of the subscription relationship and for provision of the key electronic communication services or devices. That said, the Regulation allows the operators to seek explicit consent in exchange for an additional benefit, such as free minutes, SMS and data.

As indicated, the principle is not to transfer traffic and location data abroad, for national security purposes. If traffic and location data would be transferred to third parties, operators must obtain another explicit consent by informing subscribers/users of scope of the transferred data, name and address of the transferee, transfer purpose and period, transferee country if data would be transferred abroad.

Without prejudice to the Law No. 6698, operators must inform subscribers/users of the processed traffic and location data types, processing purpose and period, in case traffic and location data would be processed.



Explicit consent obtained prior to entrance into force of the Regulation and in accordance with the applicable legislation would be deemed valid. In case of cease of subscription of the parties whose personal data were processed upon their explicit consent prior to the effective date of the Regulation, and their data is processed after cease of subscription without explicit consent, such process must be ceased within one month following the effective date of the Regulation, save for the obligations in the relevant legislation.

(vi) Obligations on Calls and Detailed Bills

Operators must enable subscribers/users to camouflage their numbers through simple and free methods. Operators must also enable subscribers/users to cease automatic directed calls through simple and free methods.

Upon request, operators must redact certain digits in telephone numbers included in usage details and detailed bills.

III. Rights of Subscribers/Users

- Operators must enable subscribers/users to withdraw their explicit consents through a method that is used for obtaining explicit consent or an easier method.
- Operators must notify subscribers/users that their personal data is processing within the scope of their explicit consents, within third quarter of each year.
- Operators must notify disabled subscribers/users in line with ICTA's regulations and through audio and visual methods.
- Explicit consent is deemed withdrawn when the subscription is terminated/expired, unless otherwise is stated by the subscriber/user.
- All the notifications made under the Regulation must be free. With regards to the notifications and explicit consents required under the Regulation, the burden of proof will be on the operators.

IV. Sanctions

The Regulation refers to Regulation on Information Communications and Technologies Authority Administrative Sanctions if the obligations set forth under the Regulation are not fulfilled, which includes administrative monetary fine up to 3% of the net sales of the previous calendar year, in case of non-compliance with data privacy obligations.

Article contact: Gönenç Gürkaynak, Esq.

Email: gonenc.gurkaynak@elig.com

(First published by Mondaq on December 10, 2020)