Authors: Gönenç Gürkaynak Esq., Ceren Yıldız, Noyan Utkan and Duhan Kurt, ELIG Gürkaynak Attorneys-at-Law

Turkey Introduces New Methods for Identity Verification in the Electronic Communications Sector

The Regulation on Verification Process of the Applicant's Identity in the Electronic Communications Sector ("**Regulation**") was published on the Official Gazette of June 26, 2021 and will enter into force on December 31, 2021.[1]

The Regulation introduces new methods and standards for identity verification in the electronic communications sector. Accordingly, the Regulation sets out the procedures and principles with respect to the process to be applied to identity verification of those who make a request on his/her behalf or on behalf of the real or legal person as its representative ("Applicant") during the creation of documents ("Transaction Documents") in electronic medium for the following transactions: subscription contracts, number porting and operator change application, qualified electronic certificate and registered e-mail ("KEP") application and SIM card change application in the electronic communications sector.

The Regulation will be applicable for and will affect (i) the operators that provide electronic communication services and/or electronic communication networks and operate its substructure with an authorization and (ii) the service providers for qualified electronic certificates and registered e-mails.

The general principles to be considered during the implication of the Regulation are as follows: (i) ensuring that the Applicant's transactions indicated in the Regulation are carried out with safe and effective methods, (ii) preventing suspicious transactions that pose a security risk (i.e. forgery, fraud), (iii) observing national and international standards, (iv) utilizing national resources to the maximum extent, (v) observing national security, public order, and emergency necessities, (vi) observing consumer rights and interests.

The Methods for Identity Verification

The Regulation adopts 4 different methods for identity verification which are (i) identity verification through e-Government System, (ii) identity verification through artificial intelligence or a representative, (iii) identity verification through Turkish Republic Identity Card by creating PAdES-LTV in face-to-face applications and (iv) identity verification through video recording in face-to-face applications.

(i) Identity verification through e-Government System: In this method, the Applicant must sign into the e-Government system with one of the following methods: secure electronic signature, the Republic of Turkey identity card, internet banking or mobile banking. In order to verify the identity of the Applicant, relevant information regarding the transaction and the Transaction Documents is provided to the Applicant and the approval of the Applicant is received. Upon the receipt of approval, the Applicant's verified identity as well as the verified contact number and e-mail address are conveyed to the operator or service provider.

[1] *See* https://www.resmigazete.gov.tr/eskiler/2021/06/20210626-21.htm (Last accessed on July 26, 2021).

(ii) Identity verification through artificial intelligence or a representative: In this method with video conference, the verification must be conducted in real time and without interruption through end-to-end secured communication. The single-use password or link must be sent to the Applicant's mobile number or e-mail address to confirm the contact information. The identity information including the identity card photo of the Applicant is received via near field communication method ("NFC") enabling wireless communication between two electronic devices in a near distance as indicated under Annex-1 of the Regulation and in accordance with the indicated standards. The validity and authenticity of the received identity information are verified as part of the process. Comparing the applicant's identity card photo with their real-time image is made through artificial intelligence as per Annex-2 of the Regulation or through an authorized representative of the operator or service provider as per Annex-3 of the Regulation. As per Annex-3, the identity verification through representative must be checked through artificial intelligence as well, otherwise the verification through representative without artificial intelligence will be deemed invalid.

In terms of the protection of personal data, the Regulation sets forth that an Applicant's explicit consent must be obtained in scope of the Law on the Protection of Personal Data numbered 6698 ("Law No. 6698"). Before the verification through artificial intelligence or a representative with video conference, operators and service providers must fulfil their obligation to inform Applicant under Law No. 6698, separately from obtaining explicit consent. As obtaining explicit consent of the Applicant, it must be clearly indicated that the identity verification process in electronic medium can also be conducted through e-Government system or face-to-face applications.

(iii) identity verification through Turkish Republic Identity Card by creating PAdES-LTV in face-to-face applications: In this method, the identity of the Applicant may be verified by creating enhanced PDF electronic signature (PadES) with a long term validation (PadES-LTV) with the Applicant's Turkish Republic Identity Card in accordance with the Annex-4 of the Regulation.

(iv) *identity verification through video recording in face-to-face applications:* In this method, as an alternative to the verification by creating PadES-LTV, the identity of the Applicant may be verified by video recording of the Applicant specified to the transaction along with their Turkish Republic Identity Card or other identity card. The requirements in scope of the Law No. 6698 explained above section of the identity verification through artificial intelligence or a representative are also applicable for this type of verification method. In this method; the Regulation prohibits operators and service providers to obtain Applicant's biometric data with pressure, acceleration and similar qualities, except for statistical data such as a two-dimensional figure of the Applicant.

In the face-to-face applications of (iii) and (iv), the single-use password or link must be sent to the Applicant's mobile number or e-mail address to confirm the contact information.

The Prohibition of Obtaining Biometric Data Electronically

The Regulation prohibits operators and service providers to obtain biometric data of Applicants electronically by using an electronic pen or similar methods, save for Article 7, Article 8 of the Regulation and TS 13678 Electronic Identity Verification System standard (such as the statistical data exception, a two-dimensional figure of the Applicant).

Adopting similar approach in terms of biometric data, a previous decision of the Turkish Data Protection Board dated August 27, 2020 and numbered 2020/649[2], states that (i) the biometric signature is considered as biometric data which is stipulated as sensitive data under Law No. 6698, (ii)

[2] *See* https://www.kvkk.gov.tr/Icerik/6815/2020-649 (Last accessed on July 14, 2021).

thus the biometric signature can only be processed in case of obtaining explicit consent or if it is clearly prescribed by law, (iii) as the provisions under the Turkish Code of Obligations numbered 6098 do not meet the requirement of being prescribed by law, biometric signature cannot be processed without explicit consent. The decision of the Board prohibiting processing biometric signature without explicit consent is in parallel with the Regulation prohibiting obtaining biometric data electronically.

When comparing the Regulation and the European Union legislation (European Union Electronic Identity and Trust Services - "eIDAS Regulation" (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market)[3], eIDAS Regulation does not include provision specific to biometric data and define electronic signature broadly as it might cover biometric signature as well: As per Article 3-(10) of the eIDAS Regulation, *"electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign"*.

Data Security

Pursuant to the Regulation, the operators and service providers must take measures for storing of identity verification information of the Applicants by ensuring privacy, security and integrity of the transaction records. The operators and service providers are also responsible for taking necessary security measures for the video conference in identity verification through artificial intelligence or a representative.

Moreover, the transactions conducted within the scope of the Regulation must be recorded and, obtained data must be used solely for the purposes of identity verification of the Applicant and the administrative and judicial authorities' processes. As per Regulation, such data must be stored for the time as it is stipulated under relevant legislation.

The operators and service providers must take all technical and administrative measures under the relevant legislation, including Law on Electronic Communication numbered 5809 and Law No. 6698 as well as in accordance with the national and international standards.

Administrative Sanctions

In case of failure to comply with the Regulation, the administrative fines regulated under Law on Electronic Signature with number 5070 and the Regulation on the Information and Communication Technologies Authority's Administrative Sanctions will be applicable. Operators and service providers bear burden of proof in all transactions including the objections to the administrative or judicial processes.

Transition Period and Enforcement

The Regulation will enter into force on December 31, 2021. The burden of proof regarding the Transaction Documents including biometric signature will be on operators and service providers. Operators and service providers must take necessary measures in order to prevent the use of three-dimensional signature design. Within three months as of the entry into force of the Regulation, the operators and service providers are required to submit information indicated in the Regulation to the mobile electronic communication operators and e-Government information system.

[3] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN (Last accessed on July 26, 2021).

Conclusion

The Regulation introduces new method and standards for identity verification including using artificial intelligence as a new technological improvement in such processes. The principles defined under the Regulation are expected to increase the security of the processes in the electronic communication sector. Operators and service providers might prepare an action plan and take necessary measures and steps stipulated under the Regulation in order to comply with the Regulation within the transition period.

Article contact: Gönenç Gürkaynak, Esq. Email: gonenc.gurkaynak@elig.com

(First published by Mondaq on July 27, 2021)