May 2021

Greece: New digital KYC application and data protection implications

Greek citizens now have an important tool to save time and protect their personal data, as the platform 'Introduce yourself - KYC (Know Your Customer)' ('the Platform'), which has been designed and implemented by the Ministry of Digital Governance ('the Ministry') in the context of the Greek Government's initiative on digitising such bureaucratic procedures, was launched on May 6. Michalis Kosmopoulos and Panagiotis Tampoureas, Partner and Senior Associate respectively at DRAKOPOULOS, discuss this development and its data protection implications.

NeoLeo / Essentials collection / istockphoto.com

In the context of Law 4557/2018 on Prevention and Suppression of the Legalisation of Proceeds of Crime and Terrorist Financing (Incorporation of Directive 2018/843/EU) and Other Provisions ('the AML/CFT Law') and the corresponding Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, the platform enables citizens who have Greek Tax Identification Num-

ber and Taxisnet credentials to avoid an in-person visit to the bank and thus save time, as they will not have to collect and submit themselves, in hardcopy, the documents required for maintaining a bank account, as was the process until now. Such supporting documents include tax and financial related data, data related to their professional activity, as well as identification and contact details.

The Platform provides for an entirely digital and paperless process, in which the customer will not need to print anything at all. Therefore, all previously required copies of identity cards, settlement notes, utility bills, and payroll have been permanently eliminated from the process of updating the data. As soon as the user/customer reviews the accuracy of its data and grants its explicit and specific consent, credit and financial institutions will immediately gain access, through the Interoperability Centre of the Ministry, to the data required by AML/CFT Law for the verification of the customer's identity, as well as to their contact details, professional activity, and annual income data. The data will be obtained via primary information systems that are managed by the public sector and will be filled out on the platform.

Nevertheless, the digitisation of the process comes with enhanced obligations in the field of data protection and privacy for both the Ministry and the credit and financial institutions. By virtue of Ministerial Decision No. 9747/EE/2021 ('the Ministerial Decision'), which enacts the operation of the Platform, the participating parties are named as separate controllers and, therefore, incur all the obligations arising from the data protection framework (i.e. the General Data Protection Regulation (Regulation (EU) 2016/679) and Law 4624/2019 on the Personal Data Protection Authority, Implementing the General Data Protection Regulation (Regulation (EU) 2016/679 and Transposing into National Law Data Protection Directive with respect to Law Enforcement (Directive (EU) 2016/680) and other Provisions), including the individuals' right to be informed on the purposes and means of the processing. Besides updated privacy notices, the parties shall comply with the general data protection principles (transparency and data minimisation), demonstrate compliance through keeping updated records of processing activities, conduct a Data Protection Impact Assessment (if so required) and, finally, apply appropriate technical and organisational measures as safeguards for data security.

In this regard, the Ministerial Decision provides that the parties have the obligation to demonstrate compliance also through the application of the necessary technical and organisational measures (such as the encryption of the databases), by taking into consideration the nature and the means of the processing, and, at a minimum, implement access recording and monitoring, traceability, and protection of transferring data from data incidents and/or breaches. Considering these obligations, the financial institutions and/or organisations shall also keep a separate record of importing data for every user/customer.

In view of the compliance prerequisites set out in the paragraphs above, it is highly recommended that the participating parties be engaged into a data protection agreement, which will address issues like the appropriate technical and organisational measures to be applied, the exercise of the data subjects' rights (e.g. withdrawal of

consent), and the allocation of liability, so that a harmonised level of data protection be achieved among the participating institutions and the Ministry. In addition, the data protection agreement should also clarify the technicalities of the data exchange and, of course, the 'interoperability' of the parties with the platform.

For the time being, the procedure is still completely optional and, of course, any citizen who so wishes, can continue to provide the required documentation in the traditional physical way.

Michalis Kosmopoulos Partner mkosmopoulos@drakopoulos-law.com

Panagiotis Tampoureas Senior Associate ptampoureas@drakopoulos-law.com

DRAKOPOULOS, Athens