Data Protection in the Crypto and Fintech World

The processing of data to prevent and deter money laundering is of greater importance than usually is acknowledged by the regulators. IT solutions can help crypto and fintech companies to run their business in a controlled and transparent manner.

Crypto has unfortunately and completely unjustifiably become a curse word recently. Somehow it seems like all have forgotten that there is a growing industry built on crypto and other blockchain solutions where the Estonian economy is already involved. And that the risks associated with crypto can be successfully mitigated with solutions from the world of technology, the same world that created the blockchain in the first place.

Compliance with data protection requirements is supervised by the Estonian Data Protection Inspectorate. However, data protection requirements are not only to be found in the GDPR but also in other legislation, and in addition compliance with data protection rules arises in different licensing procedures. For example, when applying for a licence to provide a virtual currency service (a so-called crypto licence) or when applying for a credit institution licence the applicant will need to prove its capability to handle and process data.

But all these licensing procedures are carried out by other authorities than the Data Protection Inspectorate. They are being carried out by Estonian authorities such as the Estonian Financial Intelligence Unit (the FIU for short, for crypto) and the Estonian Financial Supervision and Resolution Authority (the FSA, for banking and investment type of licensing), and by the Estonian Tax and Customs Board (for gambling licenses). And so the question arises: Are all these different regulators competent to assess the compliance of the processing of personal data with all its requirements and the suitability of solutions for their purpose?

The starting point would be to clarify what purpose the data protection requirements fulfil. The modern world is digital in many fields, especially in the crypto and fintech field. Data, their processing, and the purposes for which they are processed have become more and more important. When handling different licence applications, the different regulators must pay attention to the technical and organisational capacity of the controllers in the processing of data, i.e., how data is processed. The regulator must be able to assess the applicant's technical and organisational capacity to process data and assess its risks.

Data protection serves several purposes such as the protection of natural persons on the one hand and the prevention of money laundering and terrorist financing on the other hand, and, in addition, helping to reduce the risk of harm. This is done through different obligations in the processing of personal data. For example, the data must be correct and complete. The data controller must also know, like with cash flow, where the data comes from, who delivers them, and why. In practice, that also provides an overview of whether there are risks anywhere else than the risk of non-compliance with data processing requirements.

Thereby, compliance is not only necessary from the point of view of supervision of data protection, but clear data processing also helps to mitigate the risks of the data controller itself. For example, the abovementioned principle which requires data to be correct and complete also helps to prevent fraud and thereby reduce the risk of potential harm. It is also difficult to claim damages in the event of harm if you do not even know if the information indicates who caused the harm or how it was caused.

Technology can be of great help here. This of course does not mean that any technological solution is an automatic magic wand that would confirm perfect compliance. However, depending on functionality and capabilities, AI, for example, can be applied to the processing of both personal data as well as other data in such a way that the data controller as a valuable information holder becomes the primary and largest tool in preventing money laundering and financing of terrorism.

Thus, the above objectives may not be so obvious in a situation where the FIU starts asking how the processing of personal data and the notification of data subjects are regulated in a company. Clarity could be created by the regulator by explaining to the applicant what solutions and measures a particular licensed operator should consider. This, in turn, requires strong supervisory competence extended to in-depth knowledge of data protection and understanding the functionality of different IT solutions.

LIISI JÜRGEN
ATTORNEY AT LAW,
PARTNER

(+372) 66 76 440
LIISI.JURGEN@NJORDLAW.EE