Fintechs must stay compliant in aftermath of Covid-19 (3/27/20)

Although Latvia is a European leader in P2P crediting, the fintech[1] industry has also suffered from the Covid-19 crisis. According to financial blogger Kristaps Mors, four Latvian online platforms have closed down or stopped paying money in recent months. He says if this tendency continues, Latvia might become famous as a fraud centre of this industry. We assume that these signals have reached the State Revenue Service and the National Data Office, who are carefully monitoring the business conducted in this industry to ensure that fintechs comply with statutory requirements.

It is crucial that fintechs comply with the requirements of the Anti Money Laundering and Counter Terrorism and Proliferation Financing Act ("AML") and the General Data Protection Regulation ("GDPR"). Although the inclusion of fintech services with other financial services under this legislation requires fintechs to carry out considerable (and mostly expensive) changes, the aims set by Europe in creating these requirements is to provide integrated data protection by default and to ensure that the provision of financial services is sustainable and competitive.

The European data supervisory authorities have also begun to actively monitor fintechs. For example, the Dutch data supervisory authority has boosted its fintech supervision efforts to make sure they are aware of personal privacy risks and comply with GDPR requirements. It is no secret that fintechs are processing not only customer payment details (when, where, what is purchased and how much is paid, creating certain perceptions or observations) but also supplier details. It is crucial that fintechs process this data carefully, with adequate security measures in place, and that data subjects are informed of the data processing done by fintechs.

We have put together a brief summary of key AML and GDPR requirements that each fintech has to meet when it comes to data processing in the EU/EEA regardless of whether they operate within or outside the EU/EEA.

It is important to note that AML is a special law in relation to GDPR. The AML definition is used as a descriptive term for preventing criminals from disguising illegally obtained funds as legitimate income.

The table below displays –

1. provisions in the Anti Money Laundering and Counter Terrorism and Proliferation Financing Act arising from Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU;
2. provisions arising from Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC ("PSD2"); and
3. provisions arising from GDPR.

GDPR requirements		Reference to Article in GDPR	Penalty
Background	• Applicable to all fintechs that carry out personal data processing in the EU/EEA regardless of whether they operate within or outside the EU/EEA. • Applicable also to data controllers that are not registered in the EU but are covered by EU enactments (e.g. foreign embassies). • The rights conferred by GDPR can be exercised by every person in the EU/EEA regardless of their nationality. • PSD2 mandates compliance with the basic rights of a data subject, including the right to privacy. • A fintech may appoint one responsible person to act as a point of contact between EU data subjects and fintechs outside the EU/EEA. • GDPR is applicable only to data on individuals. However, data on legal entities can include data on individuals, such as information on owners and board members. If a company has only one owner, then data on the company can also apply to its owner as an individual. • PSD2 allows consumers to use innovative services offered by fintechs as third-party service providers as long as they maintain strict data protection and security standards.		
Legal basis for processing	Fintechs process personal data based on a contract, a law, or their legitimate interests.	Article 6(1) (b), (c) and (f)	Up to €20 million or up to 4% of total worldwide turnover
	Fintechs may process personal data also on the basis of a data subject's consent under Article 6(1)(a) of GDPR. It is important not to confuse the consent under Article 94(2) of PSD2 with a data subject's consent under GDPR.		
Signing data processing agreements	Fintechs enter into data processing agreements and define their role in each data processing: fintechs may process data as independent controllers, as processors, or as joint controllers. Each situation requires an assessment of measures to be taken, including signing a data processing agreement.	Article 28	Up to €10 million or up to 2% of total worldwide turnover
Policies and procedures	Fintechs draw up a general data processing policy document which demonstrates that processing is done in accordance with GDPR.	Article 24(2)	Up to €10 million or up to 2% of total worldwide turnover
	Fintech websites make their cookies policy available to data subjects.	Articles 13, 14 and 25	Up to €20 million or up to 4% of total worldwide turnover
	Fintechs have procedures in place for reporting incidents to the supervisory authority within 72 hours after the company became aware of a breach.	Article 33(1)	Up to €10 million or up to 2% of total worldwide turnover
	A fintech's privacy statement relating to data processing is available to data subjects.	Articles 13 and 14	Up to €20 million or up to 4% of total worldwide turnover

(to be continued)

[1] Start-ups that use information technology to offer existing financial services at a better price and to offer novel technological solutions