Fintech jāievēro prasības arī pēc Covid-19 trieciena (2) (3/28/20)

Iepriekšējās Īsziņās publicētā raksta turpinājums.

GDPR regulējums		Atsauce uz pantu	Sods
Datu subjekta piekrišana	Datu subjekta piekrišana ir nepieciešama, ja *fintech* uzņēmums izmanto neobligātās sīkdatnes (piem., *Google Analytics* mājaslapas apmeklētības statistikas uzskaites sīkdatnes). No datu subjekta saņemtā piekrišana ir brīvprātīga un nepārprotama, ar tiesībām datu subjektam iebilst pret veikto datu apstrādi.	13., 14. un 25. pants	Līdz 20 miljoniem eiro vai līdz 4% no kopējā globālā apgrozījuma
Risku novērtēšana	*Fintech* uzņēmums veic risku novērtējumu un augsta riska datu apstrādes gadījumos veic arī ietekmes novērtējumu. Piemēram, ietekmes novērtējums jāveic tādai datu apstrādei, kuras pamatā ir profilēšana un automātiska lēmumu pieņemšana. Šie novērtējumi jāaktualizē pēc nepieciešamības.	35. pants	Līdz 10 miljoniem eiro vai līdz 2% no kopējā globālā apgrozījuma
	Fintech uzņēmums nodrošina, ka datu subjektam ir piešķirtas tiesības iebilst pret veikto profilēšanu vai automātisku lēmumu pieņemšanu.	22. panta (1)	Līdz 20 miljoniem eiro vai līdz 4% no kopējā globālā apgrozījuma
Droša datu apstrāde	*Fintech* uzņēmums ir ieviesis atbilstošus drošības pasākumus un tehniskos risinājumus. Piemēram, uzņēmums ievēro Eiropas Banku iestādes izdotos tehniskos standartus https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2 vai citus standartus (piemēram, ISO 27701:2019).	32. pants	Līdz 10 miljoniem eiro vai līdz 2% no kopējā globālā apgrozījuma
	Fintech uzņēmums stingri ievēro GDPR datu apstrādes principus (piemēram, glabā personas datus ne ilgāk kā nepieciešams vai tik ilgi, cik noteikts normatīvajos aktos). *Fintech* uzņēmums neizmanto datus, nepiekļūst tiem un neuzglabā tos nekādos citos nolūkos kā vienīgi, lai sniegtu, piemēram, konta informācijas pakalpojumu, ko nepārprotami lūdzis maksājumu pakalpojumu lietotājs.	5. pants	Līdz 20 miljoniem eiro vai līdz 4% no kopējā globālā apgrozījuma
	Fintech uzņēmums izstrādā IT dokumentu, kas nosaka vadlīnijas informācijas resursu drošībai un risku analīzei, informācijas resursu fizisko un loģisko aizsardzību, informācijas sistēmu ekspluatāciju un rīcību drošības incidentu gadījumā.	24. panta (2) un 32. pants	Līdz 10 miljoniem eiro vai līdz 2% no kopējā globālā apgrozījuma
	Izstrādājot regulatīvos tehniskos standartus par autentificēšanu un saziņu, sistemātiski jāizvērtē un jāņem vērā privātuma aspekts, lai apzinātu riskus, kas saistīti ar katru no pieejamām tehniskām iespējām, un to, kādus aizsarglīdzekļus varētu ieviest, lai datu aizsardzības apdraudējumu samazinātu līdz minimumam.	32. pants	Līdz 10 miljoniem eiro vai līdz 2% no kopējā globālā apgrozījuma
Trešās valstis un tajās izvietotie IS serveri	*Fintech* uzņēmumam ir pienākums informēt datu subjektus par to, ka dati var tikt apstrādāti ārpus ES/EEZ (piemēram, datu subjektu informēšanas pienākums komandējumos, rezervējot viesnīcu vai aviobiļeti, pasūtot vīzu).	13., 14. un 44. pants	Līdz 20 miljoniem eiro vai līdz 4% no kopējā globālā apgrozījuma
	Fintech uzņēmums ievieš papildu drošības prasības, ja dati tiek sūtīti ārpus ES/EEZ vai ja IS serveri atrodas ārpus ES/EEZ.	44. pants	Līdz 20 miljoniem eiro vai līdz 4% no kopējā globālā apgrozījuma
Īpašo kategoriju personas datu apstrāde	Nejaukt: GDPR īpašo kategoriju dati nav PSD2 "sensitīvie maksājumu dati"!		
	Ja *fintech* uzņēmums apstrādā īpašo kategoriju datus, par šo datu apstrādi jāprasa datu subjekta piekrišana.	9. pants	Līdz 20 miljoniem eiro vai līdz 4% no kopējā globālā apgrozījuma
	Fintech uzņēmums drīkst apstrādāt informāciju par datu subjekta sodāmību tikai tad, ja šo apstrādi paredz normatīvie akti.	10. pants	Līdz 20 miljoniem eiro vai līdz 4% no kopējā globālā apgrozījuma
Mācību organizēšana	*Fintech* uzņēmums veic apstrādes darbībās iesaistīto darbinieku regulāru informēšanu un apmācību.	39. panta pirmās daļas (b)	Līdz 10 miljoniem eiro vai līdz 2% no kopējā globālā apgrozījuma
Ziņošana par incidentu	72 stundu laikā no incidenta atklāšanas brīža	33. pants	Līdz 10 miljoniem eiro vai līdz 2% no kopējā globālā apgrozījuma

(nobeigums – nākamajās Īsziņās)