EIROPAS
KOMISIJA

Briselē, 3.4.2023.
COM(2023) 275 final

KOMISIJAS ZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

par pirmo pārskatīšanu attiecībā uz to, kā darbojas lēmums par aizsardzības līmeņa pietiekamību Japānā

{SWD(2023) 75 final}

KOMISIJAS ZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

par pirmo pārskatīšanu attiecībā uz to, kā darbojas lēmums par aizsardzības līmeņa pietiekamību Japānā

1. PIRMĀ PĀRSKATĪŠANA: PRIEKŠVĒSTURE, SAGATAVOŠANA UN PROCESS

Eiropas Komisija 2019. gada 23. janvārī pieņēma lēmumu saskaņā ar Regulas (ES) 2016/679 (VDAR)[1] 45. pantu, kurā konstatēja, ka Japāna nodrošina pietiekamu aizsardzības līmeni personas datiem, kas no Eiropas Savienības tiek nosūtīti uzņēmumiem, kuri apstrādā personas informāciju[2] Japānā[3]. Tā rezultātā datu nosūtīšana no ES privātiem operatoriem Japānā var notikt bez papildu prasībām[4].

Komisijas lēmums par aizsardzības līmeņa pietiekamību attiecas uz Japānas Likumu par personas informācijas aizsardzību (*APPI*), kas papildināts ar Papildu noteikumiem, kuri tika pieņemti, lai pārvarētu atsevišķas būtiskas atšķirības starp *APPI* un VDAR[5]. Šie papildu aizsardzības pasākumi pastiprina, piemēram, sensitīvo datu aizsardzību (paplašinot to personas informācijas kategoriju loku, kas tiek uzskatītas par sensitīviem datiem), individuālo tiesību īstenošanu (precizējot, ka individuālās tiesības var īstenot arī attiecībā uz personas datiem, kas tiek saglabāti īsāku laiku nekā seši mēneši, un tas tobrīd nebija atbilstīgi *APPI* prasībām[6]) un nosacījumus, saskaņā ar kuriem ES datus var nosūtīt tālāk no Japānas uz citu trešo valsti[7]. Papildu noteikumi ir saistoši Japānas operatoriem, un to īstenošanu var panākt neatkarīga datu aizsardzības iestāde — Personas informācijas aizsardzības komisija (*PPC*), kā arī ES privātpersonas, tieši vēršoties Japānas tiesās[8].

Turklāt Japānas valdība sniedza Komisijai oficiālus apliecinājumus, garantijas un saistības attiecībā uz ierobežojumiem un aizsardzības pasākumiem, kas saistīti ar Japānas valsts iestāžu piekļuvi personas datiem un to izmantošanu krimināltiesību aizsardzības un valsts

---

1 OV L 119, 4.5.2016., 1. lpp.

2 Likuma par personas informācijas aizsardzību (*Act on the Protection of Personal Information, APPI*) redakcijā, kas bija spēkā attiecīgā lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas laikā, šis jēdziens tika attiecināts uz "uzņēmēju, kas izmanto personas informāciju" ("*personal information handling business operator*", *PIHBO*). Uzņēmums, kas apstrādā personas informāciju, ir definēts grozītā *APPI* 16. panta 2. punktā kā "persona, kas darījumdarbībā izmanto personas informācijas datubāzi vai līdzvērtīgu informāciju", izņemot valdību un administratīvās iestādes gan centrālā, gan vietējā līmenī. Jēdziens "darījumdarbība" atbilstoši *APPI* ir ļoti plašs un ietver ne tikai peļņas, bet arī bezpeļņas darbības, ko īsteno visu veidu organizācijas un privātpersonas. Turklāt "izmantošana darījumdarbībā" attiecas arī uz personas informāciju, ko neizmanto operatora (ārējās) komercattiecībās, bet izmanto iekšēji, piemēram, darbinieku datu apstrādē. Sk. minētā lēmuma 32., 33. un 34. apsvērumu.

3 Komisijas Īstenošanas lēmums (ES) 2019/419 (2019. gada 23. janvāris), kas pieņemts saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679, par personas datu pietiekamu aizsardzību Japānā atbilstoši Likumam par personas informācijas aizsardzību (OV L 76, 19.3.2019., 1. lpp.).

4 Sk. VDAR 45. pantu un lēmuma 5. apsvērumu.

5 Sk. lēmuma I pielikumu.

6 Tikmēr, pieņemot *APPI* 2020. gada grozījumu, tika pārskatīta "uzņēmuma rīcībā esošo personas datu" definīcija, lai vairs netiktu izslēgti tie personas dati, kurus "ir paredzēts dzēst" sešu mēnešu laikā (grozītā *APPI* 16. panta 4. punkts). *APPI* redakcijā, kas bija spēkā laikā, kad tika pieņemts minētais lēmums par aizsardzības līmeņa pietiekamību, šis jēdziens tika attiecināts uz "saglabātajiem personas datiem".

7 Lēmuma 26., 31., 43., 49.–51., 63., 68., 71., 76.–79. un 101. apsvērums.

8 Lēmuma 15. apsvērums.

drošības nolūkos, paskaidrojot, ka šāda apstrāde nepārsniedz to, kas ir nepieciešams un samērīgs, un ka attiecībā uz to tiek īstenota neatkarīga uzraudzība un efektīvi tiesiskās aizsardzības mehānismi[9]. Tiesiskās aizsardzības mehānismi šajā jomā ietver īpašu strīdu izšķiršanas procedūru, ko administrē un uzrauga *PPC* un kas tika izveidota tām ES privātpersonām, kuru personas dati tiek nosūtīti, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību[10].

Laikā, kad tika pieņemts Komisijas lēmums par aizsardzības līmeņa pietiekamību, Japāna pieņēma līdzīgu lēmumu par datu nosūtīšanu uz ES, un tas radīja pasaulē lielāko brīvas datu plūsmas zonu, kuras pamatā ir augsts datu aizsardzības līmenis[11]. Šie savstarpējie lēmumi par aizsardzības līmeņa pietiekamību papildina un pastiprina priekšrocības, ko nodrošina ES un Japānas Ekonomisko partnerattiecību nolīgums (EPN), kas stājās spēkā 2019. gada februārī[12], un Stratēģiskās partnerības nolīgums[13], kas tika apspriests vienlaikus ar EPN. Abu pušu uzņēmumi gūst labumu no sinerģijas starp savstarpējiem lēmumiem par aizsardzības līmeņa pietiekamību un EPN, jo datu brīvas plūsmas iespēja starp ES un Japānu vēl vairāk atvieglo komerciālo apmaiņu un rada lielas iespējas darījumdarbībā, nodrošinot privileģētu savstarpējo piekļuvi tirgum. Tā arī rada svarīgu precedentu, skaidri parādot, ka digitālajā laikmetā augstu privātuma standartu veicināšana nav nošķirama no starptautiskās tirdzniecības atvieglošanas.

Kopš lēmumu par aizsardzības līmeņa pietiekamību pieņemšanas ES un Japāna kā līdzīgi domājoši partneri ir vēl vairāk pastiprinājušas sadarbību digitālajos jautājumos kopumā un jo īpaši attiecībā uz datu plūsmām. Divpusējā līmenī tas jo īpaši izpaudās, 2022. gada maijā noslēdzot Digitālo partnerību[14] un 2022. gada oktobrī uzsākot sarunas, lai iekļautu EPN disciplīnas par pārrobežu datu plūsmām[15], kas vēl vairāk uzlabos sinerģiju ar abpusējas aizsardzības līmeņa pietiekamības pasākumu. Daudzpusējā līmenī ES un Japāna ir apvienojušas centienus, lai veicinātu, nostiprinātu un plaši izplatītu jēdzienu "datu brīva plūsma, pamatojoties uz uzticību", ko ierosināja bijušais premjerministrs Sindzo Abe, citstarp cieši sadarbojoties G7, Pasaules Tirdzniecības organizācijas (saistībā ar Kopīgo paziņojumu

---

9 Lēmuma 113.–170. apsvērums un II pielikums.

10 Lēmuma 141.–144., 149. un 169. apsvērums.

11 Sk. pēc šo sarunu noslēguma izdoto paziņojumu presei, kas pieejams vietnē https://ec.europa.eu/commission/presscorner/detail/lv/IP_18_4501.

12 Padomes Lēmums (ES) 2018/1907 (2018. gada 20. decembris) par to, lai noslēgtu Ekonomisko partnerattiecību nolīgumu starp Eiropas Savienību un Japānu (OV L 330, 27.12.2018., 1. un 2. lpp.). EPN mazina tirdzniecības šķēršļus, ar kuriem saskaras Eiropas uzņēmumi, eksportējot uz Japānu, un palīdz šiem uzņēmumiem sekmīgāk konkurēt šajā tirgū.

13 Stratēģiskās partnerības nolīgums starp Eiropas Savienību un tās dalībvalstīm, no vienas puses, un Japānu, no otras puses (SPN) (OV L 216, 24.8.2018., 4.–22. lpp.). SPN nodrošina juridisku satvaru tam, lai turpmāk attīstītu jau esošās ilglaicīgās un spēcīgās partnerattiecības starp Savienību, tās dalībvalstīm un Japānu visdažādākajās jomās, ieskaitot politisko dialogu, enerģētiku, transportu, cilvēktiesības, izglītību, zinātni un tehnoloģijas, tiesiskumu, patvērumu un migrāciju.

14 Pieejama vietnē https://www.consilium.europa.eu/media/56091/%E6%9C%80%E7%B5%82%E7%89%88-jp-eu-digital-partnership-clean-final-docx.pdf. Digitālā partnerība veido forumu, kas nodrošinās politisku vadību un stimulus, kopīgi izstrādājot digitālās tehnoloģijas tādās jomās kā drošs 5G tīkls, "virs 5G" / 6G tehnoloģijas, droši un ētiski mākslīgā intelekta lietojumi vai globālo piegādes ķēžu noturība pusvadītāju nozarē.

15 Sk., piem., https://policy.trade.ec.europa.eu/news/eu-and-japan-start-negotiations-include-rules-cross-border-data-flows-their-economic-partnership-2022-10-07_en.

par iniciatīvu e-komercijas jomā) un Ekonomiskās sadarbības un attīstības organizācijas (ESAO) ietvaros. ESAO ietvaros intensīvā sadarbība starp ES un Japānu šajos jautājumos bija īpaši svarīga, lai pirmo reizi starptautiskā līmenī pieņemtu kopīgus principus par valdības piekļuvi privātā sektora rīcībā esošiem personas datiem[16]. Visas šīs dažādās darba plūsmas lielākā vai mazākā mērā balstījās uz kopīgām vērtībām un prasībām, kas ir ES un Japānas abpusējas aizsardzības līmeņa pietiekamības pasākuma pamatā.

Lai regulāri pārbaudītu, vai konstatējumi lēmumā par aizsardzības līmeņa pietiekamību joprojām ir faktiski un juridiski pamatoti, Komisijai ir jāveic periodiska pārskatīšana un jāziņo par iznākumu Eiropas Parlamentam un Padomei[17]. Ar šo ziņojumu, kas aptver visus minētā lēmuma darbības aspektus, tiek noslēgta pirmā periodiskā pārskatīšana. No Japānas puses šajā pārskatīšanā piedalījās pārstāvji no *PPC*, Iekšlietu un sakaru ministrijas, Tieslietu ministrijas, Aizsardzības ministrijas un Valsts policijas iestādes. ES delegācijā papildus Eiropas Komisijas locekļiem bija iekļauti arī trīs pārstāvji, ko izraudzījusies Eiropas Datu aizsardzības kolēģija (EDAK).

Pārskatīšanas sanāksme, kurā piedalījās abas delegācijas, notika 2021. gada 26. oktobrī, un gan pirms, gan pēc tās vairākkārt tika veikta apmaiņa ar informāciju. Nolūkā sagatavot šo pārskatīšanu Komisija savāca no Japānas iestādēm informāciju par šā lēmuma darbību, jo īpaši par Papildu noteikumu īstenošanu. Komisija arī meklēja informāciju, kas sniegta publiskos avotos un ko snieguši vietējie eksperti, par lēmuma darbību un attiecīgām norisēm saistībā ar Japānas tiesību aktiem un praksi gan attiecībā uz datu aizsardzības noteikumiem, kas piemērojami privātiem operatoriem, gan attiecībā uz valdības piekļuvi. Pēc minētās pārskatīšanas sanāksmes Komisija un *PPC* vairākkārt apmainījās ar informāciju, lai īstenotu turpmākus pasākumus šajā sanāksmē apspriesto jautājumu kontekstā, jo īpaši nolūkā risināt jautājumus, kas radās, ieviešot *APPI* noteikumus par pseidonimizētu personas informāciju.

2. GALVENIE KONSTATĒJUMI

Detalizēti konstatējumi par to, kā darbojas visi lēmumā par aizsardzības līmeņa pietiekamību noteiktie aspekti, ir izklāstīti Komisijas dienestu darba dokumentā (SWD(2023) 75), kas pievienots šim ziņojumam.

Pirmā pārskatīšana parādīja, ka kopš savstarpējo lēmumu par aizsardzības līmeņa pietiekamību pieņemšanas ES un Japānas datu aizsardzības regulējumi ir vēl vairāk tuvinājušies. *APPI* tika grozīts divas reizes: 2020. gada 5. jūnijā, pieņemot *2020. gada Likumu par grozījumiem Personas informācijas aizsardzības likumā* (*APPI* 2020. gada grozījums), kas stājās spēkā 2022. gada 1. aprīlī[18]; un 2021. gada 12. maijā, pieņemot *Likumu par saistīto tiesību aktu satvaru digitālās sabiedrības veidošanai* (*APPI* 2021. gada

[16] ESAO 2022. gada 14. decembra Deklarācija par valdības piekļuvi privātā sektora uzņēmumu rīcībā esošiem personas datiem.

[17] Lēmuma 180.–183. apsvērums un 3. panta 4. punkts.

[18] Tulkojums angļu valodā ir pieejams vietnē https://www.ppc.go.jp/files/pdf/APPI_english.pdf.

grozījums)[19]. Lai atspoguļotu šos grozījumus, pēc apspriešanās ar Komisiju tika pielāgoti arī Papildu noteikumi.

Pateicoties šiem grozījumiem, ES un Japānas sistēmas ir vēl vairāk tuvinājušās, jo īpaši pastiprinot datu drošības pienākumus (ieviešot pienākumu ziņot par datu aizsardzības pārkāpumiem), datu subjekta tiesības (jo īpaši piekļuves tiesības un tiesības iebilst) un aizsardzību, kas tiek nodrošināta datu nosūtīšanas gadījumā (papildu informēšanas un uzraudzības prasību veidā, citstarp sniedzot informāciju par iespējamiem riskiem saistībā ar valdības piekļuvi galamērķa valstī). Šajā kontekstā īpaši ievērības cienīgs ir tas, ka daži papildu aizsardzības pasākumi, kas paredzēti Papildu noteikumos attiecībā uz personas datiem, kuri nāk no ES, t. i., attiecībā uz šo datu saglabāšanu un nosacījumiem, sniedzot informētu piekrišanu pārrobežu nosūtīšanai, tiek iekļauti *APPI*, tādējādi padarot tos vispārēji piemērojamus visiem personas datiem neatkarīgi no to izcelsmes vai iegūšanas vietas[20].

Vēl viens svarīgs notikums, kuru Komisija vērtē atzinīgi, ir *APPI* pārveide par visaptverošu datu aizsardzības regulējumu, kas aptver gan uz privāto, gan publisko sektoru un ko uzrauga tikai *PPC*[21]. Šāda Japānas datu aizsardzības regulējuma un *PPC* pilnvaru papildu nostiprināšana var veicināt to, ka lēmuma par aizsardzības līmeņa pietiekamību tvērums tiek paplašināts arī ārpus komerciālās apmaiņas, attiecinot to uz datu sūtījumiem, kas pašlaik no tā ir izslēgti, piemēram, regulatīvās sadarbības un pētniecības jomā.

Pirmajā pārskatīšanā liela uzmanība tika pievērsta arī jaunajiem noteikumiem par "pseidonimizētas personas informācijas" izveidi un izmantošanu, kas tika ieviesti ar *APPI* 2020. gada grozījumu[22]. Šo jauno noteikumu mērķis būtībā ir atvieglot personas informācijas (iekšēju) izmantošanu uzņēmumos, kas apstrādā personas informāciju galvenokārt statistikas nolūkos (piem., identificējot tendences un modeļus, lai nodrošinātu turpmākas darbības, arī pētniecību). Pārskatīšanas sanāksme un tai sekojošā informācijas apmaiņa starp Komisiju un *PPC* ļāva precizēt šo jauno noteikumu interpretāciju un piemērošanu. Šo diskusiju rezultātā, lai skaidrāk atspoguļotu minēto jauno noteikumu paredzēto piemērošanu un tādējādi nodrošinātu juridisko noteiktību un pārredzamību, Papildu noteikumi 2023. gada 15. martā tika grozīti divējādi[23]. Pirmkārt, Papildu noteikumos ir paredzēts, ka šādu informāciju drīkst izmantot tikai statistikas nolūkos, kas definēti kā statistisku aptauju apstrāde vai statistisku rezultātu apkopošana, lai iegūtu apkopotus datus, un ka apstrādes rezultāts netiks izmantots, lai pamatotu pasākumus vai lēmumus, kas attiecas uz kādu konkrētu privātpersonu. Otrkārt,

---

19 Tulkojums angļu valodā ir pieejams vietnē https://www.japaneselawtranslation.go.jp/ja/laws/view/4241.

20 Grozītā *APPI* 16. panta 4. punkts un 28. panta 2. punkts.

21 Jo īpaši ar *APPI* 2021. gada grozījumu tiek apvienots *APPI*, Likums par administratīvo iestāžu rīcībā esošās personas informācijas aizsardzību, Likums par reģistrēto administratīvo iestāžu rīcībā esošās personas informācijas aizsardzību utt., izveidojot vienu vienotu datu aizsardzības likumu, ko piemēro gan privātiem uzņēmumiem, gan valsts iestādēm, vienlaikus attiecīgi paplašinot *PPC* jurisdikciju. Šis grozījums stājās spēkā 2023. gada 1. aprīlī, bet atsevišķas tā daļas stājās spēkā jau 2021. gada 1. septembrī un 2022. gada 1. aprīlī.

22 Pseidonimizēta personas informācija grozītajā *APPI* ir definēta kā informācija attiecībā uz privātpersonu, kuru var "sagatavot tā, lai nebūtu iespējams identificēt konkrētu personu, ja vien tā netiek salīdzināta ar citu informāciju", izmantojot pasākumus, kas noteikti likumā un Izpildes noteikumos. Sk. grozītā *APPI* 16. panta 5. punktu un 41. pantu.

23 Pārskatītos Papildu noteikumus *PPC* pieņēma 2023. gada 15. martā, un tie stājās spēkā 2023. gada 1. aprīlī.

tajos ir skaidri norādīts, ka pseidonimizēta personas informācija, kas sākotnēji saņemta no ES, vienmēr tiks uzskatīta par personas informāciju saskaņā ar *APPI*, lai nodrošinātu, ka to datu aizsardzības nepārtrauktība, kas atzīti par personas datiem saskaņā ar VDAR, netiek apdraudēta nosūtīšanas laikā, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību[24].

Attiecībā uz datu aizsardzības pasākumu ieviešanu praksē Komisija atzinīgi vērtē dažādas *PPC* veiktās darbības. Tās ietver atjauninātu pamatnostādņu pieņemšanu, arī attiecībā uz datu starptautisku nosūtīšanu. Komisija norāda, ka šīs pamatnostādnes varētu precizēt, lai tajās tiktu pievērsta uzmanība arī īpašajām prasībām, kuras saskaņā ar Papildu noteikumiem piemēro no Savienības saņemto personas datu tālākai nosūtīšanai ārpus Japānas, citstarp — kā izriet no 4. papildu noteikuma un kā paskaidrots lēmumā par aizsardzības līmeņa pietiekamību[25] — izslēdzot tālāku nosūtīšanu, pamatojoties uz *APEC* Pārrobežu privātuma noteikumu (*CBPR*) sertifikācijas shēmu. Turklāt, lai gan *PPC* ir paskaidrojusi, ka *PHIBO* veic savu sākotnēji no ES saņemto datu tālāku nosūtīšanu, "noslēdzot līgumu, kas saista saņēmēju, liekot viņam veikt pasākumus, ar kuriem nodrošina aizsardzības nepārtrauktību", *PPC* pašlaik nesniedz norādījumus — ne kā pamatnostādnes, ne arī kā datu aizsardzības līgumu paraugus — par to "līdzvērtīgo pasākumu" (aizsargpasākumu) ieteicamo saturu, kurus izmanto attiecībā uz datu starptautisku nosūtīšanu. Šādi papildu precizējumi, kas varētu balstīties uz informācijas un paraugprakses apmaiņu starp *PPC* un Komisiju, varētu būt sevišķi noderīgi, jo attiecas uz aspektiem, kas īpaši svarīgi uzņēmumiem, kuri darbojas abās jurisdikcijās.

Attiecībā uz uzraudzību un izpildes panākšanu Komisija norāda, ka laikposmā pēc lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas *PPC* ir vairāk izmantojusi savas pilnvaras sniegt norādījumus un padomus (*APPI* 147. pants), nevis savas piespiedu pilnvaras, piemēram, izdot saistošus rīkojumus (*APPI* 148. pants). *PPC* arī ir ziņojusi, ka līdz šim nav saņemta neviena sūdzība par Papildu noteikumu neievērošanu un ka pēc *PPC* iniciatīvas par šiem jautājumiem nav veikta neviena izmeklēšana. Tomēr pārskatīšanas sanāksmē *PPC* paziņoja, ka apsver iespēju pēc savas iniciatīvas veikt izlases veida pārbaudes, lai nodrošinātu Papildu noteikumu ievērošanu. Komisija atzinīgi vērtē minēto paziņojumu, jo uzskata, ka šādas izlases veida pārbaudes būtu ļoti svarīgas, lai garantētu, ka Papildu noteikumu (iespējamie) pārkāpumi tiek novērsti, konstatēti un atrisināti, tādējādi nodrošinot šo noteikumu efektīvu ievērošanu. Tā kā ar 2020. un 2021. gada *APPI* grozījumiem ir nostiprinātas *PPC* uzraudzības pilnvaras, šādas izlases veida pārbaudes varētu būt daļa no vispārējiem centieniem paplašināt minēto pilnvaru izmantošanu.

Visbeidzot, Komisija ļoti atzinīgi vērtē īpašu kontaktpunktu izveidi ES privātpersonām, kurām ir jautājumi vai bažas par savu personas datu apstrādi Japānā, neatkarīgi no tā, vai šo apstrādi veic komerciālie operatori (Uzziņu līnija) vai valsts iestādes (Sūdzību mediācijas līnija). Vienlaikus Komisija atzīmē, ka Uzziņu līnijas tīmekļa vietnē ir norādīts, ka tā ir pieejama "tikai japāņu valodā", un tas, iespējams, atturēs ES privātpersonas no šīs iespējas

[24] Tas izslēdz grozītā *APPI* 42. panta piemērošanu, kurā paredzēti tikai ierobežota skaita drošības pasākumi attiecībā uz pseidonimizētu personas informāciju, kas netiek uzskatīta par personas informāciju.

[25] Sk. lēmuma 79. apsvērumu.

izmantošanas, lai gan *PPC* ir paskaidrojusi, ka principā ir pieejama arī palīdzība angļu valodā. Komisija izprot, ka *PPC* apsvērs, kādā veidā atvieglot šādu kontaktpunktu pieejamību eiropiešiem, citstarp precizējot minēto jautājumu.

3. SECINĀJUMS

Balstoties uz vispārējiem konstatējumiem, kas izdarīti šīs pirmās pārskatīšanas ietvaros, Komisija secina, ka Japāna joprojām nodrošina pietiekamu aizsardzības līmeni personas informācijai no Eiropas Savienības tajos personas informācijas apstrādes uzņēmumos Japānā, uz kuriem attiecas *APPI*, ko papildina Papildu noteikumi, kā arī oficiālie apliecinājumi, garantijas un saistības, kas ietvertas lēmuma II pielikumā. Šajā kontekstā Komisijas dienesti atzīst un ļoti augstu novērtē lielisko sadarbību ar Japānas iestādēm (jo īpaši ar *PPC*) pārskatīšanas gaitā.

Ņemot vērā šādu pārskatīšanas iznākumu, saskaņā ar lēmuma par aizsardzības līmeņa pietiekamību 181. apsvērumu Komisija uzskata, ka turpmāk pārskatīšanā nav jāsaglabā divu gadu cikls un ir lietderīgi pāriet uz četru gadu ciklu atbilstīgi VDAR 45. panta 3. punktam. Komisija attiecīgi apspriedīsies par šo jautājumu ar komiteju, kas izveidota saskaņā ar VDAR 93. panta 1. punktu[26].

Vienlaikus atsevišķu Japānas regulējuma aspektu nostiprināšana varētu veicināt *APPI* un Papildu noteikumos noteikto aizsargpasākumu turpmāku uzlabošanu. Tālab Komisija sniedz šādus ieteikumus.

1. Komisija atzinīgi vērtē un mudina vēl plašāk izmantot *PPC* plānotās izlases veida pārbaudes, lai nodrošinātu Papildu noteikumu ievērošanu. Komisija uzskata, ka šādas izlases veida pārbaudes būtu ļoti svarīgas, lai garantētu, ka Papildu noteikumu (iespējamie) pārkāpumi tiek konstatēti un novērsti, tādējādi nodrošinot šo noteikumu efektīvu ievērošanu.

2. Komisija atzinīgi vērtē to, ka *PPC* ir publicējusi atjauninātas pamatnostādnes par datu starptautisku nosūtīšanu, jo tās uzlabos *APPI* noteikumu pieejamību par šo tēmu un padarīs tos ērtāk lietojamus. Šajās pamatnostādnēs (vai citos norādījumu materiālos) attiecīgā gadījumā būtu jāizskaidro arī īpašās prasības, kas izriet no Papildu noteikumiem, citstarp attiecībā uz *APEC CBPR* sistēmas sertifikācijas shēmas izslēgšanu, kad tiek veikta no ES sākotnēji saņemto personas datu tālāka nosūtīšana.

3. Pārskatīšanas laikā tika apspriests, kā varētu nodrošināt, lai *PPC* Uzziņu līnija un Mediācijas līnija, kas paredzēta privātpersonu jautājumiem un sūdzībām, būtu pieejamāka ārzemniekiem. Tādēļ būtu svarīgi īpašajā tīmekļa vietnē norādīt, ka principā ir pieejama palīdzība angļu valodā.

Pārskatīšana arī ļāva identificēt iespējamās turpmākās sadarbības jomas. Kā jau norādīts, *PPC* pašlaik nesniedz norādījumus — ne kā pamatnostādnes, ne arī kā datu aizsardzības līgumu paraugus — par to "līdzvērtīgo pasākumu" (aizsargpasākumu) ieteicamo saturu,

[26] Sk. lēmuma 181. apsvērumu.

kurus izmanto attiecībā uz datu starptautisku nosūtīšanu. Ņemot vērā paraugklauzulu arvien pieaugošo nozīmi un to potenciālu kļūt par globālu datu nosūtīšanas instrumentu, kā atzinušas, piemēram, G7 valstis[27] un ESAO[28], Komisija ir izrādījusi interesi veidot turpmāku sadarbību ar Japānu šādu klauzulu izstrādē. Lēmuma par aizsardzības līmeņa pietiekamību tvēruma paplašināšana, attiecinot to ne tikai uz datu nosūtīšanu starp komerciālajiem operatoriem, ir vēl viena joma, kuru Komisija plāno izpētīt kopā ar *PPC*.

Komisija arī turpmāk stingri uzraudzīs Japānas datu aizsardzības regulējumu un reālo praksi. Šajā jomā tā vēlas turpināt informācijas apmaiņu ar Japānas iestādēm par norisēm, kas attiecas uz lēmumu[29], kā arī vēl vairāk nostiprināt sadarbību starptautiskā līmenī laikā, kad pieaug pieprasījums pēc globāliem standartiem attiecībā uz privātumu un datu plūsmām.

[27] Sk. ESAO Digitālās pārveides rīkkopu "Privātuma un datu aizsardzības regulējumu savstarpējā savietojamība" (pieejama vietnē https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf), 18. lpp.

[28] Sk. Ministru deklarācijas, kas pieņemta G7 valstu digitālo ministru sanāksmē 2022. gada 11. maijā, 1. pielikumu ("G7 rīcības plāns, kā veicināt datu brīvu plūsmu, pamatojoties uz uzticību"), kura sadaļā "Balstoties uz kopīgām iezīmēm, veicināt sadarbspēju nākotnē" ir dota atsauce uz "arvien plašāk izplatīto praksi, piem., standartizētām līgumu klauzulām".

[29] Sk. lēmuma 177. apsvērumu, saskaņā ar kuru no Japānas iestādēm tiek gaidīts, ka tās informēs Komisiju par būtiskām norisēm saistībā ar šo lēmumu, gan attiecībā uz personas datu apstrādi, ko veic uzņēmumu operatori, gan attiecībā uz ierobežojumiem un garantijām, kas piemērojamas, kad publiskās iestādes piekļūst personas datiem.