II

*(Nezakonodavni akti)*

# ODLUKE

## PROVEDBENA ODLUKA KOMISIJE (EU) 2019/419

**od 23. siječnja 2019.**

**u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća o primjerenosti zaštite osobnih podataka u Japanu na temelju Zakona o zaštiti osobnih informacija**

*(priopćeno pod brojem dokumenta C(2019) 304)*

**(Tekst značajan za EGP)**

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) („GDPR") [1], a posebno njezin članak 45. stavak 3.,

nakon savjetovanja s Europskim nadzornikom za zaštitu podataka,

### 1. UVOD

(1) Uredbom (EU) 2016/679 utvrđuju se pravila za prijenos osobnih podataka od voditelja obrade ili izvršitelja obrade u Europskoj uniji trećim zemljama i međunarodnim organizacijama, u mjeri u kojoj je takav prijenos obuhvaćen njezinim područjem primjene. Pravila o međunarodnom prijenosu osobnih podataka utvrđena su u poglavlju V. te Uredbe, točnije u člancima od 44. do 50. Protok osobnih podataka u zemlje izvan Europske unije i iz njih potreban je za proširenje međunarodne suradnje i međunarodne trgovine, a pritom se ne smije ugroziti postojeća razina zaštite osobnih podataka u Europskoj uniji.

(2) U skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 Komisija može putem provedbenog akta odlučiti da treća zemlja, područje, ili jedan ili više određenih sektora unutar treće zemlje, ili međunarodna organizacija osigurava primjerenu razinu zaštite. Pod tim se uvjetom prijenos osobnih podataka toj trećoj zemlji, području, sektoru ili međunarodnoj organizaciji može obavljati bez potrebe za daljnjim odobrenjima, kako je predviđeno člankom 45. stavkom 1. i uvodnom izjavom 103. Uredbe.

(3) Prema članku 45. stavku 2. Uredbe (EU) 2016/679 donošenje odluke o primjerenosti mora se temeljiti na sveobuhvatnoj analizi pravnog poretka treće zemlje, i kad je riječ o pravilima koja se primjenjuju na uvoznike podataka i o ograničenjima i zaštitnim mjerama u pogledu pristupa javnih tijela osobnim podacima. Procjenom se mora utvrditi jamči li predmetna treća zemlja razinu zaštite koja je „u načelu istovjetna" onoj koja je osigurana u Europskoj uniji (uvodna izjava 104. Uredbe (EU) 2016/679). Prema objašnjenju Suda Europske unije, to ne zahtijeva istovjetnu razinu zaštite [2]. Konkretno, pravna sredstva kojima se koristi predmetna treća zemlja mogu se razlikovati od onih koja se primjenjuju u Europskoj uniji, pod uvjetom da se u praksi pokažu djelotvornima za osiguranje primjerene razine zaštite [3]. Prema tome, standard primjerenosti ne podrazumijeva

[1] SL L 119, 4.5.2016., str. 1.
[2] Predmet C-362/14, *Maximillian Schrems* protiv *Data Protection Commissioner* (dalje u tekstu „*Schrems*"), EU:C:2015:650, točka 73.
[3] *Schrems*, točka 74.

doslovno ponavljanje pravila EU-a. Umjesto toga ispituje se pruža li dotični strani sustav kao cjelina potrebnu razinu zaštite podataka sadržajem prava na privatnost i njihovom djelotvornom provedbom, nadzorom i ostvarivanjem ([4]).

(4) Komisija je pomno proučila japansko pravo i praksu. Na temelju nalaza iznesenih u uvodnim izjavama od 6. do 175. Komisija zaključuje da Japan osigurava primjerenu razinu zaštite osobnih podataka koji se prenose organizacijama koje su obuhvaćene područjem primjene Zakona o zaštiti osobnih informacija ([5]) i podliježu dodatnim uvjetima navedenima u ovoj Odluci. Ti su uvjeti navedeni u Dopunskim pravilima (Prilog I.) koja je donijelo Povjerenstvo za zaštitu osobnih informacija (*Personal Information Protection Commission*, PPC) ([6]) i u službenim izjavama, jamstvima i obvezama koje je japanska vlada uputila Europskoj komisiji (Prilog II.).

(5) Ova Odluka znači da za prijenos od voditelja obrade ili izvršitelja obrade u Europskom gospodarskom prostoru (EGP) ([7]) takvim organizacijama u Japanu nisu potrebna daljnja odobrenja. Ova Odluka ne utječe na izravnu primjenu Uredbe (EU) 2016/679 na takve organizacije ako su ispunjeni uvjeti iz njezina članka 3.

## 2. PRAVILA KOJA SE PRIMJENJUJU NA OBRADU PODATAKA KOJU VRŠE POSLOVNI SUBJEKTI

### 2.1. Japanski okvir za zaštitu podataka

(6) Pravni sustav kojim se uređuje privatnost i zaštita podataka u Japanu počiva na Ustavu proglašenom 1946.

(7) U članku 13. Ustava navedeno je sljedeće:

„Svi ljudi moraju se poštovati kao pojedinci. Njihovo pravo na život, slobodu i težnju sreći, sve dok se ne kosi s javnom dobrobiti, najviša je vrednota zakonodavstva i drugih državnih poslova.”

(8) Na temelju tog članka japanski Vrhovni sud pojasnio je prava pojedinaca u pogledu zaštite osobnih informacija. Odlukom iz 1969. priznao je pravo na privatnost i zaštitu podataka kao ustavno pravo ([8]). Naime, Sud je utvrdio da „svaki pojedinac ima slobodu zaštititi svoje osobne informacije od otkrivanja trećoj strani ili objavljivanja bez opravdanog razloga”. Štoviše, u odluci od 6. ožujka 2008. („Juki-Net”) ([9]) Vrhovni je sud utvrdio da se „građanska sloboda u privatnom životu štiti od izvršavanja javnih ovlasti te se može tumačiti da, kao jednu od sloboda pojedinca u privatnom životu, svaki pojedinac ima slobodu štititi svoje osobne informacije od otkrivanja trećoj strani ili objavljivanja bez opravdanog razloga” ([10]).

(9) Japan je 30. svibnja 2003. donio niz zakona u području zaštite podataka:

— Zakon o zaštiti osobnih informacija (*Act on the Protection of Personal Information*, APPI),

— Zakon o zaštiti osobnih informacija koje posjeduju upravni organi (*Act on the Protection of Personal Information Held by Administrative Organs*, APPIHAO),

— Zakon o zaštiti osobnih informacija koje posjeduju neovisne upravne agencije (*Act on the Protection of Personal Information Held by Incorporated Administrative Agencies*, APPI-IAA).

([4]) Vidjeti Komunikaciju Komisije Europskom parlamentu i Vijeću, Razmjena i zaštita osobnih podataka u globaliziranom svijetu, COM(2017) 7 od 10.1.2017., odjeljak 3.1., str. 6.–7.
([5]) Zakon o zaštiti osobnih informacija (Zakon br. 57, 2003.).
([6]) Više informacija o PPC-u dostupno je na sljedećoj poveznici: https://www.ppc.go.jp/en/ (uključujući podatke za kontakt na koji se mogu slati upiti i pritužbe: https://www.ppc.go.jp/en/contactus/access/).
([7]) Ova je Odluka značajna za EGP. U Sporazumu o Europskom gospodarskom prostoru (Sporazum o EGP-u) predviđeno je proširenje unutarnjeg tržišta Europske unije na tri države EGP-a: Island, Lihtenštajn i Norvešku. Odluku Zajedničkog odbora (JCD) o uključivanju Uredbe (EU) 2016/679 u Prilog XI. Sporazumu o EGP-u donio je Zajednički odbor EGP-a 6. srpnja 2018. te je stupila na snagu 20. srpnja 2018. Uredba je stoga obuhvaćena tim sporazumom.
([8]) Vrhovni sud, presuda Velikog vijeća od 24. prosinca 1969., Keishu, svezak 23., br. 12, str. 1625.
([9]) Vrhovni sud, presuda od 6. ožujka 2008., Minshu, svezak 62., br. 3, str. 665.
([10]) Vrhovni sud, presuda od 6. ožujka 2008., Minshu, svezak 62., br. 3, str. 665.

(10) Zadnja dva navedena zakona (izmijenjena 2016.) sadržavaju odredbe koje se primjenjuju na zaštitu osobnih informacija koju osiguravaju subjekti iz javnog sektora. Obrada podataka koja je obuhvaćena područjem primjene tih zakona nije predmet zaključka o primjerenosti u ovoj Odluci, koja je ograničena na zaštitu osobnih informacija koju osiguravaju „poslovni subjekti koji postupaju s osobnim informacijama" (PIHBO-i) u smislu APPI-ja.

(11) U zadnjih nekoliko godina APPI je revidiran. Izmijenjeni APPI objavljen je 9. rujna 2015., a na snagu je stupio 30. svibnja 2017. Uveden je niz novih zaštitnih mjera te su ojačane postojeće, čime se japanski sustav zaštite podataka približio europskome. Među njima su, primjerice, niz ostvarivih prava pojedinaca ili osnivanje neovisnog nadzornog tijela (PPC-a), kojem su povjereni nadzor i osiguravanje provedbe APPI-ja.

(12) Na obradu osobnih informacija obuhvaćenih područjem primjene ove Odluke osim APPI-ja primjenjuju se i provedbena pravila izdana na temelju APPI-ja. To uključuje izmjenu Naloga Kabineta za provedbu Zakona o zaštiti osobnih informacija od 5. listopada 2016. i tzv. pravila provedbe Zakona o zaštiti osobnih informacija koja je donio PPC ([11]). Oba skupa pravila pravno su obvezujuća i provediva te su stupila na snagu u isto vrijeme kada i izmijenjeni APPI.

(13) Nadalje, 28. listopada 2016. Japanski kabinet (sastavljen od premijera i ministara njegove vlade) objavio je „osnovnu politiku" za „sveobuhvatno i cjelovito promicanje mjera za zaštitu osobnih informacija". Prema članku 7. APPI-ja „osnovna politika" izdaje se u obliku Odluke Kabineta i uključuje političke smjernice za provedbu APPI-ja, usmjerene i na središnju i lokalnu vlast.

(14) Nedavno je Odlukom Kabineta donesenom 12. lipnja 2018. japanska vlada izmijenila „osnovnu politiku". S ciljem olakšavanja međunarodnog prijenosa podataka tom se Odlukom Kabineta PPC-u, kao tijelu nadležnom za upravljanje APPI-jem i njegovu provedbu, delegira „ovlast za poduzimanje potrebnih mjera za premošćivanje razlika između sustava i operacija Japana i predmetne strane zemlje na temelju članka 6. tog zakona kako bi se osiguralo primjereno postupanje s osobnim informacijama primljenima od te zemlje". Prema Odluci Kabineta to uključuje ovlast PPC-a za uspostavu pojačane zaštite donošenjem strožih pravila koja dopunjuju i proširuju pravila iz APPI-ja i Naloga Kabineta. U skladu s tom odlukom ta su stroža pravila obvezujuća i provediva za japanske poslovne subjekte.

(15) Na temelju članka 6. APPI-ja i te Odluke Kabineta PPC je 15. lipnja 2018. donio „Dopunska pravila u okviru Zakona o zaštiti osobnih informacija za postupanje s osobnim podacima koji se prenose iz EU-a na temelju odluke o primjerenosti" („Dopunska pravila") kako bi se poboljšala zaštita osobnih informacija koje se prenose iz Europske unije u Japan na temelju ove odluke o primjerenosti. Ta su Dopunska pravila pravno obvezujuća za japanske poslovne subjekte, a njihovu provedbu mogu osigurati i PPC i sudovi, jednako kao i kad je riječ o odredbama APPI-ja, koje ta pravila dopunjuju strožim i/ili detaljnijim pravilima ([12]). Budući da će japanski poslovni subjekti koji primaju i/ili dalje obrađuju osobne podatke iz Europske unije imati zakonsku obvezu pridržavati se Dopunskih pravila, morat će osigurati (npr. tehničkim sredstvima („označivanjem") ili organizaciskim sredstvima (pohranom u posebnoj bazi podataka)) da mogu identificirati takve osobne podatke tijekom cijelog njihova „životnog ciklusa" ([13]). U sljedećim se odjeljcima analizira sadržaj svakog Dopunskog pravila u okviru procjene članaka APPI-ja koje dopunjuje.

(16) Prije izmjene 2015. to je bilo u nadležnosti različitih japanskih ministarstava u određenim sektorima, a sada je na temelju APPI-ja PPC ovlašten za donošenje „Smjernica" kako bi se „osigurala pravilna i djelotvorna provedba mjera koje treba poduzeti poslovni subjekt" u skladu s pravilima o zaštiti podataka. U svojim smjernicama PPC uvijek

([11]) Dostupno na: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

([12]) Vidjeti Dopunska pravila (uvodni dio).

([13]) To se ne dovodi u pitanje općim zahtjevom da se evidencija vodi (samo) određeno vrijeme. Iako je porijeklo podataka među informacijama koje PIHBO koji ih pribavlja treba potvrditi na temelju članka 26. stavka 1. APPI-ja, zahtjev iz članka 26. stavka 4. APPI-ja u vezi s člankom 18. pravila PPC-a odnosi se samo na određeni oblik zapisa (vidjeti članak 16. pravila PPC-a) i ne sprečava PIHBO-a da osigura identifikaciju podataka tijekom duljih razdoblja. To je potvrdio PPC, koji je naveo da „informacije o porijeklu podataka iz EU-a PIHBO mora čuvati onoliko dugo koliko je potrebno da bi bio u skladu s Dopunskim pravilima".

vjerodostojno tumači ta pravila, posebno APPI. Prema informacijama dobivenima od PPC-a te su Smjernice sastavni dio pravnog okvira i treba ih tumačiti zajedno s tekstom APPI-ja, Nalogom Kabineta, pravilima PPC-a te zbirkom pitanja i odgovora ([14]) koju je priredio PPC. Stoga su oni „obvezujući za poslovne subjekte". Ako se u Smjernicama navodi da poslovni subjekt „mora" ili „ne smije" djelovati na određeni način, PPC će smatrati da nepoštovanje relevantnih odredaba predstavlja kršenje zakona ([15]).

### 2.2. **Materijalno i osobno područje primjene**

(17) Područje primjene APPI-ja određuje se prema utvrđenim pojmovima osobnih informacija, osobnih podataka i poslovnog subjekta koji postupa s osobnim informacijama. U APPI-ju su ujedno predviđena neka važna izuzeća iz njegova područja primjene, prije svega za anonimno obrađene osobne podatke i za posebne vrste obrade koju obavljaju određeni subjekti. U APPI-ju se ne koristi pojam „obrada", nego istovjetan pojam „postupanje", koji, prema informacijama primljenima od PPC-a, obuhvaća „sve radnje u pogledu osobnih podataka", uključujući pribavljanje, unos, prikupljanje, organizaciju, pohranu, uređivanje/obradu, obnavljanje, brisanje, izdavanje, korištenje ili prosljeđivanje osobnih informacija.

#### 2.2.1. *Definicija osobnih informacija*

(18) Prije svega, kad je riječ o materijalnom području primjene, u APPI-ju se razlikuju osobne informacije od osobnih podataka te se samo određene odredbe tog zakona primjenjuju na prvu od tih dviju kategorija. U skladu s člankom 2. stavkom 1. APPI-ja pojam „osobne informacije" obuhvaća sve informacije o živoj osobi koje omogućuju njezinu identifikaciju. U definiciji se razlikuju dvije kategorije osobnih informacija: i. identifikacijske oznake pojedinaca i ii. druge osobne informacije na temelju kojih se može identificirati određena osoba. Druga kategorija obuhvaća i informacije koje same po sebi ne omogućuju identifikaciju, ali s kojima je, ako su „lako povezive" s drugim informacijama, moguće identificirati određenu osobu. Prema Smjernicama PPC-a ([16]) za svaki se slučaj zasebno procjenjuje mogu li se informacije smatrati „lako povezivima", a pritom se uzima u obzir stvarna situacija („stanje") poslovnog subjekta. Pretpostavit će se da je tako ako prosječan („običan") poslovni subjekt tako povezuje (ili može povezati) informacije koristeći se sredstvima koja su mu dostupna. Primjerice, informacije nisu „lako povezive" s drugim informacijama ako se poslovni subjekt mora iznimno potruditi ili počiniti nezakonite radnje kako bi od jednog ili više drugih poslovnih subjekata dobio informacije koje bi povezivao.

#### 2.2.2. *Definicija osobnih podataka*

(19) U APPI-ju su samo određeni oblici osobnih informacija obuhvaćeni pojmom „osobni podaci". „Osobni podaci" se konkretno definiraju kao „osobne informacije koje čine bazu podataka s osobnim informacijama", tj. „kolektivni skup informacija" koji sadržava osobne informacije „sustavno organizirane tako da se pomoću računala mogu tražiti pojedinačne osobne informacije" ([17]) ili „propisane Nalogom Kabineta kao sustavno organizirane tako da se mogu jednostavno tražiti pojedinačne osobne informacije", ali „isključujući one za koje je prema Nalogu Kabineta mala mogućnost da će, s obzirom na metodu njihova korištenja, nanijeti štetu pravima i interesima pojedinca" ([18]).

(20) Ta je iznimka pobliže opisana u članku 3. stavku 1. Naloga Kabineta, prema kojemu moraju biti ispunjena sva tri sljedeća uvjeta: i. kolektivni skup informacija mora biti „izdan u svrhu prodaje velikom broju neimenovanih osoba, a njegovo izdavanje nije provedeno u suprotnosti sa zakonskim odredbama ili nalogom na temelju njih"; ii. mora

([14]) PPC, Pitanja i odgovori, 16. veljače 2017. (izmijenjeno 30. svibnja 2017.), dostupno na sljedećoj poveznici: https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf. Pitanja i odgovori na praktičnim primjerima obrađuju niz tema iz Smjernica, npr. što su osjetljivi osobni podaci, tumačenje privole pojedinca, prijenos trećoj strani u kontekstu računalstva u oblaku ili obveza vođenja evidencije pri prekograničnom prijenosu. Pitanja i odgovori dostupni su samo na japanskom jeziku.

([15]) Na konkretno pitanje PPC je obavijestio Europski odbor za zaštitu podataka da „japanski sudovi pri primjeni pravila APPI-ja/PPC-a u pojedinačnim predmetima o kojima odlučuju [svoje] tumačenje temelje na Smjernicama PPC-a te su stoga u svojim presudama izravno upućivali na njihov tekst. Stoga su i iz te perspektive Smjernice PPC-a obvezujuće za poslovne subjekte. PPC nema informaciju da je Sud ikad odstupio od Smjernica". U tom pogledu PPC je Komisiju uputio na presudu u području zaštite podataka u kojoj je sud u svojim zaključcima izričito polazio od Smjernica (vidjeti Okružni sud u Osaki, odluka od 19. svibnja 2006., Hanrei Jiho, svezak 1948, str. 122., u kojoj je sud presudio da je poslovni subjekt na temelju tih smjernica bio dužan poduzeti sigurnosne kontrolne mjere).

([16]) Smjernice PPC-a (*General Rule Edition*), str. 6.

([17]) To obuhvaća sve elektroničke sustave pohrane. U Smjernicama PPC-a (*General Rule Edition*, str. 17.) za to se navode konkretni primjeri, npr. popis adresa e-pošte pohranjen u korisničkom softveru e-pošte.

([18]) Članak 2. stavci 4. i 6. APPI-ja.

ga „u svakom trenutku moći kupiti velik broj neimenovanih osoba” i iii. osobni podaci koje sadržava moraju biti „proslijeđeni u svoju prvotnu svrhu, bez dodavanja drugih informacija o živoj osobi”. Prema objašnjenjima PPC-a ta vrlo ograničena iznimka uvedena je kako bi se isključili telefonski imenici ili slične vrste popisa.

(21) Za podatke prikupljene u Japanu to razlikovanje „osobnih informacija” i „osobnih podataka” relevantno je jer takve informacije nisu nužno dio „baze podataka s osobnim informacijama” (npr. samo jedan skup podataka koji se ručno prikuplja i obrađuje) te se stoga odredbe APPI-ja koje se odnose samo na osobne podatke neće primjenjivati ([19]).

(22) No ta razlika neće biti relevantna za osobne podatke uvezene iz Europske unije u Japan na temelju odluke o primjerenosti. Budući da će se takvi podaci u pravilu prenositi elektronički (što je u digitalno doba uobičajen način razmjene podataka, pogotovo na tako velikoj udaljenosti kao između EU-a i Japana) te stoga postaju dijelom elektroničkog sustava pohrane uvoznika podataka, takvi će podaci iz EU-a prema APPI-ju biti obuhvaćeni kategorijom „osobni podaci”. U iznimnom slučaju da se osobni podaci iz EU-a prenose na druge načine (npr. u papirnatom obliku), oni će i dalje biti obuhvaćeni APPI-jem ako nakon prijenosa postaju dijelom „kolektivnog skupa informacija” sustavno organiziranog tako da se omogući lako pretraživanje određenih informacija (članak 2. stavak 4. točka ii. APPI-ja). Prema članku 3. stavku 2. Naloga Kabineta to će biti slučaj u kojem su informacije uređene „prema određenom pravilu” te baza podataka uključuje popis poput sadržaja ili kazala koji olakšava pretraživanje. To odgovara definiciji „sustava pohrane” u smislu članka 2. stavka 1. Opće uredbe o zaštiti podataka.

2.2.3. *Definicija pohranjenih osobnih podataka*

(23) Određene odredbe APPI-ja, posebno članci od 27. do 30. o pravima pojedinaca, primjenjuju se samo na određenu kategoriju osobnih podataka, i to na „pohranjene osobne podatke”. Oni su definirani u članku 2. stavku 7. APPI-ja kao osobni podaci za koje nije i. „Nalogom Kabineta utvrđeno da bi mogli nanijeti štetu javnim ili drugim interesima ako se sazna za njihovo postojanje ili nepostojanje” ili ii. „Nalogom Kabineta određeno da se brišu u roku od najviše jedne godine”.

(24) Prva od tih dviju kategorija objašnjena je u članku 4. Naloga Kabineta i obuhvaća četiri vrste izuzeća ([20]). Tim izuzećima nastoje se ostvariti ciljevi slični onima iz članka 23. stavka 1. Uredbe (EU) 2016/679, posebno zaštita ispitanika („principal” u terminologiji APPI-ja) i sloboda drugih, nacionalna sigurnost, javna sigurnost, kazneni progon ili drugi važni ciljevi od općeg javnog interesa. Osim toga, iz teksta članka 4. stavka 1. točaka od i. do iv. Naloga Kabineta proizlazi da njihova primjena uvijek podrazumijeva određeni rizik za jedan od zaštićenih važnih interesa ([21]).

(25) Druga kategorija pobliže je opisana u članku 5. Naloga Kabineta. Kad se tumači zajedno člankom 2. stavkom 7. APPI-ja, iz područja primjene pojma pohranjenih osobnih podataka, a time i iz prava pojedinaca u skladu s APPI-jem, izuzimaju se osobni podaci koje „treba izbrisati” u roku od šest mjeseci. PPC je objasnio je da se tim izuzećem poslovne subjekte želi potaknuti da podatke pohranjuju i obrađuju što kraće. Međutim, to bi značilo da ispitanici iz EU-a ne bi mogli ostvarivati važna prava samo zbog trajanja razdoblja u kojem predmetni poslovni subjekt zadržava njihove podatke.

(26) Kako bi se ta situacija riješila, prema Dopunskom pravilu 2. s osobnim podacima koji se prenose iz Europske unije mora se „postupati kao sa pohranjenim osobnim podacima u smislu članka 2. stavka 7. Zakona, bez obzira na rok u kojem ih treba izbrisati”. Dakle, razdoblje zadržavanja neće utjecati na prava koja uživaju ispitanici iz EU-a.

([19]) Npr. članak 23. APPI-ja o uvjetima dijeljenja osobnih podataka s trećom stranom.

([20]) Točnije, osobne podatke i. „za koje postoji mogućnost da će, sazna li se za njihovo postojanje ili nepostojanje, naštetiti životu, tijelu ili imetku principala ili treće strane; ii. podatke „za koje postoji mogućnost da će, sazna li se za njihovo postojanje ili nepostojanje, potaknuti ili uzrokovati nezakonito ili nepravedno postupanje”; iii. podatke „za koje postoji mogućnost da će, sazna li se za njihovo postojanje ili nepostojanje, ugroziti nacionalnu sigurnost, uništiti povjerenje uspostavljeno sa stranom zemljom ili međunarodnom organizacijom ili da će dovesti do nepovoljnog položaja u pregovorima sa stranom zemljom ili međunarodnom organizacijom”; i iv. one „za koje postoji mogućnost da će, sazna li se za njihovo postojanje ili nepostojanje, omesti održavanje javne sigurnosti i reda, primjerice sprečavanje, suzbijanje ili istraživanje kaznenog djela”.

([21]) Pod tim uvjetima nije potrebno obavijestiti pojedinca. To je u skladu s člankom 23. stavkom 2. točkom (h) Opće uredbe o zaštiti podataka, gdje se navodi da ispitanici ne moraju biti obaviješteni o ograničenju ako to „može biti štetno za svrhu tog ograničenja”.

2.2.4. *Definicija anonimno obrađenih osobnih informacija*

(27) Zahtjevi koji se primjenjuju na anonimno obrađene osobne informacije, kako je definirano u članku 2. stavku 9. APPI-ja, propisani su u odjeljku 2. poglavlja 4. Zakona („Dužnosti poslovnog subjekta koji postupa s anonimno obrađenim informacijama"). Za razliku od toga, takve informacije nisu uređene odredbama iz odjeljka 1. poglavlja IV. APPI-ja, koji uključuje članke o mjerama za zaštitu podataka i pravima koja se primjenjuju na obradu osobnih podataka na temelju tog Zakona. Prema tome, iako „anonimno obrađene osobne informacije" ne podliježu „standardnim" pravilima o zaštiti podataka (onima iz odjeljka 1. poglavlja IV. i članka 42. APPI-ja), obuhvaćene su područjem primjene APPI-ja, posebno članaka od 36. do 39.

(28) U skladu s člankom 2. stavkom 9. APPI-ja „anonimno obrađene osobne informacije" su informacije o pojedincu „nastale obradom osobnih informacija" pomoću mjera propisanih u APPI-ju (članak 36. stavak 1.) i pobliže određenih u pravilima PPC-a (članak 19.), zbog čega je nemoguće identificirati određenog pojedinca ili vratiti osobne informacije u prvotni oblik.

(29) Iz tih odredaba proizlazi, kako je potvrdio i PPC, da postupak „anonimizacije" osobnih informacija ne mora biti tehnički nepovratan. Na temelju članka 36. stavka 2. APPI-ja poslovni subjekti koji postupaju s „anonimno obrađenim osobnim informacijama" dužni su samo spriječiti ponovnu identifikaciju tako da poduzmu mjere za sigurnost „opisa itd. te identifikacijskih oznaka pojedinaca izbrisanih iz osobnih informacija kako bi se dobile anonimno obrađene informacije te informacija o provedenoj metodi obrade".

(30) S obzirom na to da „anonimno obrađene osobne informacije", kako su definirane u APPI-ju, uključuju podatke s kojima je ponovna identifikacija osobe još uvijek moguća, to bi moglo značiti da bi osobni podaci koji se prenose iz Europske unije mogli izgubiti dio dostupne zaštite u postupku koji bi se, u skladu s Uredbom (EU) 2016/679, prije smatrao oblikom „pseudonimizacije" nego „anonimizacije" (čime se njihova priroda kao osobnih podataka ne mijenja).

(31) Da bi se ta situacija riješila, u Dopunskim pravilima predviđeni su dodatni zahtjevi koji se primjenjuju samo na osobne podatke prenesene iz Europske unije na temelju ove Odluke. U skladu s pravilom 5. iz Dopunskih pravila takve se osobne informacije smatraju „anonimno obrađenim osobnim informacijama" u smislu APPI-ja samo „ako poslovni subjekt koji postupa s osobnim informacijama poduzme mjere kojima bi onemogućio ponovnu identifikaciju pojedinca, među ostalim brisanjem informacija o metodi obrade itd.". Potonje informacije opisane su u Dopunskim pravilima kao informacije koje se odnose na opise i identifikacijske oznake pojedinaca izbrisane iz osobnih informacija da bi se dobile „anonimno obrađene osobne informacije", kao i informacije povezane s metodom obrade primijenjenom pri brisanju tih opisa i identifikacijskih oznaka pojedinaca. Drugim riječima, prema Dopunskim pravilima poslovni subjekt koji proizvodi anonimno obrađene osobne informacije dužan je uništiti „ključ" koji bi omogućio ponovnu identifikaciju podataka. To znači da će osobni podaci podrijetlom iz Europske unije biti obuhvaćeni odredbama APPI-ja o „anonimno obrađenim osobnim informacijama" samo u slučajevima u kojima bi se smatrali anonimnim informacijama i u skladu s Uredbom (EU) 2016/679 ([22]).

2.2.5. *Definicija poslovnog subjekta koji postupa s osobnim informacijama (Personal Information Handling Business Operator, PIHBO)*

(32) U osobnom području primjene APPI se primjenjuje samo na PIHBO-e. PIHBO je definiran u članku 2. stavku 5. APPI-ja kao „osoba koja priređuje bazu podataka s osobnim informacijama itd. za uporabu u poslovanju", s iznimkom vlade i upravnih agencija na središnjoj i lokalnoj razini.

(33) Prema Smjernicama PPC-a „poslovanje" znači svako „postupanje usmjereno na višestruko i kontinuirano obavljanje društveno priznate djelatnosti s određenim ciljem, neovisno o tome ostvaruje li se time dobit". Organizacije bez pravne osobnosti (npr. neformalne udruge) ili pojedinci smatraju se PIHBO-om ako priređuju (upotrebljavaju) bazu podataka s osobnim informacijama itd. za svoje poslovanje ([23]). Stoga je pojam „poslovanje" u okviru APPI-ja vrlo širok jer uključuje ne samo profitne, već i neprofitne djelatnosti svih vrsta organizacija i pojedinaca. Osim toga, „uporaba u poslovanju" obuhvaća i osobne informacije koje se ne upotrebljavaju u (vanjskim) poslovnim odnosima subjekta, već interno, primjerice pri obradi podataka o zaposlenicima.

([22]) Vidjeti uvodnu izjavu 26. Uredbe (EU) 2016/679.
([23]) Smjernice PPC-a (*General Rule Edition*), str. 18.

(34) Kad je riječ o osobama koje imaju pravo na zaštitu u okviru APPI-ja, u njemu to ne ovisi o državljanstvu, boravištu ili lokaciji pojedinca. Isto vrijedi i za mogućnosti pojedinaca da zatraže pravnu zaštitu, bilo pred PPC-om ili sudovima.

2.2.6. *Pojmovi voditelja obrade i izvršitelja obrade*

(35) U okviru APPI-ja nema posebne razlike između obveza voditelja obrade i izvršitelja obrade. Nepostojanje te razlike ne utječe na razinu zaštite jer svi PIHBO-i podliježu svim odredbama Zakona. PIHBO koji postupanje s osobnim podacima povjerava skrbniku (ekvivalent izvršitelja obrade iz Opće uredbe o zaštiti podataka), u pogledu povjerenih podataka i dalje podliježe obvezama na temelju APPI-ja i Dopunskih pravila. Osim toga, u skladu s člankom 22. APPI-ja, on je dužan „provoditi potreban i primjeren nadzor" nad skrbnikom. Sam skrbnik, kao što je PPC potvrdio, podliježe svim obvezama na temelju APPI-ja i Dopunskih pravila.

2.2.7. *Sektorska izuzeća*

(36) Članak 76. APPI-ja izuzima određene vrste obrade podataka iz primjene poglavlja IV. tog zakona, koje sadržava temeljne odredbe o zaštiti podataka (osnovna načela, obveze poslovnih subjekata, prava pojedinaca, nadzor PPC-a). Obrada obuhvaćena sektorskim izuzećem iz članka 76. također je izuzeta od ovlasti prisilne provedbe PPC-a, u skladu s člankom 43. stavkom 2. APPI-ja ([24]).

(37) Relevantne kategorije za sektorsko izuzeće iz članka 76. APPI-ja određuju se prema dvostrukom kriteriju na temelju vrste PIHBO-a koji obrađuje osobne informacije i svrhe obrade. Točnije, izuzeće se primjenjuje na sljedeće: i. ustanove za radiodifuziju, novinske nakladnike, komunikacijske agencije i druge medijske organizacije (uključujući osobe koje se bave medijskim aktivnostima kao svojom djelatnošću) u mjeri u kojoj obrađuju osobne informacije u medijske svrhe; ii. osobe koje se profesionalno bave pisanjem, u mjeri u kojoj to uključuje osobne informacije; iii. sveučilišta i druge organizacije ili skupine usmjerene na akademski studij, ili osobe koje pripadaju takvoj organizaciji, u mjeri u kojoj obrađuju osobne informacije za potrebe akademskih studija; iv. vjerske zajednice, u mjeri u kojoj obrađuju osobne informacije u svrhe vjerske djelatnosti (uključujući sve s tim povezane aktivnosti); i v. politička tijela u mjeri u kojoj obrađuju osobne informacije za potrebe svoje političke aktivnosti (uključujući sve s tim povezane aktivnosti). Obrada osobnih informacija za jednu od svrha iz članka 76. koju vrše druge vrste PIHBO-a i obrada osobnih informacija koju vrši jedan od navedenih PIHBO-a u druge svrhe, primjerice u kontekstu zapošljavanja, i dalje su obuhvaćene odredbama iz poglavlja IV.

(38) Kako bi se osigurala odgovarajuća razina zaštite osobnih podataka koji se iz Europske unije prenose poslovnim subjektima u Japanu, ova bi se Odluka trebala primjenjivati samo na obradu osobnih informacija koje su obuhvaćene područjem primjene poglavlja IV. APPI-ja, tj. onu koju vrši PIHBO u mjeri u kojoj okolnosti obrade ne odgovaraju jednom od sektorskih izuzeća. Njezino područje primjene trebalo bi stoga biti usklađeno s područjem primjene APPI-ja. Prema informacijama primljenima od PPC-a, ako PIHBO obuhvaćen ovom Odlukom naknadno promijeni svrhu korištenja (u mjeri u kojoj je to dopustivo) te bi potom bio obuhvaćen jednim od sektorskih izuzeća iz članka 76. APPI-ja, to bi se smatralo međunarodnim prijenosom (s obzirom na to da u takvim slučajevima obrada osobnih informacija više ne bi bila obuhvaćena Poglavljem IV. APPI-ja, pa tako ni njegovim područjem primjene). Isto bi vrijedilo u slučaju da PIHBO proslijedi osobne informacije subjektu koji je obuhvaćen člankom 76. APPI-ja za uporabu u jednu od svrha obrade navedenih u toj odredbi. Kad je riječ o osobnim podacima koji se prenose iz Europske unije, to bi stoga predstavljalo daljnji prijenos podložan odgovarajućim zaštitnim mjerama (posebno onima iz članka 24. APPI-ja i Dodatnog pravila 4.). Ako se PIHBO oslanja na privolu ispitanika ([25]), morao bi mu pružiti sve potrebne informacije, među ostalim i o tome da osobne informacije više nisu zaštićene APPI-jem.

([24]) Kad je riječ o drugim subjektima, PPC im pri izvršavanju svojih ovlasti istrage i prisilne provedbe ne smije uskratiti pravo na slobodu izražavanja, akademsku slobodu, slobodu vjeroispovijesti i političku slobodu (članak 43. stavak 1. APPI-ja).

([25]) Kako je objasnio PPC, privola se u Smjernicama PPC-a tumači kao „izražavanje namjere principala u smislu da prihvaća da se s njegovim osobnim informacijama može postupati primjenom metode koju je navelo poduzeće koje postupa s osobnim informacijama". U Smjernicama PPC-a (*General Rule Edition*, str. 24.) popisani su načini davanja privole koji se smatraju „uobičajenom poslovnom praksom u Japanu", tj. usmena suglasnost, vraćanje obrazaca ili drugih dokumenata, suglasnost putem elektroničke pošte, označavanje opcije na internetskoj stranici, klik na početnoj stranici, korištenje gumba za pristanak, dodir zaslona osjetljivog na dodir itd. Sve su te metode oblici izričite privole.

2.3. **Zaštitne mjere, prava i obveze**

2.3.1. *Ograničenje svrhe*

(39) Osobni podaci trebali bi se obrađivati u određenu svrhu i zatim se upotrebljavati samo ako to nije protivno svrsi obrade. To načelo zaštite podataka zajamčeno je člancima 15. i 16. APPI-ja.

(40) APPI se oslanja na načelo prema kojemu poslovni subjekt mora „što preciznije" navesti svrhu korištenja (članak 15. stavak 1.), a potom je pri obradi podataka obvezan tom svrhom.

(41) U tom se pogledu člankom 15. stavkom 2. APPI-ja propisuje da PIHBO ne smije mijenjati prvotnu svrhu „više nego što se može u razumnoj mjeri povezati sa svrhom korištenja prije izmjene", što prema tumačenju u Smjernicama PPC-a odgovara onome što ispitanik može objektivno predvidjeti na temelju „uobičajenih društvenih konvencija" ([26]).

(42) Nadalje, prema članku 16. stavku 1. APPI-ja PIHBO-i ne smiju postupati s osobnim informacijama „više nego što je nužno za postizanje svrhe korištenja" u skladu s člankom 15. bez prethodne privole ispitanika, osim ako se primjenjuje jedno od odstupanja iz članka 16. stavka 3 ([27]).

(43) Kad je riječ o osobnim informacijama dobivenima od drugog poslovnog subjekta, PIHBO u načelu smije odrediti novu svrhu korištenja ([28]). Kako bi se osiguralo da, u slučaju prijenosa iz Europske unije, takav primatelj bude obvezan svrhom za koju su podaci preneseni, u skladu s Dopunskim pravilom 3. u slučajevima „u kojima [PIHBO] primi osobne podatke iz EU-a na temelju odluke o primjerenosti", ili takav subjekt „od drugog [PIHBO-a] primi osobne podatke koji su prethodno preneseni iz EU-a na temelju odluke o primjerenosti" (daljnje dijeljenje), mora „svrhu korištenja navedenih osobnih podataka navesti u okviru svrhe korištenja za koju su podaci prvotno ili naknadno primljeni". Drugim riječima, tim se pravilom osigurava da u kontekstu prijenosa svrha koja je određena u skladu s Uredbom (EU) 2016/679 i dalje određuje obradu i da bi promjena te svrhe u bilo kojoj fazi lanca obrade u Japanu zahtijevala privolu ispitanika iz EU-a. Budući da za dobivanje te privole PIHBO mora stupiti u kontakt s ispitanikom, ako to nije moguće, jednostavno se mora zadržati prvotna svrha.

2.3.2. *Zakonitost i poštenost obrade*

(44) Dodatna zaštita iz uvodne izjave 43. utoliko je važnija jer japanski sustav upravo načelom ograničenja svrhe osigurava da se osobni podaci obrađuju zakonito i pošteno.

(45) U skladu s APPI-jem PIHBO koji prikuplja osobne informacije mora detaljno navesti svrhu njihova korištenja ([29]) i odmah obavijestiti ispitanika o toj svrsi korištenja (ili je javno objaviti) ([30]). Osim toga prema članku 17. APPI-ja PIHBO ne smije pribavljati osobne informacije prijevarom ili drugim nepropisnim sredstvima. Kad je riječ o određenim kategorijama podataka, kao što su osobne informacije koje zahtijevaju posebnu pozornost, za njihovo je pribavljanje potrebna privola ispitanika (članak 17. stavak 2. APPI-ja).

([26]) Pitanja i odgovori koje je objavio PPC sadržavaju niz primjera za ilustraciju tog pojma. Primjeri situacija u kojima se izmijenjena uporaba može u razumnoj mjeri povezati sa svrhom uporabe prije izmjene ponajprije uključuju uporabu osobnih informacija dobivenih od kupaca robe ili usluga u kontekstu trgovačke transakcije u svrhu obavješćivanja tih kupaca o drugoj relevantnoj robi ili uslugama koje su na raspolaganju (npr. kad voditelj fitness kluba registrira e-adrese članova kako bi ih obavještavao o tečajevima i programima). Među pitanjima i odgovorima navodi se i primjer situacije u kojoj promjena svrhe korištenja nije dopuštena, naime ako trgovačko društvo šalje informacije o svojoj robi i uslugama na e-adrese koje je prikupilo u svrhu upozorenja na prijevaru ili krađu članske iskaznice.

([27]) Ta izuzeća mogu proizlaziti iz drugih zakona i propisa ili se odnositi na situacije u kojima je postupanje s osobnim informacijama nužno i. za „zaštitu ljudskog života, tijela ili imovine"; ii. za „poboljšanje javne higijene ili promicanje zdravlja djece"; ili iii. za „suradnju s vladinim agencijama ili tijelima ili njihovim predstavnicima" pri obavljanju njihovih zakonom propisanih zadaća. Osim toga, kategorije i. i ii. primjenjuju se samo ako je teško dobiti privolu ispitanika, a kategorija iii. samo ako postoji rizik da bi dobivanje privole ispitanika ometalo obavljanje tih zadaća.

([28]) Bez obzira na to, na temelju članka 23. stavka 1. APPI-ja privola pojedinca u načelu se zahtijeva za otkrivanje podataka trećoj strani. Na taj način pojedinac može imati određenu kontrolu nad time kako drugi poslovni subjekt upotrebljava njegove podatke.

([29]) U skladu s člankom 15. stavkom 1. APPI-ja to mora biti „što preciznije".

([30]) Članak 18. stavak 1. APPI-ja.

(46) Prema tome, kako je objašnjeno u uvodnim izjavama 41. i 42., PIHBO ne smije obrađivati osobne podatke u druge svrhe osim ako ispitanik pristaje na takvu obradu ili ako se primjenjuje jedno od odstupanja iz članka 16. stavka 3. APPI-ja.

(47) Konačno, kad je riječ o prosljeđivanju osobnih informacija trećoj strani ([31]), člankom 23. stavkom 1. APPI-ja takvo se otkrivanje ograničava na posebne slučajeve, pri čemu je u pravilu potrebna prethodna privola ispitanika ([32]). Člankom 23. stavcima 2., 3. i 4. APPI-ja predviđene su iznimke od obveze dobivanja privole. Međutim, te iznimke primjenjuju se samo na podatke koji nisu osjetljivi i pod uvjetom da poslovni subjekt unaprijed obavijesti dotične osobe o namjeri otkrivanja njihovih osobnih informacija trećoj strani i o mogućnosti prigovora na svako daljnje otkrivanje ([33]).

(48) Kad je riječ o prijenosu iz Europske unije, osobni podaci morat će najprije biti prikupljeni i obrađeni u EU-u u skladu s Uredbom (EU) 2016/679. To će s jedne strane uvijek uključivati prikupljanje i obradu, među ostalim za prijenos iz Europske unije u Japan, na temelju jedne od pravnih osnova navedenih u članku 6. stavku 1. Uredbe, a s druge strane prikupljanje za posebnu, izričitu i zakonitu svrhu te zabranu daljnje obrade, među ostalim i prijenosom, na način koji nije u skladu s takvom svrhom, kako je utvrđeno u članku 5. stavku 1. točki (b) i članku 6. stavku 4. Uredbe.

(49) Nakon prijenosa, u skladu s Dopunskim pravilom 3., PIHBO koji primi podatke morat će „potvrditi" posebnu svrhu/svrhe prijenosa (tj. svrhu određenu u skladu s Uredbom (EU) 2016/679) i te podatke dalje obrađivati u skladu s takvom svrhom/svrhama ([34]). To znači da je i prvotni pribavitelj takvih osobnih podataka u Japanu, ali i svaki budući primatelj tih podataka (uključujući skrbnika) obvezan svrhom/svrhama navedenima u Uredbi.

(50) Nadalje, u slučaju da PIHBO želi promijeniti svrhu kako je prethodno navedena u Uredbi (EU) 2016/679, u skladu s člankom 16. stavkom 1. APPI-ja u načelu bi morao dobiti privolu ispitanika. Bez te privole svaka obrada podataka koja prelazi ono što je nužno za postizanje te svrhe korištenja značila bi kršenje članka 16. stavka 1. koju PPC i sudovi mogu sankcionirati.

(51) Prema tome, budući da je u skladu s Uredbom (EU) 2016/679 za prijenos potrebna valjana pravna osnova i posebna svrha, što se odražava u svrsi korištenja „potvrđenoj" u skladu s APPI-jem, kombinacijom odgovarajućih odredaba APPI-ja i Dopunskog pravila 3. osigurava se daljnja zakonitost obrade podataka iz EU-a u Japanu.

2.3.3. *Točnost i smanjenje količine podataka*

(52) Podaci bi trebali biti točni i prema potrebi ažurirani. Trebali bi biti i primjereni, bitni i ograničeni na ono što je nužno za svrhe u koje se obrađuju.

(53) Ta su načela u japanskom pravu zajamčena člankom 16. stavkom 1. APPI-ja, kojim se zabranjuje postupanje s osobnim podacima koje bi prelazilo „ono što je nužno za postizanje svrhe korištenja". Kako je objasnio PPC, to ne isključuje samo neprimjerenu i pretjeranu uporabu podataka (koja prelazi ono što je nužno za postizanje svrhe korištenja), nego uključuje i zabranu postupanja s podacima koji nisu bitni za postizanje svrhe korištenja.

([31]) Iako su skrbnici isključeni iz pojma „treće strane" za potrebe primjene članka 23. (vidjeti stavak 5.), to se izuzeće primjenjuje samo ako skrbnik postupa s osobnim podacima u okviru ovlaštenja („u opsegu koji je nužan za postizanje svrhe korištenja"), tj. djeluje kao izvršitelj obrade.

([32]) Ostali su (iznimni) razlozi sljedeći: i. prosljeđivanje osobnih informacija „na temelju zakona i propisa"; ii. slučajevi „u kojima je potrebno zaštititi ljudski život, tijelo ili imetak te kad je teško dobiti privolu principala"; iii. slučajevi „u kojima postoji posebna potreba za poboljšanjem javne higijene ili promicanjem zdravlja djece te kad je teško dobiti privolu principala"; i iv. slučajevi „u kojima je potrebna suradnja sa središnjom državnom organizacijom ili lokalnom upravom, ili osobom kojoj je povjereno obavljanje poslova propisanih zakonima i propisima, i kad postoji mogućnost da bi dobivanje privole principala moglo omesti obavljanje tih poslova".

([33]) Informacije koje je potrebno dostaviti prije svega uključuju kategorije osobnih podataka koje će se dijeliti s trećom stranom i metodu prijenosa. Osim toga PIHBO mora obavijestiti ispitanika o mogućnosti da se usprotivi prijenosu i o tome kako da podnese takav zahtjev.

([34]) U skladu s člankom 26. stavkom 1. točkom ii. APPI-ja PIHBO koji prima osobne podatke od treće strane mora „potvrditi" (provjeriti) „pojedinosti o načinu na koji je treća strana pribavila osobne podatke", uključujući svrhu tog pribavljanja. Iako se u članku 26. ne navodi izričito da se PIHBO potom mora pridržavati te svrhe, to je izričito propisano Dopunskim pravilom 3.

(54) Kad je riječ o obvezi u pogledu točnosti i ažuriranosti podataka, prema članku 19. APPI-ja PIHBO mora „nastojati da osobni podaci budu točni i ažurirani onoliko koliko je nužno za postizanje svrhe korištenja". Ta bi se odredba trebala tumačiti zajedno s člankom 16. stavkom 1. APPI-ja: prema objašnjenjima PPC-a, ako PIHBO ne ispunjava propisane standarde točnosti, neće se smatrati da se obradom osobnih informacija postiže svrha korištenja te će postupanje s njima postati nezakonito u skladu s člankom 16. stavkom 1.

2.3.4. *Ograničenje pohrane*

(55) Podaci se u načelu ne bi trebali čuvati duže nego što je nužno za svrhe u koje se osobni podaci obrađuju.

(56) U skladu s člankom 19. APPI-ja PIHBO-i moraju „nastojati […] bez odgode izbrisati osobne podatke kad takvo korištenje više nije nužno". Tu odredbu treba tumačiti zajedno s člankom 16. stavkom 1. APPI-ja, kojim se zabranjuje postupanje s osobnim informacijama koje prelazi „ono što je nužno za postizanje svrhe korištenja". Kad se svrha korištenja postigne, obrada osobnih informacija više se ne može smatrati nužnom te se stoga ne može nastaviti (osim ako PIHBO za to dobije privolu ispitanika).

2.3.5. *Sigurnost podataka*

(57) Osobni podaci trebali bi se obrađivati tako da se jamči njihova sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja. Zato bi poslovni subjekti trebali poduzeti odgovarajuće tehničke ili organizacijske mjere za zaštitu osobnih podataka od mogućih prijetnji. Te bi mjere trebalo procijeniti uzimajući u obzir najsuvremeniju tehnologiju i povezane troškove.

(58) To je načelo ugrađeno u japansko pravo člankom 20. APPI-ja, prema kojemu PIHBO „poduzima potrebne i primjerene mjere za sigurnosnu kontrolu osobnih podataka, uključujući sprečavanje neovlaštenog odavanja, gubitka ili oštećenja osobnih podataka s kojima postupa." U Smjernicama PPC-a objašnjavaju se mjere koje treba poduzeti, uključujući metode za uspostavu osnovnih politika, pravila za postupanje s podacima i razne „kontrolne mjere" (u pogledu organizacijske sigurnosti te ljudske, fizičke i tehnološke sigurnosti) ([35]). Osim toga, u Smjernicama PPC-a i posebnoj Obavijesti (Dodatak 8. „Sadržaj mjera za upravljanje sigurnošću koje se moraju poduzeti") koju je objavio PPC navodi se više pojedinosti o mjerama koje se odnose na sigurnosne incidente, uključujući, na primjer, neovlašteno odavanje osobnih informacija, kao dio mjera za upravljanje sigurnošću koje trebaju poduzeti PIHBO-i ([36]).

(59) Nadalje, kad s osobnim informacijama postupaju zaposlenici ili podugovaratelji, u skladu s člancima 20. i 21. APPI-ja mora se osigurati „potreban i primjeren nadzor" u svrhe sigurnosne kontrole. Konačno, u skladu s člankom 83. APPI-ja, namjerno neovlašteno odavanje ili krađa osobnih informacija kažnjivi su kaznom zatvora do jedne godine.

2.3.6. *Transparentnost*

(60) Ispitanici bi trebali biti obaviješteni o glavnim aspektima obrade njihovih osobnih podataka.

(61) Prema članku 18. stavku 1. APPI-ja PIHBO mora informacije o svrsi korištenja pribavljenih osobnih informacija staviti na raspolaganje ispitaniku, osim u „slučajevima u kojima je svrha korištenja bila unaprijed javno objavljena". Ista obveza vrijedi i u slučaju dopustive promjene svrhe (članak 18. stavak 3.). Time se osigurava i da je ispitanik obaviješten o činjenici da se njegovi podaci prikupljaju. Iako prema APPI-ju PIHBO u pravilu ne mora obavijestiti ispitanika o očekivanim primateljima osobnih informacija u fazi prikupljanja, takve su informacije nužan uvjet za svako naknadno otkrivanje informacija trećoj strani (primatelju) na temelju članka 23. stavka 2., odnosno kad se to čini bez prethodne privole ispitanika.

([35]) Smjernice PPC-a (*General Rule Edition*), str. 41. i str. 86.–98.

([36]) U skladu s odjeljkom 3-3-2 Smjernica PPC-a u slučaju takvog neovlaštenog odavanja, oštećenja ili gubitka PIHBO mora provesti potrebne istrage te posebno procijeniti razmjer povrede prava i interesa pojedinca te prirodu i količinu predmetnih osobnih informacija.

(62) Kad je riječ o „pohranjenim osobnim podacima", prema članku 27. APPI-ja PIHBO mora obavijestiti ispitanika o svojem identitetu (podacima za kontakt), svrsi korištenja i postupcima odgovaranja na zahtjev u vezi s pravima ispitanika u skladu s člancima 28., 29. i 30. APPI-ja.

(63) Budući da će se prema Dopunskim pravilima osobni podaci koji se prenose iz Europske unije smatrati „pohranjenim osobnim podacima" bez obzira na razdoblje njihove pohrane (osim ako su obuhvaćeni izuzećima), na njih će se uvijek primjenjivati zahtjevi u pogledu transparentnosti na temelju obje navedene odredbe.

(64) Zahtjevi iz članka 18. i obveza obavješćivanja o svrsi korištenja u skladu s člankom 27. APPI-ja podliježu istom skupu iznimki, koje se uglavnom temelje na razmatranju javnog interesa i zaštiti prava i interesa ispitanika, treće strane i voditelja obrade ([37]). Prema tumačenju iz Smjernica PPC-a te se iznimke primjenjuju u vrlo specifičnim situacijama, primjerice u situaciji kad bi informacije o svrsi korištenja mogle ugroziti zakonite mjere koje poslovni subjekt poduzima radi zaštite određenih interesa (npr. borba protiv prijevara, industrijske špijunaže, sabotaže).

2.3.7. *Posebne kategorije podataka*

(65) Trebale bi postojati posebne zaštitne mjere ako se obrađuju „posebne kategorije" podataka.

(66) „Osobne informacije koje zahtijevaju posebnu pozornost" definirane su u članku 2. stavku 3. APPI-ja. Ta se odredba odnosi na „osobne informacije principala koje obuhvaćaju njegovu rasu, uvjerenje, socijalni status, povijest bolesti, kaznenu evidenciju, činjenicu da je pretrpio štetu zbog kaznenog djela, ili druge opise itd. za koje je Nalogom Kabineta propisano da se s njima mora postupati s posebnom pozornošću kako se ne bi prouzročila nepoštena diskriminacija, predrasude ili druge negativne posljedice za principala". Te kategorije velikim dijelom odgovaraju popisu osjetljivih podataka iz članaka 9. i 10. Uredbe (EU) 2016/679. Konkretno, „povijest bolesti" odgovara podacima koji se odnose na zdravlje, a „kaznena evidencija i činjenica da je osobi nanesena šteta kaznenim djelom" u osnovi su jednake kategorijama iz članka 10. Uredbe (EU) 2016/679. Kategorije iz članka 2. stavka 3. APPI-ja podložne su daljnjem tumačenju u Nalogu Kabineta i Smjernicama PPC-a. U skladu s odjeljkom 2.3. točkom 8. Smjernica PPC-a potkategorije „povijesti bolesti" opisane u članku 2. točkama ii. i iii. Naloga Kabineta tumače se tako da obuhvaćaju genetske i biometrijske podatke. Iako se na popisu izrijekom ne navode pojmovi „etničko podrijetlo" i „političko mišljenje", upućuje se na „rasu" i „uvjerenje". Kako je objašnjeno u odjeljku 2.3. točkama 1. i 2. Smjernica PPC-a, upućivanje na „rasu" obuhvaća i „etničke veze ili veze s određenim dijelom svijeta", a „uvjerenje" uključuje i vjerska i politička stajališta.

(67) Kao što je jasno iz teksta te odredbe, to nije iscrpan popis jer se može dodati još kategorija podataka u mjeri u kojoj njihova obrada stvara rizik od „nepravedne diskriminacije, predrasuda ili druge štete za principala".

(68) Iako je koncept „osjetljivih" podataka sam po sebi društveni konstrukt jer se temelji na kulturnim i pravnim tradicijama, moralnim razmatranjima, političkom odabiru itd. određenog društva, s obzirom na važnost osiguravanja primjerenih zaštitnih mjera za osjetljive podatke koji se prenose poslovnim subjektima u Japanu, Komisija je postigla da se posebna zaštita koja se prema japanskom pravu pruža „osobnim informacijama koje zahtijevaju posebnu pozornost" proširi na sve kategorije koje su u Uredbi (EU) 2016/679 priznate kao „osjetljivi podaci". U tu je svrhu u Dopunskom pravilu 1. predviđeno da podatke prenesene iz Europske unije o seksualnom životu, seksualnoj orijentaciji ili članstvu u sindikatu PIHBO obrađuje „na isti način kao i osobne informacije koje zahtijevaju posebnu pozornost u smislu članka 2. stavka 3. [APPI-ja]".

([37]) Riječ je o i. slučajevima u kojima postoji mogućnost da bi obavješćivanje ispitanika o svrsi korištenja ili njezino javno objavljivanje moglo „štetiti životu, tijelu, imetku ili drugim pravima i interesima principala ili treće strane" ili „pravima ili legitimnim interesima […] PIHBO-a"; ii. slučajevima u kojima je „potrebna suradnja sa središnjom državnom organizacijom ili lokalnom upravom" u obavljanju njihovih zakonskih zadaća i ako bi se takvim informacijama ili otkrivanjem omeli takvi „poslovi"; iii. slučajevima u kojima je svrha korištenja jasna iz situacije u kojoj su podaci pribavljeni.

(69) U pogledu dodatnih materijalnih zaštitnih mjera koje se primjenjuju na osobne informacije koje zahtijevaju posebnu pozornost, u skladu s člankom 17. stavkom 2. APPI-ja PIHBO-i ne smiju pribavljati takvu vrstu podataka bez prethodne privole dotičnog pojedinca, osim u malobrojnim iznimkama ([38]). Nadalje, ta kategorija osobnih informacija isključena je iz mogućnosti otkrivanja trećoj strani na temelju postupka predviđenog člankom 23. stavkom 2. APPI-ja (koji omogućuje prijenos podataka trećoj strani bez prethodne privole dotične osobe).

2.3.8. *Odgovornost*

(70) U skladu s načelom odgovornosti subjekti koji obrađuju podatke moraju uspostaviti odgovarajuće tehničke i organizacijske mjere kako bi djelotvorno ispunili svoje obveze u pogledu zaštite podataka te mogli dokazati da su ispunjene, prije svega nadležnom nadzornom tijelu.

(71) Kako je navedeno u bilješci 34. (uvodna izjava 49.), PIHBO-i su u skladu s člankom 26. stavkom 1. APPI-ja dužni provjeriti identitet treće strane koja im dostavlja osobne podatke i „okolnosti" u kojima ih je pribavila (u slučaju osobnih podataka obuhvaćenih ovom Odlukom, te okolnosti prema APPI-ju i Dopunskom pravilu 3. uključuju činjenicu da podaci potječu iz Europske unije te svrhu prvotnog prijenosa podataka). Cilj te mjere je, među ostalim, osigurati zakonitost obrade podataka u cijelom lancu PIHBO-a koji postupaju s osobnim podacima. Nadalje, u skladu s člankom 26. stavkom 3. APPI-ja PIHBO-i moraju voditi evidenciju o datumu primitka i (obveznim) informacijama primljenima od treće strane na temelju stavka 1., o imenu dotičnog pojedinca (ispitanika), kategorijama obrađenih podataka te, u mjeri u kojoj je to relevantno, činjenici da je ispitanik dao privolu za dijeljenje svojih osobnih podataka. Kako je navedeno u članku 18. Pravila PPC-a, ta se evidencija mora čuvati u razdoblju od najmanje jedne do tri godine, ovisno o okolnostima. U obavljanju svojih zadaća PPC može zahtijevati uvid u takvu evidenciju ([39]).

(72) PIHBO-i moraju odmah i na primjeren način rješavati pritužbe dotičnih pojedinaca na obradu njihovih osobnih informacija. Radi lakšeg rješavanja pritužbi oni moraju uspostaviti „sustav potreban za postizanje [te] svrhe", što znači da bi trebali uspostaviti odgovarajuće postupke unutar svoje organizacije (npr. dodijeliti odgovornosti ili odrediti kontaktnu točku).

(73) Naposljetku, APPI stvara okvir za sudjelovanje organizacija sektorske industrije u osiguravanju visoke razine usklađenosti (vidjeti poglavlje IV., odjeljak 4.). Uloga takvih akreditiranih organizacija za zaštitu osobnih informacija ([40]) jest promicati zaštitu osobnih informacija pružanjem podrške poduzećima svojim stručnim znanjem, ali i pridonijeti provedbi zaštitnih mjera, posebice rješavanjem pritužbi pojedinaca i pomaganjem u rješavanju s njima povezanih sporova. U tu svrhu oni mogu od PIHBO-a koji sudjeluju zatražiti da, prema potrebi, poduzmu potrebne mjere ([41]). Osim toga, u slučaju povrede podataka ili drugih sigurnosnih incidenata PIHBO-i u načelu obavješćuju PPC i ispitanika (ili javnost) te poduzimaju potrebne mjere, uključujući mjere za smanjivanje eventualne štete i sprečavanje ponavljanja sličnih incidenata ([42]). Iako su to dobrovoljni programi, PPC je 10. kolovoza 2017. na popis uvrstio 44 organizacije, od kojih samo najvećoj, *Japan Information Processing and*

([38]) Izuzeća su sljedeća: i. „slučajevi utemeljeni na zakonima i propisima"; ii. „slučajevi u kojima je potrebno zaštititi ljudski život, tijelo ili imetak te kad je teško dobiti privolu principala"; iii. „slučajevi u kojima postoji posebna potreba za poboljšanjem javne higijene ili promicanjem zdravlja djece te kad je teško dobiti privolu principala"; iv. „slučajevi u kojima je potrebna suradnja sa središnjom državnom organizacijom ili lokalnom upravom, ili osobom kojoj je povjereno obavljanje poslova propisanih zakonima i propisima, i kad postoji mogućnost da bi dobivanje privole principala moglo omesti obavljanje tih poslova"; i v. slučajevi u kojima osobne informacije koje zahtijevaju posebnu pozornost javno otkrije ispitanik, državna organizacija, lokalna uprava, osoba obuhvaćena jednom od kategorija iz članka 76. stavka 1. ili druge osobe navedene u pravilima PPC-a. Postoji još jedna kategorija koja se odnosi na „ostale slučajeve koji prema Nalogu Kabineta odgovaraju slučajevima iz svake od prethodnih točaka", a prema važećem Nalogu Kabineta prije svega obuhvaćaju uočljiva obilježja osobe (npr. vidljivo zdravstveno stanje) ako su osjetljivi podaci (nenamjerno) dobiveni promatranjem, snimanjem ili fotografiranjem ispitanika, npr. nadzornim kamerama.

([39]) U skladu s člankom 40. stavkom 1. APPI-ja PPC može, u mjeri u kojoj je to potrebno za provedbu odgovarajućih odredaba APPI-ja, zatražiti da PIHBO dostavi potrebne informacije ili materijal povezan s postupanjem s osobnim informacijama.

([40]) U APPI-ju su, među ostalim, propisana pravila o akreditaciji takvih organizacija; vidjeti članke od 47. do 50. APPI-ja.

([41]) Članak 52. APPI-ja.

([42]) Obavijest PPC-a br. 1/2017 „O mjerama koje treba poduzeti u slučaju povrede osobnih podataka ili drugog incidenta".

*Development Center* (JIPDEC), pripada 15 436 poslovnih subjekata ([43]). Među akreditiranim programima su sektorska udruženja kao *Japan Securities Dealers Association, Japan Association of Car Driving Schools* ili *Association of Marriage Brokers* ([44]).

(74) Akreditirane organizacije za zaštitu osobnih informacija dostavljaju godišnja izvješća o svojim aktivnostima. Prema „Pregledu statusa provedbe APPI-ja u financijskoj godini 2015.”, koji je objavio PPC, akreditirane organizacije za zaštitu osobnih informacija primile su ukupno 442 pritužbe, zatražile 123 obrazloženja od poslovnih subjekata u svojoj nadležnosti, u 41 slučaju zatražile dokumente od tih subjekata, izdale 181 uputu i dvije preporuke ([45]).

2.3.9. *Ograničenja daljnjeg prijenosa*

(75) Razina zaštite osobnih podataka koji se prenose iz Europske unije poslovnim subjektima u Japanu ne smije se ugroziti daljnjim prijenosom takvih podataka primateljima u trećim zemljama izvan Japana. Takav „daljnji prijenos”, koji je sa stajališta japanskog poslovnog subjekta međunarodni prijenos iz Japana, trebao bi biti dopušten samo ako se na daljnje primatelje izvan Japana primjenjuju pravila koja osiguravaju sličnu razinu zaštite onoj koja je zajamčena u okviru japanskog pravnog poretka.

(76) Prva zaštita sadržana je u članku 24. APPI-ja, kojim se općenito zabranjuje prijenos osobnih podataka trećoj strani izvan državnog područja Japana bez prethodne privole dotične osobe. Dopunskim pravilom 4. osigurava se da u slučaju prijenosa podataka iz Europske unije osoba koja daje privolu bude posebno dobro informirana time što se zahtijeva da se toj osobi „dostave informacije o okolnostima prijenosa koje su potrebne da bi principal mogao donijeti odluku o privoli”. Na temelju toga ispitanika se obavještava o činjenici da će podaci biti preneseni u inozemstvo (izvan područja primjene APPI-ja) i o zemlji odredišta. To će mu omogućiti da procijeni rizik prijenosa za privatnost. Isto tako, kako se može zaključiti iz članka 23. APPI-ja (vidjeti uvodnu izjavu 47.), informacije koje se dostavljaju principalu trebale bi obuhvaćati obvezne stavke iz njegova stavka 2., odnosno kategorije osobnih podataka dostavljene trećoj strani i način otkrivanja.

(77) U članku 24. APPI-ja, primijenjenom zajedno s člankom 11-2. Pravila PPC-a, utvrđeno je nekoliko iznimaka od tog pravila koje se temelji na privoli. Nadalje, u skladu s člankom 24. ista se odstupanja kao što su ona koja se primjenjuju u skladu s člankom 23. stavkom 1. APPI-ja primjenjuju i na međunarodni prijenos podataka ([46]).

(78) Kako bi se osigurao kontinuitet zaštite u slučaju osobnih podataka prenesenih iz Europske unije u Japan u skladu s ovom Odlukom, Dopunsko pravilo 4. povisuje razinu zaštite za daljnji prijenos takvih podataka od PIHBO-a primatelju u trećoj zemlji. To postiže ograničavanjem i utvrđivanjem osnova za međunarodni prijenos koje PIHBO-i mogu upotrijebiti kao alternativu privoli. Točnije, ne dovodeći u pitanje odstupanja iz članka 23. stavka 1. APPI-ja, osobni podaci preneseni na temelju ove Odluke mogu biti podložni (daljnjem) prijenosu bez privole samo u dva slučaja: i. kad se podaci šalju u treću zemlju za koju je PPC u skladu s člankom 24. APPI-ja utvrdio da pruža istovjetnu razinu zaštite onoj koja je zajamčena u Japanu ([47]); ili ii. ako su PIHBO i treća strana primatelj zajedno proveli mjere koje osiguravaju razinu zaštite istovjetnu APPI-ju, kad se tumači zajedno s Dopunskim pravilima, na temelju ugovora, drugih oblika obvezujućih sporazuma ili obvezujućih dogovora unutar grupacije. Druga kategorija odgovara instrumentima koji se upotrebljavaju u skladu s Uredbom (EU) 2016/679 kako bi se osigurale odgovarajuće zaštitne mjere (posebno ugovorne klauzule i obvezujuća korporativna pravila). Osim toga, kako je potvrdio PPC, čak i u tim slučajevima prijenos trećoj strani i dalje podliježe općim pravilima koja se primjenjuju na svako prosljeđivanje osobnih podataka u okviru APPI-ja (tj. zahtjevu za dobivanje privole u skladu s člankom 23.

([43]) Prema podacima objavljenima na internetskim stranicama *PrivacyMark* JIPDEC-a od 2. listopada 2017.
([44]) PPC, Popis akreditiranih organizacija za zaštitu osobnih informacija, dostupan na internetu na: https://www.ppc.go.jp/personal/nintei/list/ ili https://www.ppc.go.jp/files/pdf/nintei_list.pdf
([45]) PPC, Pregled statusa provedbe APPI-ja u financijskoj godini 2015. (listopad 2016.), dostupno (samo na japanskom jeziku) na internetu na: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf
([46]) Vidjeti bilješku 32.
([47]) U skladu s člankom 11. Pravila PPC-a to ne zahtijeva samo temeljne standarde istovjetne APPI-ju pod djelotvornim nadzorom neovisnog tijela za izvršavanje, već i osiguranu provedbu relevantnih pravila u trećoj zemlji.

stavkom 1. ili, alternativno, zahtjevima za informacije s mogućnošću odbijanja prijenosa iz članka 23. stavka 2. APPI-ja). Ako ispitanik nije dostupan da odgovori na zahtjev za privolu ili pruži potrebne prethodne informacije u skladu s člankom 23. stavkom 2. APPI-ja, prijenos se ne smije izvršiti.

(79) Stoga, osim u slučajevima u kojima je PPC utvrdio da predmetna treća zemlja osigurava razinu zaštite istovjetnu onoj koja je zajamčena APPI-jem ([48]), zahtjevi iz Dopunskog pravila 4. isključuju uporabu instrumenata za prijenos koji ne stvaraju obvezujući odnos između japanskog izvoznika podataka i uvoznika podataka iz treće zemlje te ne jamče zahtijevanu razinu zaštite. To je, primjerice, slučaj APEC-ova sustava pravila zaštite privatnosti pri prekograničnom prijenosu podataka (*Cross Border Privacy Rules*, CBPR), u kojem sudjeluje i Japan ([49]), jer u tom sustavu zaštita ne proizlazi iz dogovora koji obvezuje izvoznika i uvoznika u kontekstu njihova bilateralnog odnosa te je očito niža od razine zajamčene kombinacijom APPI-ja i Dopunskih pravila ([50]).

(80) Naposljetku, još jedna zaštitna mjera u slučaju (daljnjeg) prijenosa proizlazi iz članaka 20. i 22. APPI-ja. U skladu s tim odredbama, ako subjekt iz treće zemlje (uvoznik podataka) djeluje u ime PIHBO-a (izvoznika podataka), tj. kao (pod)izvršitelj obrade, PIHBO mora osigurati nadzor nad tim subjektom u pogledu sigurnosti obrade podataka.

2.3.10. *Prava pojedinaca*

(81) Kao i pravo EU-a o zaštiti podataka, APPI pojedincima jamči niz ostvarivih prava. To uključuje pravo na pristup („otkrivanje"), ispravak i brisanje te pravo na prigovor („prestanak korištenja").

(82) Prvo, u skladu s člankom 28. stavcima 1. i 2. APPI-ja ispitanik ima pravo od PIHBO-a zatražiti da „otkrije pohranjene osobne podatke na temelju kojih ga je moguće identificirati", a nakon primitka takvog zahtjeva PIHBO „mora […] otkriti pohranjene osobne podatke" ispitaniku. Članak 29. (pravo na ispravak) i 30. (pravo na prestanak korištenja) imaju istu strukturu kao članak 28.

(83) U članku 9. Naloga Kabineta navedeno je da se otkrivanje osobnih informacija, kako je navedeno u članku 28. stavku 2. APPI-ja, provodi u pisanom obliku, osim ako su se PIHBO i ispitanik dogovorili drukčije.

(84) Ta prava podliježu trima vrstama ograničenja, koja se odnose na prava i interese samih pojedinaca ili treće strane ([51]), ozbiljno zadiranje u poslovne aktivnosti PIHBO-a ([52]) te slučajeve u kojima bi se otkrivanjem prekršili drugi zakoni ili propisi ([53]). Situacije u kojima bi se ta ograničenja primjenjivala slične su nekima od iznimaka iz članka 23. stavka 1. Uredbe (EU) 2016/679, kojim se omogućuje ograničavanje prava pojedinaca zbog razloga

([48]) PPC dosad nije donio ni jednu odluku na temelju članka 24. APPI-ja kojom bi potvrdio da treća zemlja pruža istovjetnu razinu zaštite onoj koja je zajamčena u Japanu. Jedina odluka čije donošenje trenutačno razmatra odnosi se na EGP. Radi mogućih drugih odluka u budućnosti Komisija će pozorno pratiti situaciju i, bude li potrebno, poduzeti odgovarajuće mjere za uklanjanje mogućih štetnih učinaka na kontinuitet zaštite (vidjeti uvodne izjave 176., 177., 184. i članak 3. stavak 1.).

([49]) Iako su samo dva japanska društva certificirana u okviru APEC-ova sustava CBPR (vidjeti https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). Jedini poslovni subjekti izvan Japana certificirani u tom sustavu svega su 23 društva iz SAD-a (vidjeti https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list).

([50]) Na primjer, nema definicije ni posebne zaštite osjetljivih podataka, nema obveze ograničenog zadržavanja podataka. Vidjeti i Mišljenje 02/2014 Radne skupine iz članka 29. o referentnom dokumentu o zahtjevima obvezujućih korporativnih pravila koja se podnose nacionalnim tijelima za zaštitu podataka u EU-u i pravila za zaštitu privatnosti pri prekograničnom prijenosu podataka koja se podnose akterima za pozivanje na odgovornost APEC-ova CBPR-a, 6. ožujka 2014.

([51]) Prema PPC-u samo interesi koje „vrijedi štititi zakonom" mogu opravdati ograničenje. Ta se procjena mora provesti za svaki slučaj zasebno, „uzimajući u obzir zadiranje u temeljno pravo na privatnost uključujući zaštitu podataka, kako je priznato Ustavom i sudskom praksom." Zaštićeni interesi mogu primjerice uključivati poslovne tajne.

([52]) Pojam „ozbiljno ometanje pravilne provedbe poslovanja subjekta" prikazan je u Smjernicama PPC-a na različitim primjerima, na primjer kad ista osoba više puta podnese isti složeni zahtjev ako takvi zahtjevi uključuju znatno opterećenje poslovnog subjekta koje bi ugrozilo njegovu sposobnost da odgovori na druge zahtjeve (Smjernice PPC-a (*General Rule Edition*), str. 62.). Općenitije govoreći PPC je potvrdio da je ta kategorija ograničena na iznimne slučajeve koji nisu samo manja neugodnost. Konkretno, PIHBO ne može odbiti otkrivanje samo zato što je zatražena velika količina podataka.

([53]) Kako je potvrdio PPC, takvi zakoni moraju poštovati pravo na privatnost kako je zajamčeno Ustavom te stoga „održavati nužno i razumno ograničenje."

povezanih sa „zaštitom ispitanika ili pravima i slobodama drugih" ili „drugim važnim ciljevima od općeg javnog interesa". Iako je kategorija slučajeva u kojima bi se otkrivanjem prekršili „drugi zakoni ili propisi" naizgled široka, zakonima i propisima kojima se u tom pogledu predviđaju ograničenja mora se poštovati ustavno pravo na privatnost te se mogu uvoditi ograničenja samo u mjeri u kojoj bi ostvarivanje tog prava „narušavalo javnu dobrobit" ([54]). To zahtijeva uravnoteženje interesa koji su u pitanju.

(85) U skladu s člankom 28. stavkom 3. APPI-ja, ako traženi podaci ne postoje, ili ako dotični PIHBO odluči ne odobriti pristup pohranjenim podacima, o tome mora bez odgode obavijestiti pojedinca.

(86) Drugo, u skladu s člankom 29. stavcima 1. i 2. APPI-ja ispitanik ima pravo zatražiti ispravak, dopunu ili brisanje svojih pohranjenih osobnih podataka ako su ti podaci netočni. Kad primi takav zahtjev, PIHBO „mora […] provesti potrebnu istragu" i, na temelju rezultata takve istrage, „ispraviti itd. sadržaj pohranjenih podataka".

(87) Treće, u skladu s člankom 30. stavcima 1. i 2. APPI-ja ispitanik ima pravo od PIHBO-a zatražiti da prekine s uporabom osobnih informacija ili ih izbriše ako se pri postupanju s njima krši članak 16. (ograničenje svrhe) ili su nepropisno pribavljeni te se krši članak 17. APPI-ja (pribavljanje prijevarom, drugim nepropisnim sredstvima ili, u slučaju osjetljivih podataka, bez privole). Isto tako, u skladu s člankom 30. stavcima 3. i 4. APPI-ja pojedinac ima pravo od PIHBO-a zatražiti da prestane prosljeđivati informacije trećoj strani ako bi se time kršile odredbe članka 23. stavka 1. ili članka 24. APPI-ja (prosljeđivanje trećoj strani, uključujući međunarodni prijenos).

(88) Ako je zahtjev utemeljen, PIHBO mora bez odgode prekinuti s uporabom podataka ili njihovim prosljeđivanjem trećoj strani, u mjeri u kojoj je to potrebno za otklanjanje povrede ili, ako je predmet obuhvaćen iznimkom (prije svega ako bi prestanak korištenja prouzročio posebno visoke troškove) ([55]), provesti potrebne alternativne mjere za zaštitu prava i interesa dotičnih pojedinaca.

(89) Za razliku od prava EU-a, APPI i relevantna podzakonska pravila ne sadržavaju pravne odredbe koje bi se posebno odnosile na mogućnost protivljenja obradi u svrhu izravnog marketinga. Međutim, takva će se obrada, u skladu s ovom Odlukom, odvijati u kontekstu prijenosa osobnih podataka koji su prethodno prikupljeni u Europskoj uniji. Na temelju članka 21. stavka 2. Uredbe (EU) 2016/679 ispitanik uvijek ima mogućnost usprotiviti se prijenosu podataka u svrhu obrade za izravni marketing. Osim toga, kako je objašnjeno u uvodnoj izjavi 43., u skladu s Dopunskim pravilom 3. PIHBO je dužan obrađivati podatke primljene na temelju Odluke za istu svrhu za koju su preneseni iz Europske unije, osim ako ispitanik pristane na promjenu svrhe korištenja. Prema tome, ako su podaci preneseni u bilo koju drugu svrhu osim izravnog marketinga, PIHBO-i u Japanu neće smjeti obrađivati podatke u svrhu izravnog marketinga bez privole ispitanika iz EU-a.

(90) U svim slučajevima iz članaka 28. i 29. APPI-ja PIHBO mora bez odgode obavijestiti pojedinca o ishodu njegova zahtjeva, a uz to i obrazložiti (djelomično) odbijanje na temelju zakonskih iznimki iz članaka od 27. do 30. (članak 31. APPI-ja).

([54]) Vrhovni sud tumači da je člankom 13. Ustava predviđeno pravo na privatnost (vidjeti prethodne uvodne izjave 7. i 8.). Iako se to pravo može ograničiti u slučajevima kad „zadire u javnu dobrobit", u svojoj presudi od 6. ožujka 2008. (vidjeti uvodnu izjavu 8.) Vrhovni sud pojasnio je da svako ograničenje (kojim se, u ovom slučaju, javnom tijelu dopušta prikupljanje i obrada osobnih podataka) mora biti uravnoteženo s pravom na privatnost, uzimajući u obzir čimbenike kao što su priroda predmetnih podataka, rizike od obrade tih podataka za pojedince, primjenjive zaštitne mjere i koristi od javnog interesa koje proizlaze iz obrade. To je vrlo slično vrsti ravnoteže koja se zahtijeva zakonodavstvom EU-a, na temelju načela nužnosti i proporcionalnosti, za odobravanje bilo kakvog ograničenja u pogledu prava i mjera za zaštitu podataka.

([55]) Za daljnja objašnjenja tih iznimaka vidjeti prof. Katsuya Uga, *Article by Article Commentary of the revised Act on the Protection of Personal Information*, 2015., str. 217. Primjer zahtjeva koji uzrokuje „velike troškove" jest slučaj da su samo neka imena s dugog popisa (npr. u imeniku) obrađena na način koji je protivan načelu ograničenja svrhe, a imenik je već u prodaji, zbog čega bi opoziv tih primjeraka i njihova zamjena novima bili vrlo skupi. Na istom primjeru, ako je već prodano mnogo primjeraka imenika i nemoguće ih je sve prikupiti, bilo bi isto tako „teško ostvariti prestanak korištenja". U tim bi scenarijima „potrebna alternativna mjera" mogla uključivati, na primjer, objavljivanje ili distribuciju obavijesti o ispravku. Takva mjera ne isključuje druge oblike (sudske) pravne zaštite, bilo zbog narušavanja prava na privatnost, štete za ugled (klevete) uzrokovane objavom ili povrede drugih interesa.

(91) Kad je riječ o uvjetima za podnošenje zahtjeva, člankom 32. APPI-ja (zajedno s Nalogom Kabineta) PIHBO-u se omogućuje da odredi razumne postupke, među ostalim u pogledu informacija potrebnih za identifikaciju pohranjenih osobnih podataka. Međutim, prema stavku 4. tog članka, PIHBO-i ne smiju „prekomjerno opteretiti principala". U određenim slučajevima PIHBO-i mogu i naplaćivati naknade uz uvjet da njihov iznos „ne prelazi ono što se smatra razumnim s obzirom na stvarne troškove" (članak 33. APPI-ja).

(92) Konačno, pojedinac se može usprotiviti prosljeđivanju njegovih osobnih podataka trećoj strani na temelju članka 23. stavka 2. APPI-ja ili uskratiti privolu na temelju članka 23. stavka 1. (i time spriječiti otkrivanje u slučaju da nije dostupna druga pravna osnova). Isto tako, pojedinac može zaustaviti obradu podataka u drukčiju svrhu tako da odbije dati privolu u skladu s člankom 16. stavkom 1. APPI-ja.

(93) Za razliku od prava Unije, APPI i relevantna podzakonska pravila ne sadržavaju opće odredbe koje bi se odnosile na pitanje odluka koje utječu na ispitanika i koje se isključivo temelje na automatiziranoj obradi osobnih podataka. Međutim, to je pitanje obuhvaćeno određenim sektorskim pravilima koja su primjenjiva u Japanu, a koja su posebno relevantna za tu vrstu obrade. To uključuje sektore u kojima će se društva najvjerojatnije poslužiti automatiziranom obradom osobnih podataka za donošenje odluka koje utječu na pojedince (npr. financijski sektor). Na primjer, prema „Sveobuhvatnim smjernicama za nadzor nad velikim bankama", revidiranima u lipnju 2017., dotičnom se pojedincu moraju konkretno obrazložiti razlozi za odbijanje zahtjeva za sklapanje ugovora o zajmu. Ta pravila stoga pružaju zaštitu u vjerojatno manjem broju slučajeva u kojima bi automatizirane odluke donosio japanski poslovni subjekt kao „uvoznik" (a ne EU-ov voditelj obrade podataka kao „izvoznik").

(94) U svakom slučaju, kad je riječ o osobnim podacima koji su prikupljeni u Europskoj uniji, svaku odluku koja se temelji na automatiziranoj obradi obično donosi voditelj obrade podataka u Uniji (koji ima izravan odnos s dotičnim ispitanikom) te ona stoga podliježe Uredbi (EU) 2016/679 ([56]). To uključuje scenarije prijenosa u kojima obradu vrši strani (npr. japanski) poslovni subjekt koji djeluje kao posrednik (izvršitelj obrade) u ime voditelja obrade u EU-u (ili kao podobrađivač koji djeluje u ime izvršitelja obrade iz EU-a nakon što je podatke dobio od voditelja obrade u EU-u koji ih je prikupio) koji onda na temelju toga donosi odluku. Stoga nije vjerojatno da će nepostojanje posebnih pravila za automatizirano donošenje odluka u APPI-ju utjecati na razinu zaštite osobnih podataka koji se prenose na temelju ove Odluke.

### 2.4. **Nadzor i izvršavanje**

#### 2.4.1. *Neovisni nadzor*

(95) Kako bi se i u praksi osigurala odgovarajuća razina zaštite podataka, trebalo bi uspostaviti neovisno nadzorno tijelo s ovlastima za praćenje i osiguravanje usklađenosti s pravilima o zaštiti podataka. To bi tijelo pri obavljanju svojih dužnosti i izvršavanju svojih ovlasti trebalo djelovati potpuno neovisno i nepristrano.

(96) U Japanu je tijelo nadležno za praćenje i izvršavanje APPI-ja PPC. Sastoji se od predsjednika i osam povjerenika koje imenuje premijer uz suglasnost obaju domova japanskog parlamenta. Mandat predsjednika i svakog povjerenika traje pet godina, s mogućnošću ponovnog imenovanja (članak 64. APPI-ja). Povjerenike je moguće razriješiti dužnosti samo iz dobro utemeljenog razloga u ograničenom broju iznimnih okolnosti ([57]) i oni ne smiju aktivno sudjelovati u političkim aktivnostima. Nadalje, prema APPI-ju se povjerenici koji rade u punom radnom vremenu moraju suzdržati od bilo kakvih drugih plaćenih aktivnosti ili poslovnih djelatnosti. Na sve povjerenike primjenjuju se i unutarnja pravila prema kojima ne smiju sudjelovati u raspravama u slučaju mogućeg sukoba interesa. PPC-u pomaže tajništvo pod vodstvom glavnog tajnika, osnovano u svrhu obavljanja zadaća dodijeljenih PPC-u (članak 70. APPI-ja). Povjerenici i svi dužnosnici u tajništvu obvezani su strogim pravilima o čuvanju tajne (članci 72. i 82. APPI-ja).

([56]) Suprotno tome, u iznimnom slučaju kada japanski subjekt ima izravan odnos s ispitanikom iz EU-a, to je obično posljedica toga što se ciljano usmjerio na tog pojedinca u Europskoj uniji ponudom robe ili usluga ili praćenjem njegova ponašanja. U tom će scenariju sam japanski subjekt biti obuhvaćen područjem primjene Uredbe (EU) 2016/679 (članak 3. stavak 2.) te se mora izravno pridržavati prava EU-a o zaštiti podataka.

([57]) Prema članku 65. APPI-ja povjerenika je protiv njegove volje moguće razriješiti dužnosti samo iz jednog od sljedećih razloga: i. pokretanje stečajnog postupka; ii. osuda zbog povrede APPI-ja ili Zakona o uporabi brojeva za identifikaciju pojedinca u administrativnom postupku (*Numbers Use Act*); iii. osuda na kaznu zatvora bez mogućnosti rada ili strožu kaznu; iv. nesposobnost za izvršavanje dužnosti zbog duševnog ili fizičkog poremećaja ili povrede dužnosti.

(97) Ovlasti PPC-a, koje on izvršava potpuno neovisno ([58]), uglavnom su utvrđene u člancima 40., 41. i 42. APPI-ja. U skladu s člankom 40. PPC može zatražiti od PIHBO-a da ga izvijesti ili dostavi dokumente o postupcima obrade te može provoditi inspekcijske preglede na licu mjesta ili preglede evidencije ili drugih dokumenata. U mjeri u kojoj je to potrebno za izvršavanje APPI-ja PPC može PIHBO-ima dati i smjernice ili ih savjetovati o postupanju s osobnim informacijama. PPC je već iskoristio tu ovlast u skladu s člankom 41. APPI-ja uputivši smjernice Facebooku nakon nedavnog slučaja Facebook/Cambridge Analytica.

(98) Valja naglasiti da PPC u pojedinačnim slučajevima (pri poduzimanju mjera na temelju pritužbe ili na vlastitu inicijativu) ima ovlasti za izdavanje preporuka i naloga radi izvršavanja APPI-ja i obvezujućih pravila (uključujući Dopunska pravila). Te su ovlasti utvrđene u članku 42. APPI-ja. Iako se u njegovim stavcima 1. i 2. predviđa dvofazni mehanizam kojim PPC može izdati nalog (tek) kad mu prethodi preporuka, stavkom 3. omogućuje se izravno izdavanje naloga u hitnim slučajevima.

(99) Iako nisu sve odredbe poglavlja IV. odjeljka 1. APPI-ja uvrštene u popis u članku 42. stavku 1., kojim se određuje i područje primjene članka 42. stavka 2., to se može objasniti činjenicom da se neke od tih odredaba ne odnose na obveze PIHBO-a ([59]) i da je sva bitna zaštita već osigurana drugim odredbama s tog popisa. Primjerice, iako se članak 15. (kojim se od PIHBO-a zahtijeva da odredi svrhu korištenja te da relevantne osobne informacije obrađuje isključivo unutar njezina opsega) ne spominje, neispunjavanje tog zahtjeva može biti osnova za preporuku zbog povrede članka 16. stavka 1. (kojim se PIHBO-u zabranjuje obrada osobnih informacija koja prelazi ono što je potrebno za postizanje svrhe korištenja, osim ako dobije privolu ispitanika) ([60]). Sljedeća odredba koja nije na popisu u članku 42. stavku 1. jest članak 19. APPI-ja o točnosti i zadržavanju podataka. U slučaju nepoštovanja te odredbe ona se može prisilno provesti bilo na temelju kršenja članka 16. stavka 1. ili kršenja članka 29. stavka 2. ako dotična osoba zatraži ispravak ili brisanje pogrešnih ili nerazmjerno opsežnih podataka, a PIHBO odbije ispuniti taj zahtjev. Kad je riječ o pravima ispitanika u skladu s člankom 28. stavkom 1., člankom 29. stavkom 1. i člankom 30. stavkom 1., nadzor PPC-a osiguran je time što su mu dodijeljene ovlasti prisilne provedbe odgovarajućih obveza PIHBO-a iz tih članaka.

(100) U skladu s člankom 42. stavkom 1. APPI-ja PPC može, ako uviđa da postoji „potreba za zaštitom prava i interesa pojedinca u slučajevima u kojima je [PIHBO] prekršio" posebne odredbe APPI-ja, izdati preporuku da se „zaustavi kršenje ili poduzmu druge potrebne mjere za ispravljanje povrede". Takva preporuka nije obvezujuća, ali otvara put obvezujućem nalogu na temelju članka 42. stavka 2. APPI-ja. Na temelju te odredbe, ako se preporuka ne poštuje „bez opravdanih razloga", a PPC „uvidi da je ozbiljna povreda prava i interesa pojedinca neposredna", može PIHBO-u naložiti da poduzme mjere u skladu s preporukom.

(101) Dopunska pravila pobliže objašnjavaju i potkrepljuju ovlasti prisilne provedbe PPC-a. Točnije, u slučajevima koji uključuju podatke uvezene iz Europske unije, ako PIHBO bez opravdanog razloga ne poduzme mjere u skladu s preporukom PPC-a na temelju članka 42. stavka 1. APPI-ja, PPC će to uvijek smatrati ozbiljnom i neposrednom povredom prava i interesa pojedinca u smislu članka 42. stavka 2., a time i povredom koja zahtijeva izdavanje obvezujućeg naloga. Nadalje, kao „opravdan razlog" za nepridržavanje preporuke PPC prihvaća samo „izvanredni događaj [koji sprečava pridržavanje] izvan kontrole [PIHBO-a] koji se ne može razumno predvidjeti (npr. prirodne katastrofe)" ili slučajeve u kojima poduzimanje mjera u skladu s preporukom „više nije potrebno jer je [PIHBO] poduzeo alternativne mjere kojima je povreda u potpunosti ispravljena."

([58]) Vidjeti članak 62. APPI-ja.

([59]) Na primjer, određene se odredbe odnose na neobvezne mjere PIHBO-a (članci 32. i 33. APPI-ja) ili na obveze „u okviru njihovih mogućnosti" koje kao takve nije moguće prisilno provesti (članci 31. i 35. članak 36. stavak 6. i članak 39. APPI-ja). Određene odredbe nisu upućene PIHBO-u nego drugim dionicima. To je, primjerice, slučaj s člankom 23. stavkom 4., člankom 26. stavkom 2. i člankom 34. APPI-ja (no provedba članka 26. stavka 2. APPI-ja osigurana je mogućnošću kaznenih sankcija na temelju članka 88. točke i. APPI-ja).

([60]) Nadalje, kako je prethodno objašnjeno u uvodnoj izjavi 48., u kontekstu prijenosa „svrhu korištenja" određuje izvoznik podataka iz EU-a, koji je u tom smislu obvezan člankom 5. stavkom 1. točkom (b) Uredbe (EU) 2016/679. Provedbu te obveze može naložiti nadležno tijelo za zaštitu podataka u Europskoj uniji.

(102) Nepoštovanje naloga PPC-a smatra se kaznenim djelom na temelju članka 84. APPI-ja te PIHBO koji je proglašen krivim može biti osuđen na kaznu do šest mjeseci zatvora uz mogućnost rada ili dobiti novčanu kaznu u iznosu do 300 000 jena. Nadalje, u skladu s člankom 85. točkom i. APPI-ja nesuradnja s PPC-om ili ometanje njegove istrage kažnjivo je novčanom kaznom od najviše 300 000 jena. Te kaznene sankcije primjenjuju se uz one koje se mogu odrediti za bitna kršenja APPI-ja (vidjeti uvodnu izjavu 108.).

2.4.2. *Sudska zaštita*

(103) Kako bi se osigurala odgovarajuća zaštita, a posebno ostvarivanje prava pojedinca, ispitaniku bi trebalo pružiti djelotvornu upravnu i sudsku zaštitu, uključujući naknadu štete.

(104) Prije ili umjesto traženja upravne ili sudske zaštite pojedinac može odlučiti podnijeti pritužbu na obradu svojih osobnih podataka samom voditelju obrade. Na temelju članka 35. APPI-ja PIHBO-i nastoje takve pritužbe rješavati „na primjeren način i bez odlaganja" te uspostaviti interne sustave rješavanja pritužbi radi postizanja tog cilja. Osim toga, na temelju članka 61. točke ii. APPI-ja PPC je odgovoran za „potrebno posredovanje u podnesenoj pritužbi i suradnju ponuđenu poslovnom subjektu koji rješava pritužbu", koja u oba slučaja obuhvaća pritužbe koje su podnijeli stranci. U tom pogledu japanski je zakonodavac i središnjoj vlasti povjerio poduzimanje „potrebnih mjera" kako bi se PIHBO-ima omogućilo i olakšalo rješavanje pritužbi (članak 9.), a lokalne vlasti nastoje osigurati mirenje u takvim slučajevima (članak 13.). S obzirom na to pojedincima je za podnošenje pritužbe na raspolaganju više od 1 700 potrošačkih centara koje su uspostavile lokalne vlasti na temelju Zakona o sigurnosti potrošača (*Consumer Safety Act*) ([61]), uz mogućnost podnošenja pritužbe Nacionalnom centru za pitanja potrošača (*National Consumer Affairs Centre*) u Japanu. Takve se pritužbe mogu podnijeti i u vezi s kršenjem APPI-ja. U skladu s člankom 19. Temeljnog zakona o potrošačima (*Basic Consumer Act*) ([62]) lokalne vlasti moraju se nastojati uključiti u postupak mirenja u vezi s pritužbama te strankama pružiti potrebno stručno znanje. Čini se da su ti mehanizmi za rješavanje sporova prilično djelotvorni jer je 2015. u više od 75 000 pritužbi stopa rješavanja bila 91,2 %.

(105) Ako PIHBO prekrši odredbe APPI-ja, to može dovesti do pokretanja građanskih ili kaznenih postupaka sa sankcijama. Prvo, ako pojedinac smatra da su povrijeđena njegova prava iz članaka 28., 29. i 30. APPI-ja, može zatražiti privremenu mjeru tražeći od suda da PIHBO-u naloži da ispuni njegov zahtjev u skladu s tim odredbama, tj. da otkrije pohranjene osobne podatke (članak 28.), da ispravi pohranjene osobne podatke koji su netočni (članak 29.) ili da prestane s nezakonitom obradom ili prosljeđivanjem podataka trećoj strani (članak 30.). Takve se mjere mogu poduzeti bez pozivanja na članak 709. Građanskog zakonika ([63]) ili općenito na odštetno pravo ([64]). To konkretno znači da osoba ne mora dokazati da je pretrpjela štetu.

(106) Drugo, u slučaju kad se navodna povreda ne odnosi na prava pojedinca iz članaka 28., 29. i 30., nego na opća načela zaštite podataka ili obveze PIHBO-a, dotična osoba može pokrenuti parnični postupak protiv poslovnog subjekta na temelju odredaba o građanskoj odgovornosti iz japanskog Građanskog zakonika, a posebno članka 709. Iako je za pokretanje postupka u skladu s člankom 709. osim krivnje (namjere ili nemara) potrebno dokazati štetu, prema članku 710. Građanskog zakonika takva šteta može biti i materijalna i nematerijalna. Nema ograničenja za visinu iznosa naknade.

(107) Kad je riječ o dostupnim naknadama, članak 709. japanskog Građanskog zakonika upućuje na novčanu naknadu. Međutim, prema tumačenju u japanskoj sudskoj praksi taj članak omogućuje i dobivanje sudskog naloga ([65]). Stoga, ako ispitanik pokrene postupak na temelju članka 709. Građanskog zakonika i tvrdi da su njegova prava ili interesi oštećeni zbog povrede odredbe APPI-ja koju je počinio tuženik, osim naknade štete, tim se zahtjevom može tražiti izdavanje privremene mjere, posebno za obustavu nezakonite obrade.

([61]) Zakon br. 50 od 5. lipnja 2009.
([62]) Zakon br. 60 od 22. kolovoza 2012.
([63]) Članak 709. Građanskog zakonika glavna je osnova kad je riječ o građanskim sporovima za naknadu štete. U skladu s tom odredbom „osoba koja je namjerno ili iz nemara povrijedila pravo drugih, ili zakonom zaštićen interes drugih, dužna je nadoknaditi time nanesenu štetu".
([64]) Visoki sud u Tokiju, presuda od 20. svibnja 2015. (nije objavljena); Okružni sud u Tokiju, presuda od 8. rujna 2014., Westlaw Japan 2014WLJPCA09088002. Vidjeti i članak 34. stavke 1. i 3. APPI-ja.
([65]) Vidjeti Vrhovni sud, presuda od 24. rujna 2002. (Hanrei Times, svezak 1106., str. 72.)

(108) Treće, osim pravnih lijekova iz građanskog (odštetnog) prava, ispitanik može podnijeti pritužbu javnom tužitelju ili službeniku pravosudne policije zbog kršenja APPI-ja koja mogu dovesti do kaznenih sankcija. Poglavlje VII. APPI-ja sadržava niz kaznenih odredaba. Najvažnija (članak 84.) odnosi se na PIHBO-ovo neispunjavanje naloga PPC-a u skladu s člankom 42. stavcima 2. i 3. Ako poslovni subjekt ne ispuni nalog koji je izdao PPC, predsjednik PPC-a (kao i bilo koji drugi državni službenik) ([66]) može uputiti predmet javnom tužitelju ili službeniku pravosudne policije te na taj način pokrenuti kazneni postupak. Za kršenje naloga PPC-a propisana je kazna zatvora uz mogućnost rada od najviše šest mjeseci ili novčana kazna od najviše 300 000 jena. Ostale odredbe APPI-ja koje određuju sankcije u slučaju kršenja APPI-ja koja utječu na prava i interese ispitanika uključuju članak 83. APPI-ja (u vezi s „prikrivenim pružanjem ili uporabom" baze podataka s osobnim informacijama „s ciljem ostvarivanja […] nezakonite dobiti") i članak 88. točku i. APPI-ja (u vezi s neispunjavanjem obveze treće strane da PIHBO-a točno obavijesti kad on prima osobne podatke u skladu s člankom 26. stavkom 1. APPI-ja, posebno o pojedinostima o njezinu vlastitu prethodnom pribavljanju takvih podataka). Za takva je kršenja APPI-ja propisana kazna zatvora uz mogućnost rada do godine dana ili novčana kazna od najviše 500 000 jena (u slučaju članka 83.) ili administrativna novčana kazna od najviše 100 000 jena (u slučaju članka 88. točke i.). Iako će već i sama prijetnja kaznenim sankcijama vjerojatno imati snažan odvraćajući učinak na rukovodeća tijela koja upravljaju postupcima obrade PIHBO-a i na pojedince koji postupaju s podacima, u članku 87. APPI-ja pojašnjava se da se u slučaju da predstavnik, zaposlenik ili drugi radnik poduzeća ne postupi u skladu s člancima od 83. do 85. APPI-ja „počinitelj kažnjava, a predmetno društvo snosi novčanu kaznu navedenu u odgovarajućim člancima". U tom se slučaju i zaposleniku i društvu mogu odrediti sankcije do maksimalnog iznosa.

(109) Konačno, pojedinci mogu zatražiti i pravnu zaštitu od radnji ili propusta PPC-a. U tom pogledu japansko pravo pruža razne mogućnosti upravne i sudske zaštite.

(110) Ako pojedinac nije zadovoljan djelovanjem PPC-a, može podnijeti upravnu žalbu na temelju Zakona o preispitivanju odluka upravnih tijela (*Administrative Complaint Review Act*) ([67]). S druge strane, ako pojedinac smatra da je PPC propustio postupati, može u skladu s člankom 36-3. tog Zakona od PPC-a zatražiti da poduzme radnje ili pruži administrativne smjernice ako smatra da „odluka ili administrativne smjernice potrebne za ispravak povrede nisu izdane ili provedene".

(111) Kad je riječ o sudskoj zaštiti, na temelju Zakona o upravnim sporovima *Administrative Case Litigation Act*), osoba koja nije zadovoljna s upravnim postupanjem PPC-a može od suda zatražiti da PPC-u izda *mandamus* ([68]) i naloži mu da poduzme daljnje mjere ([69]). U određenim slučajevima sud može izdati i privremeni nalog *mandamus* kako bi spriječio nepopravljivu štetu ([70]). Nadalje, na temelju istog Zakona pojedinac može zatražiti opoziv odluke PPC-a ([71]).

(112) Konačno, pojedinac može na temelju članka 1. stavka 1. Zakona o naknadi štete od države (*State Redress Act*) podnijeti tužbu za naknadu štete od države protiv PPC-a u slučaju da je pretrpio štetu zbog činjenice da je nalog koji je PPC izdao poslovnom subjektu bio nezakonit ili da PPC nije izvršavao svoje ovlasti.

### 3. **PRISTUP JAVNIH TIJELA U JAPANU OSOBNIM PODACIMA PRENESENIMA IZ EUROPSKE UNIJE I NJIHOVA UPORABA TIH PODATAKA**

(113) Komisija je ocijenila i ograničenja i zaštitne mjere, uključujući mehanizme za nadzor i pravnu zaštitu pojedinaca dostupne u japanskom pravu kad je riječ o prikupljanju i naknadnoj uporabi osobnih podataka koje javna tijela prenose poslovnim subjektima u Japanu zbog javnog interesa, posebno za potrebe kaznenog progona i nacionalne sigurnosti („pristup vlade"). U tom je pogledu japanska vlada Komisiji dostavila službene izjave, jamstva i obveze potpisane na najvišoj ministarskoj razini i razini agencija, koje sadržava Prilog II. ovoj Odluci.

([66]) Članak 239. stavak 2. Zakona o kaznenom postupku.
([67]) Zakon br. 160 iz 2014.
([68]) Članak 37-2. Zakona o upravnim sporovima.
([69]) U skladu s člankom 3. stavkom 6. Zakona o upravnim sporovima pojam „mjera mandamus" odnosi se na postupak kojim se od suda traži izdavanje naloga protiv upravne agencije kako bi donijela prvotnu upravnu odluku koju je „trebala" donijeti, ali nije.
([70]) Članak 37–5. Zakona o upravnim sporovima.
([71]) Poglavlje II., odjeljak 1. Zakona o upravnim sporovima.

3.1. **Opći pravni okvir**

(114) Kao oblik izvršavanja javnih ovlasti pristup vlade u Japanu mora se provoditi potpuno u skladu sa zakonom (načelo zakonitosti). U tom pogledu japanski ustav sadržava odredbe kojima se prikupljanje osobnih podataka od strane javnih tijela ograničava i utvrđuje. Kako je već spomenuto u pogledu obrade koju provode poslovni subjekti, na temelju članka 13. Ustava koji, među ostalim, štiti pravo na slobodu, Vrhovni sud Japana priznao je pravo na privatnost i zaštitu podataka ([72]). Važan je aspekt tog prava sloboda da se osobne informacije ne otkrivaju trećoj strani bez dopuštenja dotične osobe ([73]). To podrazumijeva pravo na djelotvornu zaštitu osobnih podataka od zlouporabe i (posebno) nezakonitog pristupa. Dodatna zaštita osigurava se člankom 35. Ustava o pravu svih osoba na sigurnost vlastitog doma, dokumenata i imovine, kojim se od javnih tijela zahtijeva da za svaki slučaj „pretraga i zapljena" ishode sudski nalog izdan iz „primjerenog razloga" ([74]). U svojoj presudi od 15. ožujka 2017. (predmet GPS) Vrhovni sud pojasnio je da se zahtjev u pogledu sudskog naloga primjenjuje kad god se vlada upliće („ulazi") u privatnu sferu na način koji je protiv volje pojedinca, i to provedbom „obvezne istrage". Sudac takav nalog može izdati samo na temelju konkretne sumnje o počinjenju kaznenog djela, tj. kad mu se dostavi dokazna dokumentacija na temelju koje se može smatrati da je osoba na koju se istraga odnosi počinila kazneno djelo ([75]). Prema tome, japanska nadležna tijela nemaju pravne ovlasti prikupljati osobne informacije prisilnim sredstvima u situacijama u kojima još nije došlo do kršenja zakona ([76]), na primjer radi sprečavanja kaznenog djela ili druge sigurnosne prijetnje (kao u slučaju istraga zbog nacionalne sigurnosti).

(115) U skladu s načelom postupanja na temelju zakona svako se prikupljanje podataka kao dio prisilne istrage mora posebno odobriti u skladu sa zakonom (kao što je navedeno, na primjer, u članku 197. stavku 1. Zakona o kaznenom postupku (*Code of Criminal Procedure*, CCP) u vezi s prisilnim prikupljanjem informacija za potrebe kaznene istrage). Taj se zahtjev primjenjuje i na pristup elektroničkim informacijama.

(116) Važno je napomenuti da se člankom 21. stavkom 2. Ustava jamči tajnost svih sredstava komunikacije, a ograničenja se dopuštaju samo zakonima iz razloga javnog interesa. Člankom 4. Zakona o telekomunikacijama (*Telecommunications Business Act*), prema kojem se tajnost komunikacija s kojima postupa telekomunikacijski operater ne smije prekršiti, taj se zahtjev povjerljivosti provodi na razini zakona. To se tumači kao zabrana otkrivanja informacija iz komunikacija, osim u slučaju privole korisnika ili na temelju izričitog oslobođenja od kaznene odgovornosti prema Kaznenom zakonu ([77]).

(117) Ustavom se jamči i pravo na pristup sudovima (članak 32.) te pravo da se državu tuži za naknadu štete u slučaju da je pojedinac pretrpio štetu zbog protuzakonitog postupanja javnog službenika (članak 17.).

(118) Kad je riječ konkretno o pravu na zaštitu podataka, u poglavlju III. odjeljcima 1., 2. i 3. APPI-ja utvrđuju se opća načela koja obuhvaćaju sve sektore, uključujući javni sektor. Točnije, člankom 3. APPI-ja propisuje se da se s osobnim informacijama mora postupati u skladu s načelom poštovanja osobnosti pojedinaca. Nakon što javna tijela prikupe („pribave") osobne informacije, među ostalim kao dio elektroničke evidencije ([78]), postupanje s njima uređeno je Zakonom o zaštiti osobnih informacija u posjedu upravnih organa (*Act on the Protection of Personal*

([72]) Vidjeti npr. Vrhovni sud, presuda od 12. rujna 2003., predmet br. 1656 (2002 (Ju)). Konkretno, Vrhovni sud je utvrdio da „svaki pojedinac ima slobodu štititi svoje osobne informacije od otkrivanja trećoj strani ili objavljivanja bez opravdanog razloga".

([73]) Vrhovni sud, presuda od 6. ožujka 2008. (Juki-net).

([74]) „Primjeren razlog" postoji samo kad se smatra da je dotični pojedinac (osumnjičenik, optuženik) počinio kazneno djelo te su pretraga i zapljena nužni za kaznenu istragu. Vidjeti Vrhovni sud, presuda od 18. ožujka 1969., predmet br. 100 (1968 (Shi)).

([75]) Vidjeti članak 156. stavak 1. Pravila kaznenog postupka (*Rules of Criminal Procedure*).

([76]) Međutim, valja napomenuti da se Zakonom o kažnjavanju kaznenih djela organiziranog kriminala i kontrole imovinske koristi povezane s kaznenim djelom od 15. lipnja 2017. uvodi novo kazneno djelo pripreme kaznenog djela terorizma i određenih drugih oblika organiziranog kriminala. Istrage se mogu pokretati u slučaju konkretne sumnje, na temelju dokaza da su ispunjena sva tri nužna uvjeta za kazneno djelo (uključenost organizirane zločinačke skupine, „planiranje" i „priprema za provedbu" kaznenog djela). Vidjeti i npr. članke od 38. do 40. Zakona o sprečavanju subverzivnog djelovanja (*Subversive Activities Prevention Act*) (Zakon br. 240 od 21. srpnja 1952.).

([77]) Članak 15. stavak 8. Smjernica za zaštitu osobnih informacija u sektoru telekomunikacija.

([78]) Upravni organi kako su definirani u članku 2. stavku 1. APPIHAO-a. Prema informacijama dobivenima od japanske vlade, sva javna tijela osim prefekturalne policije obuhvaćena su definicijom „upravnih organa". Prefekturalna policija međutim djeluje u pravnom okviru Prefekturalnog pravilnika za zaštitu osobnih informacija (vidjeti članak 11. APPI-ja i osnovnu politiku), u kojem su propisane odredbe za zaštitu osobnih informacija koje odgovaraju onima iz APPIHAO-a. Vidjeti Prilog II., odjeljak I.B. Kako je objasnio PPC, u „osnovnoj politici" ti se pravilnici moraju donijeti na temelju sadržaja APPIHAO-a, a MIC objavljuje obavijesti kako bi lokalnim vlastima u tom pogledu dao potrebne smjernice. Kao što je PPC naglasio „u tim se granicama pravilnici za zaštitu osobnih informacija u svakoj prefekturi uspostavljaju […] na temelju osnovne politike i sadržaja obavijesti".

*Information held by Administrative Organs*, APPIHAO) ([79]). To u načelu uključuje ([80]) i obradu osobnih informacija u svrhu kaznenog progona ili za potrebe nacionalne sigurnosti. APPIHAO-om je, među ostalim, predviđeno da javna tijela: i. pohranjuju osobne podatke samo u mjeri u kojoj je to potrebno za izvršavanje njihovih dužnosti; ii. ne upotrebljavaju takve informacije u „nepoštene" svrhe niti ih otkrivaju trećoj strani bez opravdanja; iii. navode svrhu i ne mijenjaju je više od onoga što se razumno može smatrati relevantnim za prvotnu svrhu (ograničenje svrhe); iv. pohranjene osobne informacije u načelu ne upotrebljavaju niti pružaju trećoj strani za druge svrhe, a ako to smatraju potrebnim, za treću stranu određuju ograničenja svrhe ili metode uporabe; v. nastoje osigurati točnost informacija (kvaliteta podataka); vi. poduzimaju potrebne mjere za pravilno upravljanje informacijama i sprečavaju neovlašteno odavanje, gubitak ili oštećenje (sigurnost podataka); i vii. nastoje pravilno i brzo obraditi sve pritužbe u vezi s obradom informacija ([81]).

### 3.2. **Pristup japanskih javnih tijela podacima i njihova uporaba za potrebe kaznenog progona**

(119) Japanski zakon sadržava niz ograničenja pristupa i uporabe osobnih podataka u svrhu kaznenog progona, kao i mehanizme za nadzor i pravnu zaštitu koji su dovoljno jamstvo da će podaci biti djelotvorno zaštićeni od nezakonitog zadiranja i rizika od zlouporabe.

#### 3.2.1. *Pravna osnova i primjenjiva ograničenja/zaštitne mjere*

(120) U japanskom pravnom okviru prikupljanje elektroničkih informacija u svrhu kaznenog progona dopušteno je na temelju sudskog naloga (prisilno prikupljanje) ili zahtjeva za dobrovoljno otkrivanje.

##### 3.2.1.1. Obvezna istraga na temelju sudskog naloga

(121) Kao što je navedeno u uvodnoj izjavi 115., svako prikupljanje podataka u okviru prisilne istrage mora se posebno zakonski odobriti i može se provoditi samo na temelju sudskog naloga „izdanog iz primjerenog razloga" (članak 35. Ustava). Kad je riječ o istrazi kaznenih djela, taj se zahtjev odražava u odredbama Zakona o kaznenom postupku (CCP). Prema članku 197. stavku 1. CCP-a obvezne mjere „ne primjenjuju se osim ako su u ovom Zakonu utvrđene posebne odredbe". Jedina su relevantna ([82]) pravna osnova za prikupljanje elektroničkih informacija članak 218. CCP-a (pretraga i zapljena) i članak 222-2. CCP-a, prema kojemu se obvezne mjere za presretanje elektroničkih komunikacija bez privole jedne od strana provode na temelju drugih zakona, odnosno Zakona o prisluškivanju za kaznene istrage (*Act on Wiretapping for Criminal Investigation*, dalje u tekstu „Zakon o prisluškivanju"). U oba slučaja potreban je sudski nalog.

(122) Konkretno, u skladu s člankom 218. stavkom 1. CCP-a javni tužitelj, pomoćnik javnog tužitelja ili službenik pravosudne policije mogu, ako je to potrebno za istragu kaznenog djela, provesti pretragu ili zapljenu (među ostalim i zapisa) uz prethodni nalog suca ([83]). Taj nalog među ostalim sadržava ime osumnjičenika ili optuženika, kazneno djelo za koje se optužuje ([84]), elektromagnetne zapise koje treba zaplijeniti i „mjesto ili predmete" koje je potrebno pregledati (članak 219. stavak 1. CCP-a).

([79]) Osobne informacije koje pribave službenici upravnog organa tijekom izvršavanja svojih dužnosti te koje navedeni upravni organ pohranjuje za organizacijsku uporabu obuhvaćene su definicijom „pohranjenih osobnih informacija" u smislu članka 2. stavka 3. APPIHAO-a pod uvjetom da su evidentirane u „upravnim dokumentima". To uključuje i elektroničke informacije koje takva tijela prikupljaju i dalje obrađuju jer definicija „upravnih dokumenata" iz članka 2. stavka 2. Zakona o pristupu informacijama u posjedu upravnih organa (*Act on Access to Information Held by Administrative Organs*, Zakon br. 42 iz 1999.) obuhvaća elektromagnetske zapise.

([80]) Međutim, u skladu s člankom 53-2. Zakona o kaznenom postupku, poglavlje IV. APPIHAO-a isključeno je za „dokumente o suđenjima", koji prema primljenim informacijama uključuju elektroničke informacije pribavljene na temelju sudskog naloga ili zahtjeva za dobrovoljnu suradnju u okviru kaznene istrage. Isto tako, kad je riječ o informacijama prikupljenima u području nacionalne sigurnosti, pojedinci se neće moći uspješno pozivati na svoja prava na temelju APPIHAO-a ako čelnik javnog tijela ima „opravdanih razloga" smatrati da bi se otkrivanjem „moglo naštetiti nacionalnoj sigurnosti" (vidjeti članak 14. točku iv.). No javna tijela dužna su, kad god je to moguće, omogućiti barem djelomično otkrivanje (članak 15.).

([81]) Vidjeti konkretna upućivanja na APPIHAO u Prilogu II., odjeljak II.A.1)(b)(2).

([82]) Iako se člankom 220. CCP-a dopušta pretraga i zapljena „na licu mjesta" bez sudskog naloga ako javni tužitelj, pomoćnik javnog tužitelja ili službenik pravosudne policije uhiti osumnjičenika/očitog počinitelja, to nije relevantno u kontekstu prijenosa, a time ni za potrebe ove Odluke.

([83]) U skladu s člankom 222. stavkom 1. u vezi s člankom 110. CCP-a nalog za pretragu/zapljenu zapisa mora se predočiti osobi koja se podvrgava toj mjeri.

([84]) Vidjeti i članak 189. stavak 2. CCP-a, prema kojemu službenik pravosudne policije istražuje počinitelja i predmetne dokaze „ako smatra da je kazneno djelo počinjeno." Isto tako, prema članku 155. stavku 1. Pravila kaznenog postupka, pisani zahtjev za sudski nalog mora, među ostalim, sadržavati „kazneno djelo za koje se optužuje" i „sažetak činjeničnog stanja o kaznenom djelu".

(123) Kad je riječ o presretanju komunikacija, člankom 3. Zakona o prisluškivanju takve se mjere odobravaju samo pod strogim uvjetima. Konkretno, javna tijela moraju ishoditi prethodni sudski nalog koji se može izdati samo za istragu određenih teških kaznenih djela (navedeni u Prilogu tom Zakonu) ([85]) i kad je „iznimno teško na drugi način utvrditi identitet počinitelja ili pojasniti okolnosti/pojedinosti počinjenja" ([86]). Prema članku 5. Zakona o prisluškivanju nalog se izdaje na ograničeno vrijeme, a sudac može odrediti dodatne uvjete. Osim toga, Zakonom o prisluškivanju predviđen je niz dodatnih jamstava kao što su, primjerice, nužna prisutnost svjedoka (članci 12. i 20.), zabrana prisluškivanja komunikacije određenih povlaštenih skupina (npr. liječnika, odvjetnika) (članak 15.), obveza prekida prisluškivanja ako više nije opravdano, čak i ako je nalog još valjan (članak 18.), ili opći zahtjev obavješćivanja dotičnog pojedinca i davanja pristupa evidenciji u roku od trideset dana od završetka prisluškivanja (članci 23. i 24.).

(124) U svim obveznim mjerama na temelju sudskog naloga smije se provoditi samo ona istražna radnja „koja je nužna za ostvarivanje cilja", odnosno ako se ciljevi koji se žele postići istragom ne mogu postići na drugi način (članak 197. stavak 1. CCP-a). Iako kriteriji za određivanje nužnosti nisu detaljnije utvrđeni zakonom, Vrhovni sud Japana odlučio je da bi sudac koji izdaje nalog trebao provesti sveukupnu procjenu, uzimajući u obzir posebno i. težinu kaznenog djela i način na koji je počinjeno; ii. vrijednost i važnost materijala koji će se zaplijeniti kao dokaz; iii. vjerojatnost (rizik) prikrivanja ili uništenja dokaza; i iv. opseg u kojem zapljena može nanijeti štetu dotičnoj osobi ([87]).

3.2.1.2. Zahtjev za dobrovoljno otkrivanje na temelju „istražnog obrasca"

(125) Javna tijela mogu u granicama svoje nadležnosti prikupljati elektroničke informacije i na temelju zahtjeva za dobrovoljno otkrivanje. To se odnosi na neobvezujući oblik suradnje kad ispunjavanje zahtjeva nije moguće prisilno provesti ([88]) te su stoga javna tijela oslobođena obveze ishođenja sudskog naloga.

(126) Ako je takav zahtjev upućen poslovnom subjektu i odnosi se na osobne informacije, poslovni subjekt mora ispunjavati zahtjeve iz APPI-ja. U skladu s člankom 23. stavkom 1. APPI-ja poslovni subjekti mogu otkriti osobne informacije trećoj strani bez privole dotične osobe samo u određenim slučajevima, među ostalim i ako se otkrivanje „temelji na zakonima i propisima" ([89]). U području kaznenog progona pravnu osnovu za takve zahtjeve pruža članak 197. stavak 2. CCP-a, prema kojemu se „od privatnih organizacija može zatražiti da izvještavaju o pitanjima bitnima za istragu". Budući da je takav „istražni obrazac" dopušten samo u okviru kaznene istrage, preduvjet je konkretna sumnja na već počinjeno kazneno djelo ([90]). Štoviše, s obzirom na to da takve istrage obično provodi prefekturalna policija, primjenjuju se ograničenja u skladu s člankom 2. stavkom 2. Zakona o policiji ([91]). U skladu s tom odredbom aktivnosti policije su „strogo ograničene" na ispunjenje njihovih odgovornosti i dužnosti (tj. sprečavanje, suzbijanje i istragu kaznenih djela). Osim toga, u obavljanju svojih dužnosti policija djeluje nepristrano, bez predrasuda i pošteno te nikad ne smije zloupotrebljavati svoje ovlasti „na način kojim bi zadirala u prava i slobode pojedinaca zajamčena Ustavom Japana" (što uključuje, kako je navedeno, pravo na privatnost i zaštitu podataka) ([92]).

(127) Posebno s obzirom na članak 197. stavak 2. CCP-a Nacionalna policijska agencija (NPA), kao federalno tijelo nadležno, među ostalim, za sva pitanja povezana s kriminalističkom policijom, izdala je upute prefekturalnoj

([85]) U Prilogu je navedeno devet vrsta kaznenih djela, npr. kaznena djela povezana s drogom i vatrenim oružjem, trgovinom ljudima i organiziranim ubojstvom. Valja napomenuti da novouvedeno kazneno djelo „pripreme kaznenog djela terorizma i drugih oblika organiziranog kriminala" (vidjeti bilješku bilješku 76.) nije uključeno u taj taksativan popis.

([86]) Nadalje, prema članku 23. Zakona o prisluškivanju istražno tijelo mora pisanim putem obavijestiti osobu o presretanju njezine komunikacije (koja je stoga uključena u evidenciju o presretanju).

([87]) Vidjeti Prilog II., odjeljak II.A.1)(b)(1).

([88]) Prema primljenim informacijama poslovni subjekti koji ne surađuju ne snose negativne posljedice (uključujući sankcije) ni prema jednom zakonu. Vidjeti Prilog II., odjeljak II.A.2)(a).

([89]) U skladu sa Smjernicama PPC-a (*General Rule Edition*), članak 23. stavak 1. točka (i) osnova je za otkrivanje osobnih informacija na temelju sudskog naloga (članak 218. CCP-a) i „istražnog obrasca" (članak 197. stavak 2. CCP-a).

([90]) To znači da se „istražni obrazac" smije koristiti samo za prikupljanje informacija u pojedinačnim slučajevima, a ne za masovno prikupljanje osobnih podataka. Vidjeti i Prilog II., odjeljak I.A.2)(b)(1).

([91]) Kao i propisi Prefekturalnog povjerenstva za javnu sigurnost, vidjeti članak 189. stavak 1. CCP-a.

([92]) Vidjeti i članak 3. Zakona o policiji, prema kojem službena prisega koju polažu svi policijski službenici glasi „biti vjerni obvezi da brane i poštuju Ustav i zakone Japana te obavljati svoje dužnosti nepristrano, pravedno, pošteno i bez predrasuda".

policiji ([93]) o „pravilnoj uporabi pisanih upita u istražnim stvarima". Prema toj obavijesti zahtjevi se moraju podnijeti u prethodno utvrđenom obrascu („Obrazac br. 49" ili tzv. „istražni obrazac") ([94]), odnose se na evidenciju „o određenoj istrazi" i zatražene informacije moraju biti „nužne za [tu] istragu". U svakom slučaju glavni istražitelj mora „u potpunosti ispitati nužnost, sadržaj itd. pojedinačnog upita" te se mora dobiti interno odobrenje od visokog dužnosnika.

(128) Osim toga, u dvije presude od 1969. i 2008. ([95]). Vrhovni sud Japana predvidio je ograničenja u pogledu neobveznih mjera koje zadiru u pravo na privatnost ([96]). Točnije, sud je smatrao da takve mjere moraju biti „razumne" i u „općenito dopustivim granicama", odnosno da moraju biti nužne za istragu osumnjičenika (prikupljanje dokaza) i provedene „primjerenim metodama za postizanje svrhe [te] istrage" ([97]). Iz presuda proizlazi da to uključuje test proporcionalnosti uzimajući o obzir sve okolnosti slučaja (npr. razinu zadiranja u pravo na privatnost, uključujući očekivanja u pogledu privatnosti, ozbiljnost kaznenog djela, vjerojatnost pribavljanja korisnih dokaza, važnost tih dokaza, moguća alternativna sredstva istrage itd.) ([98]).

(129) Osim tih ograničenja za izvršavanje javnih ovlasti, i od poslovnih subjekata očekuje se da provjere („potvrde") nužnost i „racionalnost" prosljeđivanja trećoj strani ([99]). To uključuje pitanje jesu li zakonski spriječeni surađivati. Takve proturječne pravne obveze mogu prije svega proizlaziti iz obveze povjerljivosti kao što je članak 134. Kaznenog zakona (o odnosu liječnika, odvjetnika, svećenika itd. i njegova klijenta). Osim toga, „svaka osoba koja se bavi telekomunikacijskom djelatnošću mora, dok obavlja svoju dužnost, čuvati tajne drugih za koje se saznalo iz komunikacija kojima upravlja telekomunikacijski operater" (članak 4. stavak 2. Zakona o telekomunikacijama). Ta je obveza povezana sa sankcijama propisanima člankom 179. Zakona o telekomunikacijama, prema kojem je osoba koja povrijedi tajnost komunikacija kojima upravlja telekomunikacijski operater kriva za kazneno djelo te će biti kažnjena kaznom zatvora uz mogućnost rada u trajanju do dvije godine ili novčanom kaznom od najviše milijun jena ([100]). Iako taj zahtjev nije apsolutan te konkretno dopušta mjere kojima se povređuje tajnost komunikacija, a koje su „opravdane radnje" u smislu članka 35. Kaznenog zakona, ta iznimka ne obuhvaća odgovor na neobvezne zahtjeve javnih tijela za otkrivanje elektroničkih informacija u skladu s člankom 197. stavkom 2. CCP-a ([101]).

3.2.1.3. Daljnja uporaba prikupljenih informacija

(130) Kad ih prikupe japanska javna tijela, osobne informacije ulaze u područje primjene APPIHAO-a. Tim se Zakonom uređuje postupanje (obrada) „pohranjenih osobnih informacija" te se nameću brojna ograničenja i zaštitne mjere

([93]) U skladu s člankom 30. stavkom 1. i člankom 31. stavkom 2. Zakona o policiji, glavni direktor regionalnih policijskih uprava (lokalne podružnice NPA-a) „vodi i nadzire" prefekturalnu policiju.

([94]) U istražnom obrascu moraju se navesti i informacije za kontakt s „osobom koja postupa s podacima" („naziv odjeljka [položaj], ime rukovatelja, telefonski broj ureda, izravna linija itd.").

([95]) Vrhovni sud, presuda od 24. prosinca 1969. (1965(A) 1187); presuda od 15. travnja 2008. (2007(A) 839).

([96]) Iako se te presude nisu odnosile na prikupljanje elektroničkih informacija, japanska vlada pojasnila je da se kriteriji koje je odredio Vrhovni sud primjenjuju na svako zadiranje javnih tijela u pravo privatnosti, među ostalim i na sve „dobrovoljne istrage", i stoga obvezuju japanska tijela i kad podnose zahtjeve za dobrovoljno otkrivanje informacija. Vidjeti Prilog II., odjeljak II.A.2)(b)(1).

([97]) Prema primljenim informacijama ti se čimbenici trebaju smatrati „razumnima u skladu s društveno prihvaćenim konvencijama." Vidjeti Prilog II., odjeljak II.A.2)(b)(1).

([98]) Za slična razmatranja u kontekstu obveznih istraga (prisluškivanje) vidjeti i Vrhovni sud, presuda od 16. prosinca 1999., 1997 (A) 636.

([99]) U tom su pogledu japanska tijela uputila na Smjernice PPC-a (*General Rule Edition*) i točku 5/14 „Pitanja i odgovora" koje je PPC pripremio za primjenu APPI-ja. Prema mišljenju japanskih tijela „s obzirom na sve veću svijest pojedinaca o njihovim pravima na privatnost te na radno opterećenje koje stvaraju takvi zahtjevi poslovni subjekti sve su oprezniji pri odgovaranju na takve zahtjeve". Vidjeti Prilog II., odjeljak II.A.2), gdje se također upućuje na Obavijest NPA-a iz 1999. Prema primljenim informacijama doista je bilo slučajeva da su poslovni subjekti odbili surađivati. Primjerice, u svojem izvješću o transparentnosti za 2017. LINE (najpopularnija aplikacija za razmjenu poruka u Japanu) navodi sljedeće: „Nakon primitka zahtjeva istražnih agencija itd. […] provjeravamo primjerenost u pogledu zakonitosti, zaštite korisnika itd. U toj provjeri odbit ćemo zahtjev u slučaju pravnog nedostatka. Ako je opseg zahtjeva preopširan za potrebe istrage, tražimo obrazloženje od istražne agencije. Ako obrazloženje nije utemeljeno, nećemo odgovoriti na taj zahtjev". Dostupno na internetu na: https://linecorp.com/en/security/transparency/top

([100]) Kazne su tri godine zatvora uz mogućnost rada ili novčana kazna od najviše dva milijuna jena za svaku osobu koja se „bavi telekomunikacijama".

([101]) „Opravdane radnje" u skladu s Kaznenim zakonikom prije svega su one radnje telekomunikacijskog operatera pri kojima postupa u skladu s državnim mjerama koje imaju pravnu snagu (obvezne mjere), na primjer kad istražna tijela poduzimaju mjere na temelju sudskog naloga. Vidjeti Prilog II., odjeljak II.A.2)(b)(2), gdje se upućuje na Smjernice o zaštiti osobnih informacija u telekomunikacijama.

(vidjeti uvodnu izjavu 118.) ([102]). Štoviše, činjenica da upravni organ može pohraniti osobne informacije „samo ako je pohrana nužna za obavljanje poslova u njegovoj nadležnosti koji su predviđeni zakonima i propisima" (članak 3. stavak 1. APPIHAO-a) također ograničava, barem neizravno, prvotno prikupljanje.

3.2.2. *Neovisni nadzor*

(131) U Japanu je prikupljanje elektroničkih informacija u području kaznenog progona prije svega ([103]) u nadležnosti prefekturalne policije ([104]), koja u tom pogledu podliježe različitim razinama nadzora.

(132) Prvo, u svim slučajevima kad se elektroničke informacije prikupljaju prisilnim sredstvima (pretragom i zapljenom), policija mora ishoditi prethodni sudski nalog (vidjeti uvodnu izjavu 121.). Stoga će prikupljanje u tim slučajevima *ex ante* provjeriti sudac, na temelju strogog standarda „primjerenog razloga".

(133) Iako u slučaju zahtjeva za dobrovoljno otkrivanje sudac ne provodi *ex ante* provjeru, poslovni subjekti kojima su ti zahtjevi upućeni mogu ih odbiti bez rizika od bilo kakvih negativnih posljedica (i morat će uzeti u obzir učinak bilo kakvog otkrivanja na privatnost). Nadalje, u skladu s člankom 192. stavkom 1. CCP-a policijski službenici uvijek surađuju i koordiniraju svoje aktivnosti s javnim tužiteljem (i Prefekturalnim povjerenstvom za javnu sigurnost) ([105]). S druge strane, javni tužitelj može dati potrebne opće upute kojima se utvrđuju standardi za poštenu istragu i/ili izdati posebne naloge s obzirom na pojedinačnu istragu (članak 193. CCP-a). Ako se ne postupa u skladu s takvim uputama i/ili nalozima, tužiteljstvo može podnijeti zahtjev za stegovne mjere (članak 194. CCP-a). Stoga prefekturalna policija djeluje pod nadzorom javnog tužitelja.

(134) Drugo, u skladu s člankom 62. Ustava, svaki dom japanskog parlamenta može provoditi istrage povezane s vladom, među ostalim u pogledu zakonitosti prikupljanja informacija koje provodi policija. U tu svrhu može zahtijevati prisutnost i iskaz svjedoka i/ili uvid u zapise. Te su istražne ovlasti pobliže uređene Zakonom o parlamentu (*Diet Law*), posebno poglavljem XII. Konkretno, člankom 104. Zakona o parlamentu propisano je da Kabinet, javne agencije i drugi dijelovi vlade „moraju ispunjavati zahtjeve doma ili bilo kojeg od njegovih odbora u pogledu davanja uvida u izvješća i zapise koji su nužni za provođenje istrage". Odbijanje suradnje dopušteno je samo ako vlada navede uvjerljiv razlog koji je parlamentu prihvatljiv ili ako izda službenu izjavu da bi davanje izvješća ili zapisa na uvid „ozbiljno ugrozilo nacionalne interese" ([106]). Osim toga, zastupnici u parlamentu mogu pisanim putem postavljati pitanja Kabinetu (članci 74. i 75. Zakona o parlamentu), a dosad su se takvi „pisani upiti" odnosili i na postupanje uprave s osobnim informacijama ([107]). Uloga parlamenta u nadzoru izvršne vlasti ojačana je obvezama izvješćivanja, primjerice u skladu s člankom 29. Zakona o prisluškivanju.

(135) Treće, i unutar izvršne vlasti prefekturalna policija podliježe neovisnom nadzoru. To posebno uključuje Prefekturalna povjerenstva za javnu sigurnost uspostavljena na razini prefektura kako bi se osigurala demokratska uprava i politička neutralnost policije ([108]). Ta su povjerenstva sastavljena od članova koje imenuje guverner prefekture uz suglasnost prefekturalne skupštine (sastavljene od građana koji nisu bili državni službenici u policiji u proteklih pet godina) i koji imaju siguran mandat (može ih se razriješiti samo iz dobro utemeljenog razloga) ([109]). Prema primljenim informacijama oni ne podliježu uputama te se stoga mogu smatrati potpuno neovisnima ([110]). Kad

([102]) Kad je riječ o pravima dotičnih osoba, vidjeti odjeljak 3.1.
([103]) U načelu javni tužitelj ili pomoćnik javnog tužitelja po njegovu nalogu može, ako to smatra potrebnim, istražiti kazneno djelo (članak 191. stavak 1. CCP-a).
([104]) Prema primljenim informacijama Nacionalna policijska agencija ne provodi pojedinačne kaznene istrage. Vidjeti Prilog II., odjeljak II.A.1)(a).
([105]) Vidjeti i članak 246. CCP-a prema kojem pravosudna policija ima obvezu proslijediti predmet javnom tužitelju nakon što provede istragu kaznenog djela („načelo prosljeđivanja u svim slučajevima").
([106]) Osim toga, parlament može zatražiti da Odbor za nadzor i preispitivanje posebno određenih tajnih podataka (*Board of Oversight and Review of Specially Designated Secrets*) provede istragu zbog uskraćivanja odgovora. Vidjeti članak 104.-II. Zakona o parlamentu (*Diet Law*).
([107]) Vidjeti Prilog II., odjeljak II.B.4).
([108]) Osim toga, na temelju odredaba članka 100. Zakona o lokalnoj autonomiji (*Local Autonomy Act*), lokalna skupština ima ovlasti istraživati aktivnosti tijela kaznenog progona na razini prefektura, uključujući prefekturalnu policiju.
([109]) Vidjeti članke od 39. do 41. Zakona o policiji. U pogledu političke neutralnosti vidjeti i članak 42. Zakona o policiji.
([110]) Vidjeti Prilog II., odjeljak II.B.3 („sustav neovisnog vijeća").

je riječ o zadaćama i ovlastima Prefekturalnih povjerenstava za javnu sigurnost, na temelju članka 38. stavka 3. u vezi s člankom 2. i člankom 36. stavkom 2. Zakona o policiji ona su odgovorna za „zaštitu prava i slobode pojedinca". U tu svrhu ona su ovlaštena za „nadzor" ([111]) nad svim istražnim radnjama prefekturalne policije, uključujući prikupljanje osobnih podataka. Naime, povjerenstva „mogu prefekturalnu policiju uputiti u pojedinosti ili je u određenom pojedinačnom slučaju uputiti da istraži povredu dužnosti policijskog službenika, ako je potrebno" ([112]). Kad načelnik prefekturalne policije ([113]) primi takvu uputu ili sam posumnja u povredu dužnosti (uključujući kršenje zakona ili drugo zanemarivanje dužnosti), mora odmah istražiti slučaj te o rezultatu provjere izvijestiti Prefekturalno povjerenstvo za javnu sigurnost (članak 56. stavak 3. Zakona o policiji). Ako Povjerenstvo to smatra potrebnim, može i zadužiti jednog od svojih članova za preispitivanje statusa provedbe. Taj se proces nastavlja sve dok se Povjerenstvo ne uvjeri da je incident na odgovarajući način riješen.

(136) Osim toga, u vezi s pravilnom primjenom APPIHAO-a nadležni ministar ili čelnik agencije (npr. glavni povjerenik NPA-a) ima ovlasti osiguranja provedbe, a za nadzor je zaduženo Ministarstvo unutarnjih poslova i komunikacija (*Ministry of Internal Affairs and Communications*, MIC). U skladu s člankom 49. APPIHAO-a MIC „može prikupljati izvješća o statusu provedbe ovoga Zakona" od čelnika upravnih organa (ministara). Tu nadzornu funkciju MIC vrši uz potporu svojeg 51 „sveobuhvatnog informativnog centra" (po jedan u svakoj japanskoj prefekturi), koji svake godine obrađuju tisuće upita pojedinaca ([114]) (pri čemu se pak mogu otkriti moguća kršenja zakona). Kad to smatra potrebnim kako bi se osiguralo poštovanje tog Zakona, MIC može zatražiti podnošenje objašnjenja i materijala te davati mišljenja o postupanju dotičnih upravnih organa s osobnim informacijama (članci 50. i 51. APPIHAO-a).

3.2.3. *Pravna zaštita pojedinaca*

(137) Osim nadzora po službenoj dužnosti pojedinci imaju i nekoliko mogućnosti za dobivanje pravne zaštite, i putem neovisnih tijela (kao što su Prefekturalna povjerenstva za javnu sigurnost ili PPC) i putem japanskih sudova.

(138) Prvo, kad je riječ o osobnim informacijama koje prikupljaju upravni organi, ti su organi dužni „nastojati pravilno i brzo obraditi sve pritužbe" s obzirom na njihovu kasniju obradu (članak 48. APPIHAO-a). Iako se poglavlje IV. APPIHAO-a o pravima pojedinaca ne primjenjuje na osobne informacije zabilježene u „dokumentima koji se odnose na suđenja i zaplijenjene predmete" (članak 53-2. stavak 2. CCP-a), što obuhvaća osobne informacije prikupljene u okviru kaznenih istraga, pojedinci mogu podnijeti pritužbu pozivajući se na opća načela zaštite podataka, kao što je npr. obveza da se osobne informacije pohranjuju samo „kad je pohrana nužna za obavljanje [funkcija kaznenog progona]" (članak 3. stavak 1. APPIHAO-a).

(139) Osim toga, člankom 79. Zakona o policiji pojedincima koji imaju problem s „izvršavanjem dužnosti" policijskih službenika jamči se pravo na podnošenje pritužbe (nadležnom) neovisnom Prefekturalnom povjerenstvu za javnu sigurnost. Povjerenstvo će „savjesno" rješavati takve pritužbe u skladu sa zakonima i lokalnim propisima te će podnositelja pritužbe pisanim putem obavijestiti o rezultatima. Na temelju svoje ovlasti da nadzire i „izdaje upute" prefekturalnoj policiji u pogledu „povrede dužnosti osoblja" (članak 38. stavak 3. i članak 43-2. stavak 1. Zakona o policiji), može od nje zahtijevati da istraži činjenice, poduzme odgovarajuće mjere na temelju rezultata te istrage i izvijesti o rezultatima. Ako smatra da istraga koju je provela policija nije bila primjerena, Povjerenstvo može dati i upute o rješavanju pritužbe.

(140) Da bi se olakšalo rješavanje pritužbi, NPA je policiji i Prefekturalnom povjerenstvu za javnu sigurnost izdala „Obavijest" o pravilnom rješavanju pritužbi na izvršavanje dužnosti policijskih službenika. U tom dokumentu NPA određuje standarde za tumačenje i provedbu članka 79. Zakona o policiji. Među ostalim, od prefekturalne

([111]) Vidjeti članak 5. stavak 3. i članak 38. stavak 3. Zakona o policiji.

([112]) Vidjeti članak 38. stavak 3. i članak 43-2. stavak 1. Zakona o policiji. U slučaju da „izda uputu" u smislu članka 43-2. stavka 1., Prefekturalno povjerenstvo za javnu sigurnost može naložiti odboru koji je imenovalo da prati njezinu provedbu (stavak 2.). Povjerenstvo može preporučiti i stegovnu mjeru ili razrješenje načelnika prefekturalne policije (članak 50. stavak 2.) i drugih policijskih službenika (članak 55. stavak 4. Zakona o policiji).

([113]) Isto vrijedi i za glavnog nadzornika u slučaju policijske uprave za šire područje Tokija (vidjeti članak 48. stavak 1. Zakona o policiji).

([114]) Prema primljenim informacijama, u financijskoj godini 2017. (od travnja 2017. do ožujka 2018.) „sveobuhvatni informacijski centri" obradili su ukupno 5 186 upita pojedinaca.

policije zahtijeva da uspostavi „sustav za rješavanje pritužbi" i da sve pritužbe rješava i o njima izvještava nadležno Prefekturalno povjerenstvo za javnu sigurnost „bez odgode". U Obavijesti se pritužbe definiraju kao zahtjevi za ispravljanje „svake konkretne negativne posljedice uzrokovane nezakonitim ili neprimjerenim ponašanjem" ([115]) ili „propusta policijskog službenika da u izvršavanju svojih dužnosti poduzme potrebne radnje" ([116]), kao i svake „pritužbe/nezadovoljstva zbog neprimjerenog načina na koji policijski službenik izvršava svoje dužnosti". Prema tome, definicija materijalnog područja primjene pritužbe široka je te obuhvaća svaku tvrdnju o nezakonitom prikupljanju podataka, a podnositelj ne mora dokazati da je pretrpio štetu zbog radnji policijskog službenika. Važno je napomenuti da se u Obavijesti navodi da će se strancima (među ostalim) pomoći u sastavljanju pritužbe. U slučaju pritužbe Prefekturalna povjerenstva za javnu sigurnost moraju osigurati da prefekturalna policija ispita činjenice, provede mjere „u skladu s rezultatima ispitivanja" te izvijesti o rezultatima. Ako Povjerenstvo smatra ispitivanje nedostatnim, izdaje uputu o rješavanju pritužbe koje se prefekturalna policija mora pridržavati. Na temelju primljenih izvješća i poduzetih mjera Povjerenstvo obavješćuje pojedinca navodeći, među ostalim, mjere poduzete za rješavanje pritužbe. U svojoj Obavijesti NPA naglašava da bi se pritužbe trebale „časno" rješavati i da o rezultatima treba obavijestiti „u razdoblju […] koje se smatra prikladnim u smislu društvenih normi i zdravorazumskog pristupa."

(141) Drugo, s obzirom na to da će se pravna zaštita obično morati tražiti u stranom sustavu i na stranom jeziku, kako bi se olakšala pravna zaštita pojedinaca iz EU-a čiji se osobni podaci prenose poslovnim subjektima u Japanu, nakon čega im imaju pristup javna tijela, japanska vlada iskoristila je svoje ovlasti za stvaranje posebnog mehanizma, kojim upravlja i koji nadzire PPC, za obradu i rješavanje pritužbi u tom području. Taj se mehanizam temelji na obvezi suradnje koju japanska javna tijela imaju na temelju APPI-ja i posebnoj ulozi PPC-a u pogledu međunarodnog prijenosa podataka iz trećih zemalja u skladu s člankom 6. APPI-ja i osnovne politike (kako ju je utvrdila japanska vlada Nalogom Kabineta). Pojedinosti o tom mehanizmu iznesene su u službenim izjavama, jamstvima i obvezama primljenima od japanske vlade i priložene ovoj Odluci kao Prilog II. Mehanizam ne podliježe ni jednom zahtjevu i na raspolaganju je svakom pojedincu, bez obzira na to je li osumnjičen ili optužen za kazneno djelo.

(142) U okviru tog mehanizma pojedinac koji sumnja da su pri prikupljanju ili uporabi njegovih podataka prenesenih iz Europske unije javna tijela u Japanu (uključujući tijela nadležna za kazneni progon) prekršila primjenjiva pravila, može podnijeti pritužbu PPC-u (samostalno ili preko svojeg tijela za zaštitu podataka u smislu članka 51. Opće uredbe o zaštiti podataka). PPC je dužan riješiti pritužbu te u prvom koraku o tome obavijestiti nadležna javna tijela, uključujući odgovarajuća nadzorna tijela. Ta su tijela dužna surađivati s PPC-om, „među ostalim pružanjem potrebnih informacija i relevantnih materijala kako bi PPC mogao ocijeniti jesu li prikupljanje ili naknadna uporaba osobnih informacija izvršeni u skladu s primjenjivim pravilima" ([117]). Ta obveza, proizišla iz članka 80. APPI-ja (prema kojem japanska javna tijela moraju surađivati s PPC-om), općenito se primjenjuje pa se stoga odnosi i na preispitivanje istražnih mjera koje provedu takva tijela, koja su se na takvu suradnju obvezala i pisanim jamstvima nadležnih ministarstava i čelnika agencija, kako je navedeno u Prilogu II.

(143) Ako se evaluacijom utvrdi da je došlo do povrede primjenjivih pravila, „suradnja predmetnih javnih tijela s PPC-om uključuje obvezu ispravljanja povrede", koja u slučaju nezakonitog prikupljanja osobnih informacija obuhvaća brisanje takvih podataka. Važno je napomenuti da se ta obveza provodi pod nadzorom PPC-a, koji će „prije završetka evaluacije potvrditi da je povreda u potpunosti ispravljena".

(144) Nakon završetka evaluacije PPC u razumnom roku obavješćuje pojedinca o ishodu evaluacije, među ostalim o korektivnim mjerama ako su poduzete. PPC pojedinca obavješćuje i o mogućnosti traženja potvrde ishoda od nadležnog javnog tijela i o identitetu tijela kojem je takvu potvrdu potrebno podnijeti. Mogućnost primanja takve potvrde, uključujući razloge na kojima se temelji odluka nadležnog tijela, može pomoći pojedincu u poduzimanju

([115]) Uvjet „konkretne negativne posljedice" samo znači da se policijsko ponašanje (ili propust) mora odnositi na podnositelja pritužbe osobno, a ne da on mora dokazivati bilo kakvu štetu.

([116]) Poštovanje zakona, uključujući pravne zahtjeve za prikupljanje i uporabu osobnih podataka, dio je tih obveza. Vidjeti članak 2. stavak 2. i članak 3. Zakona o policiji.

([117]) U provedbi te evaluacije PPC će surađivati s MIC-om koji, kako je objašnjeno u uvodnoj izjavi 136., može zatražiti podnošenje objašnjenja i materijala te davati mišljenja o postupanju upravnog organa s osobnim informacijama (članci 50. i 51. APPIHAO-a).

daljnjih koraka, među ostalim pri traženju sudske zaštite. Detaljne informacije o ishodu evaluacije mogu se ograničiti ako postoje opravdani razlozi za pretpostavku da bi priopćavanje takvih informacija moglo predstavljati rizik za istragu u tijeku.

(145) Treće, osoba koja se ne slaže s odlukom o zapljeni (sudskim nalogom) ([118]) u pogledu svojih osobnih podataka ili s mjerama koje provodi policija ili tužiteljstvo pri izvršavanju takve odluke može podnijeti zahtjev da se ta odluka ili takve mjere opozovu ili izmijene (članak 429. stavak 1., članak 430. stavci 1. i 2. CCP-a, članak 26. Zakona o prisluškivanju) ([119]). Ako sud koji provodi nadzor smatra da je ili sam nalog ili njegovo izvršenje („postupak pljenidbe") nezakonit, odobrit će zahtjev i naložiti povrat zaplijenjenih predmeta ([120]).

(146) Četvrto, osoba koja smatra da je prikupljanje njezinih osobnih informacija u okviru kaznene istrage bilo nezakonito, može se kao neizravniji oblik sudskog nadzora pozvati na tu nezakonitost tijekom suđenja u kaznenom postupku. Ako se sud složi, dokazi će se isključiti kao nedopušteni.

(147) Naposljetku, u skladu s člankom 1. stavkom 1. Zakona o naknadi štete od države sud može odobriti odštetu ako je javni službenik koji izvršava javne ovlasti države u obnašanju svojih dužnosti nezakonito i svojom krivnjom (s namjerom ili iz nemara) nanio štetu dotičnom pojedincu. U skladu s člankom 4. Zakona o naknadi štete od države odgovornost države za naknadu štete temelji se na odredbama Građanskog zakonika. U tom je pogledu u članku 710. Građanskog zakonika propisano da odgovornost obuhvaća i naknadu štete koja nije materijalna nego moralna (primjerice u obliku „duševne boli"). To uključuje slučajeve u kojima je privatnost osobe narušena nezakonitim nadzorom i/ili prikupljanjem njezinih osobnih informacija (npr. nezakonito izvršenje sudskog naloga) ([121]).

(148) Osim novčane naknade pojedincima se u određenim uvjetima može izdati i privremena mjera (npr. brisanje osobnih podataka koje su prikupila javna tijela) na temelju njihovih prava na privatnost u skladu s člankom 13. Ustava ([122]).

(149) S obzirom na sve te oblike pravne zaštite mehanizam za rješavanje sporova koji je uspostavila japanska vlada predviđa da se pojedinac koji je i dalje nezadovoljan ishodom postupka može obratiti PPC-u, „koji će obavijestiti pojedinca o raznim mogućnostima i detaljnim postupcima za dobivanje pravne zaštite u skladu s japanskim zakonima i propisima". Štoviše, PPC „će pojedincu pružiti potporu, uključujući savjetovanje i pomoć u poduzimanju daljnjih koraka pri relevantnom upravnom ili sudskom tijelu".

(150) To uključuje primjenu postupovnih prava u skladu sa Zakonom o kaznenom postupku. Na primjer, „ako se u evaluaciji ispostavi da je pojedinac osumnjičen u kaznenom postupku, PPC će ga o tome obavijestiti" ([123]), kao i o mogućnosti da u skladu s člankom 259. CCP-a zatraži od tužiteljstva da ga obavijesti ako odluči da neće pokrenuti kazneni postupak. Također, ako se evaluacijom utvrdi da je predmet koji uključuje osobne informacije pojedinca bio otvoren te da je u međuvremenu zaključen, PPC će pojedinca obavijestiti da se evidencija predmeta može pregledati na temelju članka 53. CCP-a (i članka 4. Zakona o konačnoj kaznenoj evidenciji (*Act on Final Criminal Case Records*)). Dobivanje pristupa evidenciji o kaznenom postupku važno je jer će pojedincu pomoći da bolje

([118]) To uključuje sudski nalog za prisluškivanje, za koji je Zakonom o prisluškivanju propisana obveza posebnog obavješćivanja (članak 23.). Prema toj odredbi istražno tijelo mora pisanim putem obavijestiti osobu o presretanju njezine komunikacije (koja je stoga uključena u evidenciju o presretanju). Drugi primjer je članak 100. stavak 3. CCP-a prema kojemu sud, kad zaplijeni poštanske pošiljke ili telegrame koje je primio i poslao optuženik, o tome obavješćuje pošiljatelja ili primatelja osim ako postoji rizik da bi time omeo sudski postupak. Članak 222. stavak 1. CCP-a upućuje na tu odredbu za pretrage i zapljene koje provodi istražno tijelo.

([119]) Iako takav zahtjev nema automatski učinak suspenzije izvršenja odluke o zapljeni, sud koji provodi nadzor može naložiti suspenziju dok ne donese meritornu odluku. Vidjeti članak 429. stavak 2. i članak 432. u vezi s člankom 424. CCP-a.

([120]) Vidjeti Prilog II., odjeljak II.C(1).

([121]) Vidjeti Prilog II., odjeljak II.C.2).

([122]) Vidjeti npr. Okružni sud u Tokiju, presuda od 24. ožujka 1988. (br. 2925); Okružni sud u Osaki, presuda od 26. travnja 2007. (br. 2925). Prema stajalištu Okružnog suda u Osaki morat će se uskladiti niz čimbenika, primjerice: i. priroda i sadržaj predmetnih osobnih informacija; ii. način na koji su prikupljene; iii. negativne posljedice za pojedinca u slučaju da se podaci ne izbrišu; i iv. javni interes, uključujući negativne posljedice za javno tijelo u slučaju brisanja informacija.

([123]) U svakom slučaju, nakon pokretanja kaznenog postupka državni tužitelj daje priliku optuženiku da pregleda taj dokaz (vidjeti članke 298. i 299. CCP-a). Kad je riječ o žrtvama kaznenih djela, vidjeti članke od 316. do 333. CCP-a.

razumije istragu koja se provodi protiv njega te da se pripremi za moguće pokretanje sudskog postupka (npr. zahtjev za naknadu štete) ako smatra da su se njegovi podaci nezakonito prikupljali ili upotrebljavali.

### 3.3. **Pristup japanskih javnih tijela podacima i njihova uporaba za potrebe nacionalne sigurnosti**

(151) Prema japanskim tijelima u Japanu ne postoji zakon kojim bi se omogućili obvezni zahtjevi za informacije ili za „administrativno prisluškivanje" izvan kaznenih istraga. Stoga se zbog nacionalne sigurnosti informacije mogu dobiti samo iz izvora informacija kojemu svatko može slobodno pristupiti ili dobrovoljnim otkrivanjem. Poslovni subjekti koji zaprime zahtjev za dobrovoljnu suradnju (u obliku otkrivanja elektroničkih informacija) nemaju zakonsku obvezu pružiti takve informacije ([124]).

(152) Osim toga, prema primljenim informacijama samo su četiri državna tijela ovlaštena prikupljati elektroničke informacije u posjedu japanskih poslovnih subjekata zbog nacionalne sigurnosti, i to: i. Obavještajni i istražni ured Kabineta (*Cabinet Intelligence & Research Office*, CIRO); ii. Ministarstvo obrane (*Ministry of Defence*, MOD); iii. policija (Nacionalna policijska agencija (NPA) ([125]) i prefekturalna policija); i iv. Obavještajna agencija za javnu sigurnost (*Public Security Intelligence Agency*, PSIA). Međutim, CIRO nikad ne prikuplja informacije izravno od poslovnih subjekata, pa tako ni presretanjem komunikacije. Kad primi informacije od drugih vladinih tijela kako bi mogao pripremiti analizu za Kabinet, ta druga tijela moraju poštovati zakon, uključujući ograničenja i zaštitne mjere koje se analiziraju u ovoj Odluci. Njegove djelatnosti stoga nisu relevantne u kontekstu prijenosa.

#### 3.3.1. *Pravna osnova i primjenjiva ograničenja/zaštitne mjere*

(153) Prema primljenim informacijama MOD prikuplja (elektroničke) informacije na temelju Zakona o uspostavi MOD-a (*MOD Establishment Act*). U skladu s njegovim člankom 3. zadaća MOD-a jest upravljati i voditi vojne snage te „obavljati s time povezane poslove kako bi se osigurao mir i neovisnost zemlje te nacionalna sigurnost." Člankom 4. stavkom 4. propisuje se da je MOD nadležan za „obranu i zaštitu", za mjere koje trebaju poduzeti obrambene snage te za raspoređivanje vojnih snaga, uključujući prikupljanje informacija potrebnih za ispunjavanje tih zadaća. Samo je on ovlašten za prikupljanje (elektroničkih) informacija od poslovnih subjekata u okviru dobrovoljne suradnje.

(154) Kad je riječ o prefekturalnoj policiji, njezine odgovornosti i dužnosti uključuju „održavanje javne sigurnosti i reda" (članak 35. stavak 2. u vezi s člankom 2. stavkom 1. Zakona o policiji). U okviru tog područja nadležnosti policija može prikupljati informacije, ali samo na dobrovoljnoj osnovi, bez zakonske prisile. Osim toga, aktivnosti policije su „strogo ograničene" na ono što je nužno za obnašanje njezinih dužnosti. Ona k tome mora djelovati „nepristrano, nestranački, bez predrasuda i pošteno" i nikad ne smije zloupotrebljavati svoje ovlasti „na bilo koji način kojim bi zadirala u prava i slobode pojedinaca zajamčene Ustavom Japana" (članak 2. Zakona o policiji).

(155) Naposljetku, PSIA može provoditi istrage u skladu sa Zakonom o sprečavanju subverzivnog djelovanja (*Subversive Activities Prevention Act*, SAPA) i Zakonom o nadzoru nad organizacijama koje su počinile nasumična masovna ubojstva (*Act on the Control of Organisations Which Have Committed Acts of Indiscriminate Mass Murder*, ACO) ako su takve istrage potrebne za pripremu donošenja kontrolnih mjera protiv određenih organizacija ([126]). Prema oba zakona na zahtjev glavnog direktora PSIA-e Povjerenstvo za provjeru javne sigurnosti može izdati određene „odluke" (nadzor/zabrane u slučaju ACO-a ([127]), raspuštanje/zabrane u slučaju SAPA-e ([128])) te u tom kontekstu PSIA može provoditi istrage ([129]). Prema primljenim informacijama te se istrage uvijek provode na dobrovoljnoj

([124]) Stoga poslovni subjekti mogu slobodno odbiti suradnju, bez rizika od sankcija ili drugih negativnih posljedica. Vidjeti Prilog II., odjeljak III.A.1).

([125]) Međutim, prema primljenim informacijama glavna je uloga NPA-a koordinirati istrage različitih uprava prefekturalne policije i razmjenjivati informacije sa stranim tijelima. Čak i u toj ulozi NPA podliježe nadzoru Nacionalnog povjerenstva za javnu sigurnost, među ostalim odgovornog za zaštitu prava i sloboda pojedinaca (članak 5. stavak 1. Zakona o policiji).

([126]) Vidjeti Prilog II., odjeljak III.A.1)(3). Područje primjene tih dvaju zakona ograničeno je, pri čemu se SAPA odnosi na „terorističke subverzivne aktivnosti", a ACO na „djelo nasumičnog masovnog ubojstva" (što znači „terorističke subverzivne aktivnosti" prema SAPA-i „u kojima je nasumično ubijen velik broj osoba").

([127]) Vidjeti članke 5. i 8. ACO-a. Odluka o nadzoru uključuje i obvezu izvješćivanja za organizaciju na koju se mjera odnosi. Za postupovne zaštitne mjere, posebno zahtjeve u pogledu transparentnosti i prethodnog odobrenja Povjerenstva za ispitivanje javne sigurnosti, vidjeti članke 12. i 13. te članke od 15. do 27. ACO-a.

([128]) Vidjeti članke 5. i 7. SAPA-e. Za postupovne zaštitne mjere, posebno zahtjeve u pogledu transparentnosti i prethodnog odobrenja Povjerenstva za ispitivanje javne sigurnosti, vidjeti članke od 11. do 25. SAPA-e.

([129]) Vidjeti članak 27. SAPA-e i članke 29. i 30. ACO-a.

osnovi, što znači da PSIA ne smije prisiljavati vlasnika osobnih informacija da ih stavi na raspolaganje ([130]). Svaki put se kontrole i istrage provode samo u najmanjoj mjeri koja je potrebna da se postigne svrha kontrole te se ni u kakvim okolnostima ne smiju vršiti tako da se „nerazumno" ograniče prava i slobode zajamčene Ustavom Japana (članak 3. stavak 1. SAPA-e/ACO-a). Osim toga, u skladu s člankom 3. stavkom 2. SAPA-e/ACO-a, PSIA ni u kojim okolnostima ne smije zloupotrijebiti takve kontrole ni istrage koje se provode radi pripreme takvih kontrola. Ako je službenik obavještajne službe za javnu sigurnost zloupotrijebio svoje ovlasti na temelju odgovarajućeg zakona prisiljavanjem osobe da učini bilo što što ne mora ili zadiranjem u ostvarivanje prava osobe, mogu mu se odrediti kaznene sankcije na temelju članka 45. SAPA-e ili članka 42. ACO-a. Konačno, obim zakonima izričito se propisuje da se njihove odredbe, uključujući ovlasti koje se njima dodjeljuju, „ne smiju ni u kojim okolnostima prošireno tumačiti" (članak 2. SAPA-a/ACO-a).

(156) U svim slučajevima vladina pristupa informacijama zbog nacionalne sigurnosti opisanima u ovom odjeljku primjenjuju se ograničenja koja propisuje japanski Vrhovni sud za dobrovoljne istrage, što znači da se (elektroničke) informacije moraju prikupljati u skladu s načelima nužnosti i proporcionalnosti („primjerena metoda") ([131]). Kao što su japanska nadležna tijela izričito potvrdila, „prikupljanje i obrada informacija odvija se samo u mjeri u kojoj je to potrebno za obavljanje posebnih zadaća nadležnog javnog tijela te zbog posebnih prijetnji". Stoga „ne obuhvaća masovno i neselektivno prikupljanje ili pristup osobnim informacijama iz razloga nacionalne sigurnosti" ([132]).

(157) Nakon što su prikupljene, sve osobne informacije koje su javna tijela pohranila za potrebe nacionalne sigurnosti bit će obuhvaćene zaštitom na temelju APPIHAO-a kad je riječ o kasnijoj pohrani, uporabi i otkrivanju (vidjeti uvodnu izjavu 118.).

3.3.2. *Neovisni nadzor*

(158) Prikupljanje osobnih informacija za potrebe nacionalne sigurnosti na više razina nadziru sve tri grane vlasti.

(159) Prvo, japanski parlament u okviru svojih specijaliziranih odbora može ispitati zakonitost istraga na temelju svojih ovlasti parlamentarnog nadzora (članak 62. Ustava, članak 104. Zakona o parlamentu; vidjeti uvodnu izjavu 134.). Tu funkciju nadzora podupiru posebne obveze izvješćivanja o aktivnostima koje se provode na temelju nekih od prethodno spomenutih pravnih osnova ([133]).

(160) Drugo, u okviru izvršne vlasti postoji nekoliko nadzornih mehanizama.

(161) Kada je riječ o MOD-u, nadzor provodi Ured glavnog inspektora za praćenje poštovanja zakonitosti (*Inspector General's Office of Legal Compliance*, IGO) ([134]), koji je osnovan na temelju članka 29. Zakona o uspostavi MOD-a kao ured unutar MOD-a pod nadzorom ministra obrane (kojem podnosi izvješća), ali neovisan o operativnim odjelima MOD-a. IGO ima zadatak osigurati poštovanje zakona i propisa te pravilno izvršavanje dužnosti službenika MOD-a. Među njegovim je ovlastima nadležnost za provođenje tzv. „inspekcijskih pregleda u području obrane" (*Defence Inspections*) i u pravilnim vremenskim razmacima (redoviti inspekcijski pregledi u području obrane) i u pojedinačnim slučajevima (posebni inspekcijski pregledi u području obrane), što je dosad već obuhvaćalo i pravilno postupanje s osobnim informacijama ([135]). U kontekstu takvih inspekcijskih pregleda IGO može ući u

([130]) Vidjeti Prilog II., odjeljak III.A.1)(3).

([131]) Vidjeti Prilog II., odjeljak III.A.2)(b): „Iz sudske prakse Vrhovnog suda proizlazi da, u svrhu upućivanja zahtjeva za dobrovoljnu suradnju poslovnom subjektu, takav zahtjev mora biti nužan za istragu navodnog kaznenog djela i mora biti razuman kako bi se postigla svrha istrage. Iako se istrage koje provode istražna tijela u području nacionalne sigurnosti razlikuju od istraga koje provode istražna tijela u području kaznenog progona s obzirom na njihovu pravnu osnovu i svrhu, ključna načela ‚nužnosti za istragu' i ‚prikladnosti metode' na sličan se način primjenjuju u području nacionalne sigurnosti te se moraju poštovati uzimajući u obzir posebne okolnosti svakog slučaja".

([132]) Vidjeti Prilog II., odjeljak III.A.2)(b).

([133]) Vidjeti npr. članak 36. SAPA-e/članak 31. ACO-a (za PSIA-u).

([134]) Načelnik IGO-a bivši je javni tužitelj. Vidjeti Prilog II., odjeljak III.B.3).

([135]) Vidjeti Prilog II., odjeljak III.B.3). Prema dostavljenom su primjeru redoviti inspekcijski pregledi u području obrane 2016. s obzirom na „svjesnost/spremnost za poštovanje zakona" među ostalim obuhvaćali „status zaštite osobnih informacija" (upravljanje, pohrana itd.). U dobivenom izvješću otkriveni su slučajevi neprimjerenog upravljanja podacima te su zatražena poboljšanja u tom pogledu. MOD je objavio to izvješće na svojim internetskim stranicama.

lokacije (urede) i zatražiti dokumente ili informacije, uključujući objašnjenja zamjenika dominstra obrane. Inspekcijski pregled završava izvješćem ministru obrane u kojem se navode nalazi i mjere za poboljšanje (čija se provedba opet može provjeriti daljnjim inspekcijskim pregledima). To je izvješće osnova za upute ministra obrane za provedbu mjera potrebnih za rješavanje situacije; zamjenik dominstra zadužen je za provedbu takvih mjera te mora izvijestiti o daljnjim mjerama.

(162) Kad je riječ o prefekturalnoj policiji, nadzor osigurava neovisno Prefekturalno povjerenstvo za javnu sigurnost, kako je objašnjeno u uvodnoj izjavi 135. u pogledu kaznenog progona.

(163) Naposljetku, kako je navedeno, PSIA može provoditi istrage samo u mjeri u kojoj je to potrebno s obzirom na donošenje odluke o zabrani, raspuštanju ili nadzoru u okviru SAPA-e/ACO-a, a za te odluke neovisno ([136]) Povjerenstvo za ispitivanje javne sigurnosti provodi *ex ante* nadzor. Osim toga, redovne/redovite inspekcijske preglede (kojima se na sveobuhvatan način provjeravaju aktivnosti PSIA-e) ([137]) i posebne interne inspekcijske preglede ([138]) aktivnosti pojedinih odjela/ureda itd. provode posebno imenovani inspektori te se na temelju njih mogu izdati upute čelnicima relevantnih odjela itd. da poduzmu korektivne mjere ili mjere za poboljšanje.

(164) Ti nadzorni mehanizmi, koji su dodatno ojačani mogućnošću da pojedinci zatraže intervenciju PPC-a kao neovisnog nadzornog tijela (vidjeti odjeljak 168. u nastavku), pružaju odgovarajuća jamstva zaštite od rizika od zlouporabe ovlasti japanskih tijela u području nacionalne sigurnosti te od bilo kakvog nezakonitog prikupljanja elektroničkih informacija.

3.3.3. *Pravna zaštita pojedinaca*

(165) Kad je riječ o pravnoj zaštiti pojedinaca, s obzirom na osobne informacije koje prikupljaju i time „pohranjuju" upravni organi, potonji su obvezni „nastojati pravilno i brzo obraditi sve pritužbe" u pogledu takve obrade (članak 48. APPIHAO-a).

(166) Osim toga, za razliku od kaznenih istraga, pojedinci (uključujući strane državljane koji žive u inozemstvu) u načelu imaju pravo na otkrivanje ([139]), ispravak (uključujući brisanje) i suspenziju uporabe/prosljeđivanja u okviru APPIHAO-a. Bez obzira na to, čelnik upravnog organa može odbiti otkrivanje informacija „za koje se iz opravdanih razloga […] smatra da bi se njihovim otkrivanjem moglo naštetiti nacionalnoj sigurnosti" (članak 14. točka iv. APPIHAO-a), a da pritom ne mora otkriti ni postoje li takve informacije (članak 17. APPIHAO-a). Isto tako, iako pojedinac može zatražiti suspenziju uporabe ili brisanje u skladu s člankom 36. stavkom 1. točkom i. APPIHAO-a ako upravni organ nezakonito pribavi informacije ili ih pohranjuje/upotrebljava više od onoga što je nužno za postizanje određene svrhe, to tijelo može odbiti zahtjev ako smatra da bi suspenzija uporabe „mogla omesti pravilno izvršavanje poslova koji se odnose na svrhu uporabe pohranjenih osobnih informacija zbog prirode navedenih poslova" (članak 38. APPIHAO-a). Ipak, ako je moguće jednostavno izdvojiti i isključiti dijelove koji podliježu iznimci, upravni organi dužni su odobriti barem djelomično otkrivanje (vidjeti npr. članak 15. stavak 1. APPIHAO-a) ([140]).

([136]) Prema Zakonu o osnivanju Povjerenstva za provjeru javne sigurnosti (*Act on the Establishment of the Public Security Examination Commission*) predsjednik i članovi Povjerenstva „neovisno izvršavaju svoje ovlasti" (članak 3.). Imenuje ih premijer uz suglasnost obaju domova parlamenta i mogu biti razriješeni dužnosti samo iz „utemeljenog razloga" (npr. izdržavanje zatvorske kazne, povreda dužnosti, duševni ili fizički poremećaj, pokretanje stečajnog postupka).

([137]) Uredba o redovitim inspekcijskim pregledima Obavještajne agencije za javnu sigurnost (glavni direktor PSIA-e, Uputa br. 4, 1986.).

([138]) Uredba o posebnim inspekcijskim pregledima Obavještajne agencije za javnu sigurnost (glavni direktor PSIA-e, Uputa br. 11, 2008.). Posebni inspekcijski pregledi provodit će se kad glavni direktor PSIA-e to smatra potrebnim.

([139]) To se odnosi na pravo primitka primjerka „pohranjenih osobnih informacija".

([140]) Vidjeti i mogućnost „diskrecijskog otkrivanja" čak i u slučaju u kojem je „neotkrivanje informacija" uključeno u „pohranjene osobne informacije" čije se otkrivanje traži (članak 16. APPIHAO-a).

(167) U svakom slučaju, upravni organ mora donijeti pisanu odluku u određenom roku (od 30 dana, koji se pod određenim uvjetima može produljiti za još 30 dana). Ako je zahtjev odbijen, samo djelomično odobren ili ako pojedinac iz drugih razloga smatra postupanje upravnog organa „nezakonitim ili nepravednim", može zatražiti upravno preispitivanje na temelju Zakona o preispitivanju odluka upravnih tijela ([141]). U takvom se slučaju čelnik upravnog organa koji odlučuje o žalbi savjetuje s Odborom za preispitivanje otkrivanja informacija i zaštitu osobnih informacija (članci 42. i 43. APPIHAO-a), specijaliziranim neovisnim odborom čije članove imenuje premijer uz suglasnost obaju domova parlamenta. Prema zaprimljenim informacijama Odbor za preispitivanje može provesti pregled ([142]) i u tom pogledu od upravnog organa zatražiti da mu dostavi pohranjene osobne informacije, uključujući sav klasificirani sadržaj te dodatne informacije i dokumente. Iako završno izvješće poslano podnositelju pritužbe i upravnom organu te javno objavljeno nije pravno obvezujuće, gotovo u svim slučajevima se poštuje ([143]). Nadalje, pojedinac ima mogućnost osporiti odluku o žalbi na sudu temeljem Zakona o upravnim sporovima. To omogućuje sudski nadzor nad primjenom izuzeća zbog nacionalne sigurnosti, kao i nad time je li takva iznimka zloupotrijebljena ili je još uvijek opravdana.

(168) Kako bi se olakšalo ostvarivanje prethodno navedenih prava u skladu s APPIHAO-m, MIC je uspostavio 51 „sveobuhvatni informacijski centar" koji pruža konsolidirane informacije o tim pravima, primjenjivim postupcima za podnošenje zahtjeva i mogućim oblicima pravne zaštite ([144]). Kad je riječ o upravnim organima, oni su dužni dostaviti „informacije koje doprinose identifikaciji pohranjenih osobnih informacija" ([145]) i poduzeti „druge odgovarajuće mjere kojima se uzima u obzir praktičnost za osobu koja namjerava podnijeti zahtjev" (članak 47. stavak 1. APPIHAO-a).

(169) Kao i u slučaju istraga u području kaznenog progona, i u području nacionalne sigurnosti pojedinci mogu dobiti pravnu zaštitu izravnim obraćanjem PPC-u. Time će se pokrenuti poseban postupak rješavanja sporova koji je japanska vlada namijenila pojedincima iz EU-a čiji se osobni podaci prenose u skladu s ovom Odlukom (vidjeti detaljna objašnjenja u uvodnim izjavama od 141. do 144. i 149.).

(170) Osim toga, pojedinci mogu zatražiti sudsku zaštitu u obliku tužbe za naknadu štete u skladu sa Zakonom o naknadi štete od države, koji obuhvaća i moralnu štetu i pod određenim uvjetima brisanje prikupljenih podataka (vidjeti uvodnu izjavu 147.).

## 4. ZAKLJUČAK: PRIMJERENA RAZINA ZAŠTITE OSOBNIH PODATAKA KOJI SE IZ EUROPSKE UNIJE PRENOSE POSLOVNIM SUBJEKTIMA U JAPANU

(171) Komisija smatra da se APPI-jem dopunjenim Dopunskim pravilima iz Priloga I., zajedno sa službenim izjavama, jamstvima i obvezama iz Priloga II., za podatke koji se prenose iz Europske unije osigurava razina zaštite koja je u načelu istovjetna onoj koja se jamči Uredbom (EU) 2016/679.

(172) Osim toga, Komisija smatra da nadzorni mehanizmi i oblici pravne zaštite u japanskom pravu u cjelini omogućavaju da se povrede koje su počinili PIHBO-i koji su primili osobne podatke utvrde i kazne u praksi te ispitaniku pružaju pravne lijekove za dobivanje pristupa osobnim podacima koji se odnose na njega te, na koncu, za ispravak ili brisanje takvih podataka.

([141]) Zakon o preispitivanju odluka upravnih tijela (Zakon br. 160 iz 2014.), a posebno njegov članak 1. stavak 1.

([142]) Vidjeti članak 9. Zakona o osnivanju Odbora za preispitivanje otkrivanja informacija i zaštitu osobnih informacija (Zakon br. 60 iz 2003.).

([143]) Prema primljenim informacijama, u 13 godina od 2005. (kad je APPIHAO stupio na snagu) u samo dva od više od 2000 predmeta upravni organ nije postupio u skladu s izvješćem, unatoč tome što je Odbor za preispitivanje u mnogo navrata proturječio upravnim odlukama. Osim toga, ako upravni organ donese odluku koja odstupa od nalaza iz izvješća, mora jasno navesti razloge za to. Vidjeti Prilog II., odjeljak III.C, u kojem se upućuje na članak 50. stavak 1. točku iv. Zakona o preispitivanju odluka upravnih tijela.

([144]) Sveobuhvatni informacijski centri, po jedan u svakoj prefekturi, građanima daju objašnjenja o osobnim informacijama koje prikupljaju javna tijela (npr. postojećim bazama podataka) i primjenjivim pravilima za zaštitu podataka (APPIHAO), među ostalim i o tome kako ostvariti prava na otkrivanje, ispravak ili suspenziju uporabe. Ti su centri ujedno kontaktne točke za upite/pritužbe građana. Vidjeti Prilog II., odjeljak II.C.4)(a).

([145]) Vidjeti i članke 10. i 11. APPIHAO-a o „Registru datoteka s osobnim informacijama", koji međutim sadržavaju opsežne iznimke u pogledu „datoteka s osobnim informacijama" koje su pripremljene ili pribavljene za kaznene istrage ili koje sadržavaju sigurnosna pitanja i druge važne interese države (vidjeti članak 10. stavak 2. točke i. i ii. APPIHAO-a).

(173) Naposljetku, na temelju dostupnih informacija o japanskom pravnom poretku, uključujući izjave, jamstva i obveze japanske vlade iz Priloga II., Komisija smatra da će se svako zadiranje u temeljna prava pojedinaca čije osobne podatke iz Europske unije japanska javna tijela prenose u Japan u svrhe javnog interesa, posebno za potrebe kaznenog progona i nacionalne sigurnosti, ograničiti na ono što je strogo nužno za postizanje predmetnog legitimnog cilja te da postoji djelotvorna pravna zaštita od takvog zadiranja.

(174) Stoga Komisija s obzirom na zaključke iz ove Odluke smatra da Japan osigurava primjerenu razinu zaštite osobnih podataka koji se iz Europske unije prenose PIHBO-ima u Japanu koji podliježu APPI-ju, osim u slučajevima kad je primatelj obuhvaćen jednom od kategorija iz članka 76. stavka 1. APPI-ja te svrha obrade odgovara, djelomično ili u potpunosti, jednoj od svrha propisanih tom odredbom.

(175) Komisija na temelju toga zaključuje da je ispunjen standard primjerenosti iz članka 45. Uredbe (EU) 2016/679 kako je protumačen s obzirom na Povelju Europske unije o temeljnim pravima, posebno u presudi *Schrems* ([146]).

## 5. DJELOVANJE TIJELA ZA ZAŠTITU PODATAKA I OBAVJEŠĆIVANJE KOMISIJE

(176) U skladu sa sudskom praksom Suda Europske unije ([147]), a kako je potvrđeno u članku 45. stavku 4. Uredbe (EU) 2016/679, Komisija bi nakon donošenja odluke o primjerenosti trebala kontinuirano pratiti relevantne događaje u trećoj zemlji kako bi ocijenila osigurava li Japan i dalje u načelu istovjetnu razinu zaštite. Takva provjera potrebna je, u svakom slučaju, kad Komisija dobije informacije na temelju kojih može opravdano posumnjati u to.

(177) Stoga bi Komisija trebala kontinuirano pratiti situaciju u pravnom okviru i stvarnoj praksi za obradu osobnih podataka kako je ocijenjeno u ovoj Odluci, među ostalim poštuju li japanska tijela izjave, jamstva i obveze iz Priloga II. Kako bi se taj proces olakšao, od japanskih se tijela očekuje da obavijeste Komisiju o svim značajnim promjenama koje su relevantne za ovu Odluku, i kad je riječ o obradi osobnih podatka koju vrše poslovni subjekti i o ograničenjima i zaštitnim mjerama primjenjivima na pristup javnih tijela osobnim podacima. To bi trebalo uključivati sve odluke koje PPC donese na temelju članka 24. APPI-ja kojima se potvrđuje da treća zemlja pruža istovjetnu razinu zaštite onoj koja je zajamčena u Japanu.

(178) Osim toga, kako bi Komisija mogla djelotvorno obavljati svoju funkciju praćenja, države članice trebale bi je obavješćivati o svim relevantnim mjerama koje poduzimaju nacionalna tijela za zaštitu podataka, posebno u pogledu upita ili pritužbi ispitanika iz EU-a o prijenosu osobnih podataka iz Europske unije poslovnim subjektima u Japanu. Komisiju bi trebalo obavijestiti i o svakoj naznaci da mjere japanskih javnih tijela odgovornih za sprečavanje, istragu, otkrivanje ili progon kaznenih djela ili za nacionalnu sigurnost, uključujući nadzorna tijela, ne osiguravaju potrebnu razinu zaštite.

(179) Države članice i njihovi organi dužni su poduzeti mjere potrebne za usklađivanje s aktima institucija Unije jer se potonji smatraju zakonitima i proizvode pravne učinke do njihova povlačenja, poništenja u postupku za poništenje ili proglašavanja nevažećima nakon zahtjeva za prethodnu odluku ili tužbenog zahtjeva za proglašenje nezakonitosti. Stoga je odluka Komisije o primjerenosti donesena u skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 obvezujuća za sva tijela država članica kojima je upućena, uključujući njihova neovisna nadzorna tijela. Isto tako, kako je objašnjeno u presudi Suda Europske unije u predmetu *Schrems* ([148]) i potvrđeno u članku 58. stavku 5. Uredbe, ako tijelo za zaštitu podataka, među ostalim i na temelju pritužbe, dovede u pitanje spojivost odluke Komisije o primjerenosti s temeljnim pravima pojedinca na privatnost i zaštitu podataka, u nacionalnom pravu mora se osigurati pravni lijek za podnošenje tih prigovora nacionalnom sudu, koji u slučaju sumnje mora zastati s postupkom i uputiti Sudu EU-a zahtjev za prethodnu odluku ([149]).

([146]) Vidjeti prethodnu bilješku 3.
([147]) *Schrems*, točka 76.
([148]) *Schrems*, točka 65.
([149]) *Schrems*, točka 65.: „U tom je pogledu nacionalni zakonodavac dužan predvidjeti pravna sredstva koja neovisnom nadzornom tijelu omogućavaju isticanje prigovora pred nacionalnim sudovima koje smatra osnovanima, kako bi ti sudovi mogli, u slučaju da dijele sumnje tog tijela u vezi s valjanošću Komisijine odluke, uputiti zahtjev za prethodnu odluku radi ispitivanja valjanosti te odluke".

### 6. **PERIODIČNO PREISPITIVANJE ZAKLJUČKA O PRIMJERENOSTI**

(180) U skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 ([150]) i s obzirom na činjenicu da se razina zaštite koju pruža japanski pravni poredak može promijeniti, Komisija bi nakon donošenja ove Odluke trebala periodično provjeravati jesu li nalazi koji se odnose na primjerenost razine zaštite koju je osigurao Japan još uvijek činjenično i pravno opravdani.

(181) S tim bi ciljem ovu Odluku trebalo prvi put preispitati u roku od dvije godine od njezina stupanja na snagu. Nakon prvog preispitivanja i ovisno o njegovu ishodu Komisija će u bliskoj suradnji s Odborom osnovanim na temelju članka 93. stavka 1. Opće uredbe o zaštiti podataka odlučiti je li potrebno zadržati dvogodišnji ciklus. U svakom slučaju, sljedeća preispitivanja trebala bi se provesti najmanje svake četiri godine ([151]). To bi preispitivanje trebalo obuhvatiti sve aspekte funkcioniranja ove Odluke, a posebno primjenu Dopunskih pravila (pri čemu bi posebnu pozornost trebalo posvetiti zaštiti koja se pruža u slučaju daljnjeg prijenosa), primjenu pravila o privoli, među ostalim u slučaju povlačenja, djelotvornost ostvarivanja prava pojedinaca te ograničenja i zaštitne mjere u pogledu pristupa vlade, uključujući pravni lijek opisan u Prilogu II. ovoj Odluci. Trebalo bi obuhvatiti i djelotvornost nadzora i osiguranja provedbe u pogledu pravila koja se primjenjuju na PIHBO-e te u području kaznenog progona i nacionalne sigurnosti.

(182) Za provedbu preispitivanja Komisija bi se trebala sastati s PPC-om, prema potrebi zajedno s drugim japanskim tijelima odgovornima za pristup vlade, uključujući relevantna nadzorna tijela. Sudjelovanje na tom sastanku trebalo bi biti otvoreno za predstavnike članova Europskog odbora za zaštitu podataka. U okviru zajedničkog preispitivanja Komisija bi trebala zatražiti od PPC-a da dostavi sveobuhvatne informacije o svim aspektima relevantnima za zaključak o primjerenosti, među ostalim o ograničenjima i zaštitnim mjerama u pogledu pristupa vlade ([152]). Komisija bi trebala i zatražiti objašnjenja svih informacija relevantnih za ovu Odluku koje je zaprimila, uključujući javna izvješća japanskih tijela ili drugih dionika u Japanu, Europskog odbora za zaštitu podataka, pojedinačnih tijela za zaštitu podataka, skupina civilnog društva, medijska izvješća ili informacije iz bilo kojih drugih dostupnih izvora.

(183) Na temelju zajedničkog preispitivanja Komisija bi trebala sastaviti javno izvješće koje podnosi Europskom parlamentu i Vijeću.

### 7. **SUSPENZIJA ODLUKE O PRIMJERENOSTI**

(184) Ako na temelju redovnih i *ad hoc* provjera ili drugih dostupnih informacija Komisija zaključi da se razina zaštite koju pruža japanski pravni poredak više ne može smatrati u načelu istovjetnom onoj u Europskoj uniji, trebala bi o tome obavijestiti nadležna japanska tijela i zatražiti poduzimanje odgovarajućih mjera u određenom, razumnom roku. To uključuje pravila primjenjiva i na poslovne subjekte i na japanska javna tijela odgovorna za kazneni progon ili nacionalnu sigurnost. Na primjer, takav bi se postupak pokrenuo u slučajevima kad se daljnji prijenos, među ostalim na temelju odluka koje je donio PPC prema članku 24. APPI-ja kojima potvrđuje da treća zemlja pruža razinu zaštite istovjetnu onoj koja je zajamčena u Japanu, više neće provoditi u okviru zaštitnih mjera kojima se osigurava kontinuitet zaštite u smislu članka 44. Opće uredbe o zaštiti podataka.

(185) Ako nakon određenog roka nadležna japanska tijela ne dokažu na zadovoljavajući način da se ova Odluka i dalje temelji na primjerenoj razini zaštite, Komisija bi, u skladu s člankom 45. stavkom 5. Uredbe (EU) 2016/679, trebala pokrenuti postupak za djelomičnu ili potpunu suspenziju ili stavljanje izvan snage ove Odluke. Druga je mogućnost da Komisija pokrene postupak izmjene ove Odluke, prije svega postavljajući dodatne uvjete za prijenos podataka ili ograničavajući područje primjene zaključka o primjerenosti samo na prijenos podataka za koje je osiguran kontinuitet zaštite u smislu članka 44. Opće uredbe o zaštiti podataka.

([150]) U skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 u „provedbenom aktu predviđen je mehanizam za periodično preispitivanje, najmanje svake četiri godine, kojim će se uzeti u obzir svi relevantni događaji u toj trećoj zemlji ili međunarodnoj organizaciji".

([151]) Člankom 45. stavkom 3. Uredbe (EU) 2016/679 propisano je da se periodično preispitivanje provodi najmanje svake četiri godine. Vidjeti i Europski odbor za zaštitu podataka, *Adequacy Referential*, WP 254 rev. 01.

([152]) Vidjeti i Prilog II., odjeljak IV.: „U okviru periodičnog preispitivanja odluke o primjerenosti PPC i Europska komisija razmjenjivat će informacije o obradi podataka pod uvjetima zaključka o primjerenosti, uključujući one koje su iznesene u ovoj Izjavi."

(186) Konkretno, Komisija bi trebala pokrenuti postupak suspenzije ili stavljanja izvan snage u slučaju naznaka da poslovni subjekti koji primaju osobne podatke u skladu s ovom Odlukom ne poštuju Dopunska pravila iz Priloga I. i/ili da njihova provedba nije djelotvorno osigurana, ili ako japanska nadležna tijela ne postupaju u skladu s izjavama, jamstvima i obvezama iz Priloga II. ovoj Odluci.

(187) Komisija bi trebala razmotriti i pokretanje postupka koji vodi do izmjene, suspenzije ili stavljanja izvan snage ove Odluke ako, u kontekstu zajedničkog preispitivanja ili na drugi način, nadležna japanska tijela ne dostave informacije ili pojašnjenja koja su potrebna za procjenu razine zaštite osobnih podataka koji se prenose iz Europske unije u Japan ili poštovanja ove Odluke. U tom pogledu Komisija bi trebala uzeti u obzir opseg u kojem se relevantne informacije mogu dobiti iz drugih izvora.

(188) Zbog opravdanih hitnih razloga, kao što je rizik od ozbiljne povrede prava ispitanika, Komisija bi trebala razmotriti donošenje odluke o suspenziji ili stavljanju izvan snage ove Odluke koja bi se trebala odmah primjenjivati, u skladu s člankom 93. stavkom 3. Uredbe (EU) 2016/679 u vezi s člankom 8. Uredbe (EU) br. 182/2011 Europskog parlamenta i Vijeća ([153]).

## 8. **ZAVRŠNA RAZMATRANJA**

(189) Europski odbor za zaštitu podataka objavio je svoje mišljenje ([154]), koje je uzeto u obzir pri pripremi ove Odluke.

(190) Europski parlament donio je rezoluciju o strategiji digitalne trgovine kojom Komisiju poziva da donošenje odluka o primjerenosti s važnim trgovinskim partnerima postavi kao prioritet te ga ubrza kao važan mehanizam za zaštitu prijenosa osobnih podataka iz Europske unije, pod uvjetima utvrđenima u Uredbi (EU) 2016/679 ([155]). Europski parlament donio je i rezoluciju o primjerenosti zaštite osobnih podataka koju pruža Japan ([156]).

(191) Mjere navedene u ovoj Odluci u skladu su s mišljenjem Odbora osnovanog člankom 93. stavkom 1. Opće uredbe o zaštiti podataka.

DONIJELA JE OVU ODLUKU:

*Članak 1.*

1. Za potrebe članka 45. Uredbe (EU) 2016/679 Japan osigurava primjerenu razinu zaštite osobnih podataka koji se iz Europske unije prenose poslovnim subjektima u Japanu koji postupaju s osobnim informacijama i podliježu Zakonu o zaštiti osobnih informacija, kako je dopunjen Dopunskim pravilima iz Priloga I., te službenim izjavama, jamstvima i obvezama iz Priloga II.

([153]) Uredba (EZ) br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije (SL L 55, 28.2.2011., str. 13.)

([154]) Mišljenje 28/2018 o Nacrtu provedbene odluke Europske komisije o primjerenosti zaštite osobnih podataka u Japanu, prihvaćeno 5. prosinca 2018.

([155]) Europski parlament, Rezolucija od 12. prosinca 2017. „Ususret strategiji digitalne trgovine" (2017/2065(INI)). Vidjeti posebno točku 8. („… podsjeća na to da se osobni podaci mogu prenijeti u treće zemlje bez korištenja općih pravila iz trgovinskih sporazuma kada su, trenutačno i u budućnosti, ispunjeni zahtjevi iz […] poglavlja V. Uredbe (EU) 2016/679; priznaje da su odluke o primjerenosti, uključujući djelomične i one koje se odnose na sektor, temeljni mehanizam zaštite prijenosa osobnih podataka iz EU-a u treću zemlju; napominje da je EU sa samo četiri od svojih 20 najvećih trgovinskih partnera donio odluke o primjerenosti…" i točku 9. („poziva Komisiju da odredi prioritete i ubrza donošenje odluka o primjerenosti, pod uvjetom da treće zemlje osiguraju, na temelju nacionalnog prava ili njihovih međunarodnih obveza, razinu zaštite koja je ‚u osnovi jednaka' onoj koja se jamči u Europskoj uniji…").

([156]) Europski parlament, Rezolucija od 13. prosinca 2018. „Primjerenost zaštite osobnih podataka koju pruža Japan" (2018/2979(RSP)).

2. Ova Odluka ne odnosi se na osobne podatke koji se prenose primateljima iz jedne od sljedećih kategorija u mjeri u kojoj svrha obrade osobnih podataka odgovara, djelomično ili u potpunosti, jednoj od navedenih svrha, i to:

(a) ustanove za radiodifuziju, novinski nakladnici, komunikacijske agencije i druge medijske organizacije (uključujući pojedince koji se bave medijskim aktivnostima u svojem poslovanju) u mjeri u kojoj obrađuju osobne podatke u informativne svrhe;

(b) osobe koje se profesionalno bave pisanjem, u mjeri u kojoj to uključuje osobne podatke;

(c) sveučilišta i sve druge organizacije ili skupine usmjerene na akademski studij, ili sve osobe koje pripadaju takvoj organizaciji ili skupini, u mjeri u kojoj obrađuju osobne podatke za potrebe akademskih studija;

(d) vjerske zajednice, u mjeri u kojoj obrađuju osobne podatke u svrhe vjerske djelatnosti (uključujući sve povezane aktivnosti); i

(e) politička tijela, u mjeri u kojoj obrađuju osobne podatke za potrebe svoje političke aktivnosti (uključujući sve povezane aktivnosti).

*Članak 2.*

Kad god nadležna tijela država članica radi zaštite pojedinaca u vezi s obradom njihovih osobnih podataka izvršavaju svoje ovlasti na temelju članka 58. Uredbe (EU) 2016/679, što dovodi do suspenzije ili konačne zabrane protoka podataka prema određenom poslovnom subjektu u Japanu unutar područja primjene iz članka 1., predmetna država članica o tome bez odgode obavješćuje Komisiju.

*Članak 3.*

1. Komisija kontinuirano prati primjenu pravnog okvira na kojem se temelji ova Odluka, uključujući uvjete pod kojima se odvija daljnji prijenos, kako bi ocijenila osigurava li Japan i dalje primjerenu razinu zaštite u smislu članka 1.

2. Države članice i Komisija međusobno se obavješćuju o slučajevima u kojima Povjerenstvo za zaštitu osobnih informacija ili bilo koje drugo nadležno tijelo u Japanu ne osigura poštovanje pravnog okvira na kojem se temelji ova Odluka.

3. Države članice i Komisija međusobno se obavješćuju o naznakama da zadiranje japanskih javnih tijela u pravo pojedinaca na zaštitu njihovih osobnih podataka prelazi ono što je nužno ili da ne postoji djelotvorna pravna zaštita od takvog zadiranja.

4. U roku od dvije godine od dana kad su države članice obaviještene o ovoj Odluci, a potom najmanje svake četiri godine, Komisija ocjenjuje zaključak iz članka 1. stavka 1. na temelju svih dostupnih informacija, među ostalim na temelju informacija primljenih u okviru zajedničkog preispitivanja provedenog s relevantnim japanskim tijelima.

5. Ako Komisija ima saznanja da primjerena razina zaštite više nije osigurana, o tome obavješćuje nadležna japanska tijela. Ako je potrebno, može odlučiti suspendirati, izmijeniti ili staviti izvan snage ovu Odluku, ili ograničiti njezino područje primjene, posebno ako postoje naznake da:

(a) poslovni subjekti u Japanu koji su primili osobne podatke iz Europske unije na temelju ove Odluke ne poštuju dodatne zaštitne mjere navedene u Dopunskim pravilima iz Priloga I. ovoj Odluci ili nadzor i provedba u tom pogledu nisu dostatni;

(b) japanska javna tijela ne poštuju izjave, jamstva i obveze iz Priloga II. ovoj Odluci, među ostalim u pogledu uvjeta i ograničenja za prikupljanje osobnih podataka prenesenih na temelju ove Odluke i pristup japanskih javnih tijela tim podacima za potrebe kaznenog progona ili nacionalne sigurnosti.

Komisija može predstaviti nacrte takvih mjera i ako zbog nesuradnje japanske vlade ne može utvrditi utječe li to na zaključak iz članka 1. stavka 1. ove Odluke.

*Članak 4.*

Ova je Odluka upućena državama članicama.

Sastavljeno u Bruxellesu 23. siječnja 2019.

*Za Komisiju*
Věra JOUROVÁ
*Član Komisije*

*PRILOG 1.*

**DOPUNSKA PRAVILA U OKVIRU ZAKONA O ZAŠTITI OSOBNIH INFORMACIJA ZA POSTUPANJE S OSOBNIM PODACIMA KOJI SE PRENOSE IZ EU-A NA TEMELJU ODLUKE O PRIMJERENOSTI**

Sadržaj



[Termini]

| | |
|---|---|
| „Zakon” | Zakon o zaštiti osobnih informacija (Zakon br. 57, 2003.). |
| „Nalog Kabineta” | Nalog Kabineta za izvršenje Zakona o zaštiti osobnih informacija (Nalog Kabineta br. 507, 2003.) |
| „Pravila” | Pravila izvršenja Zakona o zaštiti osobnih informacija (Pravila Povjerenstva za zaštitu osobnih informacija br. 3, 2016.) |
| „Smjernice za Opća pravila” | Smjernice za Zakon o zaštiti osobnih informacija (svezak o Općim pravilima) (Obavijest Povjerenstva za zaštitu osobnih informacija br. 65, 2015.) |
| „EU” | Europska unija, uključujući njezine države članice i, u svjetlu Sporazuma o EGP-u, Island, Lihtenštajn i Norvešku |
| „Opća uredba o zaštiti podataka” | Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) |
| „odluka o primjerenosti” | Odluka Europske komisije o tome da treća zemlja ili područje u toj trećoj zemlji itd. osigurava primjerenu razinu zaštite osobnih podataka u skladu s člankom 45. Opće uredbe o zaštiti podataka |

U svrhu uzajamnog i neometanog prijenosa osobnih podataka između Japana i EU-a, Povjerenstvo za zaštitu osobnih informacija utvrdilo je da EU kao strana zemlja s uspostavljenim sustavom zaštite osobnih informacija ima istovjetne standarde kao Japan u pogledu zaštite prava i interesa pojedinaca na temelju članka 24. Zakona, dok je Europske komisije istodobno utvrdila da Japan osigurava primjerenu razinu zaštite osobnih podataka u skladu s člankom 45. Opće uredbe o zaštiti podataka.

Ovime će se uzajaman i neometan prijenos osobnih podataka između Japana i EU-a odvijati na način kojim se osigurava visoka razina zaštite prava i interesa pojedinaca. Kako bi se osigurala visoka razina zaštite osobnih informacije dobivenih od EU-a na temelju odluke o primjerenosti i s obzirom na činjenicu da, unatoč visokoj razini konvergencije tih dvaju sustava, postoje određene bitne razlike, Povjerenstvo za zaštitu osobnih informacija donijelo je ova Dopunska pravila, koja se temelje na odredbama Zakona o provedbi itd. suradnje s vladama drugih zemalja, kako bi se osiguralo da poslovni subjekti koji postupaju s osobnim informacijama primjereno postupaju s osobnim informacijama dobivenima od EU-a na temelju odluke o primjerenosti te u cilju ispravne i učinkovite provedbe obveza utvrđenih tim pravilima ([1]).

([1]) Članci 4., 6., 8., 24., 60. i 78. Zakona i članak 11. Pravila.

Konkretno, člankom 6. Zakona posebno su propisane ovlasti za poduzimanje potrebnih zakonodavnih i drugih mjera radi osiguranja bolje zaštite osobnih informacija i uspostave sustava za osobne informacije na međunarodnoj razini na temelju strožih pravila kojima se dopunjuju i koja nadilaze ona utvrđena u Zakonu i Nalogu Kabineta. Stoga je Povjerenstvo za zaštitu osobnih informacija, kao tijelo nadležno za upravljanje općom provedbom Zakona, ovlašteno na temelju članka 6. Zakona uvesti strože propise utvrđivanjem ovih Dopunskih pravila, kojima se osigurava viša razina zaštite prava i interesa pojedinaca u pogledu postupanja s osobnim podacima dobivenima od EU-a na temelju odluke o primjerenosti, uključujući u vezi s definicijom „osobnih informacija koje zahtijevaju posebnu pozornost" iz članka 2. stavka 3. Zakona i „pohranjenih osobnih podataka" iz članka 2. stavka 7. Zakona (uključujući i u pogledu relevantnog razdoblja pohrane).

Na toj osnovi Dopunska pravila obvezujuća su za poslovne subjekte koji postupaju s osobnim informacijama prenesenima iz EU-a na temelju odluke o primjerenosti te su ih oni dužni poštovati. Budući da su Dopunska pravila pravno obvezujuća, Povjerenstvo za zaštitu osobnih informacija izvršava prava i obveze koji iz njih proizlaze na isti način kao i odredbe Zakona koji dopunjuju strožim i/ili detaljnijim pravilima. U slučaju povrede prava i obveza koji proizlaze iz Dopunskih pravila, pojedinci imaju pravo na sudsku zaštitu jednako kao i u slučaju povrede prava i obveza koji proizlaze iz odredaba Zakona koji dopunjuju strožim i/ili detaljnijim pravilima.

U pogledu izvršenja za koje je nadležno Povjerenstvo za zaštitu osobnih informacija, ako poslovni subjekt koji postupa s osobnim informacijama ne poštuje jednu ili više obveza na temelju Dopunskih pravila, to povjerenstvo ima ovlasti donositi mjere u skladu s člankom 42. Zakona. U pogledu općenito osobnih informacija dobivenih od EU-a na temelju odluke o primjerenosti, ako poslovni subjekt koji postupa s osobnim informacijama ne poduzme mjere u skladu s preporukom dobivenom u skladu s člankom 42. stavkom 1. Zakona a da za to nema opravdan razlog ([2]), to se smatra ozbiljnom i neposrednom povredom prava i interesa pojedinca u smislu članka 42. stavka 2. Zakona.

1. Osobne informacije koje zahtijevaju posebnu pozornost (članak 2. stavak 3. Zakona)

Članak 2. stavak 3. Zakona

3. „Osobne informacije koje zahtijevaju posebnu pozornost" u Zakonu znače osobne informacije principala koje obuhvaćaju njegovu rasu, uvjerenje, socijalni status, povijest bolesti, kaznenu evidenciju, činjenicu da je pretrpio štetu zbog kaznenog djela, ili druge opise itd. za koje je Nalogom Kabineta propisano da se s njima mora postupati s posebnom pozornošću kako se ne bi prouzročila nepoštena diskriminacija, predrasude ili druge negativne posljedice za principala."

Članak 2. Naloga Kabineta

Ti opisi itd. iz članka 2. stavka 3. Zakona u skladu s Nalogom Kabineta jesu opisi itd. koji sadržavaju neku od činjenica navedenih u nastavku (osim onih koji se nalaze u zdravstvenoj ili kaznenoj evidenciji principala):

i. tjelesni invaliditet, intelektualne teškoće, mentalni invaliditet (uključujući osobe s teškoćama u razvoju) ili drugi oblici tjelesnih i mentalnih oštećenja u skladu s pravilima Povjerenstva za zaštitu osobnih informacija;

ii. rezultati liječničkog pregleda ili druge zdravstvene pretrage (dalje u tekstu: „liječnički pregled itd.") za sprečavanje i rano otkrivanje bolesti koje je obavio liječnik ili drugi zdravstveni djelatnik (dalje u tekstu: „liječnik itd.");

iii. upute, zdravstvena skrb ili recept koju je principal dobio od liječnika itd. u cilju poboljšanja tjelesnog ili mentalnog stanja na temelju rezultata liječničkog pregleda itd. ili zbog bolesti, ozljede ili drugih mentalnih ili tjelesnih promjena;

iv. uhićenje, policijska pretraga, zapljena, zadržavanje, kazneni progon ili drugi postupci povezani s kaznenim postupkom u kojem je principal osumnjičenik ili optuženik;

([2]) Opravdan razlog znači izvanredan događaj koji je izvan kontrole poslovnog subjekta koji postupa s osobnim informacijama i koji se ne može razumno predvidjeti (npr. prirodne katastrofe) ili slučaj u kojem poduzimanje mjera u skladu s preporukom koju je Povjerenstvo za zaštitu osobnih informacija izdalo u skladu s člankom 42. stavkom 1. više nije potrebno jer je poslovni subjekt koji postupa s osobnim informacijama poduzeo alternativne mjere kojima je povreda u potpunosti ispravljena.

v. istraga, mjera promatranja i zaštite, saslušanje i odluka, zaštitna mjera ili drugi postupci povezani sa zaštitom maloljetnika koji su provedeni protiv principala kao maloljetnog počinitelja kaznenih djela ili osumnjičenika za takva djela u skladu s člankom 3. stavkom 1. Zakona o maloljetnicima.

Članak 5. Pravila

Tjelesni i mentalni funkcionalni invaliditet iz članka 2. točke i. Naloga u skladu s pravilima Povjerenstva za zaštitu osobnih informacija jest sljedeći:

i. tjelesni invaliditet utvrđen u tablici priloženoj Zakonu o zaštiti osoba s tjelesnim invaliditetom (Zakon br. 283 iz 1949.);

ii. intelektualne teškoće utvrđene u Zakonu o zaštiti osoba s intelektualnim teškoćama (Zakon br. 37 iz 1960.);

iii. mentalni invaliditet utvrđen u Zakonu o mentalnom zdravlju i zaštiti osoba s mentalnim invaliditetom (Zakon br. 123 iz 1950.) (uključujući osobe s teškoćama u razvoju iz članka 2. stavka 1. Zakona o potpori osobama s teškoćama u razvoju, no ne uključujući intelektualne teškoće iz Zakona o zaštiti osoba s intelektualnim teškoćama);

iv. neizlječiva bolest ili druge bolesti u skladu s Nalogom Kabineta iz članka 4. stavka 1. Zakona o sveobuhvatnoj potpori svakodnevnom i društvenom životu osoba s invaliditetom (Zakon br. 123 iz 2005.) koje su jednako teške kao one iz Naloga Ministra zdravstva, rada i socijalne skrbi iz istog stavka.

Ako osobni podaci dobiveni od EU-a na temelju odluke o primjerenosti sadržavaju podatke koji se odnose na spolni život, spolnu orijentaciju ili članstvo u sindikatu fizičke osobe, a koji su u Općoj uredbi o zaštiti podataka definirani kao posebne kategorije osobnih podataka, poslovni subjekti koji postupaju s osobnim informacijama moraju s njima postupati na isti način kao s osobnim informacijama koje zahtijevaju posebnu pozornost u smislu članka 2. stavka 3. Zakona.

2. Pohranjeni osobni podaci (članak 2. stavak 7. Zakona)

Članak 2. stavak 7. Zakona

7. „Pohranjeni osobni podaci" u tom zakonu znači osobne informacije koje je poslovni subjekt koji postupa s osobnim informacijama ovlašten otkriti, ispraviti, dopuniti ili izbrisati njihov sadržaj, prestati koristiti, izbrisati i prestati prosljeđivati trećoj strani, a u skladu s Nalogom Kabineta nije vjerojatno da bi mogli nanijeti štetu javnim ili drugim interesima ako se sazna za njihovo postojanje ili nepostojanje odnosno nije određeno da se brišu u roku od najviše jedne godine.

Članak 4. Naloga Kabineta

Osobni podaci u skladu s člankom 2. stavkom 7. Naloga Kabineta jesu sljedeći:

i. osobni podaci za koje postoji mogućnost da će, sazna li se za njihovo postojanje ili nepostojanje, naštetiti životu, tijelu ili imetku principala ili treće strane;

ii. osobni podaci za koje postoji mogućnost da će, sazna li se za njihovo postojanje ili nepostojanje, potaknuti ili uzrokovati nezakonito ili nepravedno postupanje;

iii. osobni podaci za koje postoji mogućnost da će, sazna li se za njihovo postojanje ili nepostojanje, ugroziti nacionalnu sigurnost, uništiti povjerenje uspostavljeno sa stranom zemljom ili međunarodnom organizacijom ili da će dovesti do nepovoljnog položaja u pregovorima sa stranom zemljom ili međunarodnom organizacijom;

iv. osobni podaci za koje postoji mogućnost da će, sazna li se za njihovo postojanje ili nepostojanje, omesti održavanje javne sigurnosti i reda, primjerice sprečavanje, suzbijanje ili istraživanje kaznenog djela.

Članak 5. Naloga Kabineta

Razdoblje iz članka 2. stavka 7. Zakona u skladu s Nalogom Kabineta iznosi šest mjeseci.

S osobnim podacima dobivenima od EU-a na temelju odluke o primjerenosti mora se postupati kao s pohranjenim osobnim podacima u smislu članka 2. stavka 7. Zakona, bez obzira na rok u kojem ih treba izbrisati.

Ako su osobni podaci dobiveni od EU-a na temelju odluke o primjerenosti obuhvaćeni definicijom osobnih podataka iz Naloga Kabineta za koje je „vjerojatno da bi mogli nanijeti štetu javnim ili drugim interesima ako se sazna za njihovo postojanje ili nepostojanje", s njima se ne mora postupati kao s pohranjenim osobnim podacima (vidjeti članak 4. Naloga Kabineta; Smjernice za Opća pravila („Pohranjeni osobni podaci" članak 2. stavak 7.).

3. Navođenje svrhe korištenja, ograničenja na temelju svrhe korištenja (članak 15. stavak 1., članak 16. stavak 1. i članak 26. stavci 1. i 3. Zakona)

Članak 15. stavak 1. Zakona

1. Kada postupa s osobnim informacijama, poslovni subjekt koji postupa s osobnim informacijama dužan je što preciznije navesti svrhu njihova korištenja (dalje u tekstu „svrha korištenja").

Članak 16. stavak 1. Zakona

1. Poslovni subjekt koji postupa s osobnim informacijama ne smije postupati s osobnim informacijama bez prethodne privole principala više nego što je nužno za postizanje svrhe korištenja navedene u skladu s odredbama prethodnog članka.

Članak 26. stavci 1. i 3. Zakona

1. Kada primi osobne podatke od treće strane, poslovni subjekt koji postupa s osobnim informacijama dužan je potvrditi činjenice navedene u nastavku u skladu s pravilima Povjerenstva za zaštitu osobnih informacija: (izostavljeno)

   i. (izostavljeno)

   ii. okolnosti u kojima je navedena treća strana pribavila navedene osobne podatke.

3. Ako je poslovni subjekt koji postupa s osobnim informacijama potvrdio činjenice u skladu s odredbama stavka 1., dužan je u skladu s pravilima Povjerenstva za zaštitu osobnih informacija voditi evidenciju o datumu njihova primitka, navedenoj potvrdi i drugim činjenicama obuhvaćenima tim pravilima.

Ako poslovni subjekt koji postupa s osobnim informacijama postupa s osobnim informacijama više nego što je nužno za postizanje svrhe korištenja iz članka 15. stavka 1. Zakona, dužan je pribaviti prethodnu privolu principala (članak 16. stavak 1. Zakona). Kada primi osobne podatke od treće strane, poslovni subjekt koji postupa s osobnim informacijama dužan je u skladu s Pravilima potvrditi činjenice kao što su okolnosti u kojima je navedena treća strana pribavila navedene osobne podatke i voditi evidenciju o njima (članak 26. stavci 1. i 3. Zakona).

Ako poslovni subjekt koji postupa s osobnim informacijama primi osobne podatke iz EU-a na temelju odluke o primjerenosti, okolnosti povezane s pribavljanjem navedenih osobnih podataka koje se potvrđuju i evidentiraju u skladu s člankom 26. stavcima 1. i 3. uključuju svrhu korištenja za koju su primljeni od EU-a.

Slično tome, ako poslovni subjekt koji postupa s osobnim informacijama primi od drugog takvog poslovnog subjekata podatke koji su prethodno preneseni iz EU-a na temelju odluke o primjerenosti, okolnosti povezane s pribavljanjem navedenih osobnih podataka koje se potvrđuju se i evidentiraju u skladu s člankom 26. stavcima 1. i 3. uključuju svrhu korištenja za koju su primljeni.

U navedenim slučajevima poslovni subjekt koji postupa s osobnim informacijama dužan je navesti svrhu korištenja navedenih osobnih podataka u okviru svrhe korištenja za koju su podaci prvotno ili naknadno primljeni, kako su potvrđeni i evidentirani u skladu s člankom 26. stavcima 1. i 3., i koristiti ih u okviru svrhe korištenja (u skladu s člankom 15. stavkom 1. i člankom 16. stavkom 1. Zakona).

4. Ograničenje prosljeđivanja trećoj strani u stranoj zemlji (članak 24. Zakona; članak 11. stavak 2. Pravila)

Članak 24. Zakona

Osim u slučajevima iz prethodnog članka stavka 1., ako poslovni subjekt koji postupa s osobnim informacijama prosljeđuje osobne podatke trećoj strani (osim treće strane s uspostavljenim sustavom u skladu sa standardima propisanim pravilima Povjerenstva za zaštitu osobnih informacija koji je potreban za trajno poduzimanje mjera koje su istovjetne onima koje je poslovni subjekt koji postupa s osobnim informacijama dužan poduzeti pri postupanju s osobnim podacima u skladu s odredbama ovoj odjeljka, dalje u tekstu ovog članka isto) u stranoj zemlji (zemlja ili područje izvan državnog područja Japana; dalje u tekstu ovog članka isto) (osim onih koje su u skladu s pravilima Povjerenstva za zaštitu osobnih informacija priznate kao strana zemlja s uspostavljenim sustavom zaštite osobnih informacija koja ima istovjetne standarde kao Japan u pogledu zaštite prava i interesa pojedinaca; dalje u tekstu ovog članka isto) dužan je pribaviti prethodnu privolu principala za to prosljeđivanje trećoj strani u stranoj zemlji. U tom slučaju ne primjenjuju se odredbe prethodnog članka.

Članak 11. stavak 2. Pravila

Standardi propisani pravilima Povjerenstva za zaštitu osobnih informacija u skladu s člankom 24. Zakona moraju se poštovati u svim točkama u nastavku:

i. poslovni subjekt koji postupa s osobnim informacijama i osoba koja prima osobne podatke osigurali su da osoba koja prima osobne podatke pri postupanju s njima primjerenim i razumnim metodama provodi mjere u skladu s ciljem odredbi poglavlja IV. odjeljka 1. Zakona.

ii. osoba koja prima osobne podatke priznata je na temelju međunarodnog okvira za postupanje s osobnim podacima.

Ako poslovni subjekt koji postupa s osobnim informacijama trećoj strani u stranoj zemlji prosljeđuje osobne podatke dobivene od EU-a na temelju odluke o primjerenosti, on je za to prosljeđivanje trećoj strani u stranoj zemlji u skladu s člankom 24. Zakona dužan pribaviti prethodnu privolu principala, kojeg se mora prethodno informirati o okolnostima prijenosa koje su potrebne da bi principal mogao donijeti odluku o privoli, osim u slučajevima iz sljedećih točaka od i. do iii.:

i. ako je treća strana u zemlji koja je u skladu s Pravilima priznata kao strana zemlja s uspostavljenim sustavom zaštite osobnih informacija koja ima istovjetne standarde kao Japan u pogledu zaštite prava i interesa pojedinaca;

ii. ako su poslovni subjekt koji postupa s osobnim informacijama i treća strana koja prima osobne podatke zajedno primjerenim i razumnim metodama (ugovor, drugi oblici obvezujućih sporazuma ili obvezujući sporazumi unutar grupe trgovačkih društava) proveli mjere kojima se osigurava istovjetna razina zaštite kao na temelju Zakona, tumačenog zajedno s ovim Pravilima, kada ta treća strana postupa s osobnim podacima;

iii. u slučajevima iz članka 23. stavka 1. Zakona.

5. Anonimno obrađene informacije (članak 2. stavak 9. i članak 36. stavci 1. i 2. Zakona)

Članak 2. stavak 9. Zakona

9. „Anonimno obrađene informacije" u ovom Zakonu znači informacije koje se odnose na pojedinca i koje se mogu dobiti obradom osobnih informacija kako bi se, poduzimanjem mjera iz točaka u nastavku u skladu s podjelom osobnih informacija iz svake točke, onemogućila identifikacija određene osobe i vraćanje osobnih informacija u prvotni oblik.

i. osobne informacije iz stavka 1. točke i.;

Brisanje dijela opisa itd. iz navedenih osobnih informacija (uključujući zamjenu navedenog dijela opisa itd. drugim opisima itd. uporabom metode bez pravilnosti kojom se navedeni dio opisa može vratiti u prvotni oblik itd.)

ii. osobne informacije iz stavka 1. točke ii.;

Brisanje svih identifikacijskih oznaka pojedinaca iz navedenih osobnih informacija (uključujući zamjenu navedenih identifikacijskih oznaka pojedinaca drugim opisima itd. uporabom metode bez pravilnosti kojom se navedene identifikacijske oznake pojedinaca mogu vratiti u prvotni oblik)

Članak 36. stavak 1. Zakona

1. Poslovni subjekt koji postupa s osobnim informacijama radi dobivanja anonimno obrađenih informacija (ograničenih na one koje čine anonimno obrađenu bazu podataka itd.; dalje u tekstu isto) dužan je obraditi osobne informacije u skladu sa standardima koji su pravilima Povjerenstva za zaštitu osobnih informacija propisani kao standardi nužni za onemogućavanje identifikacije određenog pojedinca i vraćanje dobivenih osobnih informacija u prvotni oblik.

Članak 19. Pravila

Standardi propisani pravilima Povjerenstva za zaštitu osobnih informacija u skladu s člankom 36. stavkom 1. Zakona jesu sljedeći:

i. brisanje cijelih opisa itd. ili njihovih dijelova na temelju kojih se može identificirati određena osoba navedena u osobnim informacijama (uključujući zamjenu takvih opisa itd. drugim opisima itd. uporabom metode bez pravilnosti kojom se cjelokupni opisi itd. ili njihovi dijelovi mogu vratiti u prvotni oblik);

ii. brisanje svih identifikacijskih oznaka pojedinaca iz osobnih informacija (uključujući zamjenu takvih oznaka drugim opisima itd. uporabom metode bez pravilnosti kojom se identifikacijske oznake pojedinaca mogu vratiti u prvotni oblik);

iii. brisanje onih oznaka (ograničeno na oznake koje povezuju više informacija s kojima stvarno postupa poslovni subjekt koji postupa s osobnim informacijama) koje povezuju osobne informacije s informacijama dobivenima poduzimanjem mjera u vezi s osobnim informacijama (uključujući zamjenu navedenih oznaka drugim oznakama kojima se ne mogu povezati navedene osobne informacije s informacijama dobivenima poduzimanjem mjera u vezi s navedenim osobnim informacijama, uporabom metode bez pravilnosti kojom se navedene oznake mogu vratiti u prvotni oblik);

iv. brisanje idiosinkratičnih opisa itd. (uključujući zamjenu takvih opisa itd. drugim opisima itd. uporabom metode bez pravilnosti kojom se idiosinkratični opisi mogu vratiti u prvotni oblik itd.);

v. osim mjera iz prethodnih točaka, poduzimanje odgovarajućih mjera na temelju rezultata s obzirom na atribut itd. baze podataka osobnih informacija itd., npr. razlika između opisa itd. sadržanih u osobnim informacijama i opisima itd. iz drugih osobnih informacija koje čine bazu podataka osobnih informacija itd., koje obuhvaćaju navedene osobne informacije.

Članak 36. stavak 2. Zakona

2. Poslovni subjekti koji postupaju s osobnim informacijama dužni su nakon dobivanja anonimno obrađenih informacija poduzeti mjere za sigurnosni nadzor tih informacija, u skladu sa standardima propisanima u pravilima Povjerenstva za zaštitu osobnih informacija, a koji su potrebni kako bi se spriječilo curenje informacija u vezi s tim opisima itd. i identifikacijskim oznakama pojedinaca izbrisanima iz osobnih informacija, upotrijebljenih za dobivanje anonimno obrađenih informacija, te informacija o metodi obrade provedenoj u skladu s odredbama prethodnog stavka.

Članak 20. Pravila

Standardi propisani pravilima Povjerenstva za zaštitu osobnih informacija u skladu s člankom 36. stavkom 2. Zakona jesu sljedeći:

i. jasno definiranje nadležnosti i odgovornosti osobe koja postupa s informacijama koje se odnose na te opise itd. te identifikacijskim oznakama pojedinaca koje su izbrisane iz osobnih informacija, upotrijebljenima za dobivanje anonimno obrađenih informacija, te informacijama o provedenoj metodi obrade u skladu s odredbama članka 36. stavka 1. (ograničeno na one koje omogućuju vraćanje osobnih informacija u prvotni oblik uporabom takvih povezanih informacija) (dalje u tekstu ovog članka „informacije o metodi obrade itd.");

ii. utvrđivanje pravila i postupaka za postupanje s informacijama o metodi obrade itd., odgovarajuće postupanje s informacijama o metodi obrade itd. u skladu s pravilima i postupcima, ocjenjivanje postupanja te, na temelju rezultata tog ocjenjivanja, poduzimanje potrebnih mjera u cilju poboljšanja;

iii. poduzimanje potrebnih i odgovarajućih mjera kako bi se spriječilo da osoba koja nema zakonite ovlasti za postupanje s informacijama o metodi obrade itd. postupa s informacijama o metodi obrade itd.

Osobne informacije dobivene od EU-a na temelju odluke o primjerenosti smatraju se anonimno obrađenim informacijama u smislu članka 2. stavka 9. Zakona samo ako poslovni subjekt koji postupa s osobnim informacijama poduzme mjere za onemogućavanje ponovne identifikacije pojedinca od strane bilo koga, među ostalim brisanjem informacija o metodi obrade itd. (tj. informacije koje se odnose na te opise itd. i identifikacijske oznake pojedinaca koje su izbrisane iz osobnih informacija, upotrijebljene za dobivanje anonimno obrađenih informacija, te informacije o provedenoj metodi obrade u skladu s odredbama članka 36. stavka 1. Zakona (ograničeno na one koje omogućuju vraćanje osobnih informacija u prvotni oblik uporabom takvih povezanih informacija)).

*PRILOG 2.*

Njezina Ekscelencija Věra Jourová, povjerenica za pravosuđe, zaštitu potrošača i ravnopravnost spolova Europske komisije

Vaša Ekscelencijo,

pozdravljam konstruktivne razgovore između Japana i Europske komisije čiji je cilj stvaranje okvira za uzajamni prijenos osobnih podataka između Japana i EU-a.

Na zahtjev Europske komisije upućen vladi Japana, dostavljam Vam priloženi dokument u kojem se daje pregled pravnog okvira u vezi s pristupom japanske vlade informacijama.

Dokument se odnosi na brojna ministarstva i agencije vlade Japana, a kada je riječ o sadržaju dokumenta, relevantna ministarstva i agencije (Tajništvo Kabineta, Nacionalna policijska agencija, Povjerenstvo za zaštitu osobnih informacija, Ministarstvo unutarnjih poslova i komunikacije, Ministarstvo pravosuđa, Obavještajna agencija za javnu sigurnost, Ministarstvo obrane) nadležni su za dijelove u okviru njihovih nadležnosti. U nastavku su navedena relevantna ministarstva i agencije s priloženim potpisima.

Povjerenstvo za zaštitu osobnih informacija prihvaća sve upite povezane s ovim dokumentom te će koordinirati potrebne odgovore među relevantnim ministarstvima i agencijama.

Nadam se da će ovaj dokument pomoći u donošenju odluka Europske komisije.

Cijenim Vaš izniman doprinos u vezi s ovim pitanjem.

S poštovanjem

Yoko Kamikawa

Ministrica pravosuđa

Ovaj dokument sastavili su Ministarstvo pravosuđa i sljedeća relevantna ministarstva i agencije.

Koichi Hamano

Savjetnik u Tajništvu kabineta

Schunichi Kuryu

Glavni povjerenik Nacionalne policijske agencije

Mari Sonoda

Glavna tajnica Povjerenstva za zaštitu osobnih informacija

Mitsuru Yasuda

Zamjenik ministra unutarnjih poslova i komunikacija

Seimei Nakagawa

Obavještajna agencija za javnu sigurnost

Kenichi Takahashi

Zamjenik dominstra obrane

14. rujna 2018.

**Prikupljanje i uporaba osobnih informacija od strane japanskih javnih tijela za potrebe kaznenog progona i nacionalne sigurnosti**

U sljedećem se dokumentu daje pregled pravnog okvira za prikupljanje i uporabu osobnih (elektroničkih) informacija od strane japanskih javnih tijela za potrebe kaznenog progona i nacionalne sigurnosti (dalje u tekstu „pristup vlade"), posebno u pogledu dostupne pravne osnove, primjenjivih uvjeta (ograničenja) i zaštitnih mjera, uključujući neovisne mogućnosti nadzora i pojedinačne mogućnosti pravne zaštite. Izjava je upućena Europskoj komisiji kako bi se iskazala predanost i zajamčilo da će pristup vlade osobnim informacijama prenesenima iz EU-a u Japan biti ograničen na ono što je nužno i razmjerno, podložno neovisnom nadzoru te da će pojedinci na koje se to odnosi moći dobiti pravnu zaštitu u slučaju mogućih povreda njihovog temeljnog prava na privatnost i zaštitu podataka. Izjavom se predviđa i uspostava novog mehanizma pravne zaštite kojim će upravljati Povjerenstvo za zaštitu osobnih informacija (PPC), radi rješavanja pritužbi pojedinaca iz EU-a u vezi s pristupom vlade njihovim osobnim podacima prenesenima iz EU-a u Japan.

## I. **Opća pravna načela relevantna za pristup vlade**

Kao oblik izvršavanja javnih ovlasti pristup vlade mora se provoditi potpuno u skladu sa zakonom (načelo zakonitosti). Osobne su informacije u Japanu zaštićene i u privatnom i u javnom sektoru s pomoću višeslojnog mehanizma.

### A. Ustavni okvir i načelo postupanja na temelju zakona

U članku 13. Ustava i sudskoj praksi pravo na privatnost priznaje se kao ustavno pravo. U tom pogledu Vrhovni sud smatra da je prirodno da pojedinci ne žele da druge osobe dođu do njihovih osobnih informacija bez opravdanog razloga te da to očekivanje treba zaštititi ([1]). Dodatni oblici zaštite sadržani su u članku 21. stavku 2. Ustava, kojim se osigurava poštovanje tajnosti komunikacije, te članku 35. Ustava, kojim se jamči pravo da se ne bude podvrgnut pretrazi ili zapljeni bez sudskog naloga, što znači da se prikupljanje osobnih informacija prisilnim sredstvima, uključujući pristup informacijama, uvijek mora temeljiti na sudskom nalogu. Takav se sudski nalog može izdati samo za istragu već počinjenog kaznenog djela. Stoga u pravnom okviru Japana nije dopušteno prikupljanje informacija prisilnim sredstvima za potrebe nacionalne sigurnosti (a ne za potrebe kaznene istrage).

Osim toga, u skladu s načelom postupanja na temelju zakona, prisilno prikupljanje informacija mora biti izričito odobreno zakonom. U slučaju neobveznog/dobrovoljnog prikupljanja, informacije se dobivaju iz izvora kojima se može slobodno pristupiti ili dobrovoljnim otkrivanjem, tj. na temelju zahtjeva koji se ne može prisilno nametnuti fizičkoj ili pravnoj osobi koja posjeduje te informacije. Međutim, to je dopušteno samo u mjeri u kojoj je javno tijelo nadležno za provođenje istrage, s obzirom na to da svako javno tijelo može djelovati samo u okviru svoje upravne nadležnosti propisane zakonom (bez obzira na to zadiru li njegove aktivnosti u prava i slobode pojedinaca). To se načelo primjenjuje na sposobnost tijela da prikuplja osobne informacije.

### B. Posebna pravila o zaštiti osobnih informacija

Zakonom o zaštiti osobnih informacija (APPI) i Zakonom o zaštiti osobnih informacija u upravnim organima (APPIHAO), koji se temelje na ustavnim odredbama i detaljnije ih tumače, jamči se pravo na osobne informacije u privatnom i javnom sektoru.

U članku 7. APPI-ja navodi se da Povjerenstvo za zaštitu osobnih informacija formulira „Osnovnu politiku zaštite osobnih informacija" (Osnovna politika). Osnovna politika, koja se donosi odlukom Kabineta Japana kao središnjeg tijela japanske vlade (premijer i ministri), određuje smjernice za zaštitu osobnih informacija u Japanu. Na taj način Povjerenstvo kao neovisno nadzorno tijelo služi kao „zapovjedni centar" japanskog sustava za zaštitu osobnih informacija.

Kad god upravni organi prikupljaju osobne informacije, neovisno o tome služe li se pritom prisilnim sredstvima ili ne, oni u načelu ([2]) moraju ispunjavati zahtjeve APPIHAO-a. APPIHAO je opće pravo koje se primjenjuje na obradu „pohranjenih osobnih informacija" ([3]) od strane „upravnih organa" (kako je definirano u članku 2. stavku 1. APPIHAO-a). Ono stoga

([1]) Vrhovni sud, presuda od 12. rujna 2003. (br. predmeta: 2002. (Ju) br. 1656).

([2]) Za iznimke u pogledu poglavlja 4. APPIHAO-a vidjeti u nastavku str. 16.

([3]) „Pohranjene osobne informacije" iz članka 2. stavka 5. APPIHAO-a znači osobne informacije koje zaposlenik upravnog tijela pripremi ili pribavi tijekom izvršavanja svojih dužnosti te koje navedeno upravno tijelo pohranjuje za organizacijsku uporabu svojih zaposlenika.

obuhvaća i obradu podataka u području kaznenog progona i nacionalne sigurnosti. Među javnim tijelima ovlaštenima za provedbu pristupa vlade, sva tijela osim prefekturalne policije državna su tijela koja su obuhvaćena definicijom „upravnih organa". Postupanje s osobnim informacijama od strane prefekturalne policije uređeno je prefekturalnim pravilnicima ([4]), u kojima su određena načela za zaštitu osobnih informacija, prava i obveze koji su jednakovrijedni APPIHAO-u.

## II. **Pristup vlade za potrebe kaznenog progona**

### A. Pravna osnova i ograničenja

#### 1. Prikupljanje osobnih informacija prisilnim sredstvima

*(a) Pravna osnova*

U skladu s člankom 35. Ustava, pravo svih osoba na sigurnost vlastitog doma, dokumenata i imovine od ulazaka, pretraga i zapljena ne smije biti narušeno, osim ako postoji sudski nalog izdan na temelju „primjerenog razloga", koji mora sadržavati točan opis mjesta koje je potrebno pretražiti ili stvari koje treba zaplijeniti. Shodno tome, prisilno prikupljanje elektroničkih informacija od strane javnih tijela u kontekstu kaznene istrage može se provesti samo na temelju sudskog naloga. To se odnosi i na prikupljanje elektroničkih podataka koji sadržavaju (osobne) informacije i presretanje komunikacije u stvarnom vremenu (tzv. prisluškivanje). Jedina iznimka od ovog pravila (koja, međutim, nije relevantna u kontekstu elektroničkog prijenosa osobnih informacija iz inozemstva) jest članak 220. stavak 1. Zakona o kaznenom postupku ([5]), prema kojem javni tužitelj, pomoćnik javnog tužitelja ili službenik pravosudne policije pri uhićenju osumnjičenika ili „očitog počinitelja" može, prema potrebi, provesti pretragu i zapljenu „na licu mjesta u trenutku uhićenja".

Prema članku 197. stavku 1. Zakona o kaznenom postupku prisilne istražne mjere „ne primjenjuju se osim ako su u tom zakonu utvrđene posebne odredbe". Kad je riječ o prisilnom prikupljanju elektroničkih informacija, u tom su pogledu relevantna pravna osnova članak 218. stavak 1. Zakona o kaznenom postupku (prema kojemu javni tužitelj, pomoćnik javnog tužitelja ili službenik pravosudne policije može, ako je to potrebno za istragu kaznenog djela, provesti pretragu, zapljenu ili inspekcijski pregled na temelju naloga koji je izdao sudac) i članak 222.-2. Zakona o kaznenom postupku (prema kojemu se prisilne mjere za presretanje elektroničkih komunikacija bez privole jedne od strana provode na temelju drugih zakona). U potonjoj odredbi upućuje se na Zakon o prisluškivanju za kaznene istrage (Zakon o prisluškivanju), u čijem se članku 3. stavku 1. utvrđuju uvjeti pod kojima se komunikacija povezana s određenim teškim kaznenim djelima može prisluškivati na temelju naloga o prisluškivanju koji izdaje sudac ([6]).

Kada je riječ o policiji, istražnu nadležnost u svim slučajevima ima prefekturalna policija, dok Nacionalna policijska agencija (NPA) ne provodi kaznene istrage na temelju Zakona o kaznenom postupku.

*(b) Ograničenja*

Prisilno prikupljanje elektroničkih informacija ograničeno je Ustavom i propisima o prenošenju ovlasti, kako ih tumači sudska praksa, a kojima se posebice propisuju kriteriji koje primjenjuju sudovi pri izdavanju sudskog naloga. Osim toga, APPIHAO-om je uveden niz ograničenja koja se primjenjuju i na prikupljanje informacija i postupanje s njima (a lokalni propisi uglavnom sadržavaju iste kriterije za prefekturalnu policiju).

#### 1. Ograničenja koja proizlaze iz Ustava i propisa o prenošenju ovlasti

Prema članku 197. stavku 1. Zakona o kaznenom postupku prisilne odluke ne primjenjuju se osim ako su u tom zakonu utvrđene posebne odredbe. U članku 218. stavku 1. Zakona o kaznenom postupku propisano je da se zapljena i sl. može provesti na temelju sudskog naloga koji je izdao sudac samo „ako je to nužno za istragu kaznenog djela". Iako kriteriji za

([4]) Svaka prefektura ima vlastiti „prefekturalni pravilnik" kojim se služi prefekturalna policija za zaštitu osobnih informacija. Ti prefekturalni pravilnici nisu prevedeni na engleski jezik.

([5]) Člankom 220. stavkom 1. Zakona o kaznenom postupku propisano je da javni tužitelj, pomoćnik javnog tužitelja ili službenik pravosudne policije pri uhićenju osumnjičenika može, ako je to potrebno, poduzeti sljedeće mjere: (a) ulazak u prebivalište druge osobe itd. u potrazi za osumnjičenikom; (b) pretragu, zapljenu ili inspekcijski pregled na licu mjesta u trenutku uhićenja.

([6]) Točnije, u toj se odredbi propisuje da „u slučajevima iz sljedećih točaka, ako postoji situacija koja je dostatna za sumnju da će doći do komunikacije u vezi s počinjenjem kaznenog djela, njegovim pripremama, zavjerama o daljnjim mjerama kao što je uklanjanje dokaza itd., uputama i drugim oblicima komunikacije o kaznenom djelu iz svake od navedenih točaka (dalje u tekstu druge i treće točke ‚niz kaznenih djela'), kao i komunikacije koja se tiče pitanja povezanih s navedenim kaznenim djelom (dalje u tekstu ovog stavka ‚komunikacija u vezi s kaznenim djelom') i u slučajevima u kojima je iznimno teško utvrditi počinitelja ili pojasniti situacije/detalje počinjenja kaznenog djela na bilo koji drugi način, javni tužitelj ili pravosudna policija mogu prisluškivati komunikaciju o kaznenim djelima na temelju naloga o prisluškivanju koji izdaje sudac; to vrijedi za komunikacijska sredstva koja su određena telefonskim brojem i drugim brojevima/oznakama za identifikaciju izvora ili lokacije telefona, a koja osumnjičenik koristi na temelju ugovora s telekomunikacijskim operaterima itd. (osim sredstava kod kojih ne postoje razlozi za sumnju da se upotrebljavaju za ‚komunikaciju u vezi s kaznenim djelom'); kod sredstava kod kojih postoje razlozi za sumnju da se upotrebljavaju za ‚komunikaciju u vezi s kaznenim djelom' dopušteno je prisluškivanje komunikacije koja se odnosi na kaznena djela počinjena putem tih sredstava komunikacije".

ocjenu nužnosti nisu detaljnije utvrđeni zakonskim propisima, Vrhovni sud ([7]) odredio je da sudac pri procjeni nužnosti odluka treba provesti sveukupnu procjenu, uzimajući posebice u obzir sljedeće elemente:

(a) težinu kaznenog djela i način na koji je počinjeno;

(b) vrijednost i važnost zaplijenjenih materijala kao dokaza;

(c) vjerojatnost skrivanja ili uništenja zaplijenjenih materijala;

(d) razmjere negativnih posljedica zapljene;

(e) ostale povezane uvjete.

Ograničenja proizlaze i iz zahtjeva iz članka 35. Ustava da se dokaže „primjeren razlog". U skladu s kriterijem „primjerenog razloga" sudski nalozi mogu se izdati: [1.] ako je kaznena istraga nužna (vidjeti prethodno spomenutu presudu Vrhovnog suda od 18. ožujka 1969. (1968. (Shi) br. 100)), [2.] ako se smatra da je osumnjičenik (optuženik) počinio kazneno djelo (članak 156. stavak 1. Pravila kaznenog postupka (Rules of Criminal Procedure) ([8]) [3.] Sudski nalog za istragu u vezi s tijelom, predmetima, prebivalištem ili drugom lokacijom osobe koja nije optuženik treba izdati samo ako se razumno može pretpostaviti da predmeti koje bi trebalo zaplijeniti postoje (članak 102. stavak 2. Zakona o kaznenom postupku). Sudac će odbaciti zahtjev za izdavanje sudskog naloga ako smatra da dokazna dokumentacija koju su dostavila istražna tijela nije dovoljan razlog za sumnju u počinjenje kaznenog djela. U tom smislu valja napomenuti da u skladu sa Zakonom o kažnjavanju kaznenih djela organiziranog kriminala i kontrole imovinske koristi povezane s kaznenim djelom „pripremne radnje za počinjenje" planiranog kaznenog djela (npr. priprema novca za počinjenje kaznenog djela terorizma) same po sebi predstavljaju kazneno djelo te kao takve mogu biti predmet prisilne istrage na temelju sudskog naloga.

Naposljetku, ako je sudski nalog povezan s istragom u vezi s tijelom, predmetima, prebivalištem ili drugom lokacijom osobe koja nije osumnjičenik ili optuženik, izdaje se samo ako se razumno može pretpostaviti da predmeti koje bi trebalo zaplijeniti postoje (članak 102. stavak 2. i članak 222. stavak 1. Zakona o kaznenom postupku).

Konkretno, kada je riječ o presretanju komunikacije za potrebe kaznenih istraga na temelju Zakona o prisluškivanju, ono se može provesti samo ako su ispunjeni strogi zahtjevi iz njegova članka 3. stavka 1. U skladu s tom odredbom za presretanje je uvijek potrebno unaprijed pribaviti sudski nalog, koji se može izdati samo u ograničenim situacijama ([9]).

2. Ograničenja koja proizlaze iz APPIHAO-a

Kada je riječ o prikupljanju ([10]) osobnih informacija i daljnjem postupanju s njima (uključujući pohranu, upravljanje i uporabu) koje provode upravni organi, u APPIHAO-u su posebno propisana sljedeća ograničenja:

(a) U skladu s člankom 3. stavkom 1. APPIHAO-a upravni organi mogu pohraniti osobne informacije samo ako je pohrana nužna za obavljanje poslova u njihovoj nadležnosti kako je predviđeno zakonima i drugim propisima. Nakon pohrane obvezni su navesti (u mjeri u kojoj je to moguće) svrhu uporabe osobnih informacija. U skladu s člankom 3. stavcima 2. i 3. APPIHAO-a upravni organi pohranjuju osobne informacije samo u mjeri koja je potrebna za postizanje navedene svrhe uporabe te tu svrhu ne mijenjaju više od onoga što se razumno može smatrati relevantnim za prvotnu svrhu.

(b) U članku 5. APPIHAO-a predviđa se da čelnik upravnog organa nastoji da pohranjene osobne informacije uvijek budu točne i ažurne onoliko koliko je nužno za postizanje svrhe uporabe.

(c) U članku 6. stavku 1. APPIHAO-a predviđa se da čelnik upravnog organa poduzima potrebne mjere za sprečavanje neovlaštenog odavanja, gubitka ili oštećenja te za pravilno upravljanje pohranjenim osobnim informacijama.

(d) U skladu s člankom 7. APPIHAO-a nijedan zaposlenik (uključujući bivše zaposlenike) ne smije bez opravdanog razloga drugoj osobi otkriti osobne informacije koje je saznao niti te informacije upotrebljavati u nepoštene svrhe.

([7]) Presuda od 18. ožujka 1969. (1968. (Shi) br. 100).
([8]) U članku 156. stavku 1. Pravila kaznenog postupka predviđeno je: „Pri popunjavanju zahtjeva iz stavka 1. prethodnog članka tražitelj dostavlja materijale iz kojih proizlazi da je osumnjičenik ili optuženik počinio kazneno djelo".
([9]) Vidjeti bilješku 6.
([10]) Člankom 3. stavcima 1. i 2. APPIHAO-a ograničava se opseg pohrane, a time i prikupljanja osobnih informacija.

(e) Osim toga, u članku 8. stavku 1. APPIHAO-a predviđa se da, ako nije drukčije propisano zakonima i drugim propisima, čelnik upravnog organa pohranjene osobne informacije ne upotrebljava niti ih prosljeđuje drugoj osobi u druge svrhe osim navedene svrhe uporabe. U članku 8. stavku 2. navode se iznimke od tog pravila u određenim situacijama, ali se one primjenjuju samo ako takvo iznimno otkrivanje neće „nepravedno" naštetiti pravima i interesima ispitanika ili treće strane.

(f) U skladu s člankom 9. APPIHAO-a, ako se pohranjene osobne informacije proslijede drugoj osobi, čelnik upravnog organa prema potrebi određuje ograničenja svrhe ili metode uporabe te druga potrebna ograničenja; osim toga od primatelja može zatražiti i da poduzme potrebne mjere za sprečavanje neovlaštenog odavanja te za pravilno upravljanje informacijama.

(g) Člankom 48. APPIHAO-a predviđa se da čelnik upravnog organa nastoji pravilno i brzo obraditi sve pritužbe u vezi s postupanjem s osobnim informacijama.

2. Prikupljanje osobnih informacija na temelju zahtjeva za dobrovoljnu suradnju (dobrovoljna istraga)

*(a) Pravna osnova*

Osim prisilnim sredstvima, osobne informacije dobivaju se i iz izvora kojima svatko može slobodno pristupiti ili dobrovoljnim otkrivanjem, među ostalim od strane poslovnih subjekata koji posjeduju takve informacije.

Kad je riječ o prethodno spomenutim poslovnim subjektima, člankom 197. stavkom 2. Zakona o kaznenom postupku tužiteljstvo i pravosudna policija ovlašteni su podnijeti „pisane upite u istražnim stvarima" (takozvani „istražni obrasci"). U skladu sa Zakonom o kaznenom postupku osobe kojima je dostavljen upit trebaju se javiti istražnim tijelima. Međutim, ako javne službe ili javne i/ili privatne organizacije koje prime upit odbiju postupiti u skladu s tim, ne može ih se prisiliti da se jave. Ako se ne jave kako bi sudjelovali u istrazi, nije moguće izreći kaznenu kaznu ili drugu sankciju. Ako istražna tijela smatraju da su tražene informacije neophodne, te informacije trebaju pribaviti pretragom i zapljenom na temelju sudskog naloga.

S obzirom na sve veću svijest pojedinaca o njihovim pravima na privatnost te na radno opterećenje koje proizlazi iz takvih zahtjeva, poslovni subjekti sve su oprezniji pri odgovaranju na takve zahtjeve ([11]). Pri donošenju odluke o sudjelovanju poslovni subjekti posebno uzimaju u obzir prirodu traženih informacija, njihov odnos s osobom čije bi informacije mogle biti ugrožene, rizike za njihovu reputaciju, rizik od parničnog postupka itd.

*(b) Ograničenja*

Kada je riječ o prisilnom prikupljanju elektroničkih informacija, dobrovoljna istraga ograničena je Ustavom, kako ga tumači sudska praksa, i propisom o prenošenju ovlasti. Osim toga, poslovnim subjektima u određenim situacijama zakonom nije dopušteno otkrivati informacije. Naposljetku, APPIHAO-om je predviđen niz ograničenja koja se primjenjuju i na prikupljanje informacija i postupanje s njima (a lokalni propisi uglavnom sadržavaju iste kriterije za prefekturalnu policiju).

1. Ograničenja koja proizlaze iz Ustava i propisa o prenošenju ovlasti

Uzimajući u obzir svrhu članka 13. Ustava, Vrhovni sud je u dvama odlukama od 24. prosinca 1969. (1965 (A) br. 1187) i 15. travnja 2008. (2007 (A) br. 839) uveo ograničenja za dobrovoljne istrage koje provode istražna tijela. Iako se te dvije odluke odnose na predmete u kojima su osobne informacije (u obliku slika) prikupljene fotografiranjem/snimanjem, zaključci su relevantni za dobrovoljne (neprisilne) istrage kojima se zadire u privatnost pojedinaca općenito. One se prema tome primjenjuju i moraju poštovati kada je riječ o prikupljanju osobnih informacija u okviru dobrovoljne istrage, uzimajući u obzir posebne okolnosti svakog predmeta.

U skladu s tim odlukama zakonitost dobrovoljne istrage ovisi o ispunjenju sljedeća tri kriterija:

— „sumnja o počinjenju kaznenog djela" (tj. treba procijeniti je li počinjeno kazneno djelo);

— „nužnost istrage" (tj. treba procijeniti je li zahtjev ograničen na ono što je nužno za potrebe istrage); i

([11]) Vidjeti i obavijest Nacionalne policijske agencije od 7. prosinca 1999. (u nastavku na str. 9) u kojoj se navodi isto.

— „prikladnost metoda” (tj. treba procijeniti je li dobrovoljna istraga „primjerena” ili razumna za postizanje svrhe istrage) ([12]).

Općenito, uzimajući u obzir tri prethodno spomenuta kriterija, zakonitost dobrovoljne istrage ocjenjuje se na temelju toga može li se ona smatrati razumnom u skladu s društveno prihvatljivim konvencijama.

Zahtjev „nužnosti istrage” također izravno proizlazi iz članka 197. Zakona o kaznenom postupku te je potvrđena u uputama koje je Nacionalna policijska agencija (NPA) izdala prefekturalnoj policiji u pogledu uporabe „istražnih obrazaca”. U obavijesti NPA-a od 7. prosinca 1999. utvrđuje se niz postupovnih ograničenja, uključujući zahtjev u pogledu uporabe „istražnih obrazaca” samo kada je to nužno za potrebe istrage. Osim toga, članak 197. stavak 1. Zakona o kaznenom postupku ograničen je na kaznene istrage te se stoga može primjenjivati samo ako postoji konkretna sumnja da je kazneno djelo već počinjeno. Isto tako, ta pravna osnova ne može se primijeniti za prikupljanje i uporabu osobnih informacija ako zakon još nije prekršen.

2. Ograničenja u pogledu određenih poslovnih subjekata

U određenim područjima primjenjuju se dodatna ograničenja na temelju zaštita predviđenih drugim zakonima.

Prvo, i istražna tijela i telekomunikacijski operateri kod kojih se nalaze osobne informacije imaju obvezu poštovanja tajnosti komunikacija kako je zajamčeno člankom 21. stavkom 2. Ustava ([13]). Osim toga, telekomunikacijski operateri imaju istu obvezu i na temelju članka 4. Zakona o telekomunikacijama ([14]). U skladu sa „Smjernicama o zaštiti osobnih informacija u telekomunikacijama”, koje je izdalo Ministarstvo unutarnjih poslova i komunikacija (Ministry of Internal Affairs and Communications, MIC) na temelju Ustava i Zakona o telekomunikacijama, u slučajevima kada bi mogla doći u pitanje tajnost telekomunikacija telekomunikacijski operateri s obzirom na tajnost komunikacije ne smiju otkriti osobne informacije trećim stranama, osim ako su pribavili privolu pojedinca ili ako se mogu pozvati na neki od „opravdanih razloga” zbog nepoštovanja Kaznenog zakonika. Ti se razlozi odnose na „opravdane radnje” (članak 35. Kaznenog zakonika), „samoobranu” (članak 36. Kaznenog zakonika) i „odvraćanje neposredne opasnosti (članak 37. Kaznenog zakonika). „Opravdane radnje” u skladu s Kaznenim zakonikom samo su one radnje telekomunikacijskog operatera pri kojima postupa u skladu s prisilnim državnim mjerama, što ne uključuje dobrovoljnu istragu. Stoga ako istražna tijela zatraže osobne informacije na temelju „istražnog obrasca” (članak 197. stavak 2.) Zakona o kaznenom postupku, telekomunikacijski operater ne smije otkriti podatke.

Drugo, poslovni subjekti obvezni su odbiti zahtjeve za dobrovoljnu suradnju ako im je otkrivanje osobnih informacija zakonom zabranjeno. Primjer su slučajevi kada operater ima dužnost poštovati povjerljivost informacija, na primjer na temelju članka 134. Kaznenog zakonika ([15]).

3. Ograničenja na temelju APPIHAO-a

Kada je riječ o prikupljanju osobnih informacija i daljnjem postupanju s njima koje provode upravni organi, u APPIHAO-u su predviđena ograničena kako je prethodno objašnjeno u odjeljku II.A.1. (b) 2. Istovjetna ograničenja proizlaze iz prefekturalnih pravilnika koji se primjenjuju na prefekturalnu policiju.

B. Nadzor

1. Sudski nadzor

Prikupljanje osobnih informacija prisilnim sredstvima mora se temeljiti na sudskom nalogu ([16]) i prema tome podliježe prethodnom ispitivanju od strane sudca. Ako je istraga bila nezakonita, sudac takve dokaze može isključiti u naknadnom kaznenom postupku. Pojedinac može tijekom kaznenog postupka pokrenutog protiv njega tvrditi da je istraga bila nezakonita i zahtijevati isključenje tih dokaza.

([12]) Težina kaznenog djela i hitnost relevantni su čimbenici za procjenu „prikladnosti metoda”.

([13]) U članku 21. stavku 2. Ustava navedeno je sljedeće: „Zabranjena je svaka cenzura i svako kršenje tajnosti svih komunikacijskih sredstava”.

([14]) U članku 4. Zakona o telekomunikacijama navedeno je sljedeće: 1. „Tajnost komunikacija kojima upravlja telekomunikacijski operater ne smije se prekršiti. 2. Osoba koja se bavi telekomunikacijskom djelatnošću ne smije otkrivati tajne koje je saznala tijekom obavljanja svoje dužnosti iz komunikacija kojima upravlja telekomunikacijski operater. Isto vrijedi i u slučaju nakon prestanka službe”.

([15]) U članku 134. Kaznenog zakonika navedeno je sljedeće: „1. Ako liječnik, ljekarnik, distributer farmaceutskih proizvoda, primalja, odvjetnik, branitelj, javni bilježnik ili bilo koja osoba koja je ranije obavljala neko od tih zanimanja drugoj osobi bez opravdanog razloga otkrije povjerljive informacije koje je saznala tijekom obavljanja tog zanimanja, kažnjava se kaznom zatvora uz rad u trajanju do najviše šest mjeseci ili novčanom kaznom u iznosu od najviše 100 000 jena. 2. Isto vrijedi u slučaju ako osoba koja se bavi ili se ranije bavila vjerskim zanimanjem bez opravdanog razloga otkrije osobne informacije druge osobe koje je saznala tijekom obavljanja vjerskih aktivnosti”.

([16]) Za iznimku od tog pravila vidjeti bilješku 5.

2. Nadzor na temelju APPIHAO-a

U Japanu ministar ili čelnik pojedinog ministarstva ili agencije ima ovlasti za nadzor i provedbu na temelju APPIHAO-a, a ministar unutarnjih poslova i komunikacija može provoditi istrage o provedbi APPIHAO-a u svim ostalim ministarstvima.

Ako ministar unutarnjih poslova i komunikacija smatra da je to potrebno za postizanje svrhe APPIHAO-a – primjerice na temelju istrage o stanju provedbe APPIHAO-a ([17]), obrade pritužbi ili upita upućenih jednom od sveobuhvatnih informacijskih centara – on od čelnika upravnog organa može zahtijevati da dostavi materijale i objašnjenja o postupanju s osobnim informacijama u tom upravnom organu na temelju članka 50. APPIHAO-a. Ministar može čelniku upravnog organa uputiti mišljenja u vezi s obradom osobnih informacija u upravnom organu ako smatra da je to potrebno za postizanje svrhe tog zakona. Osim toga, ministar može, na primjer, zatražiti i reviziju mjera u okviru postupaka koje može poduzeti u skladu s člancima 50. i 51. tog zakona ako se sumnja da je došlo do njegova kršenja ili neodgovarajuće primjene. Na taj način se omogućuje jedinstvena primjena i usklađenost s APPIHAO-om.

3. Nadzor povjerenstava za javnu sigurnost u pogledu policije

Kada je riječ o policijskoj upravi, NPA podliježe nadzoru Nacionalnog povjerenstva za javnu sigurnost, dok prefekturalna policija podliježe nadzoru Prefekturalnih povjerenstava za javnu sigurnost koje je uspostavljeno u svakoj prefekturi. Svako od tih nadzornih tijela osigurava demokratsko upravljanje i političku neutralnost policijske uprave.

Nacionalno povjerenstvo za javnu sigurnost zaduženo je za pitanja iz svoje nadležnosti određena Zakonom o policiji i drugim zakonima. To uključuje imenovanje glavnog povjerenika NPA-a i lokalnih viših policijskih službenika te utvrđivanje sveobuhvatnih politika u kojima se navode osnovne smjernice ili mjere za upravljanje NPA-om.

Prefekturalna povjerenstva za javnu sigurnost sastoje se od članova koji zastupaju narod pojedine prefekture na temelju Zakona o policiji i upravljaju prefekturalnom policijom kao sustav neovisnog vijeća. Članove imenuje guverner prefekture uz suglasnost prefekturalne skupštine na temelju članka 39. Zakona o policiji. Njihov mandat traje tri godine, a mogu biti smijenjeni protiv svoje volje samo zbog određenih razloga navedenih u zakonu (poput nesposobnosti za obavljanje dužnosti, povrede dužnosti, neprofesionalnog ponašanja i sl.), čime je zajamčena njihova neovisnost (vidjeti članke 40. i 41. Zakona o policiji). Nadalje, kako bi se zajamčila njihova politička neutralnost, člankom 42. Zakona o policiji članu povjerenstva zabranjeno je da istodobno bude član zakonodavnog tijela, postane izvršni član političke stranke ili drugog političkog tijela ili da aktivno sudjeluje u političkim pokretima. Iako su povjerenstva u nadležnosti guvernera prefekture, to ne znači da je on ovlašten izdavati im upute u pogledu obavljanja njihovih funkcija.

U skladu s člankom 38. stavkom 3. u vezi s člankom 2. i člankom 36. stavkom 2. Zakona o policiji, Prefekturalna povjerenstva za javnu sigurnost odgovorna su za „zaštitu prava i slobode pojedinca”. Ona u tu svrhu primaju izvješća šefova prefekturalne policije o aktivnostima u području njihove nadležnosti, među ostalim na redovitim sastancima koji se održavaju tri ili četiri puta mjesečno. Povjerenstvo pruža smjernice o tim pitanjima utvrđivanjem sveobuhvatnih politika.

Nadalje, Prefekturalna povjerenstva za javnu sigurnost mogu u konkretnim pojedinačnim slučajevima izdati upute prefekturalnoj policiji kada smatraju da je to potrebno u okviru inspekcijskog pregleda aktivnosti prefekturalne policije ili neprofesionalnog ponašanja osoblja. Osim toga, povjerenstva mogu, ako to smatraju potrebnim, zatražiti da imenovani član povjerenstva preispita stanje provedbe izdane upute (članak 43-2 Zakona o policiji).

([17]) Da bi se osigurala transparentnost i olakšao nadzor MIC-a, čelnik upravnog organa je dužan, u skladu s člankom 11. APPIHAO-a, evidentirati svaku stavku propisanu u članku 10. stavku 1. APPIHAO-a, kao što je naziv upravnog organa koji pohranjuje datoteku, svrha uporabe datoteke, metoda prikupljanja osobnih informacija itd. (tzv. „Registar datoteka s osobnim informacijama”). Međutim, datoteke s osobnim informacijama koje su obuhvaćene člankom 10. stavkom 2. APPIHAO-a, primjerice one koje su pripremljene ili pribavljene u okviru kaznene istrage ili koje se odnose na pitanja važna za nacionalnu sigurnost, izuzete su od obveze prijave MIC-u i uključivanja u javni registar. Međutim, na temelju članka 7. Zakona o upravljanju javnim evidencijama i arhivima („Public Records and Archives Management Act”) čelnik upravnog organa uvijek je obvezan evidentirati klasifikaciju, naslov, razdoblje pohrane i mjesto pohrane itd. administrativnih dokumenata („Registar za upravljanje datotekama upravnih dokumenata”, eng. *Administrative Document File Management Register*). Kazalo za oba registra objavljuje se na internetu i omogućuje pojedincima da provjere koju vrstu osobnih informacija sadržava datoteka i koji upravni organ pohranjuje informacije.

4. Nadzor parlamenta (Diet)

Parlament može provoditi istrage povezane s aktivnostima javnih tijela i u tu svrhu zahtijevati uvid u dokumente i iskaz svjedoka (članak 62. Ustava). U tom kontekstu nadležni odbor parlamenta može ispitati primjerenost aktivnosti prikupljanja informacija koje provodi policija.

Te su ovlasti detaljnije utvrđene u Zakonu o parlamentu. U skladu s člankom 104. parlament može od Kabineta i javnih agencija zatražiti da daju na uvid izvješća i zapise koji su nužni za provođenje istrage. Osim toga, zastupnici u parlamentu mogu podnijeti „pisane upite" u skladu s člankom 74. Zakona o parlamentu. Te upite mora odobriti predsjednik parlamenta i, u načelu, Kabinet mora na njih odgovoriti u pisanom obliku u roku od sedam dana (ako nije moguće odgovoriti u tom roku, to se mora opravdati te se mora odrediti novi rok, članak 75. Zakona o parlamentu). U prošlosti su pisani upiti parlamenta obuhvaćali i postupanje uprave s osobnim informacijama ([18]).

C. Pravna zaštita pojedinaca

U skladu s člankom 32. Ustava Japana svaka osoba ima pravo na pristup sudovima. Osim toga, člankom 17. Ustava svakoj se osobi jamči pravo da tuži državu ili javno tijelo za odštetu (kako je predviđeno zakonom) u slučaju da je osoba pretrpjela štetu zbog protuzakonitog postupanja javnog službenika.

1. Sudska zaštita od prisilnog prikupljanja informacija na temelju sudskog naloga (članak 430. Zakona o kaznenom postupku)

U skladu s člankom 430. stavkom 2. Zakona o kaznenom postupku, pojedinac koji nije zadovoljan mjerama koje je poduzeo policijski službenik u vezi sa zapljenom predmeta (među ostalim, ako predmeti sadržavaju osobne informacije) na temelju sudskog naloga, može podnijeti zahtjev (tzv. „kvazi-pritužba") nadležnom sudu kako bi te mjere bile „opozvane ili izmijenjene".

Takav se postupak može pokrenuti a da pojedinac ne mora čekati presudu u predmetu. Ako sud ustanovi da zapljena nije bila potrebna ili da postoje drugi razlozi na temelju kojih se zapljena može smatrati nezakonitom, može naložiti da se te mjere opozovu ili izmijene.

2. Sudska zaštita na temelju Zakona o parničnom postupku i Zakona o naknadi štete od države

Ako smatraju da je prekršeno njihovo pravo na privatnost u skladu s člankom 13. Ustava, pojedinci mogu pokrenuti parnični postupak kojim se zahtijeva brisanje osobnih informacija prikupljenih u okviru kaznene istrage.

Također, pojedinac može pokrenuti postupak za naknadu štete na temelju Zakona o naknadi štete od države i u vezi s relevantnim člancima Građanskog zakonika ako smatra da je njegovo pravo na privatnost povrijeđeno te je pretrpio štetu kao posljedicu prikupljanja njegovih osobnih podataka ili nadzora ([19]). Budući da „šteta" koja podliježe zahtjevu za naknadu nije ograničena na materijalnu štetu (članak 710. Građanskog zakonika), ona može obuhvaćati i „duševnu bol". Visinu naknade za takvu moralnu štetu sudac procjenjuje na temelju „slobodne ocjene s obzirom na različite čimbenike u svakom pojedinom slučaju" ([20]).

Člankom 1. stavkom 1. Zakona o naknadi štete od države propisuje se pravo na odštetu ako je i. javni službenik koji izvršava javne ovlasti države ili javnog tijela ii. u obnašanju svojih dužnosti iii. s namjerom ili iz nemara iv. nezakonito v. nanio štetu drugoj osobi.

Pojedinac mora podnijeti tužbu u skladu sa Zakonom o parničnom postupku. U skladu s primjenjivim pravilima on to može učiniti na sudu koji je nadležan za mjesto počinjenja kaznenog djela.

([18]) Vidjeti npr. pisani upit gornjeg doma parlamenta br. 92 od 27. ožujka 2009. o postupanju s informacijama prikupljenima u kontekstu kaznenih istraga, uključujući kršenje obveza povjerljivosti od strane policije i tijela kaznenog progona.

([19]) Primjer takvog postupka jest „Slučaj popisa Agencije za obranu" (Okružni sud u Niigati, odluka od 11. svibnja 2006. (2002(Wa) br. 514)). U tom slučaju službenik Agencije za obranu pripremio je, sačuvao i distribuirao popis osoba koje su toj agenciji podnijele zahtjeve za otkrivanje upravnih dokumenata. Na tom popisu bili su navedene osobne informacije tužitelja. Smatrajući da su prekršena njegova prava na privatnost, na znanje itd., tužitelj je od tuženika zatražio da plati naknadu štete u skladu s člankom 1. stavkom 1. Zakona o naknadi štete od države. Sud je djelomično prihvatio taj zahtjev sud i tužitelju odobrio djelomičnu naknadu.

([20]) Vrhovni sud, odluka od 5. travnja 1910. (1910(O) br. 71).

3. Pravna zaštita pojedinaca od nezakonitih/neprimjerenih istraga koje provodi policija: pritužba Prefekturalnom povjerenstvu za javnu sigurnost (članak 79. Zakona o policiji)

U skladu s člankom 79. Zakona o policiji ([21]), kako je dodatno pojašnjeno u uputi čelnika NPA-a prefekturalnoj policiji i Prefekturalnim povjerenstvima za javnu sigurnost ([22]), pojedinci mogu podnijeti pisanu pritužbu ([23]) nadležnom Prefekturalnom povjerenstvu za javnu sigurnost zbog bilo kakvog nezakonitog ili neprimjerenog ponašanja policijskog službenika pri izvršavanju njegovih dužnosti; to uključuje dužnosti u pogledu prikupljanja i uporabe osobnih informacija. Povjerenstvo savjesno rješava takve pritužbe u skladu sa zakonima i lokalnim propisima te podnositelja pritužbe pisanim putem obavješćuje o rezultatu istrage.

Na temelju svojih nadzornih ovlasti u skladu s člankom 38. stavkom 3. Zakona o policiji, Prefekturalno povjerenstvo za javnu sigurnost prefekturalnoj policiji izdaje uputu da istraži činjenice, provede nužne mjere u skladu s rezultatima ispitivanja i dostavi rezultate povjerenstvu. Ako to smatra potrebnim, Povjerenstvo može izdati i uputu o postupanju s pritužbom, na primjer ako smatra da je istraga koju provodi policija nedostatna. Ta je provedba opisana u Obavijesti koju je NPA izdala za načelnike prefekturalne policije.

U obavijesti podnositelju pritužbe o rezultatu istrage uzimaju se u obzir i izvješća policije o istrazi i mjerama poduzetima na zahtjev povjerenstva.

4. Pravna zaštita pojedinaca u okviru APPIHAO-a i Zakona o kaznenom postupku

*(a) APPIHAO*

U skladu s člankom 48. APPIHAO-a upravni organi moraju nastojati pravilno i brzo obrađivati sve pritužbe koje se odnose na postupanje s osobnim informacijama. Kako bi mogao pojedincima pružiti konsolidirane informacije (npr. o dostupnim pravima na otkrivanje, ispravak i suspenziju uporabe u okviru APPIHAO-a) i kontaktnu točku za upite, MIC je uspostavio sveobuhvatne informacijske centre za otkrivanje informacija/zaštitu osobnih informacija u svakoj prefekturi na temelju članka 47. stavka 2. APPIHAO-a. Nerezidenti također mogu slati upite. Na primjer, u financijskoj godini 2017. (od travnja 2017. do ožujka 2018.) sveobuhvatni informacijski centri odgovorili su ukupno na 5186 upita.

Člancima 12. i 27. APPIHAO-a pojedincima se daje pravo na podnošenje zahtjeva za otkrivanje i ispravak pohranjenih osobnih informacija. Nadalje, u skladu s člankom 36. APPIHAO-a, pojedinci mogu zatražiti suspenziju uporabe ili brisanje svojih pohranjenih osobnih informacija ako ih je upravni organ nezakonito pribavio ili njihovom pohranom ili uporabom krši zakon.

Međutim, kada je riječ o osobnim informacijama koje se prikupljaju (bilo na temelju sudskog naloga bilo „istražnog obrasca") i pohranjuju u svrhu kaznenih istraga ([24]), takve informacije u pravilu pripadaju kategoriji „osobnih informacija zabilježenih u dokumentima koji se odnose na suđenja i zaplijenjene predmete". Takve su osobne informacije stoga isključene iz područja primjene prava pojedinaca iz poglavlja IV. APPIHAO-a u skladu s člankom 53-2. Zakona o kaznenom postupku ([25]). Obrada takvih osobnih informacija i prava pojedinca na pristup i ispravak podliježu umjesto

([21]) Članak 79. Zakona o policiji (izvadak):
1. Osoba koja ima pritužbu na izvršavanje dužnosti osoblja prefekturalne policije može podnijeti pritužbu u pisanom obliku Prefekturalnom povjerenstvu za javnu sigurnost u okviru postupka propisanog u Pravilniku Nacionalnog povjerenstva za javnu sigurnost.
2. Prefekturalno povjerenstvo za javnu sigurnost koje je zaprimilo pritužbu iz prethodnog stavka savjesno je rješava u skladu sa zakonima i lokalnim propisima te podnositelja pritužbe pisanim putem obavješćuje o njezinu rezultatu, osim u sljedećim slučajevima:
   1. ako se smatra da je pritužba podnesena kako bi se ometalo zakonito izvršavanje dužnosti prefekturalne policije;
   2. ako je trenutačno prebivalište podnositelja pritužbe nepoznato;
   3. ako se smatra da je pritužba pokrenuta zajedno s drugim podnositeljima pritužbe i drugi podnositelji pritužbe već su obaviješteni o rezultatu zajedničke pritužbe.

([22]) NPA, Obavijest o ispravnom postupanju s pritužbama koje se odnose na izvršavanje dužnosti policijskih službenika, 13. travnja 2001., s Dodatkom 1. „Standardi za tumačenje/provedbu članka 79. Zakona o policiji".

([23]) U skladu s obavijesti NPA-a (vidjeti prethodnu bilješku) pojedincima koji imaju poteškoća pri sastavljanju pritužbe u pisanom obliku pruža se pomoć. To izričito obuhvaća strance.

([24]) S druge strane, postoje dokumenti koji nisu klasificirani kao „dokumenti koji se odnose na suđenja" jer sami ne čine informacije prikupljene na temelju sudskog naloga ili pisanih upita o istražnim stvarima, nego su izrađeni na temelju takvih dokumenata. To bi bio slučaj kada privatne informacije ne podliježu članku 45. stavku 1. APPIHAO-a i stoga takve informacije ne bi bile isključene iz primjene poglavlja IV. APPIHAO-a.

([25]) Člankom 53-2. stavkom 2. Zakona o kaznenom postupku propisano je da se odredbe poglavlja IV. APPIHAO ne primjenjuju na osobne informacije zabilježene u dokumentima koji se odnose na suđenja i zaplijenjene predmete.

toga posebnim pravilima na temelju Zakona o kaznenom postupku i Zakona o konačnoj kaznenoj evidenciji (vidjeti u nastavku) ([26]). To isključenje opravdano je raznim čimbenicima, kao što su zaštita privatnosti dotičnih osoba, tajnost istraga i pravilna provedba kaznenog postupka. No i dalje se primjenjuju odredbe iz poglavlja 2. APPIHAO-a, kojima se uređuju načela postupanja s takvim informacijama.

*(b) Zakon o kaznenom postupku*

Prema Zakonu o kaznenom postupku mogućnosti pristupa osobnim informacijama prikupljenima za potrebe kaznene istrage ovise o fazi postupka i ulozi pojedinca u istrazi (osumnjičenik, optuženik, žrtva itd.).

Kao iznimka od pravila iz članka 47. Zakona o kaznenom postupku prema kojem se dokumenti koji se odnose na suđenja ne objavljuju prije početka suđenja (jer bi se time mogla narušiti čast i/ili privatnost dotičnih pojedinaca i ometati istraga/suđenje), u načelu se dopušta uvid žrtve kaznenog djela u takve informacije u mjeri u kojoj se to smatra razumnim uzimajući u obzir svrhu odredbe iz članka 47. Zakona o kaznenom postupku ([27]).

Osumnjičenici će pak u načelu saznati da su pod kaznenom istragom prilikom ispitivanja koje provodi pravosudna policija ili javni tužitelj. Ako javni tužitelj nakon toga odluči da neće pokrenuti kazneni postupak, o tome odmah obavješćuje osumnjičenika na njegov zahtjev (članak 259. Zakona o kaznenom postupku).

Osim toga, nakon pokretanja kaznenog postupka, javni tužitelj daje optuženiku ili njegovu odvjetniku priliku da unaprijed pregleda dokaze prije nego što zatraži njihovo ispitivanje od strane suda (članak 299. Zakona o kaznenom postupku). Time se optuženiku omogućuje da provjeri svoje osobne informacije prikupljene tijekom kaznene istrage.

Konačno, zaštita osobnih informacija prikupljenih u kontekstu kaznene istrage, bilo da je riječ o osumnjičeniku, optuženiku ili bilo kojoj drugoj osobi (npr. žrtva kaznenog djela), zajamčena je obvezom povjerljivosti (članak 100. Zakona o državnoj službi) i prijetnjom kazne u slučaju neovlaštenog davanja povjerljivih informacija u okviru obavljanja javnih dužnosti (članak 109. točka xii. Zakona o državnoj službi).

5. Pravna zaštita pojedinaca od nezakonitih/neprimjerenih istraga koje provode javna tijela: pritužba PPC-u

U skladu s člankom 6. APPI-ja Vlada poduzima potrebne mjere u suradnji s vladama trećih zemalja kako bi se na međunarodnoj razini izradio sustav za osobne informacije kroz poticanje suradnje s međunarodnim organizacijama i drugim međunarodnim okvirima. Na temelju te odredbe, Osnovnom politikom zaštite osobnih informacija (donesena odlukom Kabineta) PPC-u, kao tijelu nadležnom za sveobuhvatno upravljanje APPI-jem, delegira se ovlast za poduzimanje potrebnih mjera za premošćivanje razlika između sustava i operacija Japana i predmetne strane zemlje kako bi se osiguralo primjereno postupanje s osobnim informacijama primljenima od te zemlje.

Nadalje, kako je predviđeno člankom 61. točkama i. i ii. APPI-ja, PPC-u je povjerena zadaća oblikovanja i promicanja osnovne politike te posredovanja u pritužbama protiv poslovnih subjekata. Konačno, upravni organi blisko komuniciraju i surađuju (članak 80. APPI-ja).

Na temelju tih odredbi PPC će rješavati pritužbe pojedinaca na sljedeći način:

(a) Pojedinac koji sumnja da su pri prikupljanju ili uporabi njegovih podataka prenesenih iz EU-a javna tijela u Japanu, uključujući tijela nadležna za aktivnosti iz poglavlja II. i III. ove Izjave, prekršila primjenjiva pravila, uključujući ona navedena u ovoj Izjavi, može podnijeti pritužbu PPC-u (samostalno ili preko svojeg tijela za zaštitu podataka).

(b) PPC obrađuje pritužbu, među ostalim koristeći se svojim ovlastima na temelju članka 6., članka 61. točke ii. i članka 80. APPI-ja, te o pritužbi obavješćuje nadležna javna tijela, uključujući relevantna nadzorna tijela.

([26]) Na temelju Zakona o kaznenom postupku i Zakona o konačnoj kaznenoj evidenciji pristup zaplijenjenim predmetima i dokumentima/osobnim informacijama koje se odnose na kaznene postupke i njihov ispravak podliježu jedinstvenom i specifičnom sustavu pravila čiji je cilj zaštititi privatnost dotičnih osoba, tajnost istraga i propisno provođenje kaznenog postupka itd.

([27]) Točnije, žrtvama kaznenih djela u načelu se dopušta uvid u informacije povezane s objektivnim dokazima koje se odnose na evidenciju u slučajevima koji ne podliježu kaznenom postupku, a u kojima žrtve mogu sudjelovati, kako je predviđeno člankom 316. stavkom 33. Zakona o kaznenom postupku, kako bi se poboljšala zaštita žrtava kaznenih djela.

Ta su tijela dužna surađivati s PPC-om u skladu s člankom 80. APPI-ja, među ostalim pružanjem potrebnih informacija i relevantnih materijala kako bi PPC mogao ocijeniti je li prikupljanje ili naknadna upotreba osobnih informacija izvršena u skladu s primjenjivim pravilima. Pri provođenju evaluacije PPC će surađivati s MIC-om.

(c) Ako se evaluacijom utvrdi da je došlo do povrede primjenjivih pravila, suradnja predmetnih javnih tijela s PPC-om uključuje obvezu ispravljanja povrede.

To u slučaju nezakonitog prikupljanja osobnih informacija prema primjenjivim pravilima obuhvaća brisanje prikupljenih osobnih informacija.

U slučaju kršenja primjenjivih pravila PPC će prije završetka evaluacije također potvrditi da je povreda u potpunosti ispravljena.

(d) Nakon završetka evaluacije PPC u razumnom roku obavješćuje pojedinca o ishodu evaluacije, među ostalim o korektivnim mjerama ako su poduzete. U okviru te obavijesti PPC pojedinca obavješćuje i o mogućnosti traženja potvrde ishoda od nadležnog javnog tijela i o tijelu kojem se podnosi takav zahtjev za potvrdu.

Detaljne informacije o ishodu evaluacije mogu se ograničiti ako postoje opravdani razlozi za pretpostavku da bi priopćavanje takvih informacija moglo predstavljati rizik za istragu u tijeku.

Ako se pritužba odnosi na prikupljanje ili uporabu osobnih podataka u području kaznenog progona i ako se evaluacijom utvrdi da je predmet koji uključuje osobne informacije pojedinca bio otvoren te da je u međuvremenu zaključen, PPC će pojedinca obavijestiti da se evidencija predmeta može pregledati na temelju članka 53. Zakona o kaznenom postupku i članka 4. Zakona o konačnoj kaznenoj evidenciji.

Ako se u evaluaciji utvrdi da je pojedinac osumnjičen u kaznenom predmetu, PPC će pojedinca obavijestiti o toj činjenici i o mogućnosti podnošenja zahtjeva u skladu s člankom 259. Zakona o kaznenom postupku.

(e) Ako je pojedinac i dalje nezadovoljan ishodom tog postupka, može se obratiti PPC-u, koji će obavijestiti pojedinca o raznim mogućnostima i detaljnim postupcima za dobivanje pravne zaštite u skladu s japanskim zakonima i propisima. PPC će pojedincu pružiti potporu, uključujući savjetovanje i pomoć u poduzimanju daljnjih koraka pri relevantnom upravnom ili sudskom tijelu.

III. **Pristup vlade za potrebe nacionalne sigurnosti**

A. Pravne osnove i ograničenja za prikupljanje osobnih informacija

1. Pravne osnove za prikupljanje informacija od strane predmetnog ministarstva/agencije

Kako je prethodno navedeno, prikupljanje osobnih informacija u svrhu nacionalne sigurnosti koje provode upravni organi mora biti u okviru njihove upravne nadležnosti.

U Japanu ne postoji zakon kojim se omogućuje prikupljanje informacija prisilnim sredstvima isključivo u svrhu nacionalne sigurnosti. Na temelju članka 35. Ustava, prisilno prikupljanje osobnih informacija moguće je samo na temelju naloga koji je izdao sud za istragu kaznenog djela. Takav sudski nalog stoga se može izdati samo za potrebe kaznene istrage. To znači da u japanskom pravnom sustavu nije dopušteno prikupljanje/pristup informacijama prisilnim sredstvima iz razloga nacionalne sigurnosti. Umjesto toga, u području nacionalne sigurnosti, predmetna ministarstva ili agencije mogu dobiti informacije samo iz izvora kojima se može slobodno pristupiti ili im poslovni subjekti ili pojedinci mogu otkriti informacije na dobrovoljnoj osnovi. Poslovni subjekti koji zaprime zahtjev za dobrovoljnu suradnju nemaju zakonsku obvezu pružiti te informacije i stoga ne snose negativne posljedice ako suradnju odbiju.

Niz različitih odjela i agencija ministarstava imaju odgovornosti u području nacionalne sigurnosti.

1. Tajništvo Kabineta

Tajništvo Kabineta provodi prikupljanje informacija i istraživanje o važnim politikama Kabineta ([28]) kako je propisano člankom 12–2. Zakona o Kabinetu ([29]). Međutim, Tajništvo Kabineta nema ovlasti za prikupljanje osobnih informacija izravno od poslovnih subjekata. Ono prikuplja, ujedinjava, analizira i procjenjuje informacije iz javno dostupnih materijala, od drugih javnih tijela itd.

2. NPA/prefekturalna policija

U svakoj prefekturi, prefekturalna policija ovlaštena je prikupljati informacije u okviru svoje nadležnosti na temelju članka 2. Zakona o policiji. Može se dogoditi da NPA izravno prikuplja informacije u okviru svoje nadležnosti na temelju Zakona o policiji. To se posebno odnosi na aktivnosti NPA-ovih Ureda za sigurnost i Odjela za vanjske poslove i prikupljanje informacija. U skladu s člankom 24. Zakona o policiji, Ured za sigurnost zadužen je za pitanja koja se odnose na sigurnosnu policiju ([30]), a Odjel za vanjske poslove i prikupljanje informacija zadužen je za poslove koji se odnose na strane državljane i na japanske državljane koji obavljaju djelatnosti u stranim zemljama.

3. Obavještajna agencija za javnu sigurnost (Public Security Intelligence Agency, PSIA)

Primjena Zakona o sprečavanju subverzivnog djelovanja (Subversive Activities Prevention Act, SAPA) i Zakona o nadzoru nad organizacijama koje su počinile nasumična masovna ubojstva (Act on the Control of Organisations Which Have Committed Acts of Indiscriminate Mass Murder, ACO) uglavnom je u nadležnosti Obavještajne agencije za javnu sigurnost (PSIA). Ona je agencija Ministarstva pravosuđa.

SAPA-om i ACU-om propisuje se da se upravne odluke (tj. mjere kojima se nalaže ograničavanje aktivnosti takvih organizacija, njihovo ukidanje itd.) mogu pod strogim uvjetima donijeti protiv organizacija koje počine određena teška kaznena djela („teroristička subverzivna aktivnost” ili „djelo nasumičnog masovnog ubojstva”) kojima se narušava „javna sigurnost” ili „temeljni sustav društva” u skladu s Ustavom. „Terorističke subverzivne aktivnosti” spadaju u nadležnost SAPA-e (vidjeti članak 4. kojim su obuhvaćene aktivnosti kao što su pobuna, poticanje stranih država na agresiju protiv Japana, ubojstvo s političkim ciljem itd.), dok se ACO bavi „djelima nasumičnog masovnog ubojstva” (vidjeti članak 4. ACO-a). Samo točno utvrđene organizacije koje predstavljaju konkretne unutarnje ili vanjske prijetnje za javnu sigurnost mogu biti podložne odlukama u okviru SAPA-e ili ACO-a.

U tu svrhu SAPA i ACO osiguravaju pravnu osnovu za istrage. Temeljne istražne ovlasti službenika PSIA-e (PSIO) utvrđene su u članku 27. SAPA-e i članku 29. ACO-a. Istrage PSIA-e u skladu s tim odredbama provode se u mjeri u kojoj je to potrebno s obzirom na prethodno navedene odluke o kontroli određenih organizacija (npr. radikalne skupine ljevice, sekta *Aum Shinrikyo* i određena domaća skupina usko povezana sa Sjevernom Korejom bile su predmet istrage u prošlosti). Međutim, te se istrage ne mogu oslanjati na prisilna sredstva te se stoga organizaciju koja posjeduje osobne informacije ne smije prisiljavati da pruži te informacije.

Prikupljanje i uporaba informacija koje se dostavljaju PSIA-i na dobrovoljnoj osnovi podliježe odgovarajućim zaštitnim mjerama i ograničenjima predviđenima zakonom kao što su, između ostalog, tajnost komunikacije zajamčena Ustavom i pravila o postupanju s osobnim informacijama u okviru APPIHAO-a.

4. Ministarstvo obrane (Ministry of Defence, MOD)

Kad je riječ o prikupljanju informacija koje provodi Ministarstvo obrane (MOD), MOD prikuplja informacije na temelju članaka 3. i 4. Zakona o osnivanju MOD-a u mjeri potrebnoj za izvršavanje svojih upravnih nadležnosti, uključujući u pogledu obrane i zaštite, mjera koje moraju poduzeti obrambene snage te raspoređivanja kopnenih, pomorskih i obrambenih zračnih snaga. MOD može prikupljati informacije samo u te svrhe putem dobrovoljne suradnje i iz besplatno dostupnih izvora. Ne prikuplja informacije o široj javnosti.

2. Ograničenja i zaštitne mjere

*(a) Zastara*

1. Opća ograničenja na temelju APPIHAO-a

APPIHAO je opći zakon koji se primjenjuje na prikupljanje i obradu osobnih informacija od strane upravnih organa u bilo kojem području njihova djelovanja. Stoga se ograničenja i zaštitne mjere opisane u odjeljku II.A.1. točki (b)(2.) odnose i na zadržavanje, pohranu, uporabu itd. osobnih informacija u području nacionalne sigurnosti.

([28]) Njime upravlja Obavještajni i istražni ured Kabineta na temelju članka 4. Odluke o strukturi Tajništva Kabineta.
([29]) To uključuje „prikupljanje i istraživanje obavještajnih podataka o važnim politikama Kabineta”.
([30]) Sigurnosna policija odgovorna je za aktivnosti kontrole kriminala koje se odnose na javnu sigurnost i na interese države. To uključuje kontrolu kriminala i prikupljanje informacija o nezakonitim radnjama povezanima s ekstremnim skupinama ljevice, skupinama desnice i aktivnostima koje štete interesima Japana.

2. Posebna ograničenja koja se primjenjuju na policiju (NPA i prefekturalnu policiju)

Kako je prethodno navedeno u odjeljku koji se odnosi na prikupljanje informacija u svrhu kaznenog progona, policija može prikupljati informacije samo u okviru svoje nadležnosti te pri tome može, u skladu s člankom 2. stavkom 2. Zakona o policiji, djelovati samo u mjeri koja je „strogo ograničena" na obavljanje svojih dužnosti „nepristrano, nestranački, bez predrasuda i pošteno". Nadalje, „nikad ne smije zloupotrebljavati svoje ovlasti na bilo koji način kojim bi zadirala u prava i slobode pojedinaca zajamčene Ustavom Japana".

3. Posebna ograničenja koja se primjenjuju na PSIA-u

U članku 3. SAPA-e i u članku 3. ACO-a navodi se da se istrage koja se provode u skladu s tim zakonima provode samo u najmanjoj mjeri koja je potrebna da se postigne željena svrha i ne smiju se provoditi tako da se nerazumno ograničavaju temeljna ljudska prava. Nadalje, u skladu s člankom 45. SAPA-e i člankom 42. ACO-a, ako službenik PSIA-e zlouporabi svoje ovlasti, to predstavlja kazneno djelo koje se kažnjava težim kaznenim sankcijama od „općih" zlouporaba ovlasti u drugim područjima javnog sektora.

4. Posebna ograničenja koja se primjenjuju na MOD

Kad je riječ o prikupljanju/organizaciji informacija koje provodi Ministarstvo obrane (MOD), prikupljanje informacija koje provodi MOD na temelju članaka 4. Zakona o osnivanju MOD-a ograničeno je na ono što je „nužno" za obavljanje njegovih dužnosti u pogledu 1. obrane i zaštite, 2. mjera koje moraju poduzeti obrambene snage 3. organizacija, broja osoblja, strukture, opreme, i raspoređivanja kopnenih, pomorskih i obrambenih zračnih snaga.

*(b) Ostala ograničenja*

Kako je prethodno objašnjeno u odjeljku II.A.2)(b) (1) u vezi s kaznenim istragama, iz sudske prakse Vrhovnog suda proizlazi da, kako bi se zahtjev za dobrovoljnu suradnju uputio gospodarskom subjektu, takav zahtjev mora biti nužan za istragu potencijalnog zločina i mora biti razuman kako bi se postigla svrha istrage.

Iako se istrage koje provode istražna tijela u području nacionalne sigurnosti razlikuju od istraga koje provode istražna tijela u području kaznenog progona s obzirom na njihovu pravnu osnovu i svrhu, ključna načela „nužnosti za istragu" i „prikladnosti metode" na sličan se način primjenjuju u području nacionalne sigurnosti te se moraju poštovati, uzimajući u obzir posebne okolnosti svakog slučaja.

Kombinacijom navedenih ograničenja osigurava se da se prikupljanje i obrada informacija odvijaju samo u mjeri u kojoj je to potrebno za izvršavanje konkretnih zadaća nadležnog javnog tijela te na temelju konkretnih prijetnji. To isključuje masovno i neselektivno prikupljanje ili pristup osobnim informacijama iz razloga nacionalne sigurnosti.

B. Nadzor

1. Nadzor na temelju APPIHAO-a

Kako je objašnjeno u odjeljku II.B.2), u japanskom javnom sektoru ministar ili čelnik pojedinog ministarstva ili agencije ima ovlasti za nadzor i osiguravanje usklađenosti s APPIHAO-om u svojem ministarstvu ili agenciji. Nadalje, ministar unutarnjih poslova i komunikacija može istražiti status provedbe Zakona, zatražiti od svakog ministra da mu dostavi materijale i objašnjenja na temelju članka 49. i 50. Zakona, uputiti mišljenja svakom ministru na temelju članka 51. Zakona. Na primjer, može zatražiti reviziju mjera u okviru radnji na temelju članka 50. i 51. Zakona.

2. Nadzor policije koji provode povjerenstva za javnu sigurnost

Kako je objašnjeno u prethodnom odjeljku „II. Prikupljanje informacija u svrhu kaznenog progona", neovisna Prefekturalna povjerenstva za javnu sigurnost nadziru aktivnosti prefekturalne policije.

U pogledu Nacionalne policijske agencije (NPA), nadzorne funkcije obavlja Nacionalno povjerenstvo za javnu sigurnost. U skladu s člankom 5. Zakona o policiji, ovo je Povjerenstvo konkretno odgovorno za „zaštitu prava i slobode pojedinca". U tu svrhu posebno utvrđuje sveobuhvatne politike kojima se utvrđuju propisi za upravljanje poslovima koji su propisani u svakoj stavki članka 5. stavka 4. Zakona o policiji te u kojima se navode druge osnovne smjernice ili mjere na koje se treba osloniti za obavljanje navedenih aktivnosti. Nacionalno povjerenstvo za javnu sigurnost (NPSC) ima isti stupanj neovisnosti kao i Prefekturalna povjerenstva za javnu sigurnost (PPSC-ovi).

3. Nadzor MOD-a koji provodi Ured glavnog inspektora za praćenje poštovanja zakonitosti

Ured glavnog inspektora za praćenje poštovanja zakonitosti (IGO) neovisan je ured u Ministarstvu obrane (MOD) koji je pod izravnim nadzorom ministra obrane na temelju članka 29. Zakona o osnivanju MOD-a. IGO može provoditi inspekcijske preglede u pogledu poštovanja zakona i propisa dužnosnika MOD-a. Ti se pregledi nazivaju „inspekcijski pregledi u području obrane" (Defence Inspections).

IGO provodi inspekcijske preglede iz pozicije neovisnog ureda kako bi se osigurala pravna usklađenost u cijelom ministarstvu, uključujući obrambene snage (SDF). Svoje dužnosti obavlja neovisno od operativnih odjela MOD-a. Nakon inspekcijskog pregleda IGO bez odgode izravno izvješćuje ministra obrane o svojim nalazima i mjerama za poboljšanje. Na temelju izvješća IGO-a ministar obrane može izdati naloge za provedbu mjera potrebnih za rješavanje situacije. Zamjenik dominstra nadležan je za provedbu tih mjera i ministra obrane mora izvijestiti o statusu njihove provedbe.

Kao dobrovoljna mjera transparentnosti, nalazi inspekcijskih pregleda u području obrane sada se objavljuju na internetskim stranicama MOD-a (iako to nije propisano zakonom).

Tri su kategorije inspekcijskih pregleda u području obrane:

i. redoviti inspekcijski pregledi u području obrane koji se provode periodično ([31]);

ii. preventivni inspekcijski pregledi radi provjere koji se provode kako bi se provjerilo jesu li mjere za poboljšanje učinkovito poduzete; i

iii. posebni inspekcijski pregledi koje se provode u vezi s posebnim pitanjima po nalogu ministra obrane.

U kontekstu takvih inspekcijskih pregleda glavni inspektor može zatražiti izvješća od predmetnog ureda, zatražiti dostavu dokumenata, ući u lokacije radi obavljanja inspekcijskog pregleda, zatražiti objašnjenja od zamjenika dominstra itd. Zbog prirode inspekcijskih zadaća IGO-a, na čelu tog ureda su visokopozicionirani pravni stručnjaci (bivši viši tužitelj).

4. Nadzor PSIA-e

PSIA provodi redovite i posebne inspekcijske preglede rada svojih pojedinačnih ureda i službi (Obavještajni ured za javnu sigurnost, obavještajne službe za javnu sigurnost i podslužbe itd.). Za potrebe redovitih inspekcijskih pregleda, pomoćnik glavnog direktora i/ili direktor imenuje se kao inspektor. Ti se inspekcijski pregledi odnose i na upravljanje osobnim informacijama.

5. Nadzor parlamenta (Diet)

Kada je riječ o prikupljanju informacija za potrebe kaznenog progona, parlament (Diet) može putem svojeg nadležnog odbora ispitati zakonitost aktivnosti prikupljanja informacija u području nacionalne sigurnosti. Istražne ovlasti parlamenta temelje se na članku 62. Ustava i člancima 74. i 104. Zakona o parlamentu.

C. Pravna zaštita pojedinaca

Pravna zaštita pojedinaca može se ostvariti na isti način kao i u području kaznenog progona. To uključuje i novi mehanizam pravne zaštite za obradu i rješavanje pritužbi koje podnose osobe iz EU-a, kojim upravlja i koji nadzire Povjerenstvo za zaštitu osobnih informacija (PPC). U tom pogledu vidjeti relevantne odlomke odjeljka II.C.

Osim toga, u području nacionalne sigurnosti dostupne su posebne mogućnosti za pravnu zaštitu pojedinca.

Osobne informacije koje je upravni organ prikupio za potrebe nacionalne sigurnosti podliježu odredbama poglavlja 4. APPIHAO-a. To uključuje pravo da se zatraži otkrivanje informacija (članak 12.), ispravak (uključujući dopunu ili brisanje) (članak 27.) pohranjenih osobnih informacija pojedinca, kao i pravo da se zatraži suspenzija korištenja osobnih informacija u slučaju da je upravni organ predmetne informacije dobio nezakonito (članak 36.). Međutim, u području nacionalne sigurnosti ostvarivanje takvih prava podliježe određenim ograničenjima: zahtjevi za otkrivanje, ispravak informacija

([31]) Kao primjer inspekcijskog pregleda relevantnog za teme obuhvaćene ovom Izjavom, upućuje se na „Redoviti inspekcijski pregled u području obrane iz 2016." u pogledu „svjesnosti/spremnosti za poštovanje zakonodavstva" s obzirom na to da je zaštita osobnih informacija bila jedna od središnjih točaka tog inspekcijskog pregleda. Konkretnije, inspekcijski pregled odnosio se na status upravljanja, pohrane itd. osobnih informacija. U svojem izvješću IGO je utvrdio nekoliko neprimjerenih aspekata u upravljanju osobnim informacijama koje je potrebno poboljšati, kao što je propust da se informacije zaštite s pomoću lozinke. Izvješće je dostupno na internetskim stranicama MOD-a.

ili suspenziju neće biti odobreni ako se odnose na „informacije za koje čelnik upravnog organa opravdano smatra da bi se njihovim otkrivanjem moglo naštetiti nacionalnoj sigurnosti, uzrokovati štetu odnosu uzajamnog povjerenja s drugom državom ili međunarodnom organizacijom ili dovesti Japan u nepovoljan položaj u pregovorima s drugom državom ili međunarodnom organizacijom" (članak 14. stavak iv.). Prema tome, to se izuzeće ne odnosi na sve dobrovoljno prikupljanje informacija povezano s nacionalnom sigurnosti jer se za potonje uvijek zahtijeva konkretna procjena rizika povezanih s njihovim otkrivanjem.

Nadalje, ako je zahtjev pojedinca odbijen jer se smatra da se predmetne informacije ne smiju otkrivati u smislu članka 14. točke iv., on može podnijeti upravnu žalbu za preispitivanje takve odluke, navodeći na primjer da u predmetnom slučaju nisu ispunjeni uvjeti iz članka 14. točke iv. U tom se slučaju prije donošenja odluke čelnik predmetnog upravnog organa savjetuje s Odborom za preispitivanje otkrivanja informacija i zaštitu osobnih informacija. Odbor će preispitati žalbu s neovisnog stajališta. Odbor je visoko specijalizirano, neovisno tijelo čije članove imenuje premijer uz suglasnost obaju domova parlamenta, iz skupine osoba s iznimnim stručnim znanjem ([32]). Odbor ima snažne istražne ovlasti, uključujući mogućnost zahtijevanja dokumenata i otkrivanja predmetnih osobnih informacija, vođenja rasprave zatvorene za javnost i primjene postupka s indeksom Vaughn ([33]). Odbor zatim izrađuje pisano izvješće koje se dostavlja predmetnoj osobi ([34]). Rezultati izvješća se objavljuju. Iako izvješće nije službeno pravno obvezujuće, predmetni upravni organi postupaju u skladu s gotovo svim izvješćima ([35]).

Naposljetku, u skladu s člankom 3. stavkom 3. Zakona o upravnim sporovima, osoba može pokrenuti sudski postupak kojim traži opoziv odluke upravnog organa o neotkrivanju osobnih informacija.

IV. **Periodično preispitivanje**

U okviru periodičnog preispitivanja odluke o primjerenosti, PPC i Europska komisija razmjenjivat će informacije o obradi podataka pod uvjetima zaključka o primjerenosti, uključujući one koje su iznesene u ovoj Izjavi.

([32]) Vidjeti članak 4. Zakona o osnivanju Odbora za preispitivanje otkrivanja informacija i zaštitu osobnih informacija.
([33]) Vidjeti članak 9. Zakona o osnivanju Odbora za preispitivanje otkrivanja informacija i zaštitu osobnih informacija.
([34]) Vidjeti članak 16. Zakona o osnivanju Odbora za preispitivanje otkrivanja informacija i zaštitu osobnih informacija.
([35]) U posljednje tri godina nema presedana gdje je predmetni upravni organ donio odluku koja se razlikuje od zaključaka Odbora. U godinama prije toga postoji iznimno malo slučajeva u kojima se to dogodilo: samo dva slučaja od ukupno 2 000 od 2005. (godina u kojoj je APPIHAO stupio na snagu). Kad upravni organ donese rješenje/odluku koja se razlikuje od zaključaka Odbora, u skladu s člankom 50. stavkom 1. točkom 4. Zakona o upravnim pravnim sredstvima (Administrative Complaint Review Act) koji se primjenjuje sa zamjenom članka 42. stavka 2. APPIHAO-a, on to jasno obrazlaže.