

Uradni list

Evropske unije

L 76



Slovenska izdaja

Zakonodaja

Letnik 62

19. marec 2019

Vsebina

II *Nezakonodajni akti*

SKLEPI

- ★ Izvedbeni sklep Komisije 2019/419 z dne 23. januarja 2019 v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov na Japonskem na podlagi zakona o varstvu osebnih informacij ⁽¹⁾ 1

⁽¹⁾ Besedilo velja za EGP.

Akti z rahlo natisnjenimi naslovi so tisti, ki se nanašajo na dnevno upravljanje kmetijskih zadev in so splošno veljavni za omejeno obdobje.

Naslovi vseh drugih aktov so v mastnem tisku in pred njimi stoji zvezdica.

II

(Nezakonodajni akti)

SKLEPI

IZVEDBENI SKLEP KOMISIJE 2019/419

z dne 23. januarja 2019

v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov na Japonskem na podlagi zakona o varstvu osebnih informacij

(notificirano pod dokumentarno številko C(2019) 304)

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) ⁽¹⁾, zlasti njenega člena 45(3),

po posvetovanju z evropskim nadzornikom za varstvo podatkov,

1. UVOD

- (1) Uredba (EU) 2016/679 določa pravila o prenosu osebnih podatkov od upravljavcev ali obdelovalcev v Evropski uniji v tretje države in mednarodne organizacije, če taki prenosi spadajo na področje uporabe navedene uredbe. Pravila o mednarodnih prenosih osebnih podatkov so določena v poglavju V navedene uredbe, natančneje v členih 44 do 50. Pretok osebnih podatkov v države zunaj Evropske unije in iz njih je potreben za širitev mednarodnega sodelovanja in mednarodne trgovine, hkrati pa je treba zagotoviti, da raven varstva osebnih podatkov, ki se zagotavlja v Evropski uniji, ni ogrožena.
- (2) V skladu s členom 45(3) Uredbe (EU) 2016/679 lahko Komisija z izvedbenim aktom odloči, da tretja država, ozemlje ali en ali več določenih sektorjev v zadevni tretji državi ali mednarodna organizacija zagotavlja ustrezno raven varstva. Pod tem pogojem se lahko osebni podatki prenašajo v navedeno tretjo državo, na ozemlje, sektor ali v mednarodno organizacijo brez nadaljnjega dovoljenja, kot je določeno v členu 45(1) in navedeno v uvodni izjavi 103 Uredbe.
- (3) Kot je navedeno v členu 45(2) Uredbe (EU) 2016/679, mora sprejetje sklepa o ustreznosti temeljiti na celoviti analizi pravnega reda tretje države, in sicer v zvezi s pravili, ki se uporabljajo glede uvoznikov podatkov, ter omejitvami in zaščitnimi ukrepi glede dostopa javnih organov do osebnih podatkov. V oceni je treba opredeliti, ali zadevna tretja država zagotavlja raven varstva, ki je „v osnovi enakovredna“ tisti, zagotovljeni v Evropski uniji (uvodna izjava 104 Uredbe (EU) 2016/679). Kot je pojasnilo Sodišče Evropske unije, to ne zahteva povsem enake ravni varstva ⁽²⁾. To zlasti pomeni, da se lahko sredstva, ki jih zadevna tretja država uporablja, razlikujejo od tistih, ki jih uporablja Evropska unija, če se v praksi izkaže, da so učinkovita pri zagotavljanju ustrezne ravni varstva ⁽³⁾. Standard ustreznosti torej ne zahteva dobesednega prepisa pravil Unije. Bolj kot to preizkus temelji na proučitvi, ali

⁽¹⁾ UL L 119, 4.5.2016, str. 1.

⁽²⁾ Zadeva C-362/14, Maximilian Schrems proti Data Protection Commissioner (v nadaljnjem besedilu: Schrems), ECLI:EU:C:2015:650, točka 73.

⁽³⁾ Sodba v zadevi Schrems, točka 74.

tuji sistem kot celota prek vsebine pravic do zasebnosti ter njihovega učinkovitega izvajanja, nadzora in izvrševanja zagotavlja zahtevano raven varstva ⁽⁴⁾.

- (4) Komisija je skrbno proučila japonsko zakonodajo in prakso. Na podlagi ugotovitev iz uvodnih izjav 6 do 175 Komisija ugotavlja, da Japonska zagotavlja ustrezno raven varstva osebnih podatkov, ki se prenašajo organizacijam, ki spadajo na področje uporabe zakona o varstvu osebnih informacij ⁽⁵⁾, ob upoštevanju dodatnih pogojev iz tega sklepa. Ti pogoji so navedeni v dopolnilnih pravilih (Priloga I), ki jih je sprejela komisija za varstvo osebnih informacij (PPC) ⁽⁶⁾, ter v uradnih navedbah, zagotovilih in zavezah japonske vlade Evropski komisiji (Priloga II).
- (5) Učinek tega sklepa je, da za prenose od upravljavca ali obdelovalca v Evropskem gospodarskem prostoru (EGP) ⁽⁷⁾ v navedene organizacije na Japonskem ni potrebno nobeno nadaljnje dovoljenje. Ta sklep ne vpliva na neposredno uporabo Uredbe (EU) 2016/679 za take organizacije, kadar so izpolnjeni pogoji iz njenega člena 3.

2. PRAVILA, KI SE UPORABLJAJO ZA OBDELAVO PODATKOV S STRANI POSLOVNIH SUBJEKTOV

2.1 Japonski okvir varstva podatkov

- (6) Pravni sistem, ki na Japonskem ureja varstvo zasebnosti in podatkov, temelji na ustavi iz leta 1946.
- (7) Člen 13 ustave določa:

„Vsi ljudje so spoštovani kot posamezniki. Njihova pravica do življenja, svobode in prizadevanja za srečo je pglavitni cilj zakonodaje in drugih vladnih zadev, kolikor ne posega v javno dobrobit.“

- (8) Na podlagi navedenega člena je vrhovno sodišče Japonske pojasnilo pravice posameznikov glede varstva osebnih informacij. V odločbi z leta 1969 je priznalo pravico do zasebnosti in varstva podatkov kot ustavno pravico ⁽⁸⁾. Sodišče je zlasti odločilo, da „vsak posameznik lahko svobodno štiti svoje osebne informacije pred razkritjem tretji osebi ali javnosti, če za tako razkritje ni dobrega razloga“. Poleg tega je vrhovno sodišče v odločbi z dne 6. marca 2008 (Juki-Net) ⁽⁹⁾ odločilo, da „se svoboda državljanov v zasebnem življenju štiti pred izvrševanjem javnih pooblastil, sklepati pa je mogoče tudi, da lahko vsak posameznik kot eno od svojih svoboščin v okviru zasebnega življenja svobodno štiti svoje osebne informacije pred razkritjem tretji osebi ali javnostjo, če za tako razkritje ni dobrega razloga“ ⁽¹⁰⁾.
- (9) Japonska je 30. maja 2003 sprejela več zakonov na področju varstva podatkov:

— zakon o varstvu osebnih informacij,

— zakon o varstvu osebnih informacij, ki jih hranijo upravni organi,

— zakon o varstvu osebnih informacij, ki jih hranijo neodvisne upravne agencije.

⁽⁴⁾ Glej Sporočilo Komisije Evropskemu parlamentu in Svetu: Izmenjava in varstvo osebnih podatkov v globaliziranem svetu (COM(2017) 7, 10.1.2017, oddelek 3.1, str. 6–7).

⁽⁵⁾ Zakon o varstvu osebnih informacij (zakon št. 57, 2003).

⁽⁶⁾ Več informacij o komisiji za varstvo osebnih informacij je na voljo na naslednji povezavi: <https://www.ppc.go.jp/en/> (vključno s kontaktnimi podatki za poizvedbe in pritožbe: <https://www.ppc.go.jp/en/contactus/access/>).

⁽⁷⁾ Ta sklep velja za EGP. Sporazum o Evropskem gospodarskem prostoru (Sporazum EGP) določa razširitev notranjega trga Evropske unije na tri države EGP, tj. Islandijo, Lihtenštajn in Norveško. Sklep Skupnega odbora EGP, s katerim je bila Uredba (EU) 2016/679 vključena v Prilogo XI k Sporazumu EGP, je bil sprejet 6. julija 2018 in začel veljati 20. julija 2018. Navedeni sporazum torej zajema tudi Uredbo.

⁽⁸⁾ Vrhovno sodišče, sodba velikega senata z dne 24. decembra 1969, zbirka objav Keishu, zvezek 23, št. 12, str. 1625.

⁽⁹⁾ Sodba vrhovnega sodišča z dne 6. marca 2008, zbirka objav Minshu, zvezek 62, št. 3, str. 665.

⁽¹⁰⁾ Sodba vrhovnega sodišča z dne 6. marca 2008, zbirka objav Minshu, zvezek 62, št. 3, str. 665.

- (10) Slednja zakona (spremenjena leta 2016) vsebujeta določbe, ki se nanašajo na varstvo osebnih informacij s strani subjektov javnega sektorja. Obdelava podatkov, ki spada na področje uporabe navedenih zakonov, ni predmet ugotavljanja ustreznosti v tem sklepu, ki se omejuje na varstvo osebnih informacij s strani „poslovnih subjektov, ki obravnavajo osebne informacije“ v smislu japonskega zakona o varstvu osebnih informacij.
- (11) Navedeni zakon je bil nedavno spremenjen. Spremenjeni zakon o varstvu osebnih informacij je bil razglašen 9. septembra 2015 in začel veljati 30. maja 2017. S spremembo je bilo uvedenih več novih zaščitnih ukrepov, okrepljeni pa so bili tudi obstoječi, s čimer se je japonski sistem varstva podatkov bolj približal evropskemu. To na primer zajema več izvršljivih pravic posameznikov in vzpostavitev neodvisnega nadzornega organa (komisije za varstvo osebnih informacij), ki nadzoruje in izvaja zakon o varstvu osebnih informacij.
- (12) Za obdelavo osebnih informacij, ki spadajo na področje uporabe tega sklepa, se poleg zakona o varstvu osebnih informacij uporabljajo tudi izvedbeni predpisi, izdani na njegovi podlagi. To zajema spremembo vladne odredbe o izvajanju zakona o varstvu osebnih informacij z dne 5. oktobra 2016 in tako imenovani pravilnik o izvajanju zakona o varstvu osebnih informacij, ki ga je sprejela komisija za varstvo osebnih informacij⁽¹¹⁾. Oba sklopa pravil sta pravno zavezujoča in izvršljiva, veljati pa sta začela hkrati s spremenjenim zakonom o varstvu osebnih informacij.
- (13) Poleg tega je japonska vlada (ki jo sestavljajo predsednik vlade in ministri) 28. oktobra 2016 izdala „osnovno politiko“ za „celovito in skladno spodbujanje ukrepov v zvezi z varstvom osebnih informacij“. V skladu s členom 7 zakona o varstvu osebnih informacij se „osnovna politika“ izda v obliki vladne odločbe ter zajema usmeritve politike glede izvajanja zakona o varstvu osebnih informacij, namenjena pa je osrednji vladi in lokalnim vladam.
- (14) Japonska vlada je pred kratkim, 12. junija 2018, s sprejetjem sklepa vlade spremenila osnovno politiko. Zaradi olajšanja mednarodnega prenosa podatkov se komisiji za varstvo osebnih informacij, ki ima nalogo upravljanja in izvajanja zakona o varstvu osebnih informacij, z navedenim sklepom vlade „na podlagi člena 6 zakona“ podeljuje „pooblastilo za sprejetje potrebnih ukrepov za premoščanje razlik med japonskim sistemom in njegovim delovanjem ter sistemi zadevnih tujih držav in njihovim delovanjem, da se tako zagotovi ustrezna obravnava osebnih informacij, prejetih od take države“. V sklepu vlade je navedeno, da to zajema pristojnost za vzpostavitev izboljšanega varstva, tako da komisija za varstvo osebnih informacij sprejme strožja pravila, ki dopolnjujejo in presegajo tista iz zakona o varstvu osebnih informacij in vladne odredbe. Na podlagi navedenega sklepa so ta strožja pravila za japonske poslovne subjekte zavezujoča in izvršljiva.
- (15) Komisija za varstvo osebnih informacij je 15. junija 2018 na podlagi člena 6 zakona o varstvu osebnih informacij in navedenega sklepa vlade sprejela „dopolnilna pravila na podlagi zakona o varstvu osebnih informacij glede obravnave prenosa osebnih podatkov iz EU na podlagi sklepa o ustreznosti“ (v nadaljnjem besedilu: dopolnilna pravila), da se izboljša varstvo osebnih informacij, ki se prenašajo iz Evropske unije na Japonsko na podlagi tega sklepa o ustreznosti. Navedena dopolnilna pravila so pravno zavezujoča za japonske poslovne subjekte, izvršujejo pa jih komisija za varstvo osebnih informacij in sodišča na enak način kot določbe zakona o varstvu osebnih informacij, ki jih ta pravila nadomeščajo s strožjimi in/ali podrobnejšimi pravili⁽¹²⁾. Ker bodo japonski poslovni subjekti, ki prejema in/ali nadalje obdelujejo osebne podatke iz Evropske unije, pravno zavezani k spoštovanju dopolnilnih pravil, bodo morali (npr. s tehničnim „označevanjem“) ali organizacijskimi rešitvami (shranjevanje v namensko podatkovno zbirko)) zagotoviti, da lahko te osebne podatke prepoznajo v celotnem njihovem „življenjskem ciklu“⁽¹³⁾. V naslednjih oddelkih je vsebina vsakega dopolnilnega pravila analizirana kot del presoje členov zakona o varstvu osebnih informacij, ki jih dopolnjujejo.
- (16) Komisija za varstvo osebnih informacij je na podlagi zakona o varstvu osebnih informacij pristojna za sprejetje „smernic“ „za zagotavljanje ustreznega in učinkovitega izvajanja ukrepov poslovnih subjektov“ v skladu s pravili o varstvu podatkov, za razliko od ureditve pred spremembo iz leta 2015, ko so bila za navedeno pristojna različna

⁽¹¹⁾ Na voljo na: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

⁽¹²⁾ Glej dopolnilna pravila (uvodni oddelek).

⁽¹³⁾ Splošne zahteve po vzdrževanju evidence (samo) za določeno obdobje tega ne postavljajo pod vprašaj. Čeprav je izvor podatkov med informacijami, ki jih mora tisti poslovni subjekt, ki obravnava osebne informacije, ki je podatke pridobil, v skladu s členom 26(1) zakona o varstvu osebnih informacij potrditi, zahteva na podlagi člena 26(4) zakona o varstvu osebnih informacij v povezavi s členom 18 pravilnika komisije za varstvo osebnih informacij zadeva le določeno obliko evidence (glej člen 16 pravilnika komisije za varstvo osebnih informacij) in poslovnemu subjektu, ki obravnava osebne informacije, ne preprečuje, da bi zagotavljal prepoznavanje podatkov za daljša obdobja. To je potrdila komisija za varstvo osebnih informacij, ki je navedla, da mora „poslovni subjekt, ki obravnava osebne informacije, informacije o izvoru podatkov iz EU hraniti tako dolgo, kot je potrebno, da lahko spoštuje dopolnilna pravila“.

japonska ministrstva po posameznih sektorjih. Komisija za varstvo osebnih informacij v svojih smernicah zagotavlja verodostojno razlago teh pravil, zlasti zakona o varstvu osebnih informacij. Na podlagi informacij, prejetih od komisije za varstvo osebnih informacij, so navedene smernice sestavni del pravnega okvira ter jih je treba upoštevati v povezavi z besedilom zakona o varstvu osebnih informacij, vladne odredbe, pravilnika komisije za varstvo osebnih informacij ter vprašanj in odgovorov⁽¹⁴⁾, ki jih je pripravila komisija za varstvo osebnih informacij. Zato so „zavezujoče za poslovne subjekte“. Kadar smernice določajo, da poslovni subjekt „mora“ ali „ne sme“ ravnati na določen način, komisija za varstvo osebnih informacij odloči, da neskladnost z zadevnimi določbami pomeni kršitev zakona⁽¹⁵⁾.

2.2 Materialno in osebno področje uporabe

- (17) Področje uporabe zakona o varstvu osebnih informacij je določeno z opredelitvijo pojmov osebna informacija, osebni podatek in poslovni subjekt, ki obravnava osebne informacije. Hkrati so v zakonu o varstvu osebnih informacij navedene nekatere pomembne izključitve z njegovega področja uporabe, predvsem glede anonimno obdelanih osebnih podatkov in posebnih vrst obdelave s strani določenih subjektov. Čeprav zakon o varstvu osebnih informacij ne uporablja izraza „obdelava“, se opira na enakovreden pojem „obrnava“, ki po informacijah, prejetih od komisije za varstvo osebnih informacij, zajema „kakršno koli ravnanje z osebnimi podatki“, vključno s pridobitvijo, vnosom, zbiranjem, organizacijo, shranjevanjem, urejanjem/obdelavo, obnavljanjem, izbrisom, iznosom, uporabo ali zagotavljanjem osebnih informacij.

2.2.1 Opredelitev pojma osebna informacija

- (18) Najprej je treba navesti, da zakon o varstvu osebnih informacij glede materialnega področja uporabe razlikuje med osebnimi informacijami in osebnimi podatki, pri čemer se za prvo kategorijo uporabljajo samo določene določbe zakona. V skladu s členom 2(1) zakona o varstvu osebnih informacij pojem osebne informacije zajema vse informacije, ki se nanašajo na živega posameznika in omogočajo njegovo identifikacijo. Opredelitev razlikuje med dvema kategorijama osebnih informacij: (i) individualna identifikacijska koda in (ii) druge osebne informacije, na podlagi katerih je mogoče identificirati posameznika. Slednja kategorija zajema tudi informacije, ki same po sebi ne omogočajo identifikacije, lahko pa, če so „ustrezno združene“ z drugimi informacijami, omogočajo identifikacijo posameznika. Na podlagi smernic komisije za varstvo osebnih informacij⁽¹⁶⁾ velja, da se to, ali je informacije mogoče šteti za „ustrezno združene“, presoja v vsakem primeru posebej, pri čemer se upošteva dejanska situacija („razmere“) poslovnega subjekta. To se domneva, če tako združevanje opravlja (ali lahko opravlja) povprečni („običajni“) poslovni subjekt z uporabo sredstev, ki so mu na voljo. Informacije se na primer ne štejejo za „ustrezno združene“ z drugimi informacijami, če si mora poslovni subjekt za to prizadevati v neobičajni meri ali storiti nezakonita dejanja, da pridobi informacije, ki se zbirajo, od enega ali več drugih poslovnih subjektov.

2.2.2 Opredelitev pojma osebni podatek

- (19) Na podlagi zakona o varstvu osebnih informacij samo nekatere oblike osebnih informacij spadajo v okvir pojma „osebni podatek“. „Osebni podatek“ je opredeljen kot „osebna informacija, ki pomeni podatkovno zbirko osebnih informacij“, torej „združene informacije“, ki jih sestavljajo osebne informacije, „sistematično organizirane tako, da je mogoče z računalnikom iskati posamezno osebno informacijo“⁽¹⁷⁾, ali „ki so bile na podlagi vladne odredbe opredeljene kot sistematično organizirane tako, da je brez težav mogoče poiskati posamezno osebno informacijo“ – vendar „z izjemo tistih, ki so bile na podlagi vladne odredbe opredeljene kot take, pri katerih je glede na metodo njihove uporabe malo verjetnosti za povzročanje škode posameznikovim pravicam in interesom“⁽¹⁸⁾.
- (20) Ta izjema je podrobneje določena v členu 3(1) vladne odredbe, v skladu s katerim morajo biti izpolnjeni vsi trije naslednji pogoji: (i) združene informacije so morale biti „izdane za namen prodaje velikemu številu nedoločenih oseb, njihova izdaja pa ni bila izvedena v nasprotju z določbami zakona ali odredbe, ki temelji na njem“; (ii) lahko

⁽¹⁴⁾ Komisija za varstvo osebnih informacij, vprašanja in odgovori, 16. februar 2017 (spremenjeno 30. maja 2017), na voljo na naslednji povezavi: <https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf>. Vprašanja in odgovori obravnavajo več tem iz smernic, in sicer z navajanjem primerov iz prakse, kot so na primer to, kaj so občutljivi osebni podatki, razlaga privolitve posameznika, prenosi tretjim osebam v smislu računalništva v oblaku ali obveznost vodenja evidenc, ki velja za čezmejne prenose. Vprašanja in odgovori so na voljo le v japonsščini.

⁽¹⁵⁾ Na posebno vprašanje je komisija za varstvo osebnih informacij Evropski odbor za varstvo podatkov obvestila, da „japonska sodišča pri uporabi zakona o varstvu osebnih informacij/pravilnika komisije za varstvo osebnih informacij v posameznih zadevah, ki so jim predložene, svojo razlago utemeljujejo na smernicah in so se tako v svojih sodbah sklicevala neposredno na besedilo smernic. Zato so smernice komisije za varstvo osebnih informacij tudi s tega vidika zavezujoče za poslovne subjekte. Komisija za varstvo osebnih informacij ni seznanjena s tem, da bi sodišče kadar koli odstopilo od smernic.“ V zvezi s tem je komisija za varstvo osebnih informacij Evropsko komisijo napotila na sodbo s področja varstva podatkov, v kateri se je sodišče v svojih ugotovitvah izrecno oprlo na smernice (glej odločbo okrožnega sodišča v Osaki z dne 19. maja 2006, Hanrei Jiho, zvezek 1948, str. 122, v kateri je sodišče odločilo, da mora poslovni subjekt sprejeti ukrepe v zvezi z nadzorom varnosti na podlagi navedenih smernic).

⁽¹⁶⁾ Smernice komisije za varstvo osebnih informacij (izdaja splošnih pravil), str. 6.

⁽¹⁷⁾ To zajema kakršen koli elektronski sistem arhiviranja. Smernice komisije za varstvo osebnih informacij (splošna izdaja, str. 17) glede tega vsebujejo podrobne primere, na primer seznam elektronskih naslovov, shranjen v programski opremi e-poštnega odjemalca.

⁽¹⁸⁾ Člen 2(4) in (6) zakona o varstvu osebnih informacij.

jih „kadar koli kupi veliko število nedoločenih oseb“ in (iii) osebni podatki, ki jih vsebujejo, morajo biti „zagotovljeni za njihov prvotni namen, ne da bi se jim dodale druge informacije v zvezi z živim posameznikom“. Po pojasnilih komisije za varstvo osebnih informacij je bila ta ozka izjema uvedena z namenom izključitve telefonskih ali podobnih imenikov.

- (21) Glede podatkov, zbranih na Japonskem, je to razlikovanje med „osebno informacijo“ in „osebnim podatkom“ pomembno, saj navedene informacije morda niso vedno del „podatkovne zbirke osebnih informacij“ (npr. posamezen nabor podatkov, ki se zbira in obdeluje ročno), zato se določbe zakona o varstvu osebnih informacij, ki se nanašajo samo na osebne podatke, zanje ne uporabljajo ⁽¹⁹⁾.
- (22) Nasprotno pa to razlikovanje ne bo pomembno glede osebnih podatkov, ki se iz Evropske unije uvažajo na Japonsko na podlagi sklepa o ustreznosti. Ker se taki podatki običajno prenašajo z elektronskimi sredstvi (saj je v digitalni dobi to običajen način za izmenjavo podatkov, zlasti na daljavo, kakor je to med EU in Japonsko), s čimer postanejo del elektronskega sistema arhiviranja uvoznika podatkov, podatki EU vedno spadajo v okvir „osebnih podatkov“ v smislu zakona o varstvu osebnih informacij. Če bi se osebni podatki iz EU izjemoma prenesli z drugimi sredstvi (npr. v papirni obliki), bi bili še vedno zajeti z zakonom o varstvu osebnih informacij, če bi po prenosu postali potekal del „združenih informacij“, ki so sistematično organizirane tako, da omogočajo enostavno iskanje posameznih informacij (člen 2(4)(ii) zakona o varstvu osebnih informacij). V skladu s členom 3(2) vladne odredbe do takega primera pride, kadar so informacije urejene „po določenem pravilu“, zbirka podatkov pa vsebuje orodja, kot je na primer kazalo ali navedba vsebine, za lažje iskanje. To ustreza opredelitvi „zbirke“ v smislu člena 2(1) splošne uredbe o varstvu podatkov.

2.2.3 Opredelitev pojma hranjen osebni podatek

- (23) Nekatere določbe zakona o varstvu osebnih informacij, zlasti členi 27 do 30, ki se nanašajo na pravice posameznikov, se nanašajo le na nekatere kategorije osebnih podatkov, in sicer na „hranjene osebne podatke“. Ti so v členu 2(7) zakona o varstvu osebnih informacij opredeljeni kot osebni podatki, razen tistih, ki so bodisi (i) „na podlagi vladne odredbe opredeljeni kot podatki, pri katerih je verjetno, da bodo škodili javnim ali drugim interesom, če se izve za njihov obstoj ali neobstoj“ bodisi (ii) „na podlagi vladne odredbe predvideni za izbris v roku največ enega leta“.
- (24) Prva od navedenih dveh kategorij je pojasnjena v členu 4 vladne odredbe in zajema štiri različne vrste izjem ⁽²⁰⁾. Navedene izjeme imajo podoben cilj kot tiste, navedene v členu 23(1) Uredbe (EU) 2016/679, predvsem varstvo posameznika, na katerega se nanašajo osebni podatki (ki je v zakonu o varstvu osebnih informacij poimenovan „principal“), in svoboščine drugih, nacionalna varnost, javna varnost, preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj, ali drugi pomembni cilji splošnega javnega interesa. Poleg tega iz besedila člena 4(1)(i) do (iv) vladne odredbe izhaja, da njihova uporaba vedno predpostavlja posebno tveganje za enega od zaščiteneh pomembnih interesov ⁽²¹⁾.
- (25) Druga kategorija je podrobneje navedena v členu 5 vladne odredbe. V povezavi s členom 2(7) zakona o varstvu osebnih informacij so iz pojma hranjenih osebnih podatkov, in s tem s področja pravic posameznikov na podlagi zakona o varstvu osebnih informacij, izvzeti osebni podatki, ki so „predvideni za izbris“ v šestih mesecih. Komisija za varstvo osebnih informacij je pojasnila, da je cilj te določbe spodbuditi poslovne subjekte k hrambi in obdelavi podatkov v najkrajšem možnem času. Vendar pa bi to pomenilo, da posamezniki iz EU, na katere se nanašajo osebni podatki, ne bi mogli izvrševati pomembnih pravic iz enega samega razloga, in sicer trajanja obdobja, v katerem zadevni poslovni subjekt hrani njihove podatke.
- (26) Zato dopolnilno pravilo 2 zahteva, da se osebni podatki, preneseni iz Evropske unije, „obravnavajo kot hranjeni osebni podatki v smislu člena 2(7) zakona, ne glede na predvideni rok njihovega izbrisa“. To pomeni, da obdobje hrambe ne bo imelo nobenega vpliva na pravice, ki jih uživajo posamezniki iz EU, na katere se nanašajo osebni podatki.

⁽¹⁹⁾ Na primer člen 23 zakona o varstvu osebnih informacij o pogojih za izmenjavo osebnih podatkov s tretjimi osebami.

⁽²⁰⁾ In sicer osebne podatke, (i) „v zvezi s katerimi obstaja možnost povzročitve škode za življenje, telo ali premoženje principala ali tretje osebe, če se izve za njihov obstoj ali neobstoj“; (ii) podatke, „v zvezi s katerimi obstaja možnost spodbuditve ali sprožitve nezakonitega ali nepravilnega dejanja, če se izve za njihov obstoj ali neobstoj“; (iii) podatke, „v zvezi s katerimi obstaja možnost poslabšanja nacionalne varnosti, uničenja odnosa zaupanja s tujo državo ali mednarodno organizacijo ali škodovanja pogajanjem s tujo državo ali mednarodno organizacijo, če se izve za njihov obstoj ali neobstoj“; ter (iv) tiste, „v zvezi s katerimi obstaja možnost oviranja vzdrževanja javne varnosti in javnega reda, kot so preprečevanje, zatiranje ali preiskovanje kaznivih dejanj, če se izve za obstoj ali neobstoj takih osebnih podatkov“.

⁽²¹⁾ Pod temi pogoji obvestilo posameznika ni potrebno. To je v skladu s členom 23(2)(h) splošne uredbe o varstvu podatkov, ki določa, da posameznikov, na katere se nanašajo osebni podatki, ni treba obvestiti o omejitvi, če bi to „posegalo v namen omejitve“.

2.2.4 Opredelitev pojma anonimno obdelane osebne informacije

- (27) Zahteve, ki se uporabljajo za anonimno obdelane osebne informacije, kot so opredeljene v členu 2(9) zakona o varstvu osebnih informacij, so določene v oddelku 2 poglavja 4 zakona („Obveznosti poslovnega subjekta, ki obravnava anonimno obdelane informacije“). Vendar pa za te informacije ne vejajo določbe oddelka 1 poglavja IV zakona o varstvu osebnih informacij, ki vsebuje člene o zaščitnih ukrepih za varstvo podatkov in pravicah, ki se uporabljajo v zvezi z obdelavo osebnih podatkov na podlagi zakona. Posledično velja, da čeprav „anonimno obdelane osebne informacije“ niso predmet „običajnih“ pravil o varstvu podatkov (navedenih v oddelku 1 poglavja IV in v členu 42 zakona o varstvu osebnih informacij), vseeno spadajo na področje uporabe zakona o varstvu osebnih informacij, predvsem členov 36–39.
- (28) V skladu s členom 2(9) zakona o varstvu osebnih informacij so „anonimno obdelane osebne informacije“ tiste, ki se nanašajo na posameznika in so „nastale z obdelavo osebnih informacij“ z ukrepi, opisanimi v zakonu o varstvu osebnih informacij (člen 36(1)) in podrobneje opredeljenimi v pravilniku komisije za varstvo osebnih informacij (člen 19), tako da ni več mogoče identificirati posameznika ali obnoviti osebnih informacij.
- (29) Iz navedenih določb izhaja, kot potrjuje tudi komisija za varstvo osebnih informacij, da ni nujno, da je postopek „anonimizacije“ tehnično nepovraten. V skladu s členom 36(2) zakona o varstvu osebnih informacij morajo poslovni subjekti, ki obravnavajo „anonimno obdelane osebne informacije“, zgolj preprečiti ponovno identifikacijo tako, da sprejmejo ukrepe za zagotovitev varnosti „opisov itd. in individualnih identifikacijskih kod, izbrisanih iz osebnih informacij, s čimer so nastale anonimno obdelane informacije, ter informacij, ki se nanašajo na uporabljen metodo obdelave“.
- (30) Ker „anonimno obdelane osebne informacije“, kot so opredeljene v zakonu o varstvu osebnih informacij, zajemajo podatke, pri katerih je ponovna identifikacija posameznika še mogoča, to lahko pomeni, da bi osebni podatki, preneseni iz Evropske unije, lahko izgubili del varstva s postopkom, ki bi na podlagi Uredbe (EU) 2016/679 pomenil obliko „psevdonimizacije“ in ne „anonimizacije“ (s tem pa se ne bi spremenila njihova narava osebnih podatkov).
- (31) Zato dopolnilna pravila določajo dodatne zahteve, ki se uporabljajo le za osebne podatke, prenesene iz Evropske unije na podlagi tega sklepa. V skladu s pravilom 5 dopolnilnih pravil se take osebne informacije štejejo za „anonimno obdelane osebne informacije“ v smislu zakona o varstvu osebnih informacij le, „če poslovni subjekt, ki obravnava osebne informacije, sprejme ukrepe, na podlagi katerih ponovne identifikacije posameznika ne more nihče več opraviti, vključno z izbrisom informacij, ki se nanašajo na metodo obdelave itd.“. Slednje je v dopolnilnih pravilih opredeljeno kot informacije, ki se nanašajo na opise in individualne identifikacijske kode, izbrisane iz osebnih informacij, s katerimi so nastale „anonimno obdelane osebne informacije“, ter informacije, ki se nanašajo na uporabljen metodo obdelave pri izbrisu navedenih opisov in individualnih identifikacijskih kod. Z drugimi besedami, dopolnilna pravila zahtevajo, da poslovni subjekti, ki pripravljajo anonimno obdelane osebne informacije, uničijo „ključ“, ki omogoča ponovno identifikacijo podatkov. To pomeni, da osebni podatki iz Evropske unije spadajo na področje določb zakona o varstvu osebnih informacij glede „anonimno obdelanih osebnih informacij“ le v primerih, ko bi se šteli za anonimne informacije tudi na podlagi Uredbe (EU) 2016/679 ⁽²²⁾.

2.2.5 Opredelitev pojma poslovni subjekt, ki obravnava osebne informacije

- (32) Zakon o varstvu osebnih informacij se glede osebnega področja uporabe uporablja samo za poslovne subjekte, ki obravnavajo osebne informacije. Poslovni subjekt, ki obravnava osebne informacije, je opredeljen v členu 2(5) zakona o varstvu osebnih informacij kot „oseba, ki zagotavlja podatkovno zbirko osebnih informacij itd. za uporabo v poslovanju“, pri čemer so izvzete vlada in upravne agencije na osrednji in lokalni ravni.
- (33) V skladu s smernicami komisije za varstvo osebnih informacij „poslovanje“ pomeni vsako „ravljanje, katerega cilj je ponavljajoče in stalno vodenje družbeno priznanega podjetja za posamezni namen, ne glede na to, ali gre za pridobitno ali nepridobitno dejavnost“. Organizacije brez pravne osebnosti (kot so *de facto* združenja) ali posamezniki se štejejo za poslovne subjekte, ki obravnavajo osebne informacije, če zagotavljajo (uporabljajo) podatkovno zbirko osebnih informacij itd. za svoje poslovanje ⁽²³⁾. Pojem „poslovanja“ v smislu zakona o varstvu osebnih informacij je torej zelo širok, saj zajema pridobitne in nepridobitne dejavnosti, ki jih izvajajo organizacije vseh vrst in posamezniki. Poleg tega „za uporabo v poslovanju“ vključuje tudi osebne informacije, ki se ne uporabljajo v (zunanjih) poslovnih odnosih subjekta, ampak interno, na primer za obdelavo podatkov o zaposlenih.

⁽²²⁾ Glej uvodno izjavo 26 Uredbe (EU) 2016/679.

⁽²³⁾ Smernice komisije za varstvo osebnih informacij (izdaja splošnih pravil), str. 18.

- (34) Glede upravičencev do varstva iz zakona o varstvu osebnih informacij zakon med njimi ne razlikuje na podlagi posameznikovega državljanstva, prebivališča ali lokacije. Enako velja za posameznikovo možnost zahtevati pravno varstvo pri komisiji za varstvo osebnih informacij ali pred sodišči.

2.2.6 Pojma upravljavec in obdelovalec

- (35) Zakon o varstvu osebnih informacij ne razlikuje med obveznostmi, naloženimi upravljavcem in obdelovalcem. Odsotnost tega razlikovanja ne vpliva na raven varstva, saj se vse določbe zakona uporabljajo za vse poslovne subjekte, ki obravnavajo osebne informacije. Poslovni subjekt, ki obravnava osebne informacije, ki obdelavo osebnih podatkov zaupa skrbniku (enakovreden obdelovalcu po Splošni uredbi o varstvu podatkov), mora v zvezi s podatki, ki jih je zaupal, še naprej izpolnjevati obveznosti iz zakona o varstvu osebnih informacij in dopolnilnih pravil. Poleg tega mora v skladu s členom 22 zakona o varstvu osebnih informacij „opravljati potreben in ustrezen nadzor“ nad skrbnikom. Kot je potrdila komisija za varstvo osebnih informacij, skrbnika po drugi strani zavezujejo vse obveznosti iz zakona o varstvu osebnih informacij in dopolnilnih pravil.

2.2.7 Sektorske izjeme

- (36) Člen 76 zakona o varstvu osebnih informacij izvzema nekatere vrste obdelave podatkov iz uporabe poglavja IV zakona, ki vsebuje osrednje določbe o varstvu podatkov (osnovna načela, obveznosti poslovnih subjektov, pravice posameznikov, nadzor s strani komisije za varstvo osebnih informacij). Obdelava, ki je zajeta v sektorski izjemi iz člena 76, je na podlagi člena 43(2) zakona o varstvu osebnih informacij ⁽²⁴⁾ izvzeta tudi iz pristojnosti komisije za varstvo osebnih informacij.
- (37) Zadevne kategorije za sektorske izjeme iz člena 76 zakona o varstvu osebnih informacij so opredeljene z uporabo dvojnega merila na podlagi vrste poslovnega subjekta, ki obravnava osebne informacije, in namena obdelave. Podrobneje, izjema se nanaša na: (i) institucije za radiodifuzijo, časopisni založniki, agencije za komuniciranje ali druge medijske organizacije (vključno z vsemi posamezniki, ki opravljajo dejavnost obveščanja javnosti kot svojo dejavnost), če obdelujejo osebne informacije za namene obveščanja javnosti; (ii) osebe, ki se poklicno ukvarjajo s pisanjem, če to zajema osebne informacije; (iii) univerze in vse druge organizacije ali skupine, namenjene akademskemu študiju, ali vse osebe, ki pripadajo taki organizaciji, če obdelujejo osebne informacije za namene akademskega študija; (iv) verski subjekti, če obdelujejo osebne informacije za namene verskih dejavnosti (vključno z vsemi povezanimi dejavnostmi) in (v) politični subjekti, če obdelujejo osebne informacije za namene svoje politične dejavnosti (vključno z vsemi povezanimi dejavnostmi). Določbe poglavja IV se še naprej uporabljajo za obdelavo osebnih informacij za enega od namenov iz člena 76, če jo opravljajo druge vrste poslovnih subjektov, ki obravnavajo osebne informacije, ter za obdelavo osebnih informacij, ki jo za druge namene opravlja eden od navedenih poslovnih subjektov, ki obravnavajo osebne informacije, na primer v okviru zaposlovanja.
- (38) Ta sklep se nanaša samo na obdelavo osebnih informacij, ki spadajo na področje uporabe poglavja IV zakona o varstvu osebnih informacij (tj. ki jo izvaja poslovni subjekt, ki obravnava osebne informacije, če primer obdelave ne ustreza eni od sektorskih izjem), da se zagotovi ustrezna raven varstva osebnih podatkov, ki se iz Evropske unije prenašajo poslovnim subjektom na Japonskem. Njegovo področje uporabe bi bilo zato treba uskladiti s področjem uporabe zakona o varstvu osebnih informacij. Po informacijah komisije za varstvo osebnih informacij bi se, kadar bi poslovni subjekt, ki obravnava osebne informacije in je zajet s tem sklepom, naknadno spremenil namen uporabe (v dovoljenem obsegu) ter bi bil nato zajet s sektorskimi izjemami iz člena 76 zakona o varstvu osebnih informacij, to štel za mednarodni prenos (saj osebni podatki v takem primeru ne bi bili več zajeti s poglavjem IV zakona o varstvu osebnih informacij in bi tako izpadli iz njegovega področja uporabe). Isto velja, kadar poslovni subjekt, ki obravnava osebne informacije, zagotovi osebne informacije subjektu, zajetemu s členom 76 zakona o varstvu osebnih informacij, za enega od namenov obdelave iz navedene določbe. Kar zadeva osebne podatke, ki se prenesejo iz Evropske unije, bi to pomenilo nadaljnji prenos, za katerega veljajo ustrezni zaščitni ukrepi (zlasti tisti iz člena 24 zakona o varstvu osebnih informacij in dopolnilnega pravila (4)). Kadar se poslovni subjekt, ki obravnava osebne informacije, opira na privolitev posameznika, na katerega se nanašajo osebni podatki ⁽²⁵⁾, bi mu moral zagotoviti vse potrebne informacije, vključno s tem, da osebna informacija ne bo več zaščitena z zakonom o varstvu osebnih informacij.

⁽²⁴⁾ Pri izvajanju svojih pooblastil preiskovanja in izvrševanja komisija za varstvo osebnih informacij ne sme drugim subjektom preprečevati uveljavljanja njihovih pravice do svobode izražanja, svobode akademskega udejstvovanja, svobode veroizpovedi in svobode političnega udejstvovanja (člen 43(1) zakona o varstvu osebnih informacij).

⁽²⁵⁾ Kot je pojasnila komisija za varstvo osebnih informacij, se privolitev v smernicah komisije za varstvo osebnih informacij razlaga kot „izraz principalovega namena sprejeti, da se lahko njegove osebne informacije obravnavajo z metodo, ki jo navaja poslovni subjekt, ki obravnava osebne informacije“. V smernicah komisije za varstvo osebnih informacij (izdaja splošnih pravil, str. 24) so navedeni načini privolitve, ki se štejejo za „običajne poslovne prakse na Japonskem“, in sicer ustni dogovor, predložitev obrazcev ali drugih dokumentov, dogovor po elektronski pošti, označitev okenca na spletni strani, klik na domačo stran, uporaba gumba za soglasje, dotik na ekranu na dotik itd. Vse te metode so izrecna oblika privolitve.

2.3 Zaščitni ukrepi, pravice in obveznosti

2.3.1 Omejitve namena

- (39) Osební podatki bi se morali obdelovati za določen namen in se nato uporabljati samo, če to ni nezdržljivo z namenom obdelave. To načelo varstva podatkov je zagotovljeno v členih 15 in 16 zakona o varstvu osebnih informacij.
- (40) Zakon o varstvu osebnih informacij se nanaša na načelo, da mora poslovni subjekt opredeliti namen uporabe „kolikor je mogoče natančno“ (člen 15(1)), nato pa ga tako navedeni namen zavezuje pri obdelavi podatkov.
- (41) V tem smislu člen 15(2) zakona o varstvu osebnih informacij določa, da poslovni subjekt, ki obravnava osebne informacije, ne sme spremeniti prvotnega namena „bolj, kot bi bilo mogoče priznati za razumno utemeljeno glede na namen uporabe pred spremembo“, kar je v smernicah komisije za varstvo osebnih informacij razumljeno kot tisto, kar lahko posameznik, na katerega se nanašajo osebni podatki, objektivno pričakuje na podlagi „običajnih družbenih norm“⁽²⁶⁾.
- (42) Poleg tega poslovni subjekti, ki obravnavajo osebne informacije, na podlagi člena 16(1) zakona o varstvu osebnih informacij ne smejo obravnavati osebnih informacij v obsegu, ki presega, „kar je potrebno, da se doseže namen uporabe“, kot je opredeljeno v členu 15, brez pridobitve vnaprejšnje privolitve posameznika, na katerega se nanašajo osebni podatki, razen če se uporablja ena od izjem iz člena 16(3)⁽²⁷⁾.
- (43) Poslovni subjekt, ki obravnava osebne informacije, lahko glede osebnih informacij, ki jih pridobi od drugega poslovnega subjekta, načeloma svobodno določi nov namen uporabe⁽²⁸⁾. Da se zagotovi, da prejemnika v primeru prenosa iz Evropske unije zavezuje namen, za katerega so bili podatki preneseni, dopolnilno pravilo 3 zahteva, da mora v primerih, „ko [poslovni subjekt, ki obravnava osebne informacije,] prejme osebne podatke iz EU na podlagi sklepa o ustreznosti“, ali če tak subjekt „prejme osebne podatke, ki so bili predhodno preneseni iz EU na podlagi sklepa o ustreznosti, od drugega [poslovnega subjekta, ki obravnava osebne informacije,]“ (nadaljnja izmenjava), prejemnik „opredeliti namen uporabe navedenih osebnih podatkov v okviru, za katerega so bili podatki prvotno ali naknadno prejeti“. Z drugimi besedami, pravilo zagotavlja, da v okviru prenosa namen, opredeljen na podlagi Uredbe (EU) 2016/679, še naprej opredeljuje obdelavo in da je za spremembo navedenega namena v kateri koli fazi obdelave na japonskem potrebna privolitev posameznika iz EU, na katerega se nanašajo osebni podatki. Za pridobitev soglasja mora sicer poslovni subjekt, ki obravnava osebne informacije, stopiti v stik s posameznikom, na katerega se nanašajo osebni podatki, kadar to ni mogoče, pa je treba zgolj ohraniti prvotni namen.

2.3.2 Zakonitost in poštenost obdelave

- (44) Dodatno varstvo iz uvodne izjave 43 je še pomembnejše, saj japonski sistem na podlagi načela omejitve namena tudi zagotavlja, da se osebni podatki obdelujejo zakonito in pošteno.
- (45) V skladu z zakonom o varstvu osebnih informacij mora poslovni subjekt, ki obravnava osebne informacije, med zbiranjem osebnih informacij natančno opredeliti namen njihove uporabe⁽²⁹⁾ in takoj obvestiti posameznika, na katerega se nanašajo osebni podatki, o takem namenu uporabe (ali namen razkriti javnosti)⁽³⁰⁾. Poleg tega člen 17 zakona o varstvu osebnih informacij določa, da poslovni subjekt, ki obravnava osebne informacije, ne sme pridobiti osebnih informacij na podlagi prevare ali na druge neprimerne načine. Glede nekaterih kategorij podatkov, kot so osebne informacije, ki zahtevajo posebno pozornost, velja, da je za njihovo pridobitev potrebna privolitev posameznika, na katerega se nanašajo osebni podatki (člen 17(2) zakona o varstvu osebnih informacij).

⁽²⁶⁾ Vprašanja in odgovori, ki jih je objavila komisija za varstvo osebnih informacij, vsebujejo več primerov za razlago tega načela. Primeri, v katerih sprememba ostaja v okviru razumno upoštevnega področja uporabe, zajemajo predvsem uporabo osebnih informacij, pridobljenih od kupcev blaga ali storitev v okviru trgovskih poslov, za obveščanje navedenih kupcev o drugem razpoložljivem upoštevne blagu in storitvah (npr. upravljavec fitnes kluba, ki vodi evidenco e-poštnih naslovov članov, da jih obvešča o vadbi in programih). Hkrati pa vprašanja in odgovori zajemajo tudi primer, v katerem sprememba namena uporabe ni dovoljena, in sicer če družba pošlje informacije o svojem blagu in storitvah na e-poštne naslove, ki jih je zbrala za opozarjanje na goljufije ali krajo članske izkaznice.

⁽²⁷⁾ Te izjeme so lahko posledica drugih zakonov in predpisov ali se nanašajo na primere, ko je obravnava osebnih informacij potrebna (i) zaradi „varstva človeškega življenja, telesa ali premoženja“; (ii) zaradi „izboljšanja javne higiene ali spodbujanja zdravja otrok“ ali (iii) „zaradi sodelovanja z vladnimi agencijami ali organi ali njihovimi predstavniki“ pri izvajanju njihovih zakonskih nalog. Poleg tega se kategoriji (i) in (ii) uporabljata le, če je težko zagotoviti privolitev posameznika, na katerega se nanašajo osebni podatki, kategorija (iii) pa se uporablja le, če obstaja tveganje, da bi pridobitev privolitve posameznika, na katerega se nanašajo osebni podatki, posegla v izvajanje takih nalog.

⁽²⁸⁾ Ob tem velja, da je na podlagi člena 23(1) zakona o varstvu osebnih informacij načeloma potrebna privolitev posameznika za razkritje podatkov tretji osebi. Tako ima posameznik nekaj nadzora nad uporabo svojih podatkov pri drugem poslovnem subjektu.

⁽²⁹⁾ V skladu s členom 15(1) zakona o varstvu osebnih informacij mora biti taka opredelitev „kolikor je mogoče natančna“.

⁽³⁰⁾ Člen 18(1) zakona o varstvu osebnih informacij.

- (46) Nadalje, kot je pojasnjeno v uvodnih izjavah 41 in 42, poslovni subjekt, ki obravnava osebne informacije, teh ne sme obdelovati za druge namene, razen če posameznik, na katerega se nanašajo osebni podatki, v to privoli ali če se uporablja ena od izjem iz člena 16(3) zakona o varstvu osebnih informacij.
- (47) Nazadnje, glede nadaljnega zagotavljanja osebnih informacij tretjim osebam⁽³¹⁾, člen 23(1) zakona o varstvu osebnih informacij omejuje tako razkritje na posebne primere, pri čemer velja splošno načelo, da je potrebna predhodna privolitev posameznika, na katerega se nanašajo osebni podatki⁽³²⁾. V členu 23(2), (3) in (4) zakona o varstvu osebnih informacij so navedene izjeme od zahteve za pridobitev privolitve. Vendar se te izjeme uporabljajo le za podatke, ki niso občutljivi, ter zahtevajo, da poslovni subjekt zadevne posameznike vnaprej obvesti o nameri razkriti njihove osebne informacije tretji osebi in o možnosti, da vsakršnemu naknadnemu razkritju ugovarjajo⁽³³⁾.
- (48) Glede prenosov iz Evropske unije je neizogibno, da bodo osebni podatki najprej zbrani in obdelani v EU v skladu z Uredbo (EU) 2016/679. To bo po eni strani vedno zajemalo zbiranje in obdelavo, tudi za prenos iz Evropske unije na Japonsko, na podlagi ene od pravnih podlag iz člena 6(1) Uredbe, po drugi strani pa zbiranje za določen, izrecen in zakonit namen ter prepoved nadaljnje obdelave, tudi prek prenosa, na način, ki ni združljiv s tem namenom, kot je določeno v členu 5(1)(b) in členu 6(4) Uredbe.
- (49) V skladu z dopolnilnim pravilom 3 bo moral po prenosu poslovni subjekt, ki obravnava osebne informacije in ki prejme podatke, „potrditi“ posebne namene, ki so podlaga za prenos (tj. namen, opredeljen na podlagi Uredbe (EU) 2016/679), in navedene podatke nadalje obdelovati v skladu s takimi nameni⁽³⁴⁾. To pomeni, da nameni, opredeljeni na podlagi Uredbe, zavezujejo prvotnega prejemnika osebnih podatkov na Japonskem in tudi vse naknadne prejemnike (vključno z skrbnikom).
- (50) Poleg tega v skladu s členom 16(1) zakona o varstvu osebnih informacij velja, da bi moral poslovni subjekt, ki obravnava osebne informacije, če želi spremeniti namen, kot je prvotno opredeljen na podlagi Uredbe (EU) 2016/679, načeloma pridobiti privolitev posameznika, na katerega se nanašajo osebni podatki. Brez take privolitve bi vsaka obdelava podatkov, ki bi presežala, kar je potrebno za doseganje navedenega namena uporabe, pomenila kršitev člena 16(1), ki bi jo lahko obravnavali komisija za varstvo osebnih informacij in sodišča.
- (51) Ker sta na podlagi Uredbe (EU) 2016/679 za prenos potrebna veljavna pravna podlaga in določen namen, ki se izražata v namenu uporabe, ki se „potrdi“ na podlagi zakona o varstvu osebnih informacij, torej kombinacija ustreznih določb zakona o varstvu osebnih informacij in dopolnilnega pravila 3 zagotavlja nadaljnjo zakonitost obdelave podatkov iz EU na Japonskem.

2.3.3 Točnost podatkov in načelo najmanjšega obsega

- (52) Podatki bi morali biti točni in po potrebi posodobljeni. Podatki bi morali biti tudi ustrezni, relevantni in ne bi smeli presežati namenov, za katere se obdelujejo.
- (53) Ta načela se v japonskem pravu zagotavljajo v členu 16(1) zakona o varstvu osebnih informacij, ki prepoveduje obravnavo osebnih informacij, ki bi presežala, „kar je potrebno za doseganje namena uporabe“. Kot je pojasnila komisija za varstvo osebnih informacij, to izključuje neustrezno in čezmerno uporabo podatkov (ki presega, kar je potrebno za doseganje namena uporabe) poleg tega pa tudi prepoveduje obravnavo podatkov, ki niso relevantni za doseganje namena uporabe.

⁽³¹⁾ Skrbniki so sicer za namene uporabe člena 23 (glej odstavke 5) izključeni iz pojma „tretja oseba“, se pa ta izključitev uporablja samo, kolikor skrbnik obravnava osebne podatke v mejah pooblastitve („v okviru potrebnega obsega za doseganje namena uporabe“), torej, kolikor deluje kot obdelovalec.

⁽³²⁾ Drugi (izredni) razlogi so: (i) zagotavljanje osebnih informacij „na podlagi zakonov in predpisov“; (ii) primeri, „v katerih je treba zaščititi človeško življenje, telo ali premoženje in je principalovo privolitev težko zagotoviti“; (iii) primeri, „v katerih obstaja posebna potreba po izboljšanju javne higiene ali spodbujanju zdravja otrok in je principalovo privolitev težko zagotoviti“ ter (iv) primeri, „v katerih je potrebno sodelovanje z organizacijo osrednje vlade ali lokalno vlado ali osebo, ki na podlagi njenega pooblastila opravlja z zakoni ali predpisi opredeljene naloge, in obstaja možnost, da bi pridobitev principalove privolitve posegla v izvajanje navedenih nalog“.

⁽³³⁾ Informacije, ki jih je treba zagotoviti, zajemajo predvsem kategorije osebnih podatkov, ki se bodo izmenjali s tretjo osebo, in metodo prenosa. Poleg tega mora poslovni subjekt, ki obravnava osebne informacije, posameznika, na katerega se nanašajo osebni podatki, obvestiti o možnosti nasprotovanja prenosu in o tem, kako tako zahtevo vložiti.

⁽³⁴⁾ V skladu s členom 26(1)(ii) zakona o varstvu osebnih informacij mora poslovni subjekt, ki obravnava osebne informacije, ob prejemu osebnih podatkov od tretje osebe „potrditi“ (preveriti) „podrobnosti o prejemu osebnih podatkov s strani tretje osebe“, vključno z namenom navedenega prejema. Čeprav v členu 26 ni izrecno navedeno, da mora poslovni subjekt, ki obravnava osebne informacije, nato upoštevati navedeni namen, pa je to izrecno navedeno v dopolnilnem pravilu 3.

- (54) Glede obveznosti zagotavljanja točnosti in posodobljenosti podatkov člen 19 zakona o varstvu osebnih informacij določa, da si mora poslovni subjekt, ki obravnava osebne informacije, „prizadevati za zagotavljanje točnosti in posodobljenosti osebnih podatkov, kolikor je to potrebno za doseganje namena uporabe“. Navedeno določbo bi bilo treba razumeti v povezavi s členom 16(1) zakona o varstvu osebnih informacij: na podlagi pojasnil komisije za varstvo osebnih informacij se šteje, da obdelava osebnih informacij ne dosega namena uporabe, če poslovni subjekt, ki obravnava osebne informacije, ne dosega predpisanih standardov točnosti, zato v takem primeru njihova obravnava postane nezakonita na podlagi člena 16(1).

2.3.4 Omejitev hrambe

- (55) Osebni podatki se načeloma ne bi smeli hraniti dlje, kot je potrebno za namene, za katere se obdelujejo.
- (56) V skladu s členom 19 zakona o varstvu osebnih informacij si morajo poslovni subjekti, ki obravnavajo osebne informacije, „prizadevati [...] za izbris osebnih podatkov brez odlašanja, ko taka uporaba ni več potrebna“. Navedeno določbo je treba razumeti v povezavi s členom 16(1) zakona o varstvu osebnih informacij, ki prepo-veduje obravnavo osebnih informacij, ki bi presegala, „kar je potrebno za doseganje namena uporabe“. Ko je dosežen namen uporabe, obdelava osebnih informacij ni več potrebna, zato se ne more nadaljevati (razen če poslovni subjekt, ki obravnava osebne informacije, pridobi privolitev posameznika, na katerega se nanašajo osebni podatki).

2.3.5 Varovanje podatkov

- (57) Osebni podatki bi se morali obdelovati tako, da se zagotavlja njihovo varovanje, kar zajema tudi zaščito pred nepooblaščenimi ali nezakonito obdelavo in pred nenamerno izgubo, uničenjem ali poškodovanjem. Zato bi morali poslovni subjekti sprejeti ustrezne tehnične ali organizacijske ukrepe za varovanje osebnih podatkov pred morebitnimi grožnjami. Navedene ukrepe bi bilo treba presoјati glede na najsodobnejšo tehnologijo in zadevne stroške.
- (58) To načelo je v japonskem pravu izvedeno v členu 20 zakona o varstvu osebnih informacij, ki določa, da poslovni subjekt, ki obravnava osebne informacije, „sprejme potrebne in ustrezne ukrepe za varnostni nadzor osebnih podatkov, kar vključuje preprečevanje uhajanja, izgube ali poškodovanja osebnih podatkov, ki jih obravnava“. V smernicah komisije za varstvo osebnih informacij so pojasnjeni ukrepi, ki se sprejmejo, vključno z metodami za opredelitev osnovnih politik, pravila glede obravnave podatkov in različni „nadzorni ukrepi“ (glede organizacijske varnosti ter glede človeške, fizične in tehnološke varnosti) ⁽³⁵⁾. Poleg tega smernice komisije za varstvo osebnih informacij in zadevno obvestilo (Dodatek 8 o „Vsebini ukrepov za upravljanje varnosti, ki jih je treba sprejeti“), ki ju je objavila komisija za varstvo osebnih informacij, vsebujejo več informacij o ukrepih glede varnostnih incidentov, ki vključujejo na primer uhajanje osebnih informacij, kot del ukrepov za upravljanje varnosti, ki jih mora sprejeti poslovni subjekt, ki obravnava osebne informacije ⁽³⁶⁾.
- (59) Nadalje, za namene nadzora varnosti mora biti na podlagi členov 20 in 21 zakona o varstvu osebnih informacij zagotovljen „potreben in ustrezen nadzor“ vedno, ko zaposleni ali podizvajalci obravnavajo osebne informacije. Nazadnje, v skladu s členom 83 zakona o varstvu osebnih informacij se namerno uhajanje ali kraja osebnih informacij kaznuje s kaznijo do enega leta zapora.

2.3.6 Preglednost

- (60) Posamezniki, na katere se nanašajo osebni podatki, bi morali biti obveščeni o glavnih značilnostih obdelave njihovih osebnih podatkov.
- (61) Poslovni subjekt, ki obravnava osebne informacije, mora na podlagi člena 18(1) zakona o varstvu osebnih informacij posamezniku, na katerega se nanašajo osebni podatki, dati na voljo informacije o namenu uporabe pridobljenih osebnih informacij, razen v „primerih, ko je bil namen uporabe vnaprej javno razkrit“. Enaka obveznost velja v primeru dovoljene spremembe namena (člen 18(3)). S tem je tudi zagotovljeno, da je posameznik, na katerega se nanašajo osebni podatki, obveščen o tem, da se njegovi podatki zbirajo. Čeprav zakon o varstvu osebnih informacij od poslovnega subjekta, ki obravnava osebne informacije, na splošno ne zahteva obveščanja posameznika, na katerega se nanašajo osebni podatki, o predvidenih prejemnikih osebnih informacij pri zbiranju, so take informacije nujni pogoj za vsako nadaljnje razkritje informacij tretji osebi (prejemniku) na podlagi člena 23(2), torej kadar se to opravi brez predhodne privolitve posameznika, na katerega se nanašajo osebni podatki.

⁽³⁵⁾ Smernice komisije za varstvo osebnih informacij (izdaja splošnih pravil), str. 41 in str. 86–98.

⁽³⁶⁾ V skladu z oddelkom 3-3-2 smernic komisije za varstvo osebnih informacij mora poslovni subjekt, ki obravnava osebne informacije, v primeru takega uhajanja, škode ali izgube izvesti potrebne preiskave ter zlasti oceniti obseg posega v pravice in interese posameznikov in naravo in število prizadetih osebnih informacij.

- (62) Glede „hranjenih osebnih podatkov“ člen 27 zakona o varstvu osebnih informacij določa, da poslovni subjekt, ki obravnava osebne informacije, posameznika, na katerega se nanašajo osebni podatki, obvesti o svoji identiteti (kontaktni podatki), namenu uporabe in postopkih za odgovor na zahtevo glede pravic posameznika, na katerega se nanašajo osebni podatki, na podlagi členov 28, 29 in 30 zakona o varstvu osebnih informacij.
- (63) Ker se na podlagi dopolnilnih pravil osebni podatki, preneseni iz Evropske unije, štejejo za „hranjene osebne podatke“ ne glede na trajanje njihove hrambe (razen če zanje veljajo izjeme), se zanje vedno uporabljajo zahteve glede preglednosti na podlagi obeh zgoraj navedenih določb.
- (64) Za zahteve iz člena 18 in obveznost obveščanja o namenu uporabe iz člena 27 zakona o varstvu osebnih informacij veljajo enake izjeme, ki večinoma temeljijo na pomislekih glede javnega interesa ter zaščite pravic in interesov posameznika, na katerega se nanašajo osebni podatki, tretjih oseb in upravljavca⁽³⁷⁾. V skladu z razlago iz smernic komisije za varstvo osebnih informacij se navedene izjeme uporabljajo v zelo posebnih primerih, ko bi na primer informacije o namenu uporabe lahko ovirale zakonite ukrepe, ki jih poslovni subjekt izvaja za zaščito nekaterih interesov (npr. boj zoper goljufije, gospodarsko vohunjenje, sabotaže).

2.3.7 Posebne kategorije podatkov

- (65) Glede obdelave „posebnih kategorij“ podatkov bi morali obstajati posebni zaščitni ukrepi.
- (66) „Osebne informacije, ki zahtevajo posebno skrb“, so opredeljene v členu 2(3) zakona o varstvu osebnih informacij. Navedena določba se nanaša na „osebne informacije o principalovi rasi, nazoru, družbenem položaju, zdravstveni anamnezi, kazenski evidenci, dejstvu, ali je kdaj utrpel škodo zaradi kaznivega dejanja, ali druge opise itd., ki so na podlagi vladne odredbe opredeljeni kot tisti, katerih obravnava zahteva posebno skrb, da principal ne utрпи nepoštene diskriminacije, predsodkov ali da ni drugače prikrajšan“. Te kategorije v veliki meri ustrezajo seznamu občutljivih podatkov iz členov 9 in 10 Uredbe (EU) 2016/679. Zlasti „zdravstvena anamneza“ ustreza podatkom o zdravstvenem stanju, „kazenska evidenca in dejstvo, ali je kdaj utrpel škodo zaradi kaznivega dejanja“ pa sta v bistvenem enaka kot kategorije iz člena 10 Uredbe (EU) 2016/679. Kategorije iz člena 2(3) zakona o varstvu osebnih informacij so nadalje razložene v vladni odredbi in smernicah komisije za varstvo osebnih informacij. V skladu s točko 8 oddelka 2.3 smernic komisije za varstvo osebnih informacij podkategorije „zdravstvene anamneze“ iz člena 2(ii) in (iii) vladne odredbe zajemajo genske in biometrične podatke. Čeprav seznam ne zajema izrecno pojmov, kot sta „etnično poreklo“ in „politično mnenje“, pa se sklicuje na „raso“ in „nazor“. Kot je pojasnjeno v točkah 1 in 2 oddelka 2.3 smernic komisije za varstvo osebnih informacij, sklic na „raso“ zajema „etnične vezi ali vezi z določenim delom sveta“, pojem „nazor“ pa zajema verska in politična prepričanja.
- (67) Kot izhaja iz besedila določbe, seznam ni izčrpen, saj je mogoče dodati nadaljnje kategorije podatkov, če je z njihovo obdelavo povezano tveganje „nepoštene diskriminacije, predsodkov ali drugačne prikrajšanosti principala“.
- (68) Čeprav je pojem „občutljivega“ podatka v bistvu družbeni konstrukt, saj temelji na kulturnih in pravnih tradicijah, moralnih pomislekih, izbirah politike itd. posamezne družbe, je Evropska komisija glede na pomen zagotavljanja ustreznih zaščitnih ukrepov za občutljive podatke pri njihovem prenosu poslovnim subjektom na Japonskem pridobila informacijo, da posebno varstvo „osebnih informacij, ki zahtevajo posebno skrb“, v okviru japonskega prava zajema vse kategorije „občutljivih podatkov“ iz Uredbe (EU) 2016/679. Zato dopolnilno pravilo 1 določa, da poslovni subjekti, ki obravnavajo osebne informacije, obdelajo podatke o posameznikovem spolnem življenju, spolni usmerjenosti ali članstvu v sindikatu, prenesene iz Evropske unije, „na enak način kot osebne informacije, ki zahtevajo posebno skrb, v smislu člena 2(3) [zakona o varstvu osebnih informacij]“.

⁽³⁷⁾ To so (i) primeri, v katerih obstaja možnost, da bi obveščanje posameznika, na katerega se nanašajo osebni podatki, o namenu uporabe ali javna objava namena uporabe lahko „škodovala življenju, telesu, premoženju ali drugim pravicam in interesom principala ali tretje osebe“ ali „pravicam ali zakonitim interesom [...] poslovnega subjekta, ki obravnava osebne informacije“; (ii) primeri, v katerih je „potrebno sodelovanje z organizacijo osrednje vlade ali lokalno vlado“ pri izvajanju njihovih zakonskih nalog, če bi take informacije ali razkritje posegalo v navedene „zadeve“; (iii) primeri, v katerih je namen uporabe jase iz okoliščin, v katerih so bili podatki pridobljeni.

- (69) Glede dodatnih materialnih zaščitnih ukrepov, ki se uporabljajo za osebne informacije, ki zahtevajo posebno skrb, poslovni subjekti, ki obravnavajo osebne informacije, v skladu s členom 17(2) zakona o varstvu osebnih informacij ne smejo pridobivati takih podatkov brez predhodne privolitve zadevnega posameznika, za kar veljajo le omejene izjeme⁽³⁸⁾. Nadalje, te kategorije osebnih informacij ni mogoče razkriti tretjim osebam na podlagi postopka iz člena 23(2) zakona o varstvu osebnih informacij (ki omogoča prenos podatkov tretjim osebam brez predhodne privolitve zadevnega posameznika).

2.3.8 Odgovornost

- (70) V skladu z načelom odgovornosti morajo subjekti, ki obdelujejo podatke, sprejeti ustrezne tehnične in organizacijske ukrepe, da lahko uspešno izpolnjujejo svoje obveznosti glede varstva podatkov in dokažejo tako skladnost, predvsem pristojnim nadzornim organom.
- (71) Kot je navedeno v sproti opombi 34 (uvodna izjava 49), morajo poslovni subjekti, ki obravnavajo osebne informacije, v skladu s členom 26(1) zakona o varstvu osebnih informacij preveriti identiteto tretje osebe, ki jim zagotavlja osebne podatke, in „okolščine“, v katerih je tretja oseba pridobila podatke (v primeru osebnih podatkov, ki jih zajema ta sklep, navedene okoliščine v skladu z zakonom o varstvu osebnih informacij in dopolnilnim pravilom 3 vključujejo dejstvo, da podatki izvirajo iz Evropske unije, ter namen izvirnega prenosa podatkov). Cilj navedenega ukrepa je med drugim zagotoviti zakonitost obdelave podatkov v celotni verigi poslovnih subjektov, ki obravnavajo osebne informacije. Nadalje, poslovni subjekti, ki obravnavajo osebne informacije, morajo na podlagi člena 26(3) zakona o varstvu osebnih informacij voditi evidenco datuma prejema in (obveznih) informacij, ki jih prejmejo od tretje osebe na podlagi odstavka 1, ter ime zadevnega posameznika (na katerega se nanašajo osebni podatki), kategorije podatkov, ki se obdelujejo, in kolikor je ustrezno, dejstvo, da je posameznik, na katerega se nanašajo osebni podatki, privolil v izmenjavo svojih osebnih podatkov. V skladu s členom 18 pravilnika komisije za varstvo osebnih informacij se morajo navedene evidence hraniti za obdobje najmanj enega do treh let, odvisno od okoliščin. Komisija za varstvo osebnih informacij lahko pri izvrševanju svojih nalog zahteva predložitev takih evidenc⁽³⁹⁾.
- (72) Poslovni subjekti, ki obravnavajo osebne informacije, morajo hitro in ustrezno obravnavati pritožbe zadevnih posameznikov glede obdelave njihovih osebnih informacij. Za lajšanje obravnave pritožb vzpostavijo „sistem, ki je potreben za doseganje [tega] namena“, kar pomeni, da morajo v svoji organizaciji vzpostaviti ustrezne postopke (npr. opredeliti odgovornost ali zagotoviti kontaktno točko).
- (73) Nazadnje, zakon o varstvu osebnih informacij je okvir za sodelovanje sektorskih organizacij na področju industrije pri zagotavljanju visoke stopnje skladnosti (glej poglavje IV, oddelek 4). Vloga takih akreditiranih organizacij za varstvo osebnih informacij⁽⁴⁰⁾ je spodbujati varstvo osebnih informacij s podporo podjetjem prek njihovega strokovnega znanja, pa tudi s prispevkom k izvajanju zaščitnih ukrepov, predvsem z obravnavo pritožb posameznikov in pomočjo pri reševanju s tem povezanih sporov. V ta namen lahko od sodelujočih poslovnih subjektov, ki obravnavajo osebne informacije, po potrebi zahtevajo sprejetje potrebnih ukrepov⁽⁴¹⁾. Poleg tega poslovni subjekti, ki obravnavajo osebne informacije, v primeru kršitve varnosti podatkov ali drugih varnostnih incidentov načeloma obvestijo komisijo za varstvo osebnih informacij in posameznika, na katerega se nanašajo osebni podatki, (ali javnost) ter sprejmejo potrebne ukrepe, vključno z ukrepi za zmanjšanje kakršne koli škode in preprečitev ponovitve podobnih incidentov⁽⁴²⁾. Čeprav so navedeno prostovoljne sheme, je imela 10. avgusta 2017 komisija za varstvo osebnih informacij na seznamu 44 organizacij, od katerih ima samo največja, japonski center za

⁽³⁸⁾ Izjeme so: (i) „primeri na podlagi zakonov in predpisov“; (ii) „primeri, v katerih je treba zaščititi človeško življenje, telo ali premoženje in je principalovo privolitev težko zagotoviti“; (iii) „primeri, v katerih obstaja posebna potreba po izboljšanju javne higiene ali spodbujanju zdravja otrok in je principalovo privolitev težko zagotoviti“; (iv) „primeri, v katerih je potrebno sodelovanje z organizacijo osrednje vlade ali lokalno vladno ali osebo, ki na podlagi njunega pooblastila opravlja z zakoni ali predpisi opredeljene naloge, in obstaja možnost, da bi pridobitev principalove privolitve posegla v izvajanje navedenih nalog“; in (v) primeri, v katerih navedene osebne informacije, ki zahtevajo posebno skrb, javnosti razkrije posameznik, na katerega se nanašajo osebni podatki, vladna organizacija, lokalna vlada, oseba, ki spada v eno od kategorij iz člena 76(1) ali druge osebe, navedene v pravilih komisije za varstvo osebnih informacij. Nadaljnja kategorija zajema „druge primere, ki so na podlagi vladne odredbe, opredeljeni kot enakovredni primerom, navedenim v vsaki od predhodnih postavk“, ki na podlagi sedanje vladne odredbe zajema predvsem opazne značilnosti osebe (npr. vidno zdravstveno stanje), če so bili občutljivi podatki (nenamerno) pridobljeni z vidno zaznavo, snemanjem ali fotografiranjem posameznika, na katerega se nanašajo osebni podatki, na primer s kamerami sistema televizije zaprtega kroga (CCTV).

⁽³⁹⁾ V skladu s členom 40(1) zakona o varstvu osebnih informacij lahko komisija za varstvo osebnih informacij, če je to potrebno za izvajanje zadevnih določb zakona o varstvu osebnih informacij, od poslovnega subjekta, ki obravnava osebne informacije, zahteva predložitev potrebnih informacij ali gradiva, ki se nanaša na obravnavo osebnih informacij.

⁽⁴⁰⁾ Zakon o varstvu osebnih informacij med drugim vsebuje pravila o akreditaciji takih organizacij; glej člene 47–50 zakona.

⁽⁴¹⁾ Člen 52 zakona o varstvu osebnih informacij.

⁽⁴²⁾ Obvestilo komisije za varstvo osebnih informacij št. 1/2017 „O ukrepih, ki jih je treba sprejeti v primeru kršitve varnosti osebnih podatkov ali drugega incidenta“.

obdelavo informacij in razvoj, 15 436 sodelujočih poslovnih subjektov⁽⁴³⁾. Akreditirane sheme vključujejo sektorska združenja, kot so na primer japonsko združenje posrednikov pri prodaji vrednostnih papirjev, japonsko združenje šol vožnje ali združenje ženitnih posrednikov⁽⁴⁴⁾.

- (74) Akreditirane organizacije za varstvo osebnih informacij predložijo letna poročila o svojem delovanju. Iz „Pregleda stanja izvajanja zakona o varstvu osebnih informacij v poslovnem letu 2015“, ki ga je objavila komisija za varstvo osebnih informacij, so akreditirane organizacije za varstvo osebnih informacij skupaj prejele 442 pritožb, od poslovnih subjektov v okviru svoje pristojnosti zahtevale 123 pojasnil, od navedenih poslovnih subjektov zahtevale dokumente v 41 zadevah, izdale 181 navodil in dve priporočili⁽⁴⁵⁾.

2.3.9 Omejitve nadaljnjih prenosov podatkov

- (75) Raven varstva, ki se zagotavlja osebnim podatkom, prenesenim iz Evropske unije poslovnim subjektom na Japonskem, se ne sme poslabšati z nadaljnjim prenosom takih podatkov prejemnikom v tretji državi zunaj Japonske. Taki „nadaljnji prenosi“ podatkov, ki z vidika japonskega poslovnega subjekta pomenijo mednarodni prenos z Japonske, bi morali biti dovoljeni le, kadar tudi za nadaljnega prejemnika zunaj Japonske veljajo pravila, ki zagotavljajo podobno raven varstva, kot je zagotovljena v okviru japonskega pravnega reda.
- (76) Prvo varstvo vsebuje člen 24 zakona o varstvu osebnih informacij, ki na splošno prepoveduje prenos osebnih podatkov tretji osebi zunaj ozemlja Japonske brez predhodne privolitve zadevnega posameznika. Dopolnilno pravilo 4 zagotavlja, da je v primeru prenosa podatkov iz Evropske unije taka privolitve res dobro premišljena, saj se zahteva, da se zadevnemu posamezniku „zagotovijo informacije o okoliščinah prenosa, ki principalu omogočajo sprejete odločitve o svoji privolitvi“. Na tej podlagi bo posameznik, na katerega se nanašajo osebni podatki, obveščen o tem, da bodo podatki preneseni v tujino (zunaj področja uporabe zakona o varstvu osebnih informacij) in o specifični namembni državi. To mu bo omogočilo, da oceni tveganje za zasebnost, ki je povezano s prenosom. Kot je mogoče sklepati iz člena 23 zakona o varstvu osebnih informacij (glej uvodno izjavo 47), bi morale poleg tega informacije, predložene principalu, zajemati obvezne postavke iz odstavka 2 tega člena, in sicer kategorije osebnih podatkov, ki se zagotavljajo tretji osebi, in metodo razkritja.
- (77) Člen 24 zakona o varstvu osebnih informacij v povezavi s členom 11-2 pravilnika komisije za varstvo osebnih informacij določa več izjem k temu pravilu na podlagi privolitve. Nadalje, v skladu s členom 24 se tudi za mednarodne prenose podatkov uporabljajo enake izjeme kot na podlagi člena 23(1) zakona o varstvu osebnih informacij⁽⁴⁶⁾.
- (78) Dopolnilno pravilo 4 krepi raven varstva pri nadaljnjih prenosih takih podatkov od poslovnega subjekta, ki obravnava osebne informacije, do prejemnika v tretji državi, da se zagotovi stalnost varstva v primeru prenosa osebnih podatkov iz Evropske unije na Japonsko na podlagi tega sklepa. To doseže z omejevanjem in uokvirjanjem podlag za mednarodne prenose, ki jih poslovni subjekt, ki obravnava osebne informacije, lahko uporabi kot alternativo privolitvi. Podrobneje in brez poseganja v izjeme iz člena 23(1) zakona o varstvu osebnih informacij je mogoče osebne podatke, ki se prenašajo na podlagi tega sklepa, brez privolitve nadalje prenesti le v dveh primerih: (i) če se podatki pošiljajo v tretjo državo, za katero je komisija za varstvo osebnih informacij na podlagi člena 24 zakona o varstvu osebnih informacij ugotovila, da zagotavlja enakovredno raven varstva, kot se zagotavlja na Japonskem⁽⁴⁷⁾; ali (ii) če sta poslovni subjekt, ki obravnava osebne informacije, in prejemnik kot tretja oseba na podlagi pogodbe, druge vrste zavezujočega sporazuma ali zavezujočega dogovora znotraj skupine podjetij skupaj sprejela ukrepe, ki zagotavljajo raven varstva, enakovredno tisti na podlagi zakona o varstvu osebnih informacij v povezavi z dopolnilnimi pravili. Druga kategorija ustreza instrumentom na podlagi Uredbe (EU) 2016/679 za zagotavljanje ustreznih zaščitnih ukrepov (zlasti pogodbeno določila in zavezujoča poslovna pravila). Poleg tega, kot je potrdila komisija za varstvo osebnih informacij, tudi v teh primerih za prenos še vedno veljajo splošna pravila, ki veljajo za kakršno koli zagotavljanje osebnih podatkov tretji osebi v skladu z zakonom o varstvu osebnih informacij (tj. zahteva po pridobitvi privolitve iz člena 23(1) ali, alternativno, zahteva po informacijah

⁽⁴³⁾ Na podlagi podatkov, objavljenih na spletišču PrivacyMark japonskega centra za obdelavo informacij in razvoj z dne 2. oktobra 2017.

⁽⁴⁴⁾ Komisija za varstvo osebnih informacij, seznam akreditiranih organizacij za varstvo osebnih informacij je na spletu na voljo na naslovu: <https://www.ppc.go.jp/personal/nintei/list/> ali https://www.ppc.go.jp/files/pdf/nintei_list.pdf

⁽⁴⁵⁾ Komisija za varstvo osebnih informacij, Pregled stanja izvajanja zakona o varstvu osebnih informacij v poslovnem letu 2015 (oktober 2016), na voljo (le v japonščini) na spletnem naslovu: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf

⁽⁴⁶⁾ Glej sprotno opombo 32.

⁽⁴⁷⁾ V skladu s členom 11 pravilnika komisije za varstvo osebnih informacij se torej zahtevajo materialni standardi, enakovredni zakonu o varstvu osebnih informacij, ki jih učinkovito nadzoruje neodvisni organ izvrševanja, poleg tega pa tudi zagotovitev izvajanja ustreznih pravil v tretji državi.

z možnostjo zavrnitve iz člena 23(2) zakona o varstvu osebnih informacij). Če s posameznikom, na katerega se nanašajo osebni podatki, ni mogoče stopiti v stik niti s prošnjo za privolitev niti za posredovanje zahtevanih predhodnih informacij v skladu s členom 23(2) zakona o varstvu osebnih informacij, se prenos ne sme opraviti.

- (79) Poleg primerov, v katerih je komisija za varstvo osebnih informacij ugotovila, da zadevna tretja država zagotavlja raven varstva, enakovredno tisti, ki jo zagotavlja zakon o varstvu osebnih informacij⁽⁴⁸⁾, zahteve iz dopolnilnega pravila 4 izključujejo uporabo instrumentov prenosa, ki ne vzpostavljajo zavezujočega odnosa med japonskim izvoznikom podatkov in uvoznikom podatkov iz tretje države ter ne zagotavljajo zahtevane ravni varstva. To velja na primer za sistem skupine APEC za pravila o varovanju zasebnosti pri čezmejnem prenosu podatkov (CBPR), v katerem je Japonska eno od sodelujočih gospodarstev⁽⁴⁹⁾, saj v navedenem sistemu varstvo ne izhaja iz zavezujočega dogovora med izvoznikom in uvoznikom v smislu njunega dvostranskega odnosa ter je očitno nižje ravni od tiste, ki se zagotavlja s kombinacijo zakona o varstvu osebnih informacij in dopolnilnih pravil⁽⁵⁰⁾.
- (80) Nazadnje, nadaljnji zaščitni ukrep v primeru (nadaljnega) prenosa izhaja iz členov 20 in 22 zakona o varstvu osebnih informacij. V skladu s temi določbami mora poslovni subjekt, ki obravnava osebne informacije (izvoznik podatkov), zagotoviti nadzor nad subjektom iz tretje države (uvoznikom podatkov), ki deluje v imenu prvega kot obdelovalec ali podrejeni obdelovalec, glede varnosti obdelave podatkov.

2.3.10 Pravice posameznikov

- (81) Zakon o varstvu osebnih informacij tako kot pravo EU o varstvu podatkov posameznikom podeljuje več izvršljivih pravic. To vključuje pravico do dostopa („razkritja“), popravka in izbrisa ter pravico do ugovora („prenehanja uporabe“).
- (82) Najprej, posameznik, na katerega se nanašajo osebni podatki, ima na podlagi člena 28(1) in (2) zakona o varstvu osebnih informacij pravico od poslovnega subjekta, ki obravnava osebne informacije, zahtevati „razkritje hranjenih osebnih podatkov, na podlagi katerih ga je mogoče identificirati“, navedeni poslovni subjekt pa po prejemu take zahteve „razkrije hranjene osebne podatke“ navedenemu posamezniku. Člen 29 (pravica do popravka) in člen 30 (pravica do prenehanja uporabe) imata enako strukturo kot člen 28.
- (83) Člen 9 vladne odredbe opredeljuje, da se razkritje osebnih informacij, kot je navedeno v členu 28(2) zakona o varstvu osebnih informacij, opravi pisno, razen če se poslovni subjekt, ki obravnava osebne informacije, in posameznik, na katerega se nanašajo osebni podatki, ne dogovorita drugače.
- (84) Za navedene pravice veljajo tri vrste omejitev, ki se nanašajo na pravice in interese posameznika ali tretje osebe⁽⁵¹⁾, resne posege v poslovanje subjekta, ki obravnava osebne informacije⁽⁵²⁾, ter primere, v katerih bi razkritje pomenilo kršitev drugih zakonov ali predpisov⁽⁵³⁾. Primeri, v katerih bi se navedene omejitve uporabljale, so podobne nekaterim izjemam iz člena 23(1) Uredbe (EU) 2016/679, ki omogoča omejitev pravic posameznikov iz

⁽⁴⁸⁾ Do zdaj komisija za varstvo osebnih informacij še ni sprejela nobene odločitve na podlagi člena 24 zakona o varstvu osebnih informacij, s katero bi se priznalo, da tretja država zagotavlja raven varstva, ki je enakovredna tisti, ki jo zagotavlja Japonska. Edina odločitev, o katere sprejetju trenutno razmišlja, se nanaša na EGP. Kar zadeva morebitne druge odločitve v prihodnosti, bo Komisija pozorno spremljala razmere in po potrebi sprejela ustrezne ukrepe za obravnavo morebitnih škodljivih učinkov na stalnost varstva (glej uvodne izjave 176, 177, 184 in člen 3(1)).

⁽⁴⁹⁾ Samo dve japonski družbi sta se registrirali na podlagi sistema skupine APEC za pravila o varovanju zasebnosti pri čezmejnem prenosu podatkov (glej https://english.jpipdec.or.jp/sp/protection_org/cbpr/list.html). Zunaj Japonske so edini drugi poslovni subjekti, ki so se registrirali po tem sistemu, maloštevilne (23) družbe iz ZDA (glej <https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list>).

⁽⁵⁰⁾ Manjkajo na primer opredelitve in posebno varstvo občutljivih podatkov in obveznost omejene hrambe podatkov. Glej tudi mnenje št. 02/2014 Delovne skupine za varstvo podatkov iz člena 29 o referenčnem dokumentu za zahteve za zavezujoča poslovna pravila, predložena nacionalnim organom za varstvo podatkov v EU, in pravila o varovanju zasebnosti pri čezmejnem prenosu podatkov, predložena odgovornim zastopnikom skupine APEC za pravila o varovanju zasebnosti pri čezmejnem prenosu podatkov z dne 6. marca 2014.

⁽⁵¹⁾ Po mnenju komisije za varstvo osebnih informacij lahko omejitev upravičujejo le taki interesi, ki jih je „smiselno pravno zaščititi“. Ocenjuje se, da je treba opraviti za posamične primere „ob upoštevanju poseganja v pravico do zasebnosti, vključno z varstvom podatkov, kakor je priznано z ustavo in sodno prakso.“ Zaščiteni interesi lahko na primer vključujejo trgovinske ali druge poslovne skrivnosti.

⁽⁵²⁾ Koncept „resnega posega v ustrezno izvajanje poslovanja poslovnega subjekta“ je v smernicah komisije za varstvo osebnih informacij opisan na podlagi več primerov, na primer ponavljajoče se in enake zapletene zahteve istega posameznika, ki pomenijo znatno breme za poslovni subjekt in ki lahko vpliva na njegovo zmožnost odzivanja na druge zahteve (smernice komisije za varstvo osebnih informacij (izdaja splošnih pravil) str. 62). Na splošno je komisija za varstvo osebnih informacij potrdila, da je ta kategorija omejena na izjemne primere, ki presegajo zgolj nevšečnost. Poslovni subjekt, ki obravnava osebne informacije, zlasti ne more zavrniti razkritja zgolj zato, ker se je zahtevala velika količina podatkov.

⁽⁵³⁾ Kot je potrdila komisija za varstvo osebnih informacij, morajo taki zakoni spoštovati pravico do zasebnosti, kakor jo zagotavlja ustava, in tako „odražati potrebno in razumno omejitev“.

razlogov, ki se nanašajo na „varstvo posameznikov, na katere se nanašajo osebni podatki, ali pravice in svoboščine drugih“ ali „druge pomembne cilje v splošnem javnem interesu“. Čeprav se zdi kategorija primerov, v katerih bi razkritje pomenilo kršitev „drugih zakonov ali predpisov“, široka, morajo zakoni in predpisi, ki v tem smislu določajo omejitve, upoštevati ustavno pravico do zasebnosti, zato se lahko omejitve ujavajo le, če bi uveljavljanje te pravice pomenilo „poseg v javno dobrobit“⁽⁵⁴⁾. To zahteva presojo nasprotnih si interesov.

- (85) Člen 28(3) zakona o varstvu osebnih informacij določa, da če zahtevani podatki ne obstajajo ali če se zadevni poslovni subjekt, ki obravnava osebne informacije, odloči zavrnil dostop do hranjenih podatkov, mora o tem takoj obvestiti posameznika.
- (86) Drugič, posameznik, na katerega se nanašajo osebni podatki, ima na podlagi člena 29(1) in (2) zakona o varstvu osebnih informacij pravico zahtevati popravek, dodatek ali izbris svojih hranjenih osebnih podatkov, če so podatki netočni. Poslovni subjekt, ki obravnava osebne informacije, ob prejemu take zahteve „izvede potrebno preiskavo“ in na njeni podlagi „opravi popravek itd. vsebine hranjenih podatkov“.
- (87) Tretjič, posameznik, na katerega se nanašajo osebni podatki, ima na podlagi člena 30(1) in (2) zakona o varstvu osebnih informacij pravico od poslovnega subjekta, ki obravnava osebne informacije, zahtevati prenehanje uporabe osebnih informacij ali njihov izbris, če se te obravnavajo v nasprotju s členom 16 (glede omejitve namena) ali če so bile neustrezno pridobljene v nasprotju s členom 17 zakona o varstvu osebnih informacij (glede pridobitve na podlagi prevare, na druge neustrezne načine ali, v primeru občutljivih podatkov, brez privolitve). Prav tako ima posameznik na podlagi člena 30(3) in (4) zakona o varstvu osebnih informacij pravico od poslovnega subjekta, ki obravnava osebne informacije, zahtevati, da ta neha zagotavljati informacije tretji osebi, če se s tem kršijo določbe člena 23(1) ali člena 24 zakona o varstvu osebnih informacij (glede zagotavljanja tretjim osebam, vključno z mednarodnimi prenosi).
- (88) Če je zahteva utemeljena, poslovni subjekt, ki obravnava osebne informacije, brez odlašanja neha uporabljati podatke ali jih neha zagotavljati tretji osebi, če je to potrebno, da se odpravi kršitev ali (če za navedeni primer velja izjema, predvsem če bi prenehanje uporabe povzročilo posebno visoke stroške)⁽⁵⁵⁾ da se izvedejo potrebni alternativni ukrepi za zaščito pravic in interesov zadevnega posameznika.
- (89) Za razliko od prava EU zakon o varstvu osebnih informacij in zadevna podzakonska pravila ne vsebujejo pravnih določb, ki bi se posebej nanašale na možnost nasprotovanja obdelavi za namene neposrednega trženja. Vendar bo takšna obdelava v okviru področja uporabe tega sklepa vedno potekala v okviru prenosa osebnih podatkov, ki so bili predhodno zbrani v Evropski uniji. Na podlagi člena 21(2) Uredbe (EU) 2016/679 ima posameznik, na katerega se nanašajo osebni podatki, vedno možnost nasprotovati prenosu podatkov za namen obdelave za neposredno trženje. Poleg tega, kot je pojasnjeno v uvodni izjavi 43, mora poslovni subjekt, ki obravnava osebne informacije, na podlagi dopolnilnega pravila 3 podatke, prejete na podlagi tega sklepa, obdelati za isti namen, kot so bili preneseni iz Evropske unije, razen če posameznik, na katerega se nanašajo osebni podatki, privoli v spremembo namena uporabe. Če je bil torej prenos izveden za kateri koli drug namen razen neposrednega trženja, poslovni subjekt, ki obravnava osebne informacije, na Japonskem ne bo smel obdelovati podatkov za neposredno trženje brez privolitve posameznika iz EU, na katerega se nanašajo osebni podatki.
- (90) V vseh primerih iz členov 28 in 29 zakona o varstvu osebnih informacij mora poslovni subjekt, ki obravnava osebne informacije, posameznika brez odlašanja obvestiti o rezultatu njegove zahteve in obrazložiti vsako (delno) zavrnitev na podlagi zakonskih izjem iz členov 27–30 (člen 31 zakona o varstvu osebnih informacij).

⁽⁵⁴⁾ Vrhovno sodišče je člen 13 ustave razlagalo kot pravico do zasebnosti (glej zgoraj uvodni izjavi 7 in 8). Čeprav je mogoče to pravico omejiti v primerih, kadar „posega v javno dobrobit“, je vrhovno sodišče v sodbi z dne 6. marca 2008 (glej uvodno izjavo 8) pojasnilo, da mora biti vsaka omejitev (ki v tem primeru dovoljuje javnemu organu zbiranje in obdelavo osebnih podatkov) uravnotežena glede na pravico do zasebnosti, in sicer ob upoštevanju dejavnikov, kot so narava zadevnih podatkov, tveganja, ki jih obdelava teh podatkov povzroča za posameznike, veljavni zaščitni ukrepi in koristi javnega interesa, ki izhajajo iz obdelave. To je zelo podobno tehtanju, ki se zahteva za odobritev kakršnih koli omejitev pravic in zaščitnih ukrepov glede varstva podatkov v skladu s pravom EU na podlagi načel potrebnosti in sorazmernosti.

⁽⁵⁵⁾ Podrobnejšo razlago navedenih izjem vsebuje komentar revidiranega zakona o varstvu osebnih informacij po posameznih členih, ki ga je pripravil profesor Katsuya Uga, 2015, str. 217. Primer zahteve, ki bi „povzročila velike stroške“, je, če se samo nekatera imena na dolgem seznamu (npr. v imeniku) obdelujejo v nasprotju z načelom omejitve namena, imenik pa je že v prodaji ter bi odpoklic njegovih izvodov in njihova zamenjava z novimi povzročila velike stroške. „Prenehanje uporabe bi bilo težko izvesti“ tudi, če bi bilo že prodanih veliko izvodov imenika in bi bilo nemogoče spet zbrati vse. V navedenih primerih bi lahko „potreben alternativni ukrep“ zajemal tudi objavo ali razširjanje obvestila o popravku. Tak ukrep ne izključuje drugih oblik (sodnega) varstva bodisi zaradi kršitve pravic do zasebnosti bodisi zaradi škodovanja ugledu (obrekovanje) z objavo bodisi zaradi kršitve drugih interesov.

- (91) Glede pogojev za vložitev zahteve člen 32 zakona o varstvu osebnih informacij (v povezavi z vladno odredbo) omogoča poslovnemu subjektu, ki obravnava osebne informacije, da opredeli razumne postopke, vključno z določbami o informacijah, ki so potrebne za identifikacijo hranjenih osebnih podatkov. Vendar v skladu z odstavkom 4 tega člena poslovni subjekti, ki obravnavajo osebne informacije, ne smejo „principalu“ naložiti „pretiranega bremena“. V nekaterih primerih lahko poslovni subjekt, ki obravnava osebne informacije, zahteva tudi plačilo pristojbine, če njen znesek „ne presega tistega, kar je razumno glede na dejanske stroške“ (člen 33 zakona o varstvu osebnih informacij).
- (92) Nazadnje, posameznik lahko nasprotuje zagotavljanju svojih osebnih informacij tretji osebi na podlagi člena 23(2) zakona o varstvu osebnih informacij ali odreče privolitve na podlagi člena 23(1) (s čimer prepreči razkritje, če ni na voljo druge pravne podlage). Podobno lahko posameznik ustavi obdelavo podatkov za drug namen z zavrnitvijo privolitve na podlagi člena 16(1) zakona o varstvu osebnih informacij.
- (93) Za razliko od prava EU zakon o varstvu osebnih informacij in zadevna podzakonska pravila ne vsebujejo splošnih določb, ki bi se nanašale na odločitve, ki vplivajo na posameznika, na katerega se nanašajo osebni podatki, in ki temeljijo le na samodejni obdelavi osebnih podatkov. Vendar je to vprašanje obravnavano v nekaterih sektorskih pravilih, ki se uporabljajo na Japonskem in ki so še zlasti upoštevna za to vrsto obdelave. To zajema sektorje, v katerih družbe najverjetneje uporabljajo samodejno obdelavo osebnih podatkov za sprejemanje odločitev, ki vplivajo na posameznike (npr. finančni sektor). „Celovite smernice za nadzor nad večjimi bankami“, revidirane junija 2017, na primer zahtevajo, da se zadevnemu posamezniku zagotovijo podrobna pojasnila o razlogih za zavrnitev zahteve za sklenitev posojilne pogodbe. Navedena pravila torej zagotavljajo varstvo v najverjetneje omejenem številu primerov, v katerih samodejno odločitev sprejme sam „uvozni“ japonski poslovni subjekt (in ne „izvozni“ upravljavec podatkov iz EU).
- (94) Vsekakor pa glede osebnih podatkov, zbranih v Evropski uniji, velja, da vse odločitve, ki temeljijo na samodejni obdelavi, po navadi sprejme upravljavec podatkov v Uniji (ki je v neposrednem razmerju z zadevnim posameznikom, na katerega se nanašajo osebni podatki), zato se zanj uporablja Uredba (EU) 2016/679 ⁽⁵⁶⁾. To zajema tudi primere prenosa, v katerih obdelavo izvede tuji (npr. japonski) poslovni subjekt, ki deluje kot zastopnik (obdelovalec) v imenu upravljavca podatkov iz EU (ali kot podrejeni obdelovalec, ki deluje v imenu obdelovalca iz EU, ki je podatke prejel od upravljavca podatkov iz EU, ki jih je zbral) in ki na tej podlagi sprejme odločitev. Dejstvo, da zakon o varstvu osebnih informacij ne vsebuje posebnih pravil o samodejnem odločanju, torej najverjetneje ne bo vplivalo na raven varstva osebnih podatkov, ki se prenašajo na podlagi tega sklepa.

2.4 Nadzor in izvajanje

2.4.1 Neodvisen nadzor

- (95) Vzpostaviti bi bilo treba neodvisen nadzorni organ s pristojnostjo spremljanja in zagotavljanja skladnosti s pravili o varstvu podatkov, da se tudi v praksi zagotovi ustrezna raven varstva podatkov. Pri izvajanju svojih obveznosti in pooblastil bi moral ta organ ravnati popolnoma neodvisno in nepristransko.
- (96) Na Japonskem je organ, pristojen za spremljanje in izvajanje zakona o varstvu osebnih informacij, komisija za varstvo osebnih informacij. Sestavljajo jo predsednik in osem članov, ki jih imenuje predsednik vlade ob soglasju obeh domov parlamenta. Mandat predsednika in vsakega člana traja pet let, z možnostjo ponovnega imenovanja (člen 64 zakona o varstvu osebnih informacij). Člane je mogoče razrešiti le iz utemeljenih razlogov, na podlagi omejenega števila izjemnih okoliščin ⁽⁵⁷⁾; član prav tako ne sme biti dejavno vključen v politične dejavnosti. Poleg tega člani v skladu z zakonom o varstvu osebnih informacij ne smejo opravljati nobenih drugih plačanih dejavnosti ali poslovnih dejavnosti. Za vse člane veljajo tudi notranja pravila, ki jim preprečujejo sodelovanje v razpravah v primeru morebitnega navzkrižja interesov. Komisiji za varstvo osebnih informacij pomaga sekretariat, ki ga vodi generalni sekretar in ki je bil ustanovljen z namenom izvajanja nalog, dodeljenih komisiji za varstvo osebnih informacij (člen 70 zakona o varstvu osebnih informacij). Člane in vse uradnike v sekretariatu zavezujejo stroga pravila molčečnosti (člen 72 in 82 zakona o varstvu osebnih informacij).

⁽⁵⁶⁾ Nasprotno pa velja, da so izjemni primeri, v katerih ima japonski upravljavec neposreden odnos s posameznikom, na katerega se nanašajo osebni podatki, v EU, po navadi posledica tega, da se je navedeni upravljavec v Evropski uniji ciljno usmeril na posameznika s ponudbo blaga ali storitev ali s spremljanjem njegovega vedenja. V takem primeru se za samega japonskega upravljavca uporablja Uredba (EU) 2016/679 (člen 3(2)), zato mora neposredno zagotoviti skladnost s pravom EU o varstvu podatkov.

⁽⁵⁷⁾ V skladu s členom 65 zakona o varstvu osebnih informacij je mogoče člana proti njegovi volji razrešiti le na podlagi enega od naslednjih razlogov: (i) začetek stečajnega postopka; (ii) obsodba zaradi kršitve zakona o varstvu osebnih informacij ali zakona o uporabi številčnih kod za identifikacijo posameznika; (iii) obsodba na zaporno kazen brez prisilnega dela ali na strožjo kazen; (iv) nezmožnost opravljanja dolžnosti zaradi duševne ali fizične motnje ali neprimerne ravnanja.

- (97) Pristojnosti komisije za varstvo osebnih informacij, ki jih izvaja popolnoma samostojno⁽⁵⁸⁾, so večinoma določene v členih 40, 41 in 42 zakona o varstvu osebnih informacij. Komisija za varstvo osebnih informacij lahko na podlagi člena 40 od poslovnega subjekta, ki obravnava osebne informacije, zahteva poročilo ali predložitev dokumentov o dejanjih obdelave, lahko pa izvede tudi inšpekcijski pregled na lokaciji ali pregled evidenc in drugih dokumentov. Komisija za varstvo osebnih informacij lahko poslovnim subjektom, ki obravnavajo osebne informacije, zagotovi tudi smernice ali nasvete glede obravnave osebnih informacij, če je to potrebno za izvajanje zakona o varstvu osebnih informacij. Komisija za varstvo osebnih informacij je to pristojnost na podlagi člena 41 zakona o varstvu osebnih informacij že uporabila pri izdaji smernic podjetju Facebook po razkritjih v primeru Facebook/Cambridge Analytica.
- (98) Komisija za varstvo osebnih informacij ima v posameznih primerih predvsem pristojnost izdaje priporočil in odredb (na podlagi pritožbe ali svoje pobude), s ciljem izvrševanja zakona o varstvu osebnih informacij in drugih zavezujočih pravil (vključno z dopolnilnimi pravili). Navedena pristojnost je navedena v členu 42 zakona o varstvu osebnih informacij. Čeprav odstavka 1 in 2 navedenega člena določata dvostopenjski mehanizem, na podlagi katerega lahko komisija za varstvo osebnih informacij izda odredbo (le) po izdaji predhodnega priporočila, odstavka 3 omogoča neposredno sprejetje odredbe v nujnih primerih.
- (99) Čeprav v členu 42(1) (kjer je opredeljeno tudi področje uporabe člena 42(2)) niso navedene vse določbe poglavja IV, oddelka 1 zakona o varstvu osebnih informacij, je to mogoče razložiti z dejstvom, da se nekatere od navedenih določb ne nanašajo na obveznosti poslovnih subjektov, ki obravnavajo osebne informacije⁽⁵⁹⁾, in da je vse bistveno varstvo že zagotovljeno z drugimi določbami, vključenimi na navedeni seznam. Primer je člen 15 (ki zahteva, da poslovni subjekt, ki obravnava osebne informacije, opredeli namen uporabe in zadevne osebne informacije obdeluje izključno v navedenem okviru): čeprav ni naveden, se lahko na podlagi njegovega neupoštevanja izda priporočilo na podlagi kršitve člena 16(1) (prepoved poslovnemu subjektu, ki obravnava osebne informacije, obdelovati osebne informacije zunaj okvira, potrebnega za doseganje namena uporabe, razen na podlagi privolitve posameznika, na katerega se nanašajo osebni podatki)⁽⁶⁰⁾. Druga določba, ki ni navedena v členu 42(1), je člen 19 zakona o varstvu osebnih informacij o točnosti in hrambi podatkov. Neskladnost z navedeno določbo je mogoče obravnavati kot kršitev člena 16(1) ali kršitev člena 29(2), če zadevni posameznik zahteva popravek ali izbris napačnih ali odvečnih podatkov, poslovni subjekt, ki obravnava osebne informacije, pa zahtevo zavrne. Glede pravic posameznika, na katerega se nanašajo osebni podatki, na podlagi členov 28(1), 29(1) in 30(1) je nadzor komisije za varstvo osebnih informacij zagotovljen s podelitvijo pristojnosti komisiji za varstvo osebnih informacij glede ustreznih obveznosti poslovnih subjektov, ki obravnavajo osebne informacije, iz navedenih členov.
- (100) V skladu s členom 42(1) zakona o varstvu osebnih informacij lahko komisija za varstvo osebnih informacij, če meni, da „je treba zaščititi pravice in interese posameznika, kadar [poslovni subjekt, ki obravnava osebne informacije,] krši“ posamezne določbe zakona o varstvu osebnih informacij, izda priporočilo o „prenehanju kršitve ali drugih potrebnih ukrepih za odpravo kršitve“. Tako priporočilo ni zavezujoče, omogoča pa izdajo zavezujoče odredbe na podlagi člena 42(2) zakona o varstvu osebnih informacij. Na podlagi te določbe lahko komisija za varstvo osebnih informacij, če priporočilo „brez utemeljenega razloga“ ni upoštevano ter sama „meni, da je resna kršitev pravic in interesov posameznika neizogibna“, odredi poslovnemu subjektu, ki obravnava osebne informacije, naj ukrepa v skladu s priporočilom.
- (101) Dopolnilna pravila nadalje pojasnjujejo in krepijo pristojnosti izvajanja komisije za varstvo osebnih informacij. Podrobneje, če poslovni subjekt, ki obravnava osebne informacije, v primerih uvoza podatkov iz Evropske unije brez zakonitega razloga ne ukrepa v skladu s priporočilom komisije za varstvo osebnih informacij na podlagi člena 42(1) zakona o varstvu osebnih informacij, komisija za varstvo osebnih informacij to vedno šteje za resno in takojšnjo kršitev posameznikovih pravic in interesov v smislu člena 42(2), kar je podlaga za izdajo zavezujoče odredbe. Poleg tega komisija za varstvo osebnih informacij kot „zakoniti razlog“ za neupoštevanje priporočila sprejme samo „izredni dogodek, na katerega [poslovni subjekt, ki obravnava osebne informacije,] nima vpliva, ga ne more razumno predvideti (npr. primer naravne nesreče) in ki [mu onemogoča upoštevanje priporočila]“, ali primere, v katerih ni več potrebe po ukrepanju na podlagi priporočila, „saj je [poslovni subjekt, ki obravnava osebne informacije,] sprejel alternativne ukrepe, ki povsem odpravljajo kršitev“.

⁽⁵⁸⁾ Glej člen 62 zakona o varstvu osebnih informacij.

⁽⁵⁹⁾ Nekatere določbe se na primer nanašajo na prostovoljne ukrepe poslovnih subjektov, ki obravnavajo osebne informacije (člena 32 in 33 zakona o varstvu osebnih informacij), ali obveznosti „prizadevanja po najboljših močeh“, ki same po sebi niso izvršljive (členi 31, 35, 36(6) in 39 zakona o varstvu osebnih informacij). Nekatere določbe niso naslovljene na poslovne subjekte, ki obravnavajo osebne informacije, ampak na druge akterje. To velja na primer za člena 23(4) in 26(2) ter člen 34 zakona o varstvu osebnih informacij (vendar je izvrševanje člena 26(2) zakona o varstvu osebnih informacij zagotovljeno z možnostjo kazenskih sankcij na podlagi člena 88(i) zakona o varstvu osebnih informacij).

⁽⁶⁰⁾ Poleg tega velja, kot je razloženo zgoraj v uvodni izjavi 48, da v okviru prenosa „namen uporabe“ opredeli izvoznik podatkov iz EU, ki ga pri tem zavezujejo obveznosti na podlagi člena 5(1)(b) Uredbe (EU) 2016/679. Navedena obveznost je izvršljiva prek pristojnega organa za varstvo podatkov v Evropski uniji.

- (102) V skladu s členom 84 zakona o varstvu osebnih informacij se neupoštevanje odredbe komisije za varstvo osebnih informacij šteje za kaznivo dejanje in poslovni subjekt, ki obravnava osebne informacije in je spoznan za krivega, se lahko kaznuje z zaporno kaznijo s prisilnim delom do največ šest mesecev ali z globo v višini do 300 000 jenov. Nadalje, v skladu s členom 85(i) zakona o varstvu osebnih informacij se nesodelovanje s komisijo za varstvo osebnih informacij ali oviranje njene preiskave kaznuje z globo do največ 300 000 jenov. Te kazenske sankcije se uporabljajo poleg sankcij, ki se lahko naložijo za materialne kršitve zakona o varstvu osebnih informacij (glej uvodno izjavo 108).

2.4.2 Sodno varstvo

- (103) Posameznik, na katerega se nanašajo osebni podatki, mora imeti na voljo učinkovito upravno in sodno varstvo, vključno z odškodnino za škodo, da se zagotovi ustrezno varstvo in zlasti izvajanje pravic posameznika.
- (104) Posameznik se lahko odloči, da bo pred vložitvijo zahteve za upravno ali sodno varstvo oziroma namesto take zahteve vložil pritožbo glede obdelave svojih osebnih podatkov pri samem upravljavcu. Poslovni subjekt, ki obravnava osebne informacije, si v skladu s členom 35 zakona o varstvu osebnih informacij prizadeva take pritožbe obravnavati „ustrezno in hitro“ ter v ta namen ustanovi notranje sisteme obravnave pritožb. Poleg tega je v skladu s členom 61(ii) zakona o varstvu osebnih informacij komisija za varstvo osebnih informacij odgovorna za „potrebno mediacijo glede vložene pritožbe in sodelovanje s poslovnim subjektom, ki obravnava pritožbo“, kar v obeh primerih vključuje pritožbe, ki jih vložijo tujci. V zvezi s tem je japonski zakonodajalec osrednji vladi podelil tudi nalogo sprejetja „potrebnih ukrepov“, da se poslovnim subjektom, ki obravnavajo osebne informacije, omogoči in olajša obravnava pritožb (člen 9), lokalne vlade pa si morajo v takem primeru prizadevati za zagotovitev mediacije (člen 13). Posamezniki lahko torej vložijo pritožbo pri enem od več kot 1 700 centrov za pomoč potrošnikom, ki so jih ustanovile lokalne vlade na podlagi zakona o varstvu potrošnikov ⁽⁶¹⁾, poleg tega pa lahko pritožbo vložijo tudi pri nacionalnem japonskem centru za zadeve potrošnikov. Take pritožbe se lahko vložijo tudi glede kršitev zakona o varstvu osebnih informacij. Na podlagi člena 19 splošnega zakona o potrošnikih ⁽⁶²⁾ si lokalne vlade v primerih pritožb prizadevajo za izvedbo mediacije in strankam zagotovijo potrebno strokovno znanje. Navedeni mehanizmi reševanja sporov so se izkazali za zelo učinkovite, saj je bilo v letu 2015 od 75 000 primerov pritožb uspešno rešenih 91,2 %.
- (105) Če poslovni subjekt, ki obravnava osebne informacije, krši določbe zakona o varstvu osebnih informacij, je to lahko podlaga za civilno tožbo, pa tudi za uvedbo kazenskega postopka in izrek sankcije. Najprej, če posameznik meni, da so bile njegove pravice na podlagi členov 28, 29 in 30 zakona o varstvu osebnih informacij kršene, lahko zahteva sodno odredbo tako, da od sodišča zahteva, naj poslovnemu subjektu, ki obravnava osebne informacije, dredi izpolnitev njegove zahteve na podlagi ene od navedenih določb, tj. razkrije hranjene osebne podatke (člen 28), popravi netočne hranjene osebne podatke (člen 29) ali preneha z nezakonito obdelavo oziroma zagotavljanjem podatkov tretji osebi (člen 30). Tako tožbo je mogoče vložiti brez sklicevanja na člen 709 civilnega zakonika ⁽⁶³⁾ ali brez drugečnega sklicevanja na odškodninsko pravo ⁽⁶⁴⁾. To zlasti pomeni, da posamezniku ni treba dokazati škode.
- (106) Drugič, če se domnevna kršitev ne nanaša na pravice posameznika iz členov 28, 29 in 30, ampak na splošna načela in obveznosti poslovnega subjekta, ki obravnava osebne informacije, glede varstva podatkov, lahko zadevni posameznik vložijo civilno tožbo zoper poslovni subjekt na podlagi odškodninskih določb japonskega civilnega zakonika, zlasti člena 709. V okviru tožbe na podlagi člena 709 je treba poleg krivde (naklepa ali malomarnosti) dokazati tudi škodo, v skladu s členom 710 civilnega zakonika pa je lahko taka škoda materialna ali nematerialna. Višina nadomestila ni omejena.
- (107) Glede razpoložljivih nadomestil se člen 709 japonskega civilnega zakonika nanaša na denarno odškodnino. Vendar se ta člen v japonski sodni praksi razlaga tudi tako, da zagotavlja pravico do pridobitve odredbe ⁽⁶⁵⁾. Če posameznik, na katerega se nanašajo osebni podatki, vložijo tožbo na podlagi člena 709 civilnega zakonika in trdi, da so njegove pravice ali interesi utrpeli škodo zaradi kršitve določbe zakona o varstvu osebnih informacij s strani toženca, lahko navedeni zahtevek poleg nadomestila za škodo zajema tudi zahtevo za izdajo sodne odredbe o prepovedi kakršne koli nezakonite obdelave.

⁽⁶¹⁾ Zakon št. 50 z dne 5. junija 2009.

⁽⁶²⁾ Zakon št. 60 z dne 22. avgusta 2012.

⁽⁶³⁾ Člen 709 civilnega zakonika je glavna pravna podlaga civilnih odškodninskih tožb. V skladu z navedeno določbo je „oseba, ki namerno ali iz malomarnosti krši kakršne koli pravice drugih ali pravno zaščitene interese drugih, odškodninsko odgovorna za vsakršno posledično škodo“.

⁽⁶⁴⁾ Višje sodišče v Tokiu, sodba z dne 20. maja 2015 (ni objavljena); okrožno sodišče v Tokiu, sodba z dne 8. septembra 2014, Westlaw Japonska 2014WLJPCA09088002. Glej tudi člen 34(1) in (3) zakona o varstvu osebnih informacij.

⁽⁶⁵⁾ Glej sodbo vrhovnega sodišča z dne 24. septembra 2002 (zbirka odločb Hanrei Times, zvezek 1106, str. 72).

- (108) Tretjič, poleg pravnih sredstev na podlagi civilnega (odškodninskega prava) lahko posameznik, na katerega se nanašajo osebni podatki, vloži pritožbo pri državnem tožilcu ali uradniku pravosodne policije glede kršitev zakona o varstvu osebnih informacij, ki lahko imajo za posledico kazensko sankcijo. Poglavje VII zakona o varstvu osebnih informacij vsebuje več kazenskih določb. Najpomembnejša (člen 84) se nanaša na neupoštevanje odredb komisije za varstvo osebnih informacij v skladu s členom 42(2) in (3) s strani poslovnega subjekta, ki obravnava osebne informacije. Če poslovni subjekt ne upošteva odredbe, ki jo izda komisija za varstvo osebnih informacij, lahko predsednik navedene komisije (ali kateri koli drug vladni uradnik) ⁽⁶⁶⁾ zadevo preda državnemu tožilcu ali uradniku pravosodne policije in s tem začne kazenski postopek. Za kršitev odredbe komisije za varstvo osebnih informacij je zagrožena zaporna kazen s prisilnim delom do največ šest mesecev ali globa do največ 300 000 jenov. Druge določbe zakona o varstvu osebnih informacij, ki določajo sankcije v primeru kršitev navedenega zakona in se nanašajo na pravice in interese posameznikov, na katere se nanašajo osebni podatki, zajemajo člen 83 zakona o varstvu osebnih informacij (glede „tajne uporabe ali zagotavljanja“ podatkovne zbirke osebnih informacij „z namenom nezakonitega pridobivanja [...] dobička“) in člen 88(i) zakona o varstvu osebnih informacij (če tretja oseba ustrezno ne obvesti poslovnega subjekta, ki obravnava osebne informacije, ko ta prejme osebne podatke v skladu s členom 26(1) zakona o varstvu osebnih informacij, zlasti o podrobnostih predhodne pridobitve takih podatkov s strani tretje osebe). Za navedene kršitve zakona o varstvu osebnih informacij so zagrožene naslednje kazni: zaporna kazen s prisilnim delom do največ enega leta ali globa do največ 500 000 jenov (v primeru člena 83) oziroma upravna globa do največ 100 000 jenov (v primeru člena 88(i)). Medtem bo imela že grožnja kazenske sankcije verjetno močan odvračilni učinek na poslovodne organe, ki upravljajo postopke obdelave pri poslovnem subjektu, ki obravnava osebne informacije, ter na posameznike, ki obravnavajo podatke, člen 87 zakona o varstvu osebnih informacij pojasnjuje, da se, kadar zastopnik, zaposleni ali drugi delavec podjetja krši člene 83 do 85 zakona o varstvu osebnih informacij, „storilec kaznuje, navedeni pravni osebi pa se naloži denarna kazen, kakor je določena v ustreznih členih“. V tem primeru se lahko tako zaposlenemu kot podjetju naložijo sankcije do višine celotnega najvišjega zneska.
- (109) Nazadnje, posamezniki lahko zahtevajo pravno varstvo tudi zoper dejanja ali neukrepanje komisije za varstvo osebnih informacij. V tem smislu japonsko pravo omogoča več načinov upravnega in sodnega varstva.
- (110) Če posameznik ni zadovoljen z ukrepanjem komisije za varstvo osebnih informacij, lahko na podlagi zakona o upravnih pravnih sredstvih vloži upravno pritožbo ⁽⁶⁷⁾. Nasprotno, če posameznik meni, da bi komisija za varstvo osebnih informacij morala ukrepati, vendar ni, lahko posameznik na podlagi člena 36-3 navedenega zakona od komisije za varstvo osebnih informacij zahteva ukrepanje ali izdajo upravnih smernic, če meni, da „ukrepi ali upravne smernice, potrebni za odpravo kršitve, niso bili sprejeti ali izdani“.
- (111) Glede sodnega varstva velja, da lahko na podlagi zakona o upravnem sporu posameznik, ki ni zadovoljen z upravnim ukrepanjem komisije za varstvo osebnih informacij, vloži tožbo *mandamus* ⁽⁶⁸⁾ in od sodišča zahteva, naj komisiji za varstvo osebnih informacij odredi nadaljnje ukrepe ⁽⁶⁹⁾. V nekaterih primerih lahko sodišče izda tudi začasno odredbo *mandamus*, da se prepreči nepopravljiva škoda ⁽⁷⁰⁾. Nadalje, na podlagi istega zakona lahko posameznik zahteva razveljavitev odločbe komisije za varstvo osebnih informacij ⁽⁷¹⁾.
- (112) Nazadnje, posameznik lahko na podlagi člena 1(1) zakona o nadomestilih države s tožbo zoper komisijo za varstvo osebnih informacij zahteva tudi nadomestilo države, če je navedeni posameznik utrpel škodo zaradi nezakonite odredbe, ki jo je komisija za varstvo osebnih informacij izdala poslovnemu subjektu, ali ker navedena komisija ni izvršila svojih pooblastil.

3. DOSTOP DO OSEBNIH PODATKOV, KI JIH IZ EVROPSKE UNIJE PRENESEJO JAVNI ORGANI NA JAPONSKEM, IN NJIHOVA UPORABA

- (113) Evropska komisija je proučila tudi omejitve in zaščitne ukrepe, vključno z nadzorom in posameznimi mehanizmi pravnih sredstev, ki so na voljo v japonskem pravu glede zbiranja in naknadne uporabe osebnih podatkov, ki jih v javnem interesu (zlasti za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in nacionalne varnosti („vladni dostop“) poslovnim subjektom na Japonskem prenašajo javni organi. V tem smislu je japonska vlada Evropski komisiji predložila uradne navedbe, zagotovila in zaveze, podpisane na najvišji ministrski in agencijski ravni, ki jih vsebuje Priloga II k temu sklepu.

⁽⁶⁶⁾ Člen 239(2) zakonika o kazenskem postopku.

⁽⁶⁷⁾ Zakon št. 160 iz leta 2014.

⁽⁶⁸⁾ Člen 37-2 zakona o upravnem sporu.

⁽⁶⁹⁾ V skladu s členom 3(6) zakona o upravnem sporu se pojem „tožba *mandamus*“ nanaša na tožbo, s katero se od sodišča zahteva izdaja odredbe zoper upravno agencijo, na podlagi katere mora ta izvesti prvotni upravni ukrep, ki „bi“ ga morala izvesti, vendar ga ni.

⁽⁷⁰⁾ Člen 37-5 zakona o upravnem sporu.

⁽⁷¹⁾ Poglavje II, oddelek 1 zakona o upravnem sporu.

3.1 Splošni pravni okvir

- (114) V okviru izvajanja javnih pooblastil mora biti vladni dostop na Japonskem izveden ob popolnem upoštevanju zakona (načelo zakonitosti). V tem smislu japonska ustava vsebuje določbe, ki omejujejo in uokvirjajo zbiranje osebnih podatkov s strani javnih organov. Kot je bilo že navedeno glede obdelave s strani poslovnih subjektov, je vrhovno sodišče Japonske s sklicevanjem na člen 13 ustave, ki med drugim štiti pravico do svobode, priznalo pravico do zasebnosti in varstva podatkov ⁽⁷²⁾. Eden od pomembnih vidikov navedene pravice je svoboda preprečiti razkritje osebnih informacij tretji osebi brez privolitve ⁽⁷³⁾. Iz tega izhaja pravica do učinkovitega varstva osebnih podatkov zoper zlorabo in (zlasti) nezakonit dostop. Dodatno varstvo zagotavlja člen 35 ustave o pravici vseh oseb do zaščite v njihovem domu, do zaščite dokumentov in osebnih predmetov, ki od javnih organov zahteva pridobitev sodnega naloga na podlagi „ustreznega razloga“ ⁽⁷⁴⁾ v vseh primerih „iskanja in zasega“. Vrhovno sodišče je v sodbi z dne 15. marca 2017 (zadeva GPS) pojasnilo, da se zahteva glede navedenega naloga uporablja, kadar koli vlada poseže („vstopi“) v zasebno sfero na način, ki prevlada nad voljo posameznika, in sicer z „obvezno preiskavo“. Sodnik lahko tak nalog izda le na podlagi konkretnega suma kaznivega dejanja, tj. na podlagi listinskih dokazov, iz katerih je mogoče sklepati, da je oseba, na katero se nanaša preiskava, storila kaznivo dejanje ⁽⁷⁵⁾. Japonski organi torej nimajo pravne podlage za zbiranje osebnih informacij z obveznimi sredstvi v primerih, ko pravo še ni bilo kršeno ⁽⁷⁶⁾, na primer za preprečitev kaznivega dejanja ali druge varnostne grožnje (kot na primer v primerih preiskav na podlagi nacionalne varnosti).
- (115) Na podlagi načela zakonske podlage mora imeti vsako zbiranje podatkov kot del prisilne preiskave posebno pooblastilo v zakonu (kot je to izraženo na primer v členu 197(1) zakonika o kazenskem postopku (ZKP) glede obveznega zbiranja informacij za kazensko preiskavo). Ta zahteva se nanaša tudi na dostop do elektronskih informacij.
- (116) Pomembno je, da člen 21(2) ustave zagotavlja tajnost vseh komunikacijskih sredstev, omejitve tega pa so mogoče samo z zakonodajo na podlagi javnega interesa. Ta zahteva zaupnosti je na ravni zakona izvedena v členu 4 zakona o telekomunikacijskih podjetjih, ki prepoveduje kršenje tajnosti telekomunikacij, ki jih upravlja izvajalec telekomunikacijskih storitev. To se razlaga kot prepoved razkritja komunikacijskih informacij, razen ob privolitvi uporabnikov ali na podlagi ene od izrecnih izjem od kazenske odgovornosti na podlagi kazenskega zakonika ⁽⁷⁷⁾.
- (117) Ustava zagotavlja tudi pravico do sodnega varstva (člen 32) in pravico do vložitve odškodninske tožbe zoper državo, če je posameznik utrpel škodo zaradi nezakonitega dejanja javnega uslužbenca (člen 17).
- (118) Posebno glede pravice do varstva podatkov so v poglavju III, oddelkih 1, 2 in 3 zakona o varstvu osebnih informacij opredeljena osnovna načela, ki zajemajo vse sektorje, vključno z javnim sektorjem. Natančneje, člen 3 zakona o varstvu osebnih informacij določa, da je treba vse osebne informacije obravnavati v skladu z načelom spoštovanja osebnosti posameznikov. Ko javni organi zberejo („pridobijo“) osebne informacije, tudi kot del elektronske evidence ⁽⁷⁸⁾, njihovo obravnavo ureja zakon o varstvu osebnih informacij, ki jih hranijo upravni

⁽⁷²⁾ Glej na primer sodbo vrhovnega sodišča z dne 12. septembra 2003 (št. zadeve: 1656 (2002 (Ju)). Vrhovno sodišče je zlasti navedlo, da „vsak posameznik lahko svobodno štiti svoje osebne informacije pred razkritjem tretji osebi ali javnosti, če za tako razkritje ni dobrega razloga“.

⁽⁷³⁾ Sodba vrhovnega sodišča z dne 6. marca 2008 (Juki-net).

⁽⁷⁴⁾ „Ustrezní razlog“ obstaja le, če se domneva, da je zadevni posameznik (osumljenec, obtoženec) storil kaznivo dejanje ter da sta iskanje in zaseg potrebna za izvedbo kazenske preiskave. Glej sodbo vrhovnega sodišča z dne 18. marca 1969, zadeva št. 100 (1968 (Shi)).

⁽⁷⁵⁾ Glej člen 156(1) pravilnika o kazenskem postopku.

⁽⁷⁶⁾ Opozoriti je treba, da zakon o kaznovanju organiziranega kriminala in nadzoru nad premoženjsko koristjo z dne 15. junija 2017 opredeljuje novo kaznivo dejanje, s katerim se kriminalizira priprava terorističnih dejanj in nekaterih drugih vrst organiziranega kriminala. Preiskava se lahko začne le v primeru konkretnega suma na podlagi dokazov, da so izpolnjeni vsi trije potrebni pogoji za opredelitev kaznivega dejanja (vpletenost hudodelske združbe, „načrtovanje“ in „priprava na izvedbo“ kaznivega dejanja). Glej na primer tudi člene 38–40 zakona o preprečevanju subverzivnih dejavnosti (zakon št. 240 z dne 21. julija 1952).

⁽⁷⁷⁾ Člen 15(8) smernic o varstvu osebnih informacij v sektorju telekomunikacij.

⁽⁷⁸⁾ Upravni organi so opredeljeni v členu 2(1) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi. V skladu z informacijami, ki jih je poslala japonska vlada, vsi javni organi, razen prefekturne policije, spadajo v okvir „upravnih organov“. Hkrati prefekturna policija deluje v pravnem okviru prefekturnih odlokov o varstvu osebnih informacij (glej člen 11 zakona o varstvu osebnih informacij in osnovno politiko), v katerih so določbe o varstvu osebnih informacij enakovredne tistim v zakonu o varstvu osebnih informacij, ki jih hranijo upravni organi. Glej Prilogo II, oddelek I.B. Kot je pojasnila komisija za varstvo osebnih informacij, morajo biti v skladu z „osnovno politiko“ ti odloki sprejeti na podlagi vsebine zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, pri čemer ministrstvo za notranje zadeve izdaja obvestila, v katerih lokalnim upravam v zvezi s tem daje potrebna navodila. Kot je poudarila komisija za varstvo osebnih informacij, je treba „v vsaki prefekturi [...] v tem okviru [...] sprejeti odlok o varstvu osebnih informacij [...] na podlagi osnovne politike in vsebine obvestil.“

organi⁽⁷⁹⁾. To načeloma vključuje⁽⁸⁰⁾ tudi obdelavo osebnih informacij za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali nacionalne varnosti. Zakon o varstvu osebnih informacij, ki jih hranijo upravni organi, med drugim določa, da javni organi: (i) lahko hranijo osebne informacije le, kolikor je to potrebno za izvajanje njihovih dolžnosti; (ii) ne smejo takih informacij uporabiti za „nepravičen“ namen ali jih neutemeljeno razkriti tretji osebi; (iii) morajo opredeliti namen in ga ne smejo spreminjati bolj, kot je razumno ustrezno glede na izvirni namen (omejitev namena); (iv) načeloma ne smejo uporabiti ali tretji osebi predložiti hranjenih osebnih informacij za druge namene in morajo določiti omejitve glede namena ali metode uporabe pri tretjih osebah, če se jim to zdi potrebno; (v) si prizadevajo zagotoviti točnost informacij (kakovost podatkov); (vi) sprejmejo potrebne ukrepe za ustrezno upravljanje informacij in preprečevanje uhajanj, izgube ali škode (varnost podatkov) ter (vii) si prizadevajo za ustrezno in hitro obravnavo vseh pritožb glede obdelave informacij⁽⁸¹⁾.

3.2 Dostop in uporaba s strani japonskih javnih organov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

- (119) Japonsko pravo vsebuje več omejitev dostopa in uporabe osebnih podatkov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ob tem pa tudi mehanizme nadzora in pravnih sredstev, ki zagotavljajo zadostne zaščitne ukrepe za učinkovito varstvo navedenih podatkov zoper nezakonito vmešavanje in tveganje zlorabe.

3.2.1 Pravna podlaga in omejitve/zaščitni ukrepi, ki se uporabljajo

- (120) V japonskem pravnem okviru je zbiranje elektronskih informacij za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj dovoljeno na podlagi naloga (obvezno zbiranje) ali prošnje za prostovoljno razkritje.

3.2.1.1 Obvezna preiskava na podlagi sodnega naloga

- (121) Kot je navedeno v uvodni izjavi 115, je za vsako zbiranje podatkov kot del prisilne preiskave potrebno posebno pooblastilo v zakonu, izvesti pa ga je mogoče le na podlagi sodnega naloga, ki se „izda na podlagi ustreznega razloga“ (člen 35 ustave). Glede preiskave kaznivih dejanj je ta zahteva izražena v določbah zakonika o kazenskem postopku. V skladu s členom 197(1) zakonika o kazenskem postopku se obvezni ukrepi „ne uporabljajo, razen če ta zakonik vsebuje posebne določbe“. Glede zbiranja elektronskih informacij sta edini upoštevni⁽⁸²⁾ pravni podlagi v tem smislu člen 218 zakonika o kazenskem postopku (iskanje in zaseg) ter člen 222-2 zakonika o kazenskem postopku, v skladu s katerim se obvezni ukrepi za prestrežanje elektronskih komunikacij brez privolitve katere koli stranke izvedejo na podlagi drugih aktov, predvsem zakona o prisluškovanju telefonskim pogovorom za potrebe kazenske preiskave (zakon o prisluškovanju telefonskim pogovorom). V obeh primerih je potrebna izdaja naloga.
- (122) Natančneje, na podlagi člena 218(1) zakonika o kazenskem postopku lahko državni tožilec, njegov pomočnik ali uradnik pravosodne policije izvede iskanje ali zaseg (vključno z naročilom evidenc) na podlagi naloga, ki ga vnaprej izda sodnik⁽⁸³⁾, če je to potrebno za preiskavo kaznivega dejanja. Tak nalog med drugim vsebuje ime osumljenca ali obtoženca, očitano kaznivo dejanje⁽⁸⁴⁾, elektromagnetne evidence, ki jih je treba zaseči, in „kraj ali predmete“, ki jih je treba pregledati (člen 219(1) zakonika o kazenskem postopku).

⁽⁷⁹⁾ Osebne informacije, ki jih pridobijo uradniki upravnih organov v okviru izvajanja svojih dolžnosti in ki jih za potrebe organizacijske uporabe hrani navedeni upravni organ, spadajo v okvir „hranjenih osebnih informacij“ v smislu člena 2(3) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, če so navedeni v „upravnih dokumentih“. To zajema elektronske informacije, ki jih zbirajo in nadalje obdelujejo taki organi, saj opredelitev pojma „upravni dokumenti“ v členu 2(2) zakona o dostopu do informacij, ki jih hranijo upravni organi, (zakon št. 42 iz leta 1999) zajema elektromagnetne evidence.

⁽⁸⁰⁾ Vendar pa je v skladu s členom 53-2 zakonika o kazenskem postopku uporaba poglavja IV zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, izvzeta glede „dokumentov, ki se nanašajo na sojenja“, kar na podlagi prejetih informacij zajema elektronske informacije, pridobljene na podlagi naloga ali zahteve za prostovoljno sodelovanje kot del kazenske preiskave. Enako velja glede informacij, zbranih na področju nacionalne varnosti, saj se posamezniki ne morejo uspešno sklicevati na svoje pravice na podlagi zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, če ima vodja javnega organa „utemeljene razloge“ za mnenje, da bi razkritje „lahko škodovalo nacionalni varnosti“ (glej člen 14(iv)). Ob tem velja, da morajo javni organi omogočiti vsaj delno razkritje, kadar koli je to mogoče (člen 15).

⁽⁸¹⁾ Glej posamezne sklice na zakon o varstvu osebnih informacij, ki jih hranijo upravni organi, v Prilogi II, oddelek II.A.1)(b)(2).

⁽⁸²⁾ Medtem ko člen 220 zakonika o kazenskem postopku omogoča iskanje in zaseg „na kraju samem“ brez naloga, ko državni tožilec, pomočnik državnega tožilca ali uradnik pravosodne policije aretira osumljenca/očitnega storilca, to ne velja v primeru prenosa in s tem za potrebe tega sklepa.

⁽⁸³⁾ V skladu s členom 222(1) v povezavi s členom 110 zakonika o kazenskem postopku, je treba nalog za iskanje/zaseg evidenc pokazati osebi, zoper katero se ukrep izvaja.

⁽⁸⁴⁾ Glej tudi člen 189(2) zakonika o kazenskem postopku, v skladu s katerim pravosodni policist opravi preiskavo storilca in zadevnih dokazov, „ko meni, da je bilo storjeno kaznivo dejanje“. Podobno člen 155(1) pravilnika o kazenskem postopku zahteva, da mora pisna zahteva za izdajo naloga med drugim vsebovati „očitano kaznivo dejanje“ in „povzetek dejanskega stanja“.

- (123) Glede prestrezanja komunikacij člen 3 zakona o prisluškovanju telefonskim pogovorom take ukrepe omogoča le na podlagi strogih zahtev. Javni organi morajo zlasti predhodno pridobiti sodni nalog, ki se lahko izda le za preiskavo nekaterih hudih kaznivih dejanj (navedenih v prilogi k zakonu) ⁽⁸⁵⁾ in ko je „izredno težko identificirati storilca ali pojasniti okoliščine/podrobnosti storitve na drug način“ ⁽⁸⁶⁾. V skladu s členom 5 zakona o prisluškovanju telefonskim pogovorom se nalog izda za omejeno obdobje, sodnik pa lahko določi dodatne pogoje. Poleg tega zakon o prisluškovanju telefonskim pogovorom zagotavlja številna dodatna jamstva, kot so na primer potrebna navzočnost prič (člena 12 in 20), prepoved prisluškovanja telefonskim pogovorom nekaterih privilegiranih skupin (npr. zdravnikov, odvetnikov) (člen 15), obveznost prenehanja prisluškovanja telefonskim pogovorom, če ni več upravičeno, in sicer tudi v obdobju veljavnosti naloga (člen 18), ali splošna zahteva po obvestilu zadevnega posameznika in omogočanju dostopa do evidenc v tridesetih dneh po prenehanju prisluškovanja telefonskim pogovorom (člena 23 in 24).
- (124) Za namene vseh obveznih ukrepov, ki temeljijo na nalogu, se lahko izvaja le preiskava, „ki je potrebna za doseganje njenega cilja“ – tj. da ciljev preiskave ni mogoče doseči drugače (člen 197(1) zakonika o kazenskem postopku). Čeprav merila za opredeljevanje tega, kar je potrebno, v zakonodaji niso nadalje določena, je vrhovno sodišče Japonske razsodilo, da mora sodnik, ki izdaja nalog, opraviti splošno presojo in upoštevati zlasti (i) težo kaznivega dejanja in način storitve; (ii) vrednost in pomen gradiva, ki se zasega kot dokazno sredstvo; (iii) verjetnost (tveganje) prikritja ali uničenja dokazov; in (iv) v kolikšni meri bi zaseg lahko imel posledice za zadevnega posameznika ⁽⁸⁷⁾.

3.2.1.2 Prošnja za prostovoljno razkritje na podlagi „lista za poizvedbo“

- (125) Javni organi lahko v okviru svojih pooblastil elektronske informacije zbirajo tudi na podlagi prošenj za prostovoljno razkritje. To se nanaša na neobvezno obliko sodelovanja, pri kateri upoštevanje zahteve ni izvršljivo ⁽⁸⁸⁾, zaradi česar javnim organom ni treba pridobiti sodnega naloga.
- (126) Če je taka zahteva naslovljena na poslovni subjekt in se nanaša na osebne informacije, mora poslovni subjekt izpolniti zahteve zakona o varstvu osebnih informacij. V skladu s členom 23(1) zakona o varstvu osebnih informacij lahko poslovni subjekti osebne informacije razkrijejo tretjim osebam brez privolitve zadevnega posameznika le v nekaterih primerih, kar obsega tudi primere, v katerih razkritje „temelji na zakonih in predpisih“ ⁽⁸⁹⁾. Na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj je pravna podlaga za take zahteve navedena v členu 197(2) zakonika o kazenskem postopku, v skladu s katerim „se lahko od zasebnih organizacij zahteva poročanje o potrebnih vprašanih glede preiskave“. Ker je „list za poizvedbo“ dovoljen le kot del kazenske preiskave, je zanj vedno potreben konkreten sum že storjenega kaznivega dejanja ⁽⁹⁰⁾. Poleg tega velja, da ker take preiskave po navadi izvaja prefekturna policija, se uporabljajo omejitve iz člena 2(2) zakona o policiji ⁽⁹¹⁾. V skladu z navedeno določbo so dejavnosti policije „strogo omejene“ na izpolnjevanje obveznosti in dolžnosti (torej preprečevanja, zatiranja in preiskovanja kaznivih dejanj). Poleg tega policija pri opravljanju svojih dolžnosti deluje nepristransko, brez predsodkov in pošteno ter ne sme nikoli zlorabiti svojih pooblastil „tako, da bi posegala v pravice in svoboščine posameznika, ki jih zagotavlja japonska ustava“ (ki vključujejo, kot je navedeno, pravico do zasebnosti in do varstva podatkov) ⁽⁹²⁾.
- (127) Zlasti glede člena 197(2) zakonika o kazenskem postopku je nacionalna policijska agencija (kot zvezni organ, med drugim pristojen za vse zadeve, ki se nanašajo na kriminalistično policijo) izdala navodila prefekturni

⁽⁸⁵⁾ Priloga se nanaša na devet vrst kaznivih dejanj, na primer kazniva dejanja, ki se nanašajo na droge in strelno orožje, trgovino z ljudmi in organizirane umore. Navesti je treba, da novo uvedeno kaznivo dejanje „priprave terorističnih dejanj in drugega organiziranega kriminala“ (glej sprotno opombo 76) ni vključeno na ta omejujoči seznam.

⁽⁸⁶⁾ Poleg tega mora v skladu s členom 23 zakona o prisluškovanju telefonskim pogovorom preiskovalni organ posameznika, čigar komunikacija je bila prestrežena (in s tem vključena v evidenco prestreženih komunikacij), o tem pisno obvestiti.

⁽⁸⁷⁾ Glej Prilogo II, oddelek II.A.1(b)(1).

⁽⁸⁸⁾ V skladu s prejetimi informacijami poslovni subjekti, ki ne sodelujejo, na podlagi nobenega zakona ne trpijo negativnih posledic (vključno s sankcijami). Glej Prilogo II, oddelek II.A.2(a).

⁽⁸⁹⁾ V skladu s smernicami komisije za varstvo osebnih informacij (izdaja splošnih pravil) člen 23(1)(i) določa podlago za razkritje osebnih informacij na podlagi naloga (člen 218 zakonika o kazenskem postopku) in „lista za poizvedbo“ (člen 197(2) zakonika o kazenskem postopku).

⁽⁹⁰⁾ To pomeni, da se lahko „list za poizvedbo“ uporablja le za zbiranje informacij v posameznih primerih in ne za kakršno koli obsežno zbiranje osebnih podatkov. Glej tudi Prilogo II, oddelek I.A.2(b)(1).

⁽⁹¹⁾ Poleg predpisov prefekturne komisije za javno varnost glej tudi člen 189(1) zakonika o kazenskem postopku.

⁽⁹²⁾ Glej tudi člen 3 zakona o policiji, v skladu s katerim se prisega vseh policistov glasi: „izpolnjevati obveznost braniti in zagovarjati ustavo in zakone Japonske ter svoje dolžnosti opravljati nepristransko, pravično, pošteno in brez predsodkov“.

policiji⁽⁹³⁾ o „ustrezni uporabi pisnih poizvedb v preiskovalnih zadevah“. V skladu z navedenim obvestilom je treba zahteve vložiti na vnaprej pripravljenem obrazcu („obrazec št. 49“ ali tako imenovani „list za poizvedbo“) ⁽⁹⁴⁾, nanašati se morajo na evidence „v zvezi s posamezno preiskavo“, zahtevane informacije pa morajo biti „potrebne za [navedeno] preiskavo“. V vsakem primeru vodja preiskave „v celoti prouči potrebnost, vsebino itd. posamezne poizvedbe“ in mora prejeti notranjo odobritev visokega uradnika.

- (128) Poleg tega je vrhovno sodišče Japonske v dveh sodbah iz leta 1969 in leta 2008 ⁽⁹⁵⁾ opredelilo omejitve glede neobveznih ukrepov, ki posegajo v pravico do zasebnosti ⁽⁹⁶⁾. Sodišče je zlasti navedlo, da morajo biti taki ukrepi „razumni“ in v okviru „splošno dovoljenih omejitev“, to pomeni, da morajo biti potrebni za preiskavo osumljenca (zbiranje dokazov) in izvedeni „z ustreznimi metodami za doseganje namena preiskave“ ⁽⁹⁷⁾. Iz sodb izhaja, da je za to potreben preskus sorazmernosti in upoštevanje vseh okoliščin zadeve (npr. stopnja poseganja v pravico do zasebnosti, vključno s pričakovano zasebnostjo, teža kaznivega dejanja, verjetnost pridobitve uporabnih dokazov, pomen takih dokazov, morebitni drugi načini preiskave itd.) ⁽⁹⁸⁾.
- (129) Poleg teh omejitev izvajanja javnih pooblastil morajo tudi poslovni subjekti sami preveriti („potrditi“) potrebnost in „racionalnost“ zagotavljanja tretji osebi ⁽⁹⁹⁾. To zajema tudi vprašanje, ali jim sodelovanje preprečuje zakon. Take nasprotujoče si pravne obveznosti lahko izhajajo zlasti iz obveznosti varovanja zaupnosti, kot je člen 134 kazenskega zakonika (glede odnosa med zdravnikom, odvetnikom, duhovnikom itd. in njegovo stranko). Poleg tega „vsaka oseba, ki se ukvarja s poslovanjem na področju telekomunikacij, v času opravljanja svojih nalog ohranja skrivnosti drugih, za katere je izvedela iz komunikacij, ki jih obravnava izvajalec telekomunikacijskih storitev“ (člen 4(2) zakona o poslovanju na področju telekomunikacij). To obveznost potrjuje sankcija iz člena 179 zakona o poslovanju na področju telekomunikacij, v skladu s katerim vsaka oseba, ki prekrši tajnost komunikacij, ki jih obravnava izvajalec telekomunikacijskih storitev, stori kaznivo dejanje, za katero je zagrožena zaporna kazen s prisilnim delom do dveh let ali globa največ milijon jenov ⁽¹⁰⁰⁾. Čeprav ta zahteva ni absolutna in omogoča zlasti ukrepe, s katerimi se krši tajnost komunikacij, če jih je mogoče opredeliti kot „upravičena dejanja“ v smislu člena 35 kazenskega zakonika ⁽¹⁰¹⁾, pa navedena izjema ne zajema odgovorov na neobvezne zahteve javnih organov za razkritje elektronskih informacij na podlagi člena 197(2) zakonika o kazenskem postopku.

3.2.1.3 Nadaljnja uporaba zbranih informacij

- (130) Ko japonski javni organi zberejo osebne informacije, se zanje začne uporabljati zakon o varstvu osebnih informacij, ki jih hranijo upravni organi. Navedeni zakon ureja obravnavo (obdelavo) „hranjenih osebnih informacij“ ter

⁽⁹³⁾ V skladu s členoma 30(1) in 31(2) zakona o policiji generalni direktor regionalnih policijskih uradov (lokalnih izpostav nacionalne policijske agencije) „usmerja in nadzoruje“ prefekturno policijo.

⁽⁹⁴⁾ Na listu za poizvedbo morajo biti navedene tudi kontaktne informacije o „osebi, ki obravnava informacije“ („naziv oddelka [delovnega mesta], ime osebe, telefonska številka urada, interna klicna številka itd.“).

⁽⁹⁵⁾ Sodba vrhovnega sodišča z dne 24. decembra 1969 (1965(A) 1187); sodba vrhovnega sodišča z dne 15. aprila 2008 (2007(A) 839).

⁽⁹⁶⁾ Čeprav se navedeni sodbi ne nanašata na zbiranje elektronskih informacij, je japonska vlada pojasnila, da se uporaba meril vrhovnega sodišča nanaša na vsakršno vmešavanje javnih organov v pravico do zasebnosti, vključno za vse „prostovoljne preiskave“, zato merila zavezujejo japonske organe tudi pri vlaganju prošelj za prostovoljno razkritje informacij. Glej Prilogo II, oddelek II.A.2)(b)(1).

⁽⁹⁷⁾ V skladu s prejetimi informacijami morajo biti ti dejavniki „razumni v skladu z družbeno sprejetimi običaji“. Glej Prilogo II, oddelek II.A.2)(b)(1).

⁽⁹⁸⁾ Glede podobnih ugotovitev v zvezi z obveznimi preiskavami (prisluškovanje telefonskim pogovorom) glej tudi sodbo vrhovnega sodišča z dne 16. decembra 1999 (1997 (A) 636).

⁽⁹⁹⁾ V tem smislu so se japonski organi sklicevali na smernice komisije za varstvo osebnih informacij (izdaja splošnih pravil) in točko 5/14 vprašanj in odgovorov, ki jih je pripravila navedena komisija glede uporabe zakona o varstvu osebnih informacij. Po podatkih japonskih organov „so poslovni subjekti, ob vse večji ozaveščenosti posameznikov o njihovih pravicah glede zasebnosti in glede na delovno obremenitev, ki jo take zahteve prinašajo, vse previdnejši pri odgovorih na take zahteve“. Glej Prilogo II, oddelek II.A.2), tudi ob sklicevanju na obvestilo nacionalne policijske agencije iz leta 1999. V skladu s prejetimi informacijami obstajajo tudi primeri, ko so poslovni subjekti zavrnili sodelovanje. LINE (najbolj priljubljena aplikacija za pošiljanje sporočil na Japonskem) v svojem poročilu o preglednosti iz leta 2017 na primer navede: „Po prejemu zahtev preiskovalnih agencij itd. [...] preverimo njihovo ustreznost z vidika zakonitosti, zaščite uporabnika itd. Pri tem začasno zavrnemo zahtevo, če je pravno šibka. Če je obseg zahteve preširok glede na preiskavo, od preiskovalne agencije zahtevamo pojasnilo. Če pojasnilo ni utemeljeno, se na zahtevo ne odzovemo.“ Na voljo na spletu: <https://linecorp.com/en/security/transparency/top>

⁽¹⁰⁰⁾ Za vsako osebo, ki „sodeluje pri poslovanju na področju telekomunikacij“, je zagrožena triletna zaporna kazen s prisilnim delom ali globa največ dva milijona jenov.

⁽¹⁰¹⁾ „Upravičena dejanja“ v smislu kazenskega zakonika so zlasti tista dejanja izvajalca telekomunikacijskih storitev, s katerimi upošteva pravno zavezujoče ukrepe države (obvezne ukrepe), na primer ko preiskovalni organi sprejmejo ukrepe na podlagi naloga sodnika. Glej Prilogo II, oddelek II.A.2)(b)(2), ob sklicevanju na smernice glede varstva osebnih informacij pri poslovanju na področju telekomunikacij.

uvaja več omejitev in zaščitnih ukrepov (glej uvodno izjavo 118) ⁽¹⁰²⁾. Poleg tega dejstvo, da upravni organ lahko hrani osebne informacije „samo, če je hramba potrebna za opravljanje zadev v njegovi pristojnosti, kot jih določajo zakoni in predpisi“ (člen 3(1) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi), prav tako uvaja omejitev (vsaj posredno) prvotnega zbiranja.

3.2.2 Neodvisen nadzor

- (131) Na Japonskem zbiranje elektronskih informacij na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj spada predvsem ⁽¹⁰³⁾ v okvir odgovornosti prefekturne policije ⁽¹⁰⁴⁾, ki je glede tega podvržena več ravnem nadzora.
- (132) Prvič, v vseh primerih zbiranja elektronskih informacij z obveznimi sredstvi (iskanje in zaseg) si mora policija predhodno zagotoviti sodni nalog (glej uvodno izjavo 121). Zato zbiranje v navedenih primerih vnaprej preveri sodnik na podlagi strogega standarda „ustreznega razloga“.
- (133) Čeprav v primeru prošelj za prostovoljno razkritje ni predhodnega preverjanja sodnika, lahko poslovni subjekti, na katere so take zahteve naslovljene, ugovarjajo brez negativnih posledic (in morajo upoštevati vpliv razkritja na zasebnost). Poleg tega člen 192(1) zakonika o kazenskem postopku določa, da policisti vedno sodelujejo z državnim tožilcem (in s prefekturno komisijo za javno varnost) in z njim usklajujejo svoje ukrepe ⁽¹⁰⁵⁾. Državni tožilec lahko v zameno zagotovi potrebna splošna navodila ter opredeli standarde poštene preiskave in/ali izda posebne odredbe v zvezi s posameznimi preiskavami (člen 193 zakonika o kazenskem postopku). Če se taka navodila in/ali odredbe ne upoštevajo, lahko tožilstvo zahteva disciplinske ukrepe (člen 194 zakonika o kazenskem postopku). Prefekturna policija torej deluje pod nadzorom državnega tožilca.
- (134) Drugič, v skladu s členom 62 ustave lahko vsak dom japonskega parlamenta (Diet) izvaja preiskave, ki se nanašajo na vlado, tudi o zakonitosti zbiranja informacij s strani policije. V ta namen lahko zahteva navzočnost in pričanje prič in/ali predložitev evidenc. Navedena pooblastila so nadalje določena v zakonu o parlamentu, zlasti v poglavju XII. Natančneje, člen 104 zakona o parlamentu določa, da morajo ministri in predsednik vlade, javne agencije in drugi deli vlade „upoštevati zahteve doma parlamenta ali katerega koli njegovega odbora glede predložitve poročil in evidenc, potrebnih za izvedbo preiskave“. Vlada lahko zahtevo zavrne le, če navede verjeten razlog, ki ga parlament sprejme, ali na podlagi izdaje uradne izjave, da bi predložitev poročil ali evidenc „močno škodovala nacionalnim interesom“ ⁽¹⁰⁶⁾. Poleg tega lahko člani parlamenta ministrom in predsedniku vlade predložijo pisna vprašanja (člena 74 in 75 zakona o parlamentu); v preteklosti so se take „pisne poizvedbe“ že nanašale na obravnavo osebnih informacij s strani upravnih organov ⁽¹⁰⁷⁾. Vlogo parlamenta pri nadzoru izvršilne veje oblasti podpira tudi obveznost poročanja, na primer na podlagi člena 29 zakona o prisluškovanju telefonskim pogovorom.
- (135) Tretjič, tudi v okviru izvršilne veje oblasti je prefekturna policija podvržena neodvisnemu nadzoru. Ta obsega zlasti prefekturne komisije za javno varnost, ustanovljene na ravni prefekture, da se zagotovi demokratično upravljanje in politična nevtralnost policije ⁽¹⁰⁸⁾. Navedene komisije sestavljajo člani, ki jih imenuje guverner prefekture na podlagi soglasja parlamenta prefekture (izbira med državljani, ki v predhodnih petih letih niso bili javni uslužbenci pri policiji) in ki imajo zagotovljen mandat (razrešitev je mogoča samo iz utemeljenih razlogov) ⁽¹⁰⁹⁾. V skladu s prejetimi informacijami niso zavezani upoštevati navodil, zato se lahko štejejo za popolnoma neodvisne ⁽¹¹⁰⁾. V

⁽¹⁰²⁾ Glede pravic zadevnih posameznikov glej oddelek 3.1.

⁽¹⁰³⁾ Državni tožilec (ali njegov pomočnik po navodilu državnega tožilca) lahko načeloma preiskuje kaznivo dejanje, če meni, da je to potrebno (člen 191(1) zakonika o kazenskem postopku).

⁽¹⁰⁴⁾ V skladu s prejetimi informacijami nacionalna policijska agencija ne izvaja posameznih kazenskih preiskav. Glej Prilogo II, oddelek II.A.1)(a).

⁽¹⁰⁵⁾ Glej tudi člen 246 zakonika o kazenskem postopku, v skladu s katerim mora pravosodna policija državnemu tožilcu poslati spis zadeve, ko opravi preiskavo kaznivega dejanja („načelo predaje vseh zadev“).

⁽¹⁰⁶⁾ Parlament pa lahko tudi zahteva, da odbor za nadzor in pregled posebej opredeljenih skrivnosti izvede preiskavo zavrnitve odgovora. Glej člen 104-II zakona o parlamentu.

⁽¹⁰⁷⁾ Glej Prilogo II, oddelek II.B.4).

⁽¹⁰⁸⁾ Poleg tega je v skladu z določbami člena 100 zakona o lokalni samoupravi lokalna skupščina pristojna za preiskavo dejavnosti izvršilnih organov, ustanovljenih na ravni prefektur, vključno s prefekturno policijo.

⁽¹⁰⁹⁾ Glej člene 39 do 41 zakona o policiji. Glede politične nevtralnosti glej tudi člen 42 zakona o policiji.

⁽¹¹⁰⁾ Glej Prilogo II, oddelek II.B.3) („sistem neodvisnih odborov“).

zvezi z nalogami in pooblastili prefekturnih komisij za javno varnost člen 38(3) v povezavi s členom 2 in členom 36(2) zakona o policiji določa, so te pristojne za „varstvo pravic in svoboščin posameznika“. V ta namen so pooblašene za „nadzor“⁽¹¹¹⁾ vseh preiskovalnih dejavnosti prefekturne policije, vključno z zbiranjem osebnih podatkov. Zlasti lahko komisije „po potrebi podrobno usmerjajo prefekturno policijo ali jo usmerjajo v posameznem primeru preiskave neprimerne ravnanja osebja policije“⁽¹¹²⁾. Ko vodja prefekturne policije⁽¹¹³⁾ prejme tako navodilo ali ko sam zazna morebiten primer neprimerne ravnanja (vključno s kršitvami zakonodaje ali druge vrste zanemarjanja dolžnosti), mora zadevo takoj preiskati in o rezultatih poročati prefekturni komisiji za javno varnost (člen 56(3) zakona o policiji). Če ta meni, da je potrebno, lahko tudi imenuje enega od svojih članov, ki preveri stanje izvajanja. Postopek se nadaljuje, dokler se prefekturna komisija za javno varnost ne prepriča, da je bil dogodek ustrezno obravnavan.

- (136) Poleg tega ima pristojni minister ali vodja agencije (npr. generalni komisar nacionalne policijske agencije) glede pravnega izvajanja zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, izvršilna pooblastila, nadzor pa izvaja ministrstvo za notranje zadeve in komunikacije. V skladu s členom 49 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, lahko ministrstvo za notranje zadeve in komunikacije „zbira poročila stanju izvajanju tega zakona“ od vodij upravnih organov (ministrov). Nadzorna funkcija je podprta prek 51 „celovitih informacijskih centrov“ ministrstva za notranje zadeve in komunikacije (en v vsaki prefekturi na Japonskem), ki vsako leto obravnavajo tisoče poizvedb posameznikov⁽¹¹⁴⁾ (iz katerih se lahko razkrijejo morebitne kršitve zakona). Ministrstvo za notranje zadeve in komunikacije lahko zahteva predložitev pojasnil in gradiv ter izdaja mnenja o tem, kako zadevni upravni organi obravnavajo osebne informacije, če meni, da je to potrebno za zagotavljanje skladnosti z zakonom (člena 50 in 51 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi).

3.2.3 Pravna sredstva posameznikov

- (137) Poleg uradnega nadzora imajo posamezniki na voljo tudi več pravnih sredstev, ki jih lahko vložijo pri neodvisnih organih (kot so na primer prefekturne komisije za javno varnost ali komisija za varstvo osebnih informacij) ali pri japonskih sodiščih.
- (138) Prvič, glede osebnih informacij, ki jih zbirajo upravni organi, si morajo slednji „prizadevati za ustrezno in hitro obravnavo vsake pritožbe“ v zvezi z nadaljnjo obdelavo (člen 48 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi). Čeprav se poglavje IV zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, o pravicah posameznikov ne uporablja v zvezi z osebnimi informacijami, ki jih vsebujejo „dokumenti, ki se nanašajo na sojenja in zasežene predmete“ (člen 53-2(2) zakonika o kazenskem postopku) in ki zajemajo osebne informacije, zbrane v okviru kazenske preiskave, lahko posamezniki vložijo pritožbo na podlagi splošnih načel varstva podatkov, kot je na primer obveznost, da se osebne informacije hranijo samo, „če je hramba potrebna za [preprečevanje, odkrivanje in preiskovanje kaznivih dejanj]“ (člen 3(1) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi).
- (139) Poleg tega člen 79 zakona o policiji posameznikom, ki imajo pomisleke glede „izvrševanja dolžnosti“ policijskega osebja, zagotavlja pravico do vložitve pritožbe pri (pristojni) neodvisni prefekturni komisiji za javno varnost. Komisija „natančno“ obravnava take pritožbe v skladu z zakoni in lokalnimi odloki ter o rezultatu pisno obvesti pritožnika. Na podlagi svoje pristojnosti nadzora nad prefekturno policijo in njenega „usmerjanja“ glede „nepriemerne ravnanja osebja“ (člena 38(3) in 43-2(1) zakona o policiji) lahko od prefekturne policije zahteva preiskavo dejanskega stanja, sprejetje ustreznih ukrepov na podlagi rezultatov navedene preiskave in poročanje o rezultatih. Če meni, da preiskava policije ni ustrezna, lahko komisija tudi da navodila o obravnavi pritožbe.
- (140) Nacionalna policijska agencija je izdala „obvestilo“ policiji in prefekturni komisiji za javno varnost o ustreznih obravnavi pritožb v zvezi z izvrševanjem dolžnosti policistov, da se olajša obravnavanje pritožb. V navedenem dokumentu nacionalna policijska agencija navaja standarde za razlago in izvajanje člena 79 zakona o policiji. Med drugim od prefekturne policije zahteva vzpostavitev „sistema za obravnavo pritožb“ ter „takojšnjo“ obravnavo

⁽¹¹¹⁾ Glej člena 5(3) in 38(3) zakona o policiji.

⁽¹¹²⁾ Glej člena 38(3) in 43-2(1) zakona o policiji. Če prefekturna komisija za javno varnost „da navodilo“ v smislu člena 43-2(1), lahko odboru, ki ga sama imenuje, odredi spremljanje izvajanja takega navodila (odstavek 2). Komisija lahko tudi predlaga disciplinske ukrepe ali razrešitev vodje prefekturne policije (člen 50(2)) ali drugih policistov (člen 55(4) zakona o policiji).

⁽¹¹³⁾ Enako velja za glavnega načelnika tokijske metropolitanske policije (glej člen 48(1) zakona o policiji).

⁽¹¹⁴⁾ Na podlagi prejetih informacij so „celoviti informacijski centri“ v poslovnem letu 2017 (od aprila 2017 do marca 2018) obravnavali skupno 5 186 poizvedb posameznikov.

vseh pritožb, vloženih pri pristojni prefekturni komisiji za javno varnost, in poročanje o njih. Obvestilo opredeljuje pritožbe kot zahtevek za popravek „zaradi kakršne koli posebne prikrajšanosti, ki je bila povzročena zaradi nezakonitega ali neprimerne vedenja“⁽¹¹⁵⁾, ali „opustitve potrebnih ukrepov s strani policista pri opravljanju nalog“⁽¹¹⁶⁾ ter morebitne „očitke/nezadovoljstvo v zvezi z neustreznim načinom opravljanja nalog s strani policista“. Tako je materialno področje uporabe pritožbe široko opredeljeno, saj zajema vsako zatrjevanje nezakonitega zbiranja podatkov, pritožniku pa ni treba dokazati, da mu je zaradi delovanja policista nastala kakršna koli škoda. Pomembno je, da to obvestilo določa, da se tujcem (med drugim) zagotovi pomoč pri oblikovanju pritožbe. Prefekturne komisije za javno varnost morajo na podlagi pritožbe zagotoviti, da prefekturna policija prouči dejansko stanje, izvede ukrepe „v skladu z rezultati preiskave“ in poroča o rezultatih. Če komisija meni, da preiskava ni bila zadostna, izda navodilo o obravnavi pritožbe, ki ga mora prefekturna policija upoštevati. Na podlagi prejetih poročil in sprejetih ukrepov komisija obvesti posameznika ter med drugim navede sprejete ukrepe za obravnavo pritožbe. V obvestilu nacionalne policijske agencije je poudarjeno, da je treba pritožbe obravnavati „iskreno“ ter da je treba rezultat sporočiti „v ustreznem roku [...] glede na družbene norme in zdrav razum“.

- (141) Drugič, glede na to, da bo običajno treba pravno sredstvo vložiti v tujini, v okviru tujega sistema in v tujem jeziku, je japonska vlada uporabila svoja pooblastila in ustvarila poseben mehanizem, ki ga vodi in nadzoruje komisija za varstvo osebnih informacij, za obravnavo in reševanje pritožb na tem področju, da se olajša uporaba pravnih sredstev posameznikom iz EU, katerih osebni podatki se prenašajo poslovnim subjektom na Japonskem, nato pa imajo do njih dostop javni organi. Navedeni mehanizem temelji na obveznosti sodelovanja, ki jo imajo japonski javni organi na podlagi zakona o varstvu osebnih informacij in posebne vloge komisije za varstvo osebnih informacij v zvezi z mednarodnimi prenosi podatkov iz tretjih držav na podlagi člena 6 zakona o varstvu osebnih informacij in osnovne politike (kot je opredelila japonska vlada na podlagi vladne odredbe). Podrobnosti tega mehanizma so opredeljene v uradnih navedbah, zagotovilih in zavezah, prejetih od japonske vlade, in so temu sklepu priložene kot Priloga II. Za mehanizem ni potrebno nobeno procesno upravičenje, odprt pa je za vse posameznike, ne glede na to, ali so osumljeni ali obtoženi kaznivega dejanja.
- (142) Na podlagi navedenega mehanizma lahko posameznik, ki sumi, da je javni organ na Japonskem (vključno s tistimi, odgovornimi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj) zbral ali uporabil njegove podatke, ki so bili preneseni iz Evropske unije, v nasprotju s pravili, ki se uporabljajo, vložiti pritožbo na komisijo za varstvo osebnih informacij (samostojno ali prek svojega organa za varstvo podatkov v smislu člena 51 Splošne uredbe o varstvu podatkov). Komisija za varstvo osebnih informacij mora pritožbo obravnavati in o njej najprej obvestiti pristojne javne organe, vključno z ustreznimi nadzornimi organi. Navedeni organi morajo sodelovati s komisijo za varstvo osebnih informacij, „tudi z zagotavljanjem potrebnih informacij in ustreznega gradiva, da lahko navedena komisija presodi, ali je bilo zbiranje oziroma nadaljnja uporaba osebnih informacij v skladu s pravili, ki se uporabljajo“⁽¹¹⁷⁾. Ta obveznost, ki izhaja iz člena 80 zakona o varstvu osebnih informacij (in od japonskih javnih organov zahteva sodelovanje s komisijo za varstvo osebnih informacij), je splošno veljavna in tako zajema nadzor nad vsemi ukrepi takih organov, ki so se poleg tega k takemu sodelovanju zavezali s pisnimi zagotovili pristojnih ministrov in vodij agencij, kot je razvidno iz Priloge II.
- (143) Če se v okviru presoje izkaže, da so bila kršena pravila, ki se uporabljajo, „sodelovanje zadevnih javnih organov s komisijo za varstvo osebnih informacij zajema obveznost odprave kršitve“, kar v primeru nezakonitega zbiranja osebnih informacij vključuje izbris takih podatkov. Pomembno je, da se ta obveznost izvaja pod nadzorom komisije za varstvo osebnih informacij, ki „pred zaključkom presoje potrdi, da je kršitev v celoti odpravljena“.
- (144) Po zaključku presoje komisija za varstvo osebnih informacij posameznika v razumnem roku obvesti o rezultatu presoje in o morebitnih popravnih ukrepih, če je ustrezno. Hkrati obvesti posameznika o možnosti zahtevati potrditev rezultata od pristojnega javnega organa in navede organ, pri katerem se vložiti taka zahteva za potrditev. Možnost prejema take potrditve, vključno z razlogi za odločitev pristojnega organa, je lahko posamezniku v

⁽¹¹⁵⁾ Pogoj „posebne prikrajšanosti“ izraža le to, da mora ravnanje (ali neukrepanje) policije zadevati pritožnika, ne pa tudi tega, da bi moral ta dokazati kakršno koli škodo.

⁽¹¹⁶⁾ Del teh nalog je upoštevanje zakona, vključno s pravnimi zahtevami o zbiranju in uporabi osebnih podatkov. Glej člen 2(2) in člen 3 zakona o policiji.

⁽¹¹⁷⁾ Komisija za varstvo osebnih informacij bo pri presoji sodelovala z ministrstvom za notranje zadeve in komunikacije, ki (kot je pojasnjeno v uvodni izjavi 136) lahko zahteva predložitev pojasnil in gradiva ter izdaja mnenja o tem, kako zadevni upravni organi obravnavajo osebne informacije (člena 50 in 51 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi).

pomoč pri nadaljnjih korakih, tudi pri uveljavljanju sodnega varstva. Podrobne informacije o rezultatu presoje se lahko omejijo, če obstajajo utemeljeni razlogi, da bi lahko razkritje takih informacij pomenilo tveganje za potekajočo preiskavo.

- (145) Tretjič, posameznik, ki se ne strinja s sodnikovo odločbo o zasegu (nalogom) ⁽¹¹⁸⁾, ki se nanaša na njegove osebne podatke, ali z ukrepi policije oziroma tožilstva, ki izvršuje tako odločbo, lahko vloži zahtevo, da se taka odločba ali ukrepi razveljavijo ali spremenijo (člen 429(1) ter člen 430(1) in (2) zakonika o kazenskem postopku ter člen 26 zakona o prisluškovanju telefonskim pogovorom) ⁽¹¹⁹⁾. Če pritožbeno sodišče meni, da je nalog nezakonit ali da je nezakonito njegovo izvrševanje („postopek zasega“), odobri zahtevo in odredi vrnitev zaseženih predmetov ⁽¹²⁰⁾.
- (146) Četrtrič, posameznik, ki meni, da je bilo zbiranje njegovih osebnih informacij kot del kazenske preiskave nezakonito, se lahko kot bolj posredno obliko sodnega varstva v okviru svojega kazenskega sodnega postopka sklicuje na to nezakonitost. Če se sodišče z njim strinja, se dokazi izločijo kot nedopustni.
- (147) Nazadnje, sodišče lahko na podlagi člena 1(1) zakona o nadomestilih države odobri odškodnino, če je javni uslužbenec z javnimi pooblastili države pri izvajanju svojih dolžnosti nezakonito in krivdno (naklepno ali iz malomarnosti) povzročil škodo zadevnemu posamezniku. V skladu s členom 4 zakona o nadomestilih države odškodninska odgovornost države temelji na določbah civilnega zakonika. S tem v zvezi člen 710 civilnega zakonika določa, da odgovornost vključuje tudi drugo škodo, ne samo škodo na premoženju, torej tudi nematerialno škodo (npr. v obliki „duševnih bolečin“). To zajema primere kršitev zasebnosti posameznikov z nezakonitim opazovanjem in/ali zbiranjem njegovih osebnih informacij (npr. nezakonita izvršitev naloga) ⁽¹²¹⁾.
- (148) Poleg denarnega nadomestila se lahko posameznikom pod nekaterimi pogoji izda tudi sodna odredba (npr. o izbrisu osebnih podatkov, ki jih je zbral javni organ) na podlagi njegovih pravic do zasebnosti iz člena 13 ustave ⁽¹²²⁾.
- (149) Glede vseh navedenih pravnih sredstev mehanizem reševanja sporov, ki ga je oblikovala japonska vlada, omogoča posamezniku, ki še vedno ni zadovoljen z rezultatom postopka, da se obrne na komisijo za varstvo osebnih informacij, „ki posameznika obvesti o različnih možnostih in podrobnih postopkih v zvezi s pravnimi sredstvi na podlagi japonskega prava in predpisov“. Poleg tega komisija za varstvo osebnih informacij „posamezniku zagotovi podporo, kar vključuje tudi svetovanje in pomoč pri vložitvi nadaljnjih vlog zadevnim upravnim ali pravosodnim organom“.
- (150) To zajema uporabo procesnih pravic na podlagi zakonika o kazenskem postopku. Na primer, „kadar se v okviru presoje izkaže, da je posameznik osumljenec v kazenski zadevi, komisija za varstvo osebnih informacij o tem obvesti posameznika“ ⁽¹²³⁾, pa tudi o možnosti na podlagi člena 259 zakonika o kazenskem postopku, v skladu s katerim se lahko od tožilstva zahteva obvestilo, če se tožilstvo odloči, da ne bo uvedlo kazenskega postopka. Poleg tega velja, da če se v okviru presoje izkaže, da je bila zadeva v zvezi z osebnimi informacijami posameznika obravnavana in zaključena, komisija za varstvo osebnih informacij obvesti posameznika, da lahko vpogleda v spis zadeve na podlagi člena 53 zakonika o kazenskem postopku (in člena 4 zakona o spisih pravnomočnih kazenskih zadev). Za posameznika je dostop do spisa svoje zadeve pomemben, saj lahko tako bolje razume opravljeno

⁽¹¹⁸⁾ To zajema nalog za prisluškovanje telefonskim pogovorom, glede katerega zakon o prisluškovanju telefonskim pogovorom zahteva posebno obvestilo (člen 23). V skladu z navedeno določbo mora preiskovalni organ posameznike, katerih komunikacija je bila prestrežena (in je s tem vključena v evidenco prestrežene komunikacije), o tem pisno obvestiti. Drug primer je člen 100(3) zakonika o kazenskem postopku, v skladu s katerim sodišče, ko zaseže poštna pošiljke ali telegrame, poslane obtoženemu ali ki jih je ta sam poslal, obvestiti pošiljatelja ali prejemnika, razen če obstaja tveganje, da bi tako obvestilo oviralo sodni postopek. Člen 222(1) zakonika o kazenskem postopku se navzkrižno sklicuje na to določbo glede iskanja in zasega, ki ga izvede preiskovalni organ.

⁽¹¹⁹⁾ Čeprav taka zahteva samodejno ne zadrži izvršitve odločbe o zasegu, lahko pritožbeno sodišče odredi zadržanje, dokler ne izda vsebinske odločitve. Glej člen 429(2) in člen 432 v povezavi s členom 424 zakonika o kazenskem postopku.

⁽¹²⁰⁾ Glej Prilogo II, oddelek II.C(1).

⁽¹²¹⁾ Glej Prilogo II, oddelek II.C(2).

⁽¹²²⁾ Glej na primer sodbo okrožnega sodišča v Tokiu z dne 24. marca 1988 (št. 2925) in sodbo okrožnega sodišča v Osaki z dne 26. aprila 2007 (št. 2925). Okrožno sodišče v Osaki je navedlo, da je treba upoštevati več dejavnikov, na primer: (i) naravo in vsebino zadevnih osebnih informacij; (ii) način njihovega zbiranja; (iii) negativen učinek na posameznika, če se informacije ne izbrišejo; (iv) javni interes, vključno z negativnimi učinki za javni organ, če se informacije izbrišejo.

⁽¹²³⁾ V vsakem primeru tožilstvo obtožencu po začetku kazenskega postopka omogoči proučitev navedenih dokazov (glej člene 298–299 zakonika o kazenskem postopku). Glede žrtev kaznivih dejanj glej člene 316–333 zakonika o kazenskem postopku.

preiskavo zoper sebe in se pripravi na morebitni sodni postopek (npr. odškodninski zahtevek), če meni, da so bili njegovi podatki nezakonito zbrani ali uporabljeni.

3.3 Dostop in uporaba s strani japonskih javnih organov za namene nacionalne varnosti

- (151) V skladu z navedbami japonskih organov na Japonskem ne obstaja zakon, ki bi omogočal obvezne zahteve po informacijah ali „upravno prisluškovanje telefonskim pogovorom“ zunaj kazenskih preiskav. Informacije se na podlagi nacionalne varnosti torej lahko pridobivajo le od virov, do katerih ima vsakdo prost dostop, ali na podlagi prostovoljnega razkritja. Poslovni subjekti, ki prejmejo prošnjo za prostovoljno sodelovanje (v obliki razkritja elektronskih informacij) niso z ničemer pravno zavezani k zagotavljanju takih informacij ⁽¹²⁴⁾.
- (152) Poleg tega so na podlagi prejetih informacij samo štirje vladni subjekti pooblašeni za zbiranje elektronskih informacij, ki jih hranijo japonski poslovni subjekti, na podlagi nacionalne varnosti, in sicer: (i) urad vlade za obveščevalno dejavnost in raziskave; (ii) ministrstvo za obrambo; (iii) policija (nacionalna policijska agencija ⁽¹²⁵⁾ in prefekturna policija) ter (iv) obveščevalna agencija za javno varnost. Vendar pa urad vlade za obveščevalno dejavnost in raziskave informacij nikoli ne zbira neposredno od poslovnih subjektov, niti s sredstvi za prestrezanje komunikacij. Kadar prejme informacije od drugih vladnih organov, da bi opravil analizo za vlado, morajo ti drugi organi ravnati v skladu z zakonom, vključno z omejitvami in zaščitnimi ukrepi, analiziranimi v tem sklepu. Njegove dejavnosti torej niso relevantne v smislu prenosa.

3.3.1 Pravna podlaga in omejitve/zaščitni ukrepi, ki se uporabljajo

- (153) V skladu s prejetimi podatki ministrstvo za obrambo zbira (elektronske) informacije na podlagi zakona o ustanovitvi ministrstva za obrambo. V skladu s členom 3 navedenega zakona je cilj ministrstva za obrambo vodenje in delovanje vojaških sil ter „opravljanje dejavnosti, ki so s tem povezane, da se zagotovi nacionalni mir in neodvisnost ter varnost naroda“. Člen 4(4) določa, da je ministrstvo za obrambo pristojno za „obrambo in varovanje“, za dejanja sil za samoobrambo ter za napotitev vojaških sil, vključno z zbiranjem informacij, potrebnih za opravljanje navedenih nalog. Ministrstvo je pristojno samo za zbiranje (elektronskih) informacij od poslovnih subjektov na podlagi prostovoljnega sodelovanja.
- (154) Odgovornosti in dolžnosti prefekturne policije pa vključujejo „vzdrževanje javne varnosti in reda“ (člen 35(2) v povezavi s členom 2(1) zakona o policiji). Policija lahko v okviru teh pristojnosti zbira informacije, vendar le na prostovoljni podlagi brez pravne obveznosti. Dejavnosti policije so tudi „strogo omejene“ na tisto, kar je potrebno za opravljanje njenih nalog. Poleg tega policija ravna „nepriustransko, neopredeljeno, brez predsodkov in pošteno“ in nikoli ne zlorablja svojih pooblastil „na noben način, ki bi posegal v pravice in svoboščine posameznika, kot so zagotovljene v ustavi Japonske“ (člen 2 zakona o policiji).
- (155) Nazadnje, obveščevalna agencija za javno varnost lahko izvaja preiskave na podlagi zakona o preprečevanju subverzivnih dejavnosti in zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora, kadar so take preiskave potrebne za pripravo na sprejetje nadzornih ukrepov zoper nekatere organizacije ⁽¹²⁶⁾. Na podlagi obeh zakonov lahko komisija za proučevanje javne varnosti na zahtevo generalnega direktorja obveščevalne agencije za javno varnost odredi nekatere „ukrepe“ (v primeru zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora, je to opazovanje oziroma prepoved ⁽¹²⁷⁾, v primeru zakona o preprečevanju subverzivnih dejavnosti pa razpustitev oziroma prepoved ⁽¹²⁸⁾), v okviru tega pa lahko obveščevalna agencija za javno varnost opravi preiskavo ⁽¹²⁹⁾. Iz prejetih informacij izhaja, da se navedene preiskave vedno izvajajo na

⁽¹²⁴⁾ Poslovni subjekti se lahko torej svobodno odločijo, da ne bodo sodelovali, pri tem pa ne tvegajo nobenih sankcij ali drugih negativnih posledic. Glej Prilogo II, oddelek III.A.1).

⁽¹²⁵⁾ Na podlagi prejetih informacij je glavna vloga nacionalne policijske agencije usklajevanje preiskav različnih oddelkov prefekturne policije in izmenjava informacij s tujimi organi. Tudi v tej vlogi je nacionalna policijska agencija pod nadzorom nacionalne komisije za javno varnost, ki je med drugim odgovorna za varstvo pravic in svoboščin posameznikov (člen 5(1) zakona o policiji).

⁽¹²⁶⁾ Glej Prilogo II, oddelek III.A.1)(3). Zadevno področje uporabe navedenih zakonov je omejeno, saj se zakon o preprečevanju subverzivnih dejavnosti nanaša na „teroristične subverzivne dejavnosti“, zakon o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora, pa na „dejanje vsesplošnega množičnega umora“ (kar pomeni „teroristično subverzivno dejavnost“ v smislu zakona o preprečevanju subverzivnih dejavnosti, „katere posledica je vsesplošen množični umor večjega števila oseb“).

⁽¹²⁷⁾ Glej člena 5 in 8 zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora. Ukrepi opazovanja vključuje tudi obveznost poročanja organizacije, na katero se ukrep nanaša. Glede postopkovnih zaščitnih ukrepov, zlasti zahtev glede preglednosti in predhodne odobritve komisije za proučevanje javne varnosti, glej člena 12 in 13 ter člene 15–27 zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora.

⁽¹²⁸⁾ Glej člena 5 in 7 zakona o preprečevanju subverzivnih dejavnosti. Glede postopkovnih zaščitnih ukrepov, zlasti zahtev glede preglednosti in predhodne odobritve komisije za proučevanje javne varnosti, glej člene 11–25 zakona o preprečevanju subverzivnih dejavnosti.

⁽¹²⁹⁾ Glej člen 27 zakona o preprečevanju subverzivnih dejavnosti ter člena 29 in 30 zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora.

prostovoljni podlagi, kar pomeni, da obveščevalna agencija za javno varnost ne sme prisiliti lastnika osebnih informacij k njihovi predložitvi ⁽¹³⁰⁾. V vsakem primeru velja, da se nadzor in preiskava opravi samo v najmanjšem potrebnem obsegu, da se doseže namen nadzora, v nobenem primeru pa se ne izvaja tako, da bi „neupravičeno“ omejevala pravice in svoboščine, ki jih zagotavlja ustava Japonske (člen 3(1) zakona o preprečevanju subverzivnih dejavnosti oziroma zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora). Poleg tega v skladu s členom 3(2) zakona o preprečevanju subverzivnih dejavnosti oziroma zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora, velja, da obveščevalna agencija za javno varnost v nobenem primeru ne sme zlorabiti takega nadzora ali preiskave, ki se izvaja za pripravo na tak nadzor. Če uslužbenec obveščevalne agencije za javno varnost zlorabi svoja pooblastila na podlagi zadevnega zakona, tako da osebo prisili k nečemu, kar ni zavezana storiti, ali če posega v uveljavljanje pravic osebe, se mu lahko izreče kazenska sankcija na podlagi člena 45 zakona o preprečevanju subverzivnih dejavnosti ali člena 42 zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora. Nazadnje, oba zakona izrecno določata, da se njune določbe, vključno s podeljenimi pooblastili, „v nobenem primeru ne smejo razširjeno razlagati“ (člen 2 zakona o preprečevanju subverzivnih dejavnosti oziroma zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora).

- (156) V vseh primerih vladnega dostopa na podlagi nacionalne varnosti, opisanih v tem oddelku, se uporabljajo omejitve, ki jih je navedlo japonsko vrhovno sodišče glede prostovoljnih preiskav, kar pomeni, da mora biti zbiranje (elektronskih) informacij skladno z načeli potrebnosti in sorazmernosti („ustrezna metoda“) ⁽¹³¹⁾. Kot so izrecno potrdili japonski organi, „zbiranje in obdelava informacij potekata le v obsegu, ki je potreben za izvajanje specifičnih nalog pristojnega javnega organa, in na podlagi specifičnih groženj“. Tako „to izključuje množično in neselektivno zbiranje osebnih podatkov ali dostop do njih iz razlogov nacionalne varnosti“ ⁽¹³²⁾.
- (157) Poleg tega velja, da vse osebne informacije, ki jih hranijo javni organi za namen nacionalne varnosti, ko so enkrat zbrane, spadajo v okvir zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, zato morajo biti deležne ustreznega varstva pri njihovi nadaljnji hrambi, uporabi in razkritju (glej uvodno izjavo 118).

3.3.2 Neodvisen nadzor

- (158) Zbiranje osebnih informacij za namene nacionalne varnosti je podvrženo več ravnem nadzora treh vej oblasti.
- (159) Prvič, japonski parlament lahko prek svojih posebnih odborov prouči zakonitost preiskav na podlagi svojih pooblastil parlamentarnega nadzora (člen 62 ustave, člen 104 zakona o parlamentu; glej uvodno izjavo 134). To funkcijo nadzora podpirajo posebne obveznosti poročanja o dejavnostih, izvedenih na podlagi nekaterih zgoraj navedenih pravnih podlag ⁽¹³³⁾.
- (160) Drugič, več nadzornih mehanizmov je vzpostavljenih v okviru izvršilne veje oblasti.
- (161) Glede ministrstva za obrambo nadzor izvaja urad generalnega inšpektorja za pravno skladnost ⁽¹³⁴⁾, ustanovljen na podlagi člena 29 zakona o ustanovitvi ministrstva za obrambo kot urad znotraj ministrstva za obrambo in pod nadzorom ministra za obrambo (ki mu tudi poroča), vendar neodvisen od operativnih oddelkov ministrstva. Urad generalnega inšpektorja za pravno skladnost ima nalogo zagotoviti skladnost z zakoni in predpisi ter ustrezno izvajanje dolžnosti uslužbencev ministrstva za obrambo. Med drugim ima pooblastilo za izvajanje tako imenovanih „obrambnih inšpekcijskih pregledov“, in sicer periodičnih („redni obrambni inšpekcijski pregledi“) in v posameznih primerih („posebni obrambni inšpekcijski pregledi“), ki so v preteklosti obsegali tudi ustrezno obravnavo osebnih informacij ⁽¹³⁵⁾. Urad generalnega inšpektorja za pravno skladnost lahko v okviru takih inšpekcijskih pregledov

⁽¹³⁰⁾ Glej Prilogo II, oddelek III.A.1)(3).

⁽¹³¹⁾ Glej Prilogo II, oddelek III.A.2)(b): „Iz sodne prakse vrhovnega sodišča izhaja, da mora biti prošnja za prostovoljno sodelovanje poslovnega subjekta za to, da se obravnava, potrebna za preiskavo suma kaznivega dejanja in ter biti razumna, da se doseže namen preiskave. Čeprav se preiskave, ki jih izvajajo preiskovalni organi na področju nacionalne varnosti, razlikujejo od preiskav, ki jih izvajajo preiskovalni organi na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, v smislu njihove pravne podlage in namena, se na področju nacionalne varnosti podobno uporabljajo osrednja načela ‚potrebnosti preiskave‘ in ‚ustreznosti metode‘, ki jih je treba upoštevati, pri tem pa ustrezno upoštevati tudi posebne okoliščine vsake zadeve.“

⁽¹³²⁾ Glej Prilogo II, oddelek III.A.2)(b).

⁽¹³³⁾ Glej na primer člen 36 zakona o preprečevanju subverzivnih dejavnosti oziroma člen 31 zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora (za obveščevalno agencijo za javno varnost).

⁽¹³⁴⁾ Vodja urada generalnega inšpektorja za pravno skladnost je nekdanji državni tožilec. Glej Prilogo II, oddelek III.B.3).

⁽¹³⁵⁾ Glej Prilogo II, oddelek III.B.3. Iz predloženega primera izhaja, da je redni obrambni inšpekcijski pregled v letu 2016 o „zavedanju pravne skladnosti oziroma pripravljenosti nanjo“ med drugim vključeval „stanje varstva osebnih informacij“ (upravljanje, hramba itd.). V poročilu o tem so navedeni primeri neustreznega upravljanja podatkov, zato poročilo vsebuje tudi poziv k izboljšanju na tem področju. Ministrstvo za obrambo je poročilo objavilo na svoji spletni strani.

vstopi v prostore (pisarne) in zahteva predložitev dokumentov ali informacij, vključno s pojasnili namestnika pomočnika ministra za obrambo. Inšpekcijski pregled se zaključi s poročilom ministru za obrambo, v katerem se navedejo ugotovitve in ukrepi za izboljšanje (njihovo izvajanje je mogoče preveriti v okviru nadaljnjih inšpekcijskih pregledov). Poročilo je nato podlaga za izdajo navodil ministra za obrambo glede izvajanja ukrepov, potrebnih za obravnavo primera; pooblastilo za izvajanje takih ukrepov ima namestnik pomočnika ministra, ki mora o tem tudi poročati.

- (162) Nadzor prefekturne policije zagotavljajo neodvisne prefekturne komisije za javno varnost, kot je pojasnjeno v uvodni izjavi 135 glede preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.
- (163) Nazadnje, kot je bilo navedeno, lahko obveščevalna agencija za javno varnost izvaja preiskave le, kolikor je to potrebno v zvezi s sprejetjem prepovedi, razpustitve ali opazovanja na podlagi zakona o preprečevanju subverzivnih dejavnosti oziroma zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora, in v zvezi s temi ukrepi neodvisna ⁽¹³⁶⁾ komisija za proučevanje javne varnosti izvaja vnaprejšnji nadzor. Poleg tega posebej imenovani inšpektorji opravljajo redne oziroma periodične inšpekcijske preglede (ki celovito preverijo delovanje obveščevalne agencije za javno varnost) ⁽¹³⁷⁾ in posebne notranje inšpekcijske preglede ⁽¹³⁸⁾ dejavnosti posameznih oddelkov oziroma uradov itd.; na njihovi podlagi pa se lahko izdajo navodila vodjem zadevnih oddelkov itd. glede popravnih ukrepov ali ukrepov za izboljšanje.
- (164) Ti nadzorni mehanizmi, ki jih nadalje krepi možnost posameznikov zahtevati poseg komisije za varstvo osebnih informacij kot neodvisnega nadzornega organa (glej v nadaljevanju oddelek 168), zagotavljajo ustrezno varstvo pred tveganji, da bi japonski organi zlorabili svoja pooblastila na področju nacionalne varnosti, in pred kakršnim koli nezakonitim zbiranjem elektronskih informacij.

3.3.3 Pravna sredstva posameznikov

- (165) V zvezi s pravnimi sredstvi posameznikov velja, da si morajo upravni organi glede osebnih informacij, ki jih zbirajo in s tem „hranijo“, „prizadevati za ustrezno in hitro obravnavo vsake pritožbe“ v zvezi s tako obdelavo (člen 48 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi).
- (166) Poleg tega za razliko od kazenskih preiskav velja, da imajo posamezniki (vključno s tujimi državljani, ki živijo v tujini) na podlagi zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, načeloma pravico do razkritja ⁽¹³⁹⁾, popravka (vključno z izbrisom) in začasnega prenehanja uporabe/posredovanja. Ob tem pa velja, da lahko vodja upravnega organa zavrne razkritje informacij, „v zvezi s katerimi obstajajo utemeljeni razlogi [...] za domnevo, da bi razkritje lahko škodovalo nacionalni varnosti“ (člen 14(iv) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi); to lahko stori tudi tako, da ne razkrije niti obstoja takih informacij (člen 17 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi). Podobno velja, da čeprav lahko posameznik zahteva začasno prenehanje uporabe ali izbris na podlagi člena 36(1)(i) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, če je upravni organ informacije pridobil nezakonito ali če jih hrani oziroma uporablja zunaj okvira, ki je potreben za doseganje posameznega namena, lahko organ zavrne zahtevo, če ugotovi, da bi začasno prenehanje uporabe „lahko oviralo ustrezno izvajanje nalog, ki se nanašajo na namen uporabe hranjenih osebnih informacij, zaradi narave takih nalog“ (člen 38 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi). Kljub temu velja, da če je mogoče brez težav ločiti in izločiti dele, za katere velja izjema, morajo upravni organi odobriti vsaj delo razkritje (glej na primer člen 15(1) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi) ⁽¹⁴⁰⁾.

⁽¹³⁶⁾ V skladu z zakonom o ustanovitvi komisije za proučevanje javne varnosti predsednik in člani komisije „neodvisno izvajajo svoje pristojnosti“ (člen 3). Imenuje jih predsednik vlade ob soglasju obeh domov parlamenta, razrešijo pa se lahko samo „z razlogom“ (npr. zaporna kazen, neprimerno ravnanje, duševna ali fizična motnja, začetek stečajnega postopka).

⁽¹³⁷⁾ Ureditev periodičnih inšpekcijskih pregledov obveščevalne agencije za javno varnost (generalni direktor navedene agencije, navdilo št. 4 iz leta 1986).

⁽¹³⁸⁾ Ureditev posebnih inšpekcijskih pregledov obveščevalne agencije za javno varnost (generalni direktor navedene agencije, navdilo št. 11 iz leta 2008). Posebni inšpekcijski pregledi se izvajajo, kadar generalni direktor obveščevalne agencije za javno varnost meni, da so potrebni.

⁽¹³⁹⁾ To se nanaša na pravico prejeti izvod „hranjenih osebnih informacij“.

⁽¹⁴⁰⁾ Glej tudi možnost „diskrecijskega razkritja“, tudi kadar so del „hranjenih osebnih informacij“, za katere se zahteva razkritje, „informacije, ki se ne razkrivajo“ (člen 16 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi).

- (167) V vsakem primeru mora upravni organ v določenem roku sprejeti pisno odločbo (30 dni; ta rok se pod nekaterimi pogoji lahko podaljša še za 30 dni). Če je zahteva zavrnjena ali ji je ugodeno le delno ali pa posameznik iz drugih razlogov meni, da je ravnanje upravnega organa „nezakonito ali nepravilno“, lahko posameznik zahteva upravno presojo na podlagi zakona o upravnih pravnih sredstvih⁽¹⁴¹⁾. V takem primeru se vodi upravnega organa, ki odloča o pritožbi, posvetuje z nadzornim odborom za razkritje informacij in varstvo osebnih informacij (člena 42 in 43 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi), ki je specializiran neodvisen odbor, katerega člane imenuje predsednik vlade ob soglasju obeh domov parlamenta. Iz prejetih informacij izhaja, da lahko nadzorni odbor izvede preiskavo⁽¹⁴²⁾ in s tem v zvezi od upravnega organa zahteva predložitev hranjenih osebnih informacij, vključno z morebitnimi tajnimi vsebinami, ter nadaljnjih informacij in dokumentov. Čeprav končno poročilo, ki se pošlje pritožniku in upravnemu organu ter razkrije javnosti, ni pravno zavezujoče, se v skoraj vseh primerih upošteva⁽¹⁴³⁾. Poleg tega ima posameznik možnost pred sodiščem izpodbijati odločitev o pritožbi, na podlagi zakona o upravnem sporu. To omogoča sodni nadzor nad uporabo izjem iz razloga nacionalne varnosti, vključno s tem, ali je bila taka izjema zlorabljena oziroma ali je še upravičena.
- (168) Ministrstvo za notranje zadeve in komunikacije je z namenom olajšati uveljavljanja zgoraj navedenih pravic na podlagi zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, ustanovilo 51 „celovitih informacijskih centrov“, ki zagotavljajo celovite informacije o navedenih pravicah, postopkih, ki se uporabljajo za vložitev zahteve, in morebitnih pravnih sredstvih⁽¹⁴⁴⁾. Upravni organi pa morajo zagotoviti „informacije, ki pripomorejo k opredelitvi hranjenih osebnih informacij“⁽¹⁴⁵⁾, in sprejeti „druge ustrezne ukrepe, ki so v korist osebi, ki namerava vložiti zahtevo“ (člen 47(1) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi).
- (169) Tako kot v primeru preiskav na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj lahko posamezniki tudi na področju nacionalne varnosti izkoristijo pravno varstvo tako, da se neposredno obrnejo na komisijo za varstvo osebnih informacij. S tem se začne poseben postopek reševanja sporov, ki ga je vzpostavila japonska vlada za posameznike iz EU, katerih osebni podatki se prenašajo na podlagi tega sklepa (glej podrobno pojasnilo v uvodnih izjavah 141–144 in v uvodni izjavi 149).
- (170) Poleg tega lahko posamezniki zahtevajo sodno varstvo v obliki odškodninske tožbe na podlagi zakona o nadomestilih države, ki vključuje tudi nematerialno škodo in pod nekaterimi pogoji tudi izbris zbranih podatkov (glej uvodno izjavo 147).

4. SKLEP: USTREZNA RAVEN VARSTVA OSEBNIH PODATKOV, KI SE POSLOVNIM SUBJEKTOM NA JAPONSKEM PRENAŠAJO IZ EVROPSKE UNIJE

- (171) Evropska komisija meni, da zakon o varstvu osebnih informacij in dopolnilna pravila iz Priloge I ter uradne navedbe, zagotovila in zaveze iz Priloge II zagotavljajo raven varstva osebnih podatkov, ki se prenašajo iz Evropske unije, ki je v osnovi enakovredna tisti, ki jo zagotavlja Uredba (EU) 2016/679.
- (172) Poleg tega Evropska komisija meni, da gledano v celoti nadzorni mehanizmi in pravna sredstva v japonskem pravu v praksi omogočajo ugotavljanje in kaznovanje kršitev, ki jih storijo poslovni subjekti, ki obravnavajo osebne informacije in ki take informacije prejmejo, ter da posameznikom, na katere se nanašajo osebni podatki, zagotavljajo pravna sredstva, s katerimi lahko pridobijo dostop do osebnih podatkov, ki se nanašajo nanj, in po potrebi zagotovijo popravek ali izbris takih podatkov.

⁽¹⁴¹⁾ Zakon o upravnih pravnih sredstvih (zakon št. 160 iz leta 2014), zlasti člen 1(1).

⁽¹⁴²⁾ Glej člen 9 zakona o ustanovitvi nadzornega odbora za razkritje informacij in varstvo osebnih informacij (zakon št. 60 iz leta 2003).

⁽¹⁴³⁾ Iz prejetih informacij izhaja, da v 13 letih od leta 2005 (ko je začel veljati zakon o varstvu osebnih informacij, ki jih hranijo upravni organi) upravni organ ni upošteval poročila samo v dveh primerih od več kot 2000 primerov, čeprav je nadzorni odbor v številnih primerih nasprotoval upravnim odločbam. Poleg tega mora upravni organ, ki sprejme odločitev, ki odstopa od ugotovitev v poročilu, jasno navesti razloge za to. Glej Prilogo II, oddelek III.C, s sklicevanjem na člen 50(1)(iv) zakona o upravnih pravnih sredstvih.

⁽¹⁴⁴⁾ Celoviti informacijski centri – eden v vsaki prefekturi – državljanom dajejo pojasnila glede osebnih podatkov, ki jih zbirajo javni organi (npr. obstoječe podatkovne zbirke), in veljavnih pravil o varstvu podatkov (zakon o varstvu osebnih informacij, ki jih hranijo upravni organi), vključno s tem, kako uveljavljati pravico do razkritja popravka ali začasnega prenehanja uporabe. Hkrati delujejo kot kontaktna točka za poizvedbe in pritožbe državljanov. Glej Prilogo II, oddelek II.C.4)(a).

⁽¹⁴⁵⁾ Glej tudi člena 10 in 11 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, o „evidenci datotek osebnih informacij“, ki pa vključuje obsežne izjeme glede „datotek osebnih informacij“, pripravljenih ali pridobljenih za namene kazenske preiskave ali ki se nanašajo na varnost in druge pomembne interese države (glej člen 10(2)(i) in (ii) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi).

- (173) Nazadnje, Evropska komisija na podlagi razpoložljivih informacij o japonskem pravnem redu, vključno z navedbami, zagotovili in zavezami japonske vlade iz Priloge II, meni, da so vsi posegi v temeljne pravice posameznikov, katerih osebne podatke iz Evropske unije na Japonsko prenašajo japonski javni organi v imenu javnega interesa, zlasti preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in nacionalne varnosti, omejeni na to, kar je nujno potrebno za doseganje zadevnega zakonitega cilja, ter da obstaja učinkovita pravna zaščita zoper take posege.
- (174) Zato Evropska komisija glede na ugotovitve iz tega sklepa meni, da Japonska zagotavlja ustrezno raven varstva osebnih podatkov, ki se iz Evropske unije prenašajo poslovnim subjektom, ki obravnavajo osebne informacije na Japonskem in za katere se uporablja zakon o varstvu osebnih informacij, razen v primerih, ko prejemnik spada v eno od kategorij iz člena 76(1) zakona o varstvu osebnih informacij in vsi nameni obdelave ali njihov del ustrezajo enemu od namenov iz navedene določbe.
- (175) Na tej podlagi Evropska komisija ugotavlja, da je standard ustreznosti iz člena 45 Uredbe (EU) 2016/679, razlagan v smislu Listine Evropske unije o temeljnih pravicah, zlasti ob upoštevanju sodbe v zadevi Schrems ⁽¹⁴⁶⁾, izpolnjen.

5. UKREPI ORGANOV ZA VARSTVO PODATKOV IN OBVEŠČANJE KOMISIJE

- (176) V skladu s sodno prakso Sodišča ⁽¹⁴⁷⁾ in kot je navedeno v členu 45(4) Uredbe (EU) 2016/679, bi morala Evropska komisija po sprejetju sklepa o ustreznosti redno spremljati razvoj dogodkov v tretji državi, da se presodi, ali Japonska še zagotavlja v osnovi enakovredno raven varstva. Tako preverjanje se v vsakem primeru zahteva, kadar Evropska komisija prejme kakršne koli informacije, ki zbujajo upravičen dvom o tem.
- (177) Evropska komisija bi zato morala stalno spremljati razmere glede pravnega okvira in dejanske prakse obdelave osebnih podatkov, kot je ovrednoteno v tem sklepu, vključno z zagotavljanjem skladnosti japonskih organov z navedbami, zagotovili in zavezami iz Priloge II. Za olajšanje tega postopka bi morali japonski organi Evropsko komisijo obveščati o razvoju dogodkov, bistvenih za ta sklep, in sicer glede obdelave osebnih podatkov s strani poslovnih subjektov ter glede omejitev in zaščitnih ukrepov, ki se uporabljajo v zvezi z dostopom javnih organov do osebnih podatkov. To bi moralo vključevati vse odločitve, ki jih komisija za varstvo osebnih informacij sprejme na podlagi člena 24 zakona o varstvu osebnih informacij in s katerimi se prizna, da tretja država zagotavlja raven varstva, ki je enakovredna tisti, ki jo zagotavlja Japonska.
- (178) Poleg tega bi morale države članice Evropsko komisijo obveščati o vseh pomembnih ukrepih nacionalnih organov za varstvo podatkov, zlasti glede poizvedb ali pritožb posameznikov iz EU, na katere se nanašajo osebni podatki, glede prenosa osebnih podatkov iz Evropske unije poslovnim subjektom na Japonskem, da se Evropski komisiji omogoči učinkovito izvajanje njene funkcije spremljanja. Evropska komisija bi morala biti obveščena tudi o vseh indicijah, da ukrepi japonskih javnih organov, odgovornih za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj oziroma za nacionalno varnost, vključno z vsemi nadzornimi organi, ne zagotavljajo zahtevane ravni varnosti.
- (179) Države članice in njihovi organi morajo sprejeti ukrepe, potrebne za zagotavljanje skladnosti z akti institucij Unije, saj se domneva, da so ti zakoniti in imajo pravne učinke, dokler niso umaknjeni, razveljavljeni na podlagi izpodbijne tožbe ali razglašeni za neveljavne na podlagi predloga za sprejetje predhodne odločbe ali sklicevanja na nezakonnost. Zato je sklep Evropske komisije o ustreznosti varstva, sprejet na podlagi člena 45(3) Uredbe (EU) 2016/679, zavezujoč za vse organe držav članic, na katere je naslovljen, vključno z njihovimi neodvisnimi nadzornimi organi. Hkrati pa velja, kot je bilo pojasnjeno v sodbi Sodišča ⁽¹⁴⁸⁾ v zadevi Schrems in priznано v členu 58(5) Uredbe, da če organ za varstvo podatkov prejme pritožbo, ki zbujajo dvom o skladnosti sklepa Evropske komisije o ustreznosti varstva s temeljnimi pravicami posameznika do zasebnosti in varstva podatkov, ter meni, da so predloženi očitki dobro utemeljeni, mu mora nacionalna zakonodaja zagotavljati pravno sredstvo za predložitev teh očitkov nacionalnemu sodišču, ki mora v primeru dvomov prekiniti postopek in Sodišču predložiti predlog za sprejetje predhodne odločbe ⁽¹⁴⁹⁾.

⁽¹⁴⁶⁾ Glej sprotno opombo 3.

⁽¹⁴⁷⁾ Sodba v zadevi Schrems, točka 76.

⁽¹⁴⁸⁾ Sodba v zadevi Schrems, točka 65.

⁽¹⁴⁹⁾ Sodba v zadevi Schrems, točka 65: „V zvezi s tem mora nacionalni zakonodajalec določiti pravna sredstva, ki zadevnemu nacionalnemu nadzornemu organu omogočajo, da očitke, ki jih šteje za utemeljene, predloži nacionalnim sodiščem, da bi ta, če bi prav tako kot ta organ dvomila o veljavnosti odločbe Komisije, sprožila postopek predhodnega odločanja za preizkus veljavnosti navedene odločbe.“

6. REDNI PREGLEDI UGOTOVITEV GLEDE USTREZNOSTI

- (180) Evropska komisija bi morala po sprejetju tega sklepa, na podlagi člena 45(3) Uredbe (EU) 2016/679⁽¹⁵⁰⁾ in glede na dejstvo, da se raven varstva, ki ga zagotavlja japonski pravni red, lahko spremeni, redno preverjati, ali so ugotovitve, ki se nanašajo na ustreznost ravni varnosti, ki jo zagotavlja Japonska, še vedno dejansko in pravno upravičene.
- (181) V ta namen bi bilo treba ta sklep prvič pregledati v dveh letih po njegovem začetku veljavnosti. Komisija v tesnem posvetovanju z odborom, ustanovljenim v skladu s členom 93(1) Splošne uredbe o varstvu podatkov, po tem prvem pregledu in glede na njegove rezultate odloči, ali je treba ohraniti dveletni cikel. V vsakem primeru morajo nadaljnji pregledi potekati vsaj vsaka štiri leta⁽¹⁵¹⁾. Pregled bi moral obsegati vse vidike učinkovanja tega sklepa, zlasti uporabo dopolnilnih pravil (pri čemer je treba posebno pozornost nameniti varstvu, ki se zagotavlja v primeru nadaljnjih prenosov), uporabo pravil o privolitvi, tudi v primeru umika, učinkovitost uveljavljanja pravic posameznikov ter omejitve in zaščitne ukrepe glede vladnega dostopa, vključno z mehanizmom pravnih sredstev, kot je navedeno v Prilogi II k temu sklepu. Prav tako bi moral zajemati učinkovitost nadzora in izvrševanja v zvezi s pravili, ki se uporabljajo za poslovne subjekte, ki obravnavajo osebne informacije, ter na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in nacionalne varnosti.
- (182) Evropska komisija bi se morala pri izvajanju pregleda srečati s komisijo za varstvo osebnih informacij, ki bi jo po potrebi spremljali drugi japonski organi, odgovorni za vladni dostop, vključno z zadevnimi nadzornimi organi. Možnost sodelovanja na takem sestanku bi morali imeti tudi predstavniki članov Evropskega odbora za varstvo podatkov. Evropska komisija bi morala v okviru skupnega pregleda od komisije za varstvo osebnih informacij zahtevati predložitev celovitih informacij o vseh vidikih, pomembnih za ugotavljanje ustreznosti, tudi o omejitvah in zaščitnih ukrepih v zvezi z vladnim dostopom⁽¹⁵²⁾. Evropska komisija bi morala tudi zahtevati pojasnila o vseh prejetih informacijah, pomembnih za ta sklep, vključno z javnimi poročili japonskih organov ali drugih deležnikov na japonskem, Evropskega odbora za varstvo podatkov, posameznih organov za varstvo podatkov, skupin civilne družbe, poročil medijev ali katerih koli drugih razpoložljivih virov informacij.
- (183) Evropska komisija bi morala na podlagi skupnega pregleda pripraviti javno poročilo, ki se predloži Evropskemu parlamentu in Svetu.

7. ZADRŽANJE IZVAJANJA SKLEPA O USTREZNOSTI VARSTVA

- (184) Če Evropska komisija na podlagi rednih in občasnih preverjanj ali na podlagi katerih koli drugih razpoložljivih informacij ugotovi, da ravni varstva, ki ga zagotavlja japonski pravni red, ni mogoče več šteti kot v osnovi enakovredno tisti v Evropski uniji, bi morala o tem obvestiti pristojne japonske organe ter zahtevati sprejetje ustreznih ukrepov v določenem razumnem roku. To vključuje pravila, ki se nanašajo na poslovne subjekte in japonske javne organe, odgovorne za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali za nacionalno varnost. Tak postopek bi se na primer sprožil v primerih, ko se nadaljnji prenosi, tudi na podlagi odločitev, ki jih komisija za varstvo osebnih informacij sprejme na podlagi člena 24 zakona o varstvu osebnih informacij in s katerimi se prizna, da tretja država zagotavlja raven varstva, ki je enakovredna tisti, ki jo zagotavlja Japonska, ne bodo več opravljali ob upoštevanju zaščitnih ukrepov, ki zagotavljajo stalnost varstva v smislu člena 44 Splošne uredbe o varstvu podatkov.
- (185) Če v določenem obdobju pristojni japonski organi ne dokažejo, da ta sklep še temelji na ustrezni ravni varnosti, bi morala Evropska komisija na podlagi člena 45(5) Uredbe (EU) 2016/679 začeti postopek za začasno zadržanje izvajanje dela ali celotnega tega sklepa oziroma za njegovo razveljavitev. Druga možnost je, da bi Evropska komisija začela postopek za spremembo tega sklepa, zlasti z uvedbo dodatnih pogojev za prenos podatkov ali omejitvijo področja uporabe ugotovitve o ustreznosti varstva samo na prenose podatkov, za katere je zagotovljena stalnost varstva v smislu člena 44 Splošne uredbe o varstvu podatkov.

⁽¹⁵⁰⁾ V skladu s členom 45(3) Uredbe (EU) 2016/679 se v „izvedbenem aktu [...] določi mehanizem za redni pregled, vsaj vsaka štiri leta, ki v celoti upošteva razvoj dogodkov na zadevnem področju v tretji državi ali mednarodni organizaciji“.

⁽¹⁵¹⁾ Člen 45(3) Uredbe (EU) 2016/679 določa, da mora biti redni pregled izveden vsaj vsaka štiri leta. Glej tudi Evropski odbor za varstvo podatkov, referenčni dokument o ustreznosti, WP 254 rev.01.

⁽¹⁵²⁾ Glej tudi Prilogo II, oddelek IV: „V okviru rednega pregleda sklepa o ustreznosti si komisija za varstvo osebnih informacij in Evropska komisija izmenjujeta informacije o obdelavi podatkov pod pogoji iz ugotovitev glede ustreznosti, vključno s tistimi iz teh navedb.“

- (186) Evropska komisija bi morala zlasti začeti postopek za začasno zadržanje izvajanja ali razveljavitev v primeru indicov, da poslovni subjekti, ki prejemajo osebne podatke na podlagi tega sklepa, ne upoštevajo dopolnilnih pravil iz Priloge I in/ali da se ta pravila ne izvršujejo učinkovito, ali da japonski organi ne upoštevajo navedb, zagotovil in zavez iz Priloge II k temu sklepu.
- (187) Evropska komisija bi morala o začetku postopka za spremembo, začasno zadržanje izvajanja ali razveljavitev tega sklepa presoditi tudi, če v okviru skupnega pregleda ali na drug način japonski organi ne zagotovijo informacij ali pojasnil, potrebnih za oceno ravni varstva, ki se zagotavlja glede osebnih podatkov, prenesenih iz Evropske unije na Japonsko, ali skladnosti s tem sklepom. V tem smislu bi morala Evropska komisija upoštevati, v kolikšni meri je mogoče zadevne informacije pridobiti iz drugih virov.
- (188) Evropska komisija bi morala na podlagi ustreznih utemeljenih razlogov nujnosti, kot je tveganje resne kršitve pravic posameznikov, na katere se nanašajo osebni podatki, preučiti možnost sprejetja sklepa o začasnem zadržanju izvajanja ali razveljavitvi tega sklepa, ki bi se začel takoj uporabljati, na podlagi člena 93(3) Uredbe (EU) 2016/679 v povezavi s členom 8 Uredbe št. 182/2011 Evropskega parlamenta in Sveta ⁽¹⁵³⁾.

8. SKLEPNE UGOTOVITVE

- (189) Evropski odbor za varstvo podatkov je objavil svoje mnenje ⁽¹⁵⁴⁾, ki je bilo upoštevano pri pripravi tega sklepa.
- (190) Evropski parlament je sprejel resolucijo o digitalni trgovinski strategiji, ki Evropsko komisijo poziva, naj pod pogoji iz Uredbe (EU) 2016/679 nameni prednost sprejemanju sklepov o ustreznosti s pomembnimi trgovinskimi partnerji in ga pospeši, saj je to pomemben mehanizem za zaščito prenosa osebnih podatkov iz Evropske unije ⁽¹⁵⁵⁾. Evropski parlament je sprejel tudi resolucijo o ustreznosti varstva osebnih podatkov, ki ga zagotavlja Japonska ⁽¹⁵⁶⁾.
- (191) Ukrepi v tem sklepu so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 93(1) Direktive Splošne uredbe o varstvu podatkov –

SPREJELA NASLEDNJI SKLEP:

Člen 1

1. Japonska za namene člena 45 Uredbe (EU) 2016/679 zagotavlja ustrezno raven varstva osebnih podatkov, ki se iz Evropske unije prenašajo poslovnim subjektom, ki obravnavajo osebne informacije na Japonskem in za katere se uporablja zakon o varstvu osebnih informacij, kot ga dopolnjujejo dopolnilna pravila iz Priloge I ter uradne navedbe, zagotovila in zaveze iz Priloge II.

⁽¹⁵³⁾ Uredba (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije (UL L 55, 28.2.2011, str. 13).

⁽¹⁵⁴⁾ Mnenje 28/2018 o osnutku izvedbenega sklepa Evropske komisije o ustreznem varstvu osebnih podatkov na Japonskem, sprejeto 5. decembra 2018.

⁽¹⁵⁵⁾ Resolucija Evropskega parlamenta z dne 12. decembra 2017 „Digitalni trgovinski strategiji naproti“ (2017/2065(INI)). Glej zlasti točko 8 („[...] želi spomniti, da se lahko osebni podatki prenesejo v tretje države brez uporabe splošnih obveznosti iz trgovinskih sporazumov, kadar so izpolnjene zahteve – tako v sedanosti kot v prihodnosti – iz [...] poglavja V Uredbe (EU) 2016/679; priznava, da so sklepi o ustreznosti, vključno z delnimi in sektorskimi sklepi, eden temeljnih mehanizmov za zaščito prenosa osebnih podatkov iz EU v tretjo državo; ugotavlja, da je EU sprejela sklepe o ustreznosti s samo štirimi od svojih 20 največjih trgovinskih partnerjev [...]“) in točko 9 („poziva Komisijo, naj nameni prednost sprejemanju sklepov o ustreznosti in ga pospeši, v kolikor tretje države v skladu s svojo zakonodajo ali svojimi mednarodnimi obveznostmi zagotovijo raven zaščite, ki je ‚v bistvu enakovredna‘ ravni, zagotovljeni v EU [...]“).

⁽¹⁵⁶⁾ Resolucija Evropskega parlamenta z dne 13. decembra 2018 o ustreznosti varstva osebnih podatkov, ki ga zagotavlja Japonska (2018/2979 (RSP)).

2. Ta sklep se ne nanaša na osebne podatke, ki se prenašajo prejemnikom, ki spadajo v eno od naslednjih kategorij, kolikor vsi nameni obdelave osebnih podatkov ali samo njihov del ustrezajo enemu od navedenih namenov, in sicer:

- (a) institucije za radiodifuzijo, časopisni založniki, agencije za komuniciranje ali druge medijske organizacije (vključno z vsemi posamezniki, ki opravljajo dejavnost obveščanja javnosti kot svojo dejavnost), kolikor obdelujejo osebne informacije za namene obveščanja javnosti;
- (b) osebe, ki se poklicno ukvarjajo s pisanjem, kolikor to zajema osebne podatke;
- (c) univerze in vse druge organizacije ali skupine, namenjene akademskemu študiju, ali vse osebe, ki pripadajo taki organizaciji ali skupini, kolikor obdelujejo osebne podatke za namene akademskega študija;
- (d) verski subjekti, kolikor obdelujejo osebne podatke za namene verskih dejavnosti (vključno z vsemi povezanimi dejavnostmi) ter
- (e) politični subjekti, kolikor obdelujejo osebne podatke za namene svoje politične dejavnosti (vključno z vsemi povezanimi dejavnostmi).

Člen 2

Kadar pristojni organi države članice z namenom zaščite posameznikov v zvezi z obdelavo njihovih osebnih podatkov izvajajo svoja pooblastila na podlagi člena 58 Uredbe (EU) 2016/679, kar ima za posledico začasno zadržanje ali dokončno prepoved pretoka podatkov k določenemu poslovnemu subjektu na Japonskem v okviru področja uporabe iz člena 1, zadevna država članica o tem brez odlašanja obvesti Komisijo.

Člen 3

1. Komisija stalno spremlja uporabo pravnega okvira, na katerem temelji ta sklep, vključno s pogoji, pod katerimi se izvajajo nadaljnji prenosi tretjemu, da se oceni, ali Japonska še naprej zagotavlja ustrezno raven varstva v smislu člena 1.
2. Države članice in Komisija se medsebojno obveščajo o primerih, ko komisija za varstvo osebnih informacij ali kateri koli drug japonski pristojni organ ne zagotovi skladnosti s pravnim okvirom, na katerem temelji ta sklep.
3. Države članice in Komisija se medsebojno obveščajo o vseh utemeljenih sumih, da posegi japonskih javnih organov v pravico posameznikov do varstva njihovih osebnih podatkov presegajo tisto, kar je nujno potrebno, ali da zoper take posege ni učinkovitega pravnega varstva.
4. Komisija v dveh letih od uradnega obvestila državam članicam o tem sklepu, nato pa vsaj vsaka štiri leta, oceni ugotovitve iz člena 1(1) na podlagi vseh razpoložljivih informacij, vključno z informacijami, prejetimi v okviru skupnega pregleda, ki se opravi z zadevnimi japonskimi organi.
5. Če Komisija utemeljeno sumi, da ustrezna raven varstva ni več zagotovljena, o tem obvesti pristojne japonske organe. Po potrebi se lahko odloči začasno zadržati izvajanje tega sklepa, ga spremeniti ali razveljaviti ali pa omejiti njegovo področje uporabe, zlasti kadar obstajajo indici, da:
 - (a) poslovni subjekti na Japonskem, ki prejmejo osebne podatke iz Evropske unije na podlagi tega sklepa, ne upoštevajo dodatnih zaščitnih ukrepov iz dopolnilnih pravil iz Priloge I k temu sklepu, ali da nadzor in izvrševanje glede tega nista zadostna;
 - (b) japonski javni organi ne zagotavljajo skladnosti z navedbami, zagotovili in zavezami iz Priloge II k temu sklepu, vključno v zvezi s pogoji in omejitvami glede zbiranja osebnih podatkov, ki se prenašajo na podlagi tega sklepa, in dostopa do njih s strani japonskih javnih organov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali nacionalne varnosti.

Komisija lahko osnutke takih ukrepov predstavi tudi, če zaradi nesodelovanja japonskih organov ne more ugotoviti, ali je ugotovitev iz člena 1(1) tega sklepa prizadeta.

Člen 4

Ta sklep je naslovljen na države članice.

V Bruslju, 23. januarja 2019

Za Komisijo
Věra JOUROVÁ
Članica Komisije

PRILOGA 1

DOPOLNILNA PRAVILA NA PODLAGI ZAKONA O VARSTVU OSEBNIH INFORMACIJ GLEDE OBRAVNAVE PRENOSA OSEBNIH PODATKOV IZ EU NA PODLAGI SKLEPA O USTREZNOSTI

Kazalo

(1) Osebnne informacije, ki zahtevajo posebno skrb (odstavek 3 člena 2 zakona)	38
(2) Hranjeni osebni podatki (člen 2(7) zakona)	39
(3) Določanje namena uporabe, omejitev zaradi namena uporabe (odstavek 1 člena 15, odstavek 1 člena 16 ter odstavek 1 in 3 člena 26 zakona)	40
(4) Omejitve glede zagotavljanja tretji osebi v tuji državi (člen 24 zakona; člen 11-2 pravilnika)	41
(5) Anonimno obdelane informacije (člena 2(9) ter 36(1) in (2) zakona)	41

[Izrazi]

„zakon“	Zakon o varstvu osebnih informacij (zakon št. 57, 2003)
„vladna odredba“	Vladna odredba o izvajanju zakona o varstvu osebnih informacij (vladna odredba št. 507, 2003)
„pravilnik“	Pravilnik o izvajanju zakona o varstvu osebnih informacij (pravilnik komisije za varstvo osebnih informacij št. 3, 2016)
„smernice o splošnih pravilih“	Smernice za zakon o varstvu osebnih informacij (zvezek s splošnimi pravili) (obvestilo komisije za varstvo osebnih informacij št. 65, 2015)
„EU“	Evropska unija, vključno z državami članicami, ter, glede na sporazum o EGP, Islandijo, Lihtenštajnom in Norveško
„Splošna uredba o varstvu podatkov“	Uredba Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)
„sklep o ustreznosti“	sklep Evropske komisije, da tretja država ali ozemlje znotraj navedene tretje države itd. zagotavlja ustrezno raven varstva osebnih podatkov v skladu s členom 45 Splošne uredbe o varstvu podatkov

Komisija za varstvo osebnih podatkov je z namenom medsebojnega in nemotenega prenosa osebnih podatkov med Japonsko in EU opredelila EU kot tujo državo, ki vzpostavlja sistem varstva osebnih informacij, za katerega se priznava, da ima standarde glede varstva pravic in interesov posameznika, enakovredne standardom na Japonskem na podlagi člena 24 zakona, Evropska komisija pa je hkrati sklenila, da Japonska zagotavlja ustrezno raven varstva osebnih podatkov v skladu s členom 45 Splošne uredbe o varstvu podatkov.

S tem bo med Japonsko in EU medsebojen in nemoten prenos osebnih podatkov potekal na način, ki zagotavlja visoko raven varstva pravic in interesov posameznika. Komisija za varstvo osebnih podatkov je sprejela ta dopolnilna pravila, ki temeljijo na določbah zakona in zadevajo izvajanje itd. sodelovanja z vladami v drugih državah, da se zagotovi visoka raven varstva osebnih podatkov, prejetih iz EU na podlagi sklepa o ustreznosti, in sicer glede na to, da kljub visoki stopnji konvergence med sistemoma obstaja nekaj upoštevnihih razlik, ter zaradi zagotavljanja ustreznega obravnavanja osebnih podatkov, prejetih iz EU na podlagi sklepa o ustreznosti, s strani poslovnih subjektov, ki obravnavajo osebne informacije, in ustreznega in učinkovitega izvajanja obveznosti, določenih v takih pravilih⁽¹⁾.

⁽¹⁾ Člen 4, člen 6, člen 8, člen 24, člen 60 in člen 78 zakona ter člen 11 pravilnika.

Natančneje, člen 6 zakona določa pristojnost za sprejemanje potrebnih zakonodajnih in drugih ukrepov, da se zagotovi okrepljeno varstvo osebnih podatkov in vzpostavi mednarodno ustrezen sistem v zvezi z osebnimi podatki s strožjimi pravili, ki dopolnjujejo in presegajo tista iz zakona in vladne odredbe. Zato je komisija za varstvo osebnih podatkov kot organ, pristojen za upravljanje splošne uporabe zakona, pristojna za to, da v skladu s členom 6 zakona določi strožje predpise z oblikovanjem teh dopolnilnih pravil, ki določajo višjo raven varstva pravic in interesov posameznika v zvezi z obdelavo osebnih podatkov, prejetih iz EU na podlagi sklepa o ustreznosti, vključno glede opredelitve osebnih informacij, ki zahtevajo posebno skrb, v skladu z odstavkom 3 člena 2 zakona in hranjenih osebnih podatkov v skladu z odstavkom 7 člena 2 zakona (vključno z zadevnim obdobjem hrambe).

Na tej podlagi so dopolnilna pravila zavezujoča za poslovni subjekt, ki obravnava osebne informacije, ki prejme osebne podatke, prenesene iz EU na podlagi sklepa o ustreznosti, tako da jih mora ta poslovni subjekt spoštovati. Kot pravno zavezujoči predpisi so vse pravice in obveznosti izvršljive s strani komisije za varstvo osebnih podatkov na enak način kot določbe zakona, ki jih te dopolnjujejo s strožjimi in/ali podrobnejšimi pravili. V primeru kršitve pravic in obveznosti, ki izhajajo iz dopolnilnih pravil, lahko posamezniki uveljavljajo tudi pravna sredstva pred sodišči na enak način kot v zvezi z določbami zakona, ki jih te dopolnjujejo s strožjimi in/ali podrobnejšimi pravili.

Kar zadeva izvrševanje s strani komisije za varstvo osebnih podatkov, je komisija za varstvo osebnih podatkov v primeru, da poslovni subjekt, ki obravnava osebne informacije, ne izpolnjuje ene ali več obveznosti iz dopolnilnih pravil, pristojna za sprejetje ukrepov v skladu s členom 42 zakona. Na splošno glede osebnih informacij, prejetih iz EU na podlagi sklepa o ustreznosti, velja, da če poslovni subjekt, ki obravnava osebne informacije, brez zakonitega razloga ⁽²⁾ ne ukrepa v skladu s priporočilom, prejetim na podlagi odstavka 1 člena 42 zakona, to šteje za resno in takojšnjo kršitev posameznikovih pravic in interesov v smislu odstavka 2 člena 42 zakona.

(1) Osebne informacije, ki zahtevajo posebno skrb (odstavek 3 člena 2 zakona)

Člen 2(3) zakona

(3) „Osebne informacije, ki zahtevajo posebno skrb“ v tem zakonu pomenijo osebne informacije o principalovi rasi, nazoru, družbenem položaju, zdravstveni anamnezi, kazenski evidenci, dejstvu, ali je kdaj utrpel škodo zaradi kaznivega dejanja, ali druge opise itd., ki so na podlagi vladne odredbe opredeljeni kot tisti, katerih obravnava zahteva posebno skrb, da principal ne utрпи nepoštene diskriminacije, predsodkov ali da ni drugače prikrajšan.

Člen 2 vladne odredbe

Opisi itd., predpisani v vladni odredbi na podlagi odstavka 3 člena 2 zakona, so tisti, ki vsebujejo kar koli od spodaj navedenega (razen opisov, ki spadajo v zdravstveno kartoteko ali kazensko evidenco principala):

- (i) telesna invalidnost, motnje v intelektualnem razvoju, duševna prizadetost (vključno z motnjami v razvoju) ali druge funkcionalne telesne in duševne motnje, ki so zajete s pravilnikom komisije za varstvo osebnih informacij;
- (ii) rezultati zdravniških pregledov ali drugih preiskav (v nadaljnjem besedilu: zdravniški pregledi itd.) za namen preprečevanja in zgodnjega odkrivanja bolezni, ki jih principal opravi pri zdravniku ali drugi osebi, ki opravlja naloge, povezane z medicino (v nadaljnjem besedilu: zdravnik itd.);
- (iii) dejstvo, da je zdravnik itd. principalu dal napotke za izboljšanje duševnega in telesnega stanja, nudil zdravniško oskrbo ali predpisal zdravniški recept na podlagi rezultatov zdravniškega pregleda itd. ali zaradi bolezni, telesnih poškodb ali drugih duševnih in fizičnih sprememb;
- (iv) dejstvo, da so bili zoper principala kot osumljenca ali obtoženca opravljeni odvzem prostosti, preiskava, zaseg, pridržanje, kazenski pregon ali drugi postopki v zvezi s kazensko zadevo;

⁽²⁾ Zakoniti razlog pomeni dogodek izredne narave, ki je zunaj nadzora poslovnega subjekta, ki obravnava osebne informacije, in ki ga ni mogoče razumno predvideti (na primer naravne nesreče), ali položaj, ko potreba po ukrepanju v zvezi s priporočilom, ki ga je izdala komisija za varstvo osebnih podatkov na podlagi odstavka 1 člena 42 zakona, preneha, ker je poslovni subjekt, ki obravnava osebne informacije, sprejel alternativne ukrepe, s katerimi se je kršitev v celoti odpravila.

- (v) dejstvo, da so bili zoper principala kot mladoletnega prestopnika ali osebo, osumljeno mladoletnega prestopništva, v skladu z odstavkom 1 člena 3 zakona o mladoletnikih opravljeni preiskava, ukrep za opazovanje in zaščito, zaslišanje in odločba, zaščitni ukrep ali drugi postopki, povezani z zadevo v zvezi z varstvom mladoletnikov.

Člen 5 pravilnika

Funkcionalne telesne in duševne motnje, zajete s pravilnikom komisije za varstvo osebnih informacij na podlagi točke (i) člena 2 odredbe, so naslednje:

- (i) telesne motnje iz razpredelnice, priložene k zakonu o socialnih pravicah oseb s telesnimi motnjami (zakon št. 283 iz leta 1949);
- (ii) motnje v intelektualnem razvoju iz zakona o socialnih pravicah oseb z motnjami v intelektualnem razvoju (zakon št. 37 iz leta 1960);
- (iii) duševne motnje iz zakona o duševnem zdravju in socialnih pravicah oseb z duševno prizadetostjo (zakon št. 123 iz leta 1950) (vključno z motnjami v razvoju iz odstavka 1 člena 2 zakona o podpori osebam z motnjami v razvoju in brez motenj v intelektualnem razvoju iz zakona o socialnih pravicah oseb z motnjami v intelektualnem razvoju);
- (iv) bolezni, za katere ni vzpostavljenih metod zdravljenja, ali druge posebne bolezni, katerih resnost je z vladno odredbo na podlagi odstavka 1 člena 4 zakona o celoviti podpori za dnevno in socialno življenje invalidov (zakon št. 123 iz leta 2005) opredeljena kot enakovredna tistim, ki jih je na podlagi navedenega odstavka opredelil minister za zdravje, delo in socialne zadeve.

Če osebni podatki, prejeti iz EU na podlagi sklepa o ustreznosti, vsebujejo podatke o spolnem življenju ali spolni usmerjenosti fizične osebe ali o njenem članstvu v sindikatu, ki so v skladu s Splošno uredbo o varstvu podatkov opredeljeni kot posebne vrste osebnih podatkov, morajo poslovni subjekti, ki obravnavajo osebne informacije, te osebne podatke obravnavati enako kot osebne informacije, ki zahtevajo posebno skrb, v smislu odstavka 3 člena 2 zakona.

(2) Hranjeni osebni podatki (člen 2(7) zakona)

Člen 2(7) zakona

- (7) „Hranjeni osebni podatki“ v tem zakonu pomenijo osebne podatke, ki jih poslovni subjekt, ki obravnava osebne informacije, lahko razkrije, popravi, doda ali izbriše njihovo vsebino, preneha uporabljati, izbriše in preneha zagotavljati tretjim osebam, in ki z vladno odredbo niso opredeljeni kot taki, ki bi verjetno škodili javnim ali drugim interesom, če bi se zvedelo za njihov obstoj ali neobstoj, niti niso tisti, ki jih je treba izbrisati v roku, ki ni daljši od enega leta in je predpisan z vladno odredbo.

Člen 4 vladne odredbe

Osebni podatki, opredeljeni z vladno odredbo na podlagi odstavka 7 člena 2, so naslednji:

- (i) tisti, v zvezi s katerimi obstaja možnost povzročitve škode za življenje, telo ali premoženje principala ali tretje osebe, če se izve za njihov obstoj ali neobstoj;
- (ii) tisti, v zvezi s katerimi obstaja možnost spodbuditve ali sprožitve nezakonitega ali nepravičnega dejanja, če se izve za njihov obstoj ali neobstoj;
- (iii) tisti, v zvezi s katerimi obstaja možnost poslabšanja nacionalne varnosti, uničenja odnosa zaupanja s tujo državo ali mednarodno organizacijo ali škodovanja pogajanjem s tujo državo ali mednarodno organizacijo, če se izve za njihov obstoj ali neobstoj;
- (iv) tisti, v zvezi s katerimi obstaja možnost oviranja vzdrževanja javne varnosti in javnega reda, kot so preprečevanje, zatiranje ali preiskovanje kaznivih dejanj, če se izve za obstoj ali neobstoj takih osebnih podatkov.

Člen 5 vladne odredbe

Obdobje, določeno z vladno odredbo na podlagi odstavka 7 člena 2 zakona, je šest mesecev.

Osební podatki, prejeti iz EU na podlagi sklepa o ustreznosti, se obravnavajo kot hranjeni osebni podatki v smislu odstavka 7 člena 2 zakona, ne glede na predvideni rok njihovega izbrisa.

Če osebni podatki, prejeti iz EU na podlagi sklepa o ustreznosti, spadajo med osebne podatke, ki so z vladno odredbo opredeljeni kot tisti, pri katerih je „verjetno, da bodo škodili javnim ali drugim interesom, če se izve za njihov obstoj ali neobstoj,“ takih podatkov ni treba obravnavati kot hranjene osebne podatke (glej člen 4 vladne odredbe; Smernice o splošnih pravilih, „2-7. Hranjeni osebni podatki“).

(3) Določanje namena uporabe, omejitev zaradi namena uporabe (odstavek 1 člena 15, odstavek 1 člena 16 ter odstavek 1 in 3 člena 26 zakona)

Člen 15(1) zakona

- (1) Poslovni subjekt, ki obravnava osebne informacije, mora pri obravnavi osebnih informacij čim bolj izrecno opredeliti namen, za katerega bo uporabljal osebne informacije (v nadaljnjem besedilu: namen uporabe).

Člen 16(1) zakona

- (1) Poslovni subjekt, ki obravnava osebne informacije, osebnih informacij brez predhodno pridobljenega soglasja principala ne obravnava zunaj okvira, ki je potreben za doseganje namena uporabe, opredeljenega v skladu z določbami iz prejšnjega člena.

Člen 26(1) in (3) zakona

- (1) Poslovni subjekt, ki obravnava osebne informacije, ob prejemu osebnih podatkov, ki jih je zagotovila tretja oseba, v skladu s pravilnikom komisije za varstvo osebnih informacij preveri naslednje: (izpuščeno)

(i) (izpuščeno)

(ii) okoliščine, v katerih je navedena tretja oseba pridobila navedene osebne podatke.

- (3) Poslovni subjekt, ki obravnava osebne informacije, mora po preverjanju v skladu z določbami odstavka 1 v skladu s pravilnikom komisije za varstvo osebnih informacij voditi evidenco o datumu prejema zagotovljenih osebnih podatkov, zadevah v zvezi z navedenim preverjanjem in drugih elementih, določenih s pravilnikom komisije za varstvo osebnih informacij.

Če poslovni subjekt, ki obravnava osebne informacije, osebne informacije obravnava zunaj okvira, ki je potreben za doseganje namena uporabe iz odstavka 1 člena 15 zakona, mora predhodno pridobiti soglasje zadevnega principala (odstavek 1 člena 16 zakona). Poslovni subjekt, ki obravnava osebne informacije, ob prejemu osebnih podatkov, ki jih je zagotovila tretja oseba, v skladu s pravilnikom preveri elemente, kot so okoliščine, v katerih je navedena tretja oseba pridobila navedene osebne podatke, in to evidentira (odstavek 1 in 3 člena 26 zakona).

Kadar poslovni subjekt, ki obravnava osebne informacije, prejme osebne podatke iz EU na podlagi sklepa o ustreznosti, okoliščine v zvezi s pridobitvijo navedenih osebnih podatkov, ki jih je treba preveriti in evidentirati v skladu z odstavkom 1 in 3 člena 26, vključujejo namen uporabe, za katerega so bili prejeti iz EU.

Podobno, kadar poslovni subjekt, ki obravnava osebne informacije, od drugega poslovnega subjekta, ki obravnava osebne informacije, prejme osebne podatke, ki so bili predhodno preneseni iz EU na podlagi sklepa o ustreznosti, okoliščine v zvezi s pridobitvijo navedenih osebnih podatkov, ki jih je treba preveriti in evidentirati v skladu z odstavkom 1 in 3 člena 26, vključujejo namen uporabe, za katerega so bili prejeti.

V zgoraj navedenih primerih mora poslovni subjekt, ki obravnava osebne informacije, opredeliti namen uporabe navedenih osebnih podatkov v okviru namena uporabe, za katerega so bili podatki prvotno ali naknadno prejeti, kakor je preverjen in evidentiran v skladu z odstavkom 1 in 3 člena 26, ter te podatke uporabljati v navedenem okviru (kot je določeno v odstavku 1 člena 15 in odstavku 1 člena 16 zakona).

(4) Omejitev glede zagotavljanja tretji osebi v tuji državi (člen 24 zakona; člen 11-2 pravilnika)

Člen 24 zakona

Kadar poslovni subjekt, ki obravnava osebne informacije, razen v primerih iz posameznih točk odstavka 1 prejšnjega člena, zagotavlja osebne podatke tretji osebi (razen osebe, ki vzpostavi sistem, ki je skladen s standardi, določenimi s pravilnikom komisije za varstvo osebnih podatkov, potrebnimi za stalno ukrepanje, ki je enakovredno tistemu, ki ga poslovni subjekt, ki obravnava osebne informacije, sprejme v zvezi z obravnavanjem osebnih podatkov v skladu z določbami tega oddelka (v nadaljnjem besedilu tega člena enako)) v tuji državi (kar pomeni državo ali regijo zunaj ozemlja Japonske; (v nadaljnjem besedilu enako)) (razen držav, ki so s pravilnikom komisije za varstvo osebnih informacij opredeljene kot tuje države, ki imajo vzpostavljen sistem varstva osebnih informacij, za katerega se priznava, da ima glede varstva pravic in interesov posameznika standarde, enakovredne standardom na Japonskem; (v nadaljnjem besedilu tega člena enako)), mora vnaprej pridobiti soglasje principala, ki izkazuje, da se ta strinja z zagotavljanjem tretji osebi v tuji državi. V tem primeru se določbe prejšnjega člena ne uporabljajo.

Člen 11-2 pravilnika

Standardi, ki jih določa pravilnik komisije za varstvo osebnih podatkov na podlagi člena 24 zakona, se uvrščajo v katero koli od naslednjih točk:

- (i) poslovni subjekt, ki obravnava osebne informacije, in oseba, ki prejme zagotovljene osebne podatke, sta v zvezi z obravnavanjem osebnih podatkov s strani osebe, ki prejme zagotovljene osebne podatke, poskrbela za izvajanje ukrepov v skladu z namenom določb oddelka 1 poglavja IV zakona z ustrezno in razumno metodo;
- (ii) oseba, ki prejme zagotovljene osebne podatke, je pridobila potrdilo na podlagi mednarodnega okvira v zvezi z obdelavo osebnih podatkov.

Poslovni subjekt, ki obravnava osebne informacije, v primerih, ko tretji osebi v tuji državi posreduje osebne podatke, ki jih je prejel od EU na podlagi sklepa o ustreznosti, vnaprej pridobi principalovo privolitve, da se ti podatki posredujejo tretji osebi v tuji državi v skladu s členom 24 zakona, potem ko so mu bile predložene informacije o okoliščinah prenosa, ki jih potrebuje za odločitev o privolitvi, razen v primerih, ki spadajo pod eno od naslednjih točk (i) do (iii):

- (i) kadar je tretja oseba v državi, ki je v pravilniku določena kot tuja država, ki vzpostavlja sistem varstva osebnih informacij, za katerega se priznava, da ima standarde glede varstva pravic in interesov posameznika, enakovredne standardom na Japonskem;
- (ii) kadar sta poslovni subjekt, ki obravnava osebne informacije, in tretja oseba, ki se ji posredujejo osebni podatki, v zvezi z obdelavo osebnih podatkov s strani tretje osebe z ustrezno in razumno metodo (tj. s pogodbo, drugo vrsto zavezujočega sporazuma ali zavezujočim dogovorom znotraj skupine podjetij) skupaj sprejela ukrepe, ki zagotavljajo raven varstva, enakovredno tisti na podlagi zakona v povezavi s sedanjim pravilnikom;

(iii) v primerih, ki spadajo pod vsako od točk člena 23(1) zakona.

(5) Anonimno obdelane informacije (člena 2(9) ter 36(1) in (2) zakona)

Člen 2(9) zakona

(9) „Anonimno obdelane informacije“ v tem zakonu pomenijo informacije, ki se nanašajo na posameznika in se lahko pridobijo iz obdelave osebnih informacij, tako da ni mogoče identificirati posameznika z ukrepi, določenimi v vsaki od naslednjih točk, v skladu z razdelitvijo osebnih podatkov, določeno v vsaki od teh točk, ali obnoviti osebnih informacij:

(i) osebne informacije iz točke (i) odstavka 1:

izbris dela opisov itd. iz navedenih osebnih informacij (vključno z nadomestitvijo navedenega dela opisov itd. z drugimi opisi itd. z uporabo metode brez rednega vzorca, ki bi omogočal obnovo navedenega dela opisov itd.);

(ii) osebne informacije iz točke (ii) odstavka 1:

izbris vseh identifikacijskih kod iz navedenih osebnih informacij (vključno z nadomestitvijo navedenih individualnih identifikacijskih kod z drugimi opisi itd. z uporabo metode brez rednega vzorca, ki bi omogočal obnovo navedenih individualnih identifikacijskih kod).

Člen 36(1) zakona

(1) Poslovni subjekt, ki obravnava osebne informacije, pri pripravi anonimno obdelanih informacij (ki so v nadaljnjem besedilu omejene na tiste, ki so del podatkovne zbirke anonimno obdelanih informacij itd.) obdeluje osebne informacije v skladu s standardi, ki so v pravilniku komisije za varstvo osebnih informacij določeni kot potrebni za preprečitev identifikacije določenega posameznika in obnove osebnih informacij, uporabljenih pri pripravi.

Člen 19 pravilnika

Standardi, ki jih določa pravilnik komisije za varstvo osebnih podatkov na podlagi člena 36(1) zakona, so naslednji:

- (i) izbris vseh ali dela opisov itd. iz osebnih informacij, ki omogočajo identifikacijo določenega posameznika (vključno z nadomestitvijo takih opisov itd. z drugimi opisi itd. z uporabo metode brez rednega vzorca, ki bi omogočal obnovo vseh ali dela opisov itd.);
- (ii) izbris vseh identifikacijskih kod iz osebnih informacij (vključno z nadomestitvijo takih kod z drugimi opisi itd. z uporabo metode brez rednega vzorca, ki bi omogočal obnovo individualnih identifikacijskih kod);
- (iii) izbris kod (omejeno na kode, ki povezujejo več informacij, ki jih dejansko obravnava poslovni subjekt, ki obravnava osebne informacije), ki povezujejo osebne podatke in informacije, pridobljene s sprejetjem ukrepov v zvezi z osebnimi informacijami (vključno z nadomestitvijo navedenih kod z drugimi kodami, ki ne povezujejo navedenih osebnih informacij in informacij, pridobljenih s sprejetjem ukrepov v zvezi z navedenimi osebnimi informacijami, z uporabo metode brez rednega vzorca, ki bi omogočal obnovo navedenih kod);
- (iv) izbris idiosinkratičnih opisov itd. (vključno z nadomestitvijo takih opisov itd. z drugimi opisi itd. z metodo brez rednega vzorca, ki bi omogočal obnovo idiosinkratičnih opisov itd.);
- (v) poleg ukrepov, določenih v vsaki od predhodnih točk, sprejetje ustreznih ukrepov na podlagi rezultatov preučitve atributov itd. podatkovne zbirke osebnih informacij itd., kot je razlika med opisi itd. iz osebnih informacij in opisi itd. iz drugih osebnih informacij, ki so del podatkovne zbirke osebnih podatkov itd., ki zajema navedene osebne informacije.

Člen 36(2) zakona

(2) Poslovni subjekt, ki obravnava osebne informacije, po pripravi anonimno obdelanih informacij v skladu s standardi, ki so v pravilih komisije za varstvo osebnih informacij določeni kot potrebni za preprečitev uhajanja informacij v zvezi z navedenimi opisi itd. in individualnimi identifikacijskimi kodami, izbrisanimi iz osebnih informacij, uporabljenih za pripravo anonimno obdelanih informacij, in informacij v zvezi z metodo obdelave, izvedeno v skladu z določbami prejšnjega odstavka, sprejme ukrepe za varnostni nadzor takih informacij.

Člen 20 pravilnika

Standardi, ki jih določa pravilnik komisije za varstvo osebnih podatkov na podlagi člena 36(2) zakona, so naslednji:

- (i) jasna opredelitev pristojnosti in odgovornosti osebe, ki obravnava informacije v zvezi z navedenimi opisi itd. in individualnimi identifikacijskimi kodami, izbrisanimi iz osebnih informacij, uporabljenih za pripravo anonimno obdelanih informacij, in informacije v zvezi z metodo obdelave, izvedeno v skladu z določbami člena 36(1) (omejeno na tiste, ki omogočajo obnovo osebnih informacij z uporabo takih povezanih informacij; v nadaljnjem besedilu tega člena: informacije, ki se nanašajo na metodo obdelave itd.);
- (ii) določitev pravil in postopkov za obravnavo informacij, ki se nanašajo na metodo obdelave itd., ustrezna obravnavo informacij, ki se nanašajo na metodo obdelave itd., v skladu s pravili in postopki, ocena obravnave in sprejetje ukrepov za izboljšanje na podlagi rezultatov take ocene;
- (iii) sprejetje potrebnih in ustreznih ukrepov za preprečitev, da bi oseba brez zakonite pristojnosti za obdelavo informacij, ki se nanašajo na metodo obdelave itd., obravnavala take informacije.

Osebnosti, prejete iz EU na podlagi sklepa o ustreznosti, se štejejo za anonimno obdelane informacije v smislu člena 2(9) zakona le, če poslovni subjekt, ki obravnava osebne informacije, sprejme ukrepe, na podlagi katerih ponovne identifikacije posameznika ne more nihče več opraviti, vključno z izbrisom informacij, ki se nanašajo na metodo obdelave itd. (tj. informacij v zvezi z navedenimi opisi itd. in individualnimi identifikacijskimi kodami, izbrisanimi iz osebnih informacij, uporabljenih za anonimno obdelavo informacij, in informacij v zvezi z metodo obdelave, izvedeno v skladu z določbami člena 36(1) zakona (omejeno na tiste, ki omogočajo obnovo osebnih informacij z uporabo takih povezanih informacij)).

PRILOGA 2

Njena ekscelenca ga. Věra Jourová, evropska komisarka za pravosodje, potrošnike in enakost spolov

Spoštovana komisarka,

Pozdravljam konstruktivne razprave med Japonsko in Evropsko komisijo za oblikovanje okvira za vzajemni prenos osebnih podatkov med Japonsko in EU.

Na zahtevo, ki jo je Evropska komisija naslovila na vlado Japonske, pošiljam priložen dokument, ki vsebuje pregled pravnega okvira v zvezi z dostopom vlade Japonske do informacij.

Ta dokument se nanaša na številna ministrstva in agencije vlade Japonske, pri čemer so zadevna ministrstva in agencije (vladni sekretariat, nacionalna policijska agencija, komisija za varstvo osebnih informacij, ministrstvo za notranje zadeve in komunikacije, ministrstvo za pravosodje, obveščevalna agencija za javno varnost in ministrstvo za obrambo) odgovorni za posamezne dele tega dokumenta, ki spadajo v okvir njihovih pristojnosti. V nadaljevanju so navedena zadevna ministrstva in agencije, vključno z njihovimi podpisi.

Komisija za varstvo osebnih informacij bo sprejemala vse poizvedbe v zvezi s tem dokumentom ter usklajevala potrebne odzive med zadevnimi ministrstvi in agencijami.

Upam, da bo ta dokument v pomoč pri odločanju Evropske komisije.

Cenim vaš dosedanji prispevek k tej zadevi.

S spoštovanjem,

Yoko Kamikawa

Ministrica za pravosodje

Ta dokument so pripravili ministrstvo za pravosodje ter naslednja zadevna ministrstva in agencije:

Koichi Hamano

Svetovalec, sekretariat vlade

Schunichi Kuryu

Generalni komisar nacionalne policijske agencije

Mari Sonoda

Generalna sekretarka, komisija za varstvo osebnih podatkov

Mitsuru Yasuda

Namestnik ministra, ministrstvo za notranje zadeve in komunikacije

Seimei Nakagawa

Obveščevalna agencija za javno varnost

Kenichi Takahashi

Upravni namestnik ministra za obrambo

14. september 2018

Zbiranje in uporaba osebnih informacij s strani japonskih javnih organov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter nacionalne varnosti

Naslednji dokument vsebuje pregled pravnega okvira za zbiranje in uporabo osebnih (elektronskih) informacij s strani japonskih javnih organov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in nacionalne varnosti (v nadaljnjem besedilu: vladni dostop), zlasti kar zadeva razpoložljivo pravno podlago ter pogoje (omejitve) in zaščitne ukrepe, ki se uporabljajo, vključno z neodvisnim nadzorom in individualnimi možnostmi pravnega varstva. Ta dokument je naslovljen na Evropsko komisijo, da bi se izrazila zavezanost in jamstva, da bo vladni dostop do osebnih informacij, prenesenih iz EU na Japonsko, omejen na to, kar je potrebno in sorazmerno, in pod neodvisnim nadzorom ter da bodo imeli zadevni posamezniki v primeru morebitnih kršitev njihove temeljne pravice do zasebnosti in varstva podatkov možnost pravnega varstva. Ta dokument določa tudi vzpostavitev novega mehanizma pravnega varstva, ki ga upravlja komisija za varstvo osebnih informacij, za obravnavo pritožb posameznikov iz EU v zvezi z vladnim dostopom do njihovih osebnih podatkov, prenesenih iz EU na Japonsko.

I. Splošna pravna načela, pomembna za vladni dostop

V okviru izvajanja javnih pooblastil mora biti vladni dostop izveden ob popolnem upoštevanju zakona (načelo zakonitosti). Na Japonskem so osebne informacije tako v zasebnem kot v javnem sektorju zaščitene z večplastnim mehanizmom.

A. Ustavni okvir in načelo zakonske podlage

Člen 13 ustave in sodna praksa priznavata pravico do zasebnosti kot ustavno pravico. V zvezi s tem je vrhovno sodišče razsodilo, da je naravno, da posamezniki ne želijo, da bi bili drugi brez tehtnega razloga seznanjeni z njihovimi osebnimi informacijami, in da je treba to pričakovanje zaščititi⁽¹⁾. Dodatna zaščita je določena v členu 21(2) ustave, ki zagotavlja spoštovanje tajnosti komunikacij, in členu 35 ustave, ki zagotavlja pravico posameznika, da ni predmet preiskovanja in zasega brez naloga, kar pomeni, da mora zbiranje osebnih informacij z obveznimi sredstvi, vključno z dostopom, vedno temeljiti na sodnem nalogu. Tak nalog se lahko izda samo za preiskavo že storjenega kaznivega dejanja. Zato v pravnem okviru Japonske zbiranje informacij z obveznimi sredstvi za namene nacionalne varnosti (in ne za namene kazenske preiskave) ni dovoljeno.

Poleg tega mora biti v skladu z načelom zakonske podlage obvezno zbiranje podatkov posebej dovoljeno z zakonom. V primeru neobveznega/prostovoljnega zbiranja informacij so informacije pridobljene iz vira, do katerega se lahko prosto dostopa, ali se prejemajo na podlagi zahteve za prostovoljno razkritje, tj. zahteve, ki je ni mogoče uveljavljati zoper fizično ali pravno osebo, ki poseduje informacije. Vendar je to dovoljeno le, če je javni organ pristojen za izvedbo preiskave, saj lahko vsak javni organ deluje samo v okviru svoje upravne pristojnosti, ki jo določa zakon (ne glede na to, ali njegove dejavnosti posegajo v pravice in svoboščine posameznikov ali ne). To načelo velja za zmožnost organa za zbiranje osebnih informacij.

B. Posebna pravila o varstvu osebnih informacij

Zakon o varstvu osebnih informacij in zakon o varstvu osebnih informacij, ki jih hranijo upravni organi, ki temeljita na ustavnih določbah in slednje podrobneje določata, zagotavljata pravico do osebnih informacij tako v zasebnem kot tudi javnem sektorju.

Člen 7 zakona o varstvu osebnih informacij določa, da komisija za varstvo osebnih informacij oblikuje osnovno politiko varstva osebnih informacij (v nadaljnjem besedilu: osnovna politika). Osnovna politika, ki je sprejeta s sklepom japonske vlade kot osrednjega organa japonske državne uprave (predsednik vlade in nacionalni ministri), določa smer varstva osebnih informacij na Japonskem. Tako komisija za varstvo osebnih informacij kot neodvisni nadzorni organ deluje kot „poveljniški center“ japonskega sistema varstva osebnih informacij.

Kadar upravni organi zbirajo osebne informacije in ne glede na to, ali to storijo z obveznimi sredstvi ali ne, morajo načeloma⁽²⁾ izpolnjevati zahteve iz zakona o varstvu osebnih informacij, ki jih hranijo upravni organi. Slednji je splošni zakon, ki se uporablja za obdelavo „hranjenih osebnih informacij“⁽³⁾ s strani „upravnih organov“ (kot je opredeljeno v

⁽¹⁾ Sodba vrhovnega sodišča z dne 12. septembra 2003 (št. zadeve: 1656 (2002 (Ju))).

⁽²⁾ Za izjeme glede poglavja 4 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, glej stran 16.

⁽³⁾ „Hranjene osebne informacije“ v členu 2(5) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, pomeni osebne informacije, ki jih pripravi ali pridobi uslužbenec upravnega organa med opravljanjem svojih nalog in ki jih navedeni upravni organ hrani za organizacijsko uporabo s strani svojih zaposlenih.

členu 2(1) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi). Zato zajema tudi obdelavo podatkov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in nacionalne varnosti. Med javnimi organi, ki imajo dovoljenje za uporabo vladnega dostopa, so vsi organi, razen prefekturne policije, nacionalni vladni organi, ki spadajo pod opredelitev pojma „upravni organi“. Obravnavo osebnih informacij s strani prefekturne policije urejajo prefekturni odloki ⁽⁴⁾, v katerih so določena načela varstva osebnih informacij, pravic in obveznosti, enakovredna tistim iz zakona o varstvu osebnih informacij, ki jih hranijo upravni organi.

II. Vladni dostop za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

A) Pravna podlaga in omejitve

1) Zbiranje osebnih informacij z obveznimi sredstvi

a) Pravna podlaga

V skladu s členom 35 ustave se v pravico vseh oseb do zaščite v njihovem domu, do zaščite dokumentov oziroma do zaščite osebnih predmetov pred vstopom, iskanjem oziroma zasegom ne posega, razen na podlagi naloga, ki je izdan na podlagi „ustreznega razloga“ ter izrecno opisuje lokacijo, ki jo je treba preiskati, in predmete, ki jih je treba zaseči. Zato se lahko obvezno zbiranje elektronskih informacij s strani javnih organov v okviru kazenske preiskave izvede le na podlagi naloga. To velja tako za zbiranje elektronskih zapisov, ki vsebujejo (osebne) informacije, kot tudi za prestrezanje komunikacij v realnem času (t. i. prisluškovanje telefonskim pogovorom). Edina izjema k temu pravilu (ki pa ni pomembna v okviru elektronskega prenosa osebnih informacij iz tujine) je člen 220(1) zakonika o kazenskem postopku ⁽⁵⁾, v skladu s katerim lahko državni tožilec, njegov pomočnik ali uradnik pravosodne policije pri prijetju osumljenca ali „očitnega storilca“ po potrebi izvede iskanje in zaseg „na kraju samem ob prijetju“.

Člen 197(1) zakonika o kazenskem postopku določa, da se obvezni preiskovalni ukrepi „ne uporabljajo, razen če ta zakonik vsebuje posebne določbe“. Kar zadeva obvezno zbiranje elektronskih informacij, sta ustrezna pravna podlaga v tem smislu člen 218(1) zakonika o kazenskem postopku (v skladu s katerim lahko državni tožilec, njegov pomočnik ali uradnik pravosodne policije, če je to potrebno za preiskavo kaznivega dejanja, izvede iskanje, zaseg ali inšpekcijski pregled na podlagi naloga, ki ga izda sodnik) in člen 222-2 zakonika o kazenskem postopku (v skladu s katerim se obvezni ukrepi za prestrezanje elektronskih komunikacij brez privolitve katere koli stranke izvedejo na podlagi drugih aktov). Slednja določba se nanaša na zakon o prisluškovanju telefonskim pogovorom za potrebe kazenske preiskave (v nadaljnjem besedilu: zakon o prisluškovanju telefonskim pogovorom), katerega člen 3(1) določa pogoje, pod katerimi se lahko komunikacijam v zvezi z nekaterimi hudimi kaznivimi dejanji prisluškuje na podlagi ustreznega naloga, ki ga izda sodnik. ⁽⁶⁾

Kar zadeva policijo, je za preiskave v vseh primerih pristojna prefekturna policija, medtem ko nacionalna policijska agencija na podlagi zakonika o kazenskem postopku ne izvaja kazenskih preiskav.

b) Omejitve

Obvezno zbiranje elektronskih informacij je omejeno z ustavo in pooblastitvenimi statuti, kot se razlagajo v sodni praksi in ki določajo zlasti merila, ki jih morajo sodišča uporabljati pri izdaji naloga. Poleg tega zakon o varstvu osebnih informacij, ki jih hranijo upravni organi, določa številne omejitve, ki se uporabljajo tako za zbiranje kot tudi za obravnavo informacij (medtem ko lokalni odloki določajo v bistvu enaka merila za prefekturno policijo).

(1) Omejitve, ki izhajajo iz ustave in pooblastitvenega statuta

V skladu s členom 197(1) zakonika o kazenskem postopku se obvezni ukrepi ne uporabljajo, razen če ta zakonik vsebuje posebne določbe. Člen 218(1) zakonika o kazenskem postopku določa, da se zaseg itd. na podlagi naloga, ki ga izda

⁽⁴⁾ Vsaka prefektura ima svoj „prefekturni odlok“, ki se uporablja za varstvo osebnih informacij s strani prefekturne policije. Ti prefekturni odloki niso prevedeni v angleški jezik.

⁽⁵⁾ Člen 220(1) zakonika o kazenskem postopku določa, da lahko državni tožilec, njegov pomočnik ali uradnik pravosodne policijske ob prijetju osumljenca po potrebi sprejme naslednje ukrepe: (a) vstop v bivališče druge osebe itd. za iskanje osumljenca; (b) iskanje, zaseg ali inšpekcijski pregled na kraju samem ob prijetju.

⁽⁶⁾ Natančneje, ta določba določa naslednje: „Državni tožilec ali uradnik pravosodne policije lahko prisluškuje komunikacijam v zvezi s kaznivim dejanjem na podlagi ustreznega naloga, ki ga izda sodnik, v naslednjih primerih: kadar obstaja zadosten razlog za sum, da bo prišlo do komunikacij o storitvi ali načrtovanju kaznivega dejanja, dejanjih po storitvi kaznivega dejanja, kot je uničenje dokazov itd., ali navodilih ali kakršni koli drugi interakciji v zvezi s kaznivim dejanjem, določenim v naslednjih točkah (v nadaljnjem besedilu: druge in tretje točke: ‚vrsta kaznivih dejanj‘), ter komunikacij, ki vsebujejo zadeve, povezane z navedenim kaznivim dejanjem (v nadaljnjem besedilu tega odstavka: ‚komunikacije v zvezi s kaznivim dejanjem‘), ter kadar je z drugimi sredstvi izredno težko prepoznati storilca ali pojasniti stanje/podrobnosti o storjenem kaznivem dejanju, kadar so komunikacijska sredstva opredeljena s telefonsko številko in drugimi številkami/kodami za identifikacijo vira ali lokacije telefona ter kadar jih osumljenec uporablja na podlagi pogodbe s ponudnikom telekomunikacijskih storitev (razen sredstev, pri katerih ne obstaja sum, da se uporabljajo za ‚komunikacije v zvezi s kaznivim dejanjem‘) ali kadar obstaja razlog za sum, da se tovrstna komunikacijska sredstva uporabljajo za ‚komunikacije v zvezi s kaznivim dejanjem‘.“

sodnik, lahko izvede le, „če je to potrebno za preiskavo kaznivega dejanja“. Čeprav merila za presojo potrebe v zakonskem pravu niso podrobneje opredeljena, je vrhovno sodišče ⁽⁷⁾ razsodilo, da bi moral sodnik pri ocenjevanju potrebe po ukrepih opraviti splošno oceno in pri tem upoštevati zlasti naslednje elemente:

- (a) resnost kaznivega dejanja in način, kako je bilo storjeno;
- (b) vrednost in pomen zaseženih predmetov kot dokazov;
- (c) verjetnost prikritja ali uničenja zaseženih predmetov;
- (d) obseg prikrajšanosti zaradi zasega;
- (e) druge povezane pogoje.

Omejitve izhajajo tudi iz zahteve iz člena 35 ustave po „ustreznem razlogu“. V skladu s standardom „ustreznega razloga“ se lahko nalogi izdajo, če: [1] obstaja potreba po kazenski preiskavi (glej sodbo vrhovnega sodišča z dne 18. marca 1969 (št. zadeve: 100 (1968 (Shi))); [2] obstajajo okoliščine, v katerih se domneva, da je osumljenec (obtoženec) storil kaznivo dejanje (člen 156(1) pravilnika o kazenskem postopku) ⁽⁸⁾. [3] Nalog za preiskavo telesa, predmetov, bivališča ali katere koli druge nepremičnine osebe, ki ni obtoženec, se lahko izda le, če se razumno domneva, da obstajajo predmeti, ki bi jih bilo treba zaseči (člen 102(2) zakonika o kazenskem postopku). Če sodnik meni, da listinski dokazi, ki so jih predložili preiskovalni organi, ne zadostujejo za sum kaznivega dejanja, zavrne zahtevo za nalog. V zvezi s tem je treba opozoriti, da v skladu z zakonom o kaznovanju organiziranega kriminala in nadzoru nad premoženjsko koristjo „pripravljalna dejanja“ za storitev načrtovanega kaznivega dejanja (npr. priprava denarja za storitev terorističnega kaznivega dejanja) sama po sebi pomenijo kaznivo dejanje in so zato lahko predmet obvezne preiskave na podlagi naloga.

Kadar nalog zadeva preiskavo telesa, predmetov, bivališča ali katere koli druge nepremičnine osebe, ki ni osumljenec ali obtoženec, se izda le, če se lahko upravičeno domneva, da obstajajo predmeti, ki bodo zaseženi (člena 102(2) in 222 (1) zakonika o kazenskem postopku).

Kar zadeva prestrežanje komunikacij za namene kazenskih preiskav na podlagi zakona o prisluškovanju telefonskim pogovorom, se to lahko izvaja le, če so izpolnjene stroge zahteve iz člena 3(1). V skladu s to določbo je treba za prestrežanje vedno vnaprej zahtevati sodni nalog, ki se lahko izda le v omejenih primerih ⁽⁹⁾.

(2) Omejitve, ki izhajajo iz zakona o varstvu osebnih informacij, ki jih hranijo upravni organi.

Kar zadeva zbiranje ⁽¹⁰⁾ in nadaljnjo obravnavo (vključno s hrambo, upravljanjem in uporabo) osebnih informacij s strani upravnih organov, zakon o varstvu osebnih informacij, ki jih hranijo upravni organi, določa zlasti naslednje omejitve:

- (a) V skladu s členom 3(1) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, lahko upravni organi hranijo osebne informacije le, če je hramba potrebna za opravljanje nalog, ki so v njihovi pristojnosti, kot je določeno v zakonih in drugih predpisih. Pri tem morajo tudi navesti (v kolikor je to mogoče) namen uporabe osebnih informacij. V skladu s členom 3(2) in (3) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, upravni organi ne hranijo osebnih informacij v obsegu, ki presega to, kar je potrebno za doseganje navedenega namena uporabe, in ne spreminjajo namena uporabe, da bi presegal to, kar se lahko razumno šteje kot ustrezno za prvotni namen.
- (b) Člen 5 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, določa, da si vodja upravnega organa prizadeva, da ohrani točnost in ažurnost hranjenih osebnih informacij v obsegu, ki je potreben za doseganje namena uporabe.
- (c) Člen 6(1) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, določa, da vodja upravnega organa sprejme potrebne ukrepe za preprečevanje uhajanja, izgube ali uničenja ter za pravilno upravljanje hranjenih osebnih informacij.
- (d) Člen 7 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, določa, da noben zaposleni (vključno z nekdanjimi zaposlenimi) ne sme razkriti pridobljenih osebnih informacij drugi osebi brez upravičenega razloga ali uporabiti teh informacij za neupravičene namene.

⁽⁷⁾ Sodba z dne 18. marca 1969 (št. zadeve: 100 (1968 (Shi))).

⁽⁸⁾ Člen 156(1) pravilnika o kazenskem postopku določa naslednje: „Pri vložitvi zahteve iz odstavka (1) prejšnjega člena vložnik zagotovi gradivo, na podlagi katerega se domneva, da je osumljenec ali obtoženec storil kaznivo dejanje.“

⁽⁹⁾ Glej opombo 6.

⁽¹⁰⁾ Člen 3(1) in (2) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, omejuje obseg hrambe in s tem tudi zbiranje osebnih informacij.

- (e) Poleg tega člen 8(1) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, določa, da vodja upravnega organa, razen če ni z zakoni in predpisi določeno drugače, hranjenih osebnih informacij ne sme uporabiti ali posredovati drugi osebi za namene, ki niso navedeni kot namen uporabe. Člen 8(2) vsebuje izjeme od tega pravila v posebnih primerih, vendar se te uporabljajo samo, če ni verjetno, da bi takšno izjemno razkritje „nepravilno“ kršilo pravice in interese posameznika, na katerega se nanašajo osebni podatki, ali tretjih oseb.
- (f) V skladu s členom 9 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, če se hranjene osebne informacije posredujejo drugi osebi, vodja upravnega organa po potrebi uvede omejitve glede namena ali načina uporabe ali katere koli druge potrebne omejitve; prav tako lahko zahteva od osebe, ki informacije prejme, da sprejme potrebne ukrepe za preprečevanje uhajanja in ustrezno upravljanje informacij.
- (g) Člen 48 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, določa, da si vodja upravnega organa prizadeva ustrezno in hitro obravnavati vse pritožbe v zvezi z obravnavo osebnih informacij.

2) Zbiranje osebnih informacij na podlagi prošnji za prostovoljno sodelovanje (prostovoljna preiskava)

a) Pravna podlaga

Poleg uporabe obveznih sredstev se osebne informacije pridobijo iz vira, ki je prosto dostopen ali temelji na prostovoljnem razkritju, med drugim s strani poslovnih subjektov, ki razpolagajo s takimi informacijami.

Glede slednjega člen 197(2) zakonika o kazenskem postopku pooblašča tožilstvo in pravosodno policijo za „pisne poizvedbe o preiskovalnih zadevah“ (tako imenovani „listi za poizvedbo“). V skladu z zakonikom o kazenskem postopku se od oseb, katerim je poslana poizvedba, zahteva, da poročajo preiskovalnim organom. Vendar jih ni mogoče prisiliti, da poročajo, če javni uradi ali javne in/ali zasebne organizacije, ki so prejele poizvedbe, zahtevo zavrnejo. Če v zvezi s poizvedbami ne poročajo, se jim ne sme naložiti kazenskih ali drugih sankcij. Če preiskovalni organi menijo, da so zahtevane informacije nujne, bodo informacije morali pridobiti s preiskavo in zasegom na podlagi sodnega naloga.

Ob vse večji ozaveščenosti posameznikov o njihovih pravicah glede zasebnosti in glede na delovno obremenitev, ki jo take zahteve prinašajo, so poslovni subjekti vse previdnejši pri odgovorih na take zahteve⁽¹¹⁾. Poslovni subjekti pri odločanju o sodelovanju upoštevajo zlasti naravo zahtevanih informacij, svoje razmerje z osebo, na katero se nanašajo zadevne informacije, tveganja za svoj ugled, tveganja sodnih postopkov itd.

b) Omejitve

Kar zadeva obvezno zbiranje elektronskih informacij, je prostovoljna preiskava omejena z ustavo, kot se razlaga v sodni praksi, in s statutom o pooblastitvi. Poleg tega poslovnim subjektom v nekaterih primerih zakon ne dovoljuje razkrivanja informacij. Poleg tega je v zakonu o varstvu osebnih informacij, ki jih hranijo upravni organi, določena vrsta omejitev, ki veljajo tako za zbiranje informacij kot za ravnanje z njimi (medtem ko lokalni odloki v bistvu reproducirajo enaka merila za prefekturno policijo).

(1) Omejitve, ki izhajajo iz ustave in statuta o pooblastitvi

Z upoštevanjem namena člena 13 ustave je vrhovno sodišče v dveh sklepih z dne 24. decembra 1969 (1965 (A) št. 1187) in 15. aprila 2008 (2007 (A) št. 839) uvedlo omejitve za prostovoljne preiskave, ki jih izvajajo preiskovalni organi. Čeprav sta se ta sklepa nanašala na primera, ko so bile osebne informacije (v obliki slik) zbrane s fotografiranjem/snemanjem, so ugotovitve pomembne za prostovoljne (neobvezne) preiskave, ki se nanašajo na zasebnost posameznikov na splošno. Zato veljata in ju je treba upoštevati glede zbiranja osebnih informacij s prostovoljno preiskavo, pri čemer se upoštevajo posebne okoliščine vsakega primera.

V skladu s temi sklepi je zakonitost prostovoljne preiskave odvisna od izpolnjevanja treh meril, ki so:

— „sum kaznivega dejanja“ (tj. oceniti je treba, ali je bilo storjeno kaznivo dejanje),

— „potrebnost preiskave“ (tj. oceniti je treba, ali zahtevki ne presegajo obsega potrebnega za namene preiskave) in

⁽¹¹⁾ Glej tudi obvestilo nacionalne policijske agencije z dne 7. decembra 1999 (v nadaljevanju na str. 9), v katerem je navedeno isto.

— „ustreznost metod“ (tj. oceniti je treba, ali je prostovoljna preiskava „ustrezna“ ali razumna, da bi se dosegel namen preiskave) ⁽¹²⁾.

Na splošno se ob upoštevanju navedenih treh meril zakonitost prostovoljne preiskave presoja z vidika, ali se lahko šteje za razumno v skladu s socialno sprejetimi konvencijami.

Zahteva o „potrebnosti“ preiskave izhaja tudi neposredno iz člena 197 zakonika o kazenskem postopku in je bila potrjena v navodilih nacionalne policijske agencije prefekturni policiji v zvezi z uporabo „listov za poizvedbo“. Obvestilo nacionalne policijske agencije z dne 7. decembra 1999 določa vrsto postopkovnih omejitev, vključno z zahtevo, da se „listi za poizvedbo“ uporabljajo samo, če je to potrebno za namene preiskave. Poleg tega je člen 197(1) zakonika o kazenskem postopku omejen na kazenske preiskave, zato se lahko uporabi le, če obstaja konkreten sum na že storjeno kaznivo dejanje. Nasprotno pa ta pravna podlaga ni na voljo za zbiranje in uporabo osebnih informacij, če do kršitve zakonodaje še ni prišlo.

(2) Omejitve v zvezi z nekaterimi poslovnimi subjekti

Na nekaterih področjih veljajo dodatne omejitve na podlagi varstva iz drugih zakonov.

Preiskovalni organi in izvajalci telekomunikacijskih storitev, ki razpolagajo z osebnimi informacijami, so dolžni spoštovati tajnost komunikacij, ki jo zagotavlja člen 21(2) ustave ⁽¹³⁾. Poleg tega imajo izvajalci telekomunikacijskih storitev enako dolžnost v skladu s členom 4 zakona o telekomunikacijskih podjetjih ⁽¹⁴⁾. V skladu s „Smernicami glede varstva osebnih informacij pri poslovanju na področju telekomunikacij“, ki jih je izdalo ministrstvo za notranje zadeve in komunikacije na podlagi ustave in zakona o telekomunikacijskih podjetjih, v primerih, ko gre za tajnost komunikacij, izvajalci telekomunikacijskih storitev ne smejo razkriti osebnih informacij v zvezi z zaupnostjo komunikacij tretjim osebam, razen če so pridobili soglasje posameznika ali če se lahko sklicujejo na enega od „upravičenih razlogov“ za neupoštevanje kazenskega zakonika. Slednji se nanašajo na „upravičena dejanja“ (člen 35 kazenskega zakonika), „samoobrambo“ (člen 36 kazenskega zakonika) in „preprečevanje sedanje nevarnosti“ (člen 37 kazenskega zakonika). „Upravičena dejanja“ v skladu s kazenskim zakonikom so le tista dejanja izvajalca telekomunikacijskih storitev, s katerimi izpolnjuje obvezne ukrepe države, kar izključuje prostovoljno preiskavo. Če torej preiskovalni organi zahtevajo osebne informacije na podlagi „lista za poizvedbo“ (člen 197(2) zakonika o kazenskem postopku), izvajalec telekomunikacijskih storitev informacij ne sme razkriti.

Poslovni subjekti morajo zavrniti zahteve za prostovoljno sodelovanje, če jim zakon prepoveduje razkritje osebnih informacij. To na primer vključuje primere, v katerih je subjekt dolžan spoštovati zaupnost informacij, na primer v skladu s členom 134 kazenskega zakonika ⁽¹⁵⁾.

(3) Omejitve na podlagi zakona o varstvu osebnih informacij, ki jih hranijo upravni organi

V zvezi z zbiranjem osebnih informacij s strani upravnih organov in nadaljnjim ravnanjem s temi informacijami so v zakonu o varstvu osebnih informacij, ki jih hranijo upravni organi, navedene omejitve, kot je pojasnjeno zgoraj v oddelku II.A)1)b)(2). Enakovredne omejitve izhajajo iz prefekturnih odlokov, ki veljajo za prefekturno policijo.

B) Nadzor

1) Sodni nadzor

Zbiranje osebnih informacij z obveznimi sredstvi mora temeljiti na nalogu ⁽¹⁶⁾ in je zato predmet predhodne obravnave s strani sodnika. V primeru, da je bila preiskava nezakonita, lahko sodnik takšne dokaze izključi v poznejšem sojenju v kazenski zadevi. Posameznik lahko zahteva takšno izključitev iz svojega kazenskega sodnega postopka, pri čemer trdi, da je bila preiskava nezakonita.

⁽¹²⁾ Resnost kaznivega dejanja in nujnost sta pomembna dejavnika za oceno „ustreznosti metod“.

⁽¹³⁾ Člen 21(2) ustave določa: „Ne sme se izvajati cenzura niti kršiti tajnost katerega koli komunikacijskega sredstva.“

⁽¹⁴⁾ Člen 4 zakona o telekomunikacijskih podjetjih določa: „(1) Tajnost komunikacij, ki jih upravlja izvajalec telekomunikacijskih storitev, ne sme biti kršena. (2) Nobena oseba, ki sodeluje pri poslovanju na področju telekomunikacij, ne sme razkriti skrivnosti, pridobljenih v času opravljanja svojih nalog v zvezi s komunikacijami, ki jih upravlja izvajalec telekomunikacijskih storitev. Enako velja tudi po prenehanju opravljanja teh nalog.“

⁽¹⁵⁾ Člen 134 kazenskega zakonika določa: „(1) Če zdravnik, farmacevt, distributer zdravil, babica, odvetnik, zagovornik, notar ali katere koli druga oseba, ki je nekdaj opravljala tak poklic, brez utemeljenih razlogov razkrije zaupne informacije druge osebe, s katerimi se je seznanila pri opravljanju tega poklica, se ta oseba kaznuje z zaporno kaznijo s prisilnim delom do 6 mesecev ali globo v višini do 100 000 jenov. (2) Enako velja v primeru, če oseba, ki opravlja ali je opravljala verski poklic, brez utemeljenih razlogov razkrije zaupne informacije druge osebe, s katerimi se je seznanila pri opravljanju verskih dejavnosti.“

⁽¹⁶⁾ Glede izjeme od tega pravila glej opombo 5.

2) Nadzor na podlagi zakona o varstvu osebnih informacij, ki jih hranijo upravni organi

Na Japonskem je minister ali vodja vsakega ministrstva ali agencije pristojen za nadzor in izvrševanje na podlagi zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, medtem ko lahko minister za notranje zadeve in komunikacije preiskuje izvrševanje zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, s strani vseh drugih ministrstev.

Če minister za notranje zadeve in komunikacije – na primer na podlagi preiskave o stanju izvrševanja zakona o varstvu osebnih informacij, ki jih hranijo upravni organi⁽¹⁷⁾, obravnavanja pritožb ali poizvedb, naslovljenih na enega od njegovih celovitih informacijskih centrov – meni, da je to potrebno za doseganje namena zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, lahko zahteva, da vodja upravnega organa predloži gradivo in pojasnila v zvezi z obravnavo osebnih informacij s strani zadevnega upravnega organa na podlagi člena 50 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi. Minister lahko posreduje mnenja vodji upravnega organa v zvezi z obdelavo osebnih informacij v upravnem organu, če meni, da je to potrebno za doseganje namena tega zakona. Poleg tega lahko minister na primer zahteva revizijo ukrepov z ukrepi, ki jih lahko sprejme v skladu s členoma 50 in 51 zakona, če obstaja sum, da je prišlo do kršitve ali neprimerne izvajanja zakona. S tem se zagotovi enotna uporaba zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, in skladnost z njim.

3) Nadzor, ki ga izvajajo komisije za javno varnost v zvezi s policijo

Kar zadeva policijsko upravo, je nacionalna policijska agencija pod nadzorom nacionalne komisije za javno varnost, medtem ko prefekturno policijo nadzoruje ena od prefekturnih komisij za javno varnost, ki so bile ustanovljene v vsaki prefekturi. Vsak od teh nadzornih organov zagotavlja demokratično upravljanje in politično nevtralnost policijske uprave.

Nacionalna komisija za javno varnost je odgovorna za zadeve, ki so v njeni pristojnosti na podlagi zakona o policiji in drugih zakonov. To vključuje imenovanje generalnega komisarja nacionalne policijske agencije in lokalnih visokih policijskih uradnikov ter oblikovanje celovitih politik, ki določajo osnovne usmeritve ali ukrepe v zvezi z upravljanjem nacionalne policijske agencije.

Prefekturne komisije za javno varnost sestavljajo člani, ki zastopajo ljudstvo v zadevni prefekturi na podlagi zakona o policiji in upravljaajo prefekturno policijo kot sistem neodvisnih odborov. Člane imenuje guverner prefekture s soglasjem parlamenta prefekture na podlagi člena 39 zakona o policiji. Njihov mandat traja tri leta in proti njihovi volji jih je mogoče razrešiti le iz posebnih razlogov, navedenih v zakonu (kot je nezmožnost opravljanja njihovih nalog, kršitve pri opravljanju nalog, neprimerno ravnanje itd.), s čimer se zagotovi njihova neodvisnost (glej člena 40 in 41 zakona o policiji). Da se zagotovi njihova politična nevtralnost, člen 42 zakona o policiji članu komisije prepoveduje, da bi hkrati deloval kot član zakonodajnega organa, postal vodilni član politične stranke ali katerega koli drugega političnega organa ali aktivno sodeloval pri političnih gibanjih. Medtem ko je vsaka komisija v pristojnosti zadevnega guvernerja prefekture, to ne pomeni, da je regulator pristojen za izdajanje navodil glede izvajanja njenih nalog.

V skladu s členom 38(3) v povezavi s členom 2 in členom 36(2) zakona o policiji so za „varstvo pravic in svoboščin posameznika“ pristojne prefekturne komisije za javno varnost. V ta namen prejemajo poročila vodij prefekturne policije, ki se nanašajo na dejavnosti pod njihovo jurisdikcijo, tudi na rednih sestankih tri- ali štirikrat mesečno. Komisija zagotavlja smernice o teh zadevah v vzpostavljeno celovitih politik.

Poleg tega lahko prefekturne komisije za javno varnost v okviru svoje nadzorne funkcije dajejo navodila prefekturni policiji v posameznih konkretnih primerih, kadar menijo, da je to potrebno v okviru inšpekcijskega pregleda dejavnosti prefekturne policije ali neprimerne ravnanja njenega osebja. Poleg tega lahko komisije, če je po njihovem mnenju to potrebno, zadolžijo člana komisije, da pregleda stanje izvajanja izdanih navodil (člen 43-2 zakona o policiji).

⁽¹⁷⁾ Za zagotovitev preglednosti in olajšanje nadzora, ki ga izvaja ministrstvo za notranje zadeve in komunikacije, mora vodja upravnega organa v skladu s členom 11 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, evidentirati vsako točko iz člena 10(1) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, kot je ime upravnega organa, ki hrani datoteko, namen uporabe datoteke, način zbiranja osebnih informacij itd. (t. i. „evidenca datotek osebnih informacij“). Vendar pa so datoteke osebnih informacij, ki spadajo v okvir člena 10(2) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, kot so tiste, ki so pripravljene ali pridobljene v okviru kazenske preiskave ali ki se nanašajo na zadeve, pomembne za nacionalno varnost, izvzete iz obveznosti priglasitve ministrstvu za notranje zadeve in komunikacije in vključitve v javno evidenco. Vendar pa mora v skladu s členom 7 zakona o upravljanju javnih evidenc in arhivov vodja upravnega organa vedno evidentirati razvrstitev, naslov, obdobje ter lokacijo hrambe itd. upravnih dokumentov („evidenca upravljanja datotek upravnih dokumentov“). Informacije o kazalu za obe evidenci so objavljene na spletu in posameznikom omogočajo, da preverijo, katere vrste osebnih informacij vsebuje datoteka in kateri upravni organ hrani te informacije.

4) Nadzor, ki ga izvaja parlament

Parlament lahko izvaja preiskave v zvezi z dejavnostmi javnih organov in v ta namen zahteva predložitev dokumentov in zaslišanje prič (člen 62 ustave). V tem okviru lahko pristojni odbor v parlamentu prouči ustreznost dejavnosti zbiranja informacij, ki jih izvaja policija.

Ta pooblastila so podrobneje opredeljena v zakonu o parlamentu. V skladu s členom 104 lahko parlament od vlade in javnih agencij zahteva, da pripravijo poročila in evidence, potrebne za izvajanje preiskave. Poleg tega lahko poslanci vložijo „pisne poizvedbe“ v skladu s členom 74 zakona o parlamentu. Take poizvedbe mora odobriti predsednik parlamenta in načeloma je potreben odgovor vlade v pisni obliki v sedmih dneh (če je nemogoče odgovoriti v tem roku, je treba to utemeljiti in določiti nov rok, člen 75 zakona o parlamentu). V preteklosti so pisne poizvedbe parlamenta zajemale tudi obravnavo osebnih informacij s strani uprave⁽¹⁸⁾.

C) Pravna sredstva posameznikov

V skladu s členom 32 japonske ustave se nikomur ne sme kratiti pravica do dostopa do sodnega varstva. Poleg tega člen 17 ustave zagotavlja pravico do vložitve odškodninske tožbe zoper državo ali javni subjekt (kot določa zakon) vsakomur, ki je utrpel škodo zaradi nezakonitega ravnanja javnega uslužbenca.

1) Sodno varstvo proti obveznemu zbiranju informacij na podlagi naloga (člen 430 zakonika o kazenskem postopku)

V skladu s členom 430(2) zakonika o kazenskem postopku lahko posameznik, ki ni zadovoljen z ukrepi policista v zvezi z zasegom predmetov (tudi če vsebujejo osebne informacije) na podlagi naloga, vloži zahtevek (t. i. „kvazipritožbo“) pri pristojnem sodišču, da se takšni ukrepi „razveljavijo ali spremenijo“.

Takšno izpodbijanje je mogoče, ne da bi posameznik moral čakati, da se zadeva zaključi. Če sodišče ugotovi, da zaseg ni bil potreben ali da obstajajo drugi razlogi, zaradi katerih je bil zaseg nezakonit, lahko odredi, naj se takšni ukrepi razveljavijo ali spremenijo.

2) Sodno varstvo v skladu z zakonikom o civilnem postopku in zakonom o nadomestilih države

Če posamezniki menijo, da je bila kršena njihova pravica do zasebnosti iz člena 13 ustave, lahko vložijo civilno tožbo, v kateri zahtevajo izbris osebnih informacij, zbranih v okviru kazenske preiskave.

Posameznik lahko tudi vloži odškodninsko tožbo na podlagi zakona o nadomestilih države v povezavi z ustreznimi členi civilnega zakonika, če meni, da je bila kršena njegova pravica do zasebnosti in če je utrpel škodo zaradi zbiranja njegovih osebnih informacij ali opazovanja⁽¹⁹⁾. Glede na to, da „škoda“, ki je predmet odškodninskega zahtevka, ni omejena na materialno škodo (člen 710 civilnega zakonika), lahko to zajema tudi „duševne bolečine“. Znesek nadomestila za takšno nematerialno škodo bo sodnik ocenil na podlagi „proste presoje ob upoštevanju različnih dejavnikov v vsaki zadevi“⁽²⁰⁾.

Člen 1(1) zakona o nadomestilih države podeljuje pravico do odškodnine, če je i) javni uslužbenec z javnimi pooblastili države ali javnega subjekta ii) pri opravljanju svojih nalog iii) naklepno ali iz malomarnosti iv) nezakonito v) povzročil škodo drugi osebi.

Posameznik mora vložiti tožbo v skladu z zakonikom o civilnem postopku. V skladu z veljavnimi pravili lahko to stori pri sodišču, ki je pristojno v kraju, kjer je bilo škodno dejanje storjeno.

⁽¹⁸⁾ Glej npr. pisno poizvedbo doma svetnikov št. 92 z dne 27. marca 2009 v zvezi z obravnavo informacij, zbranih v okviru kazenskih preiskav, vključno s kršitvami obveznosti glede zaupnosti s strani policije in organov pregona.

⁽¹⁹⁾ Primer take tožbe je „zadeva v zvezi s seznamom obrambne agencije“ (okrožno sodišče v Niigati, sklep z dne 11. maja 2006 (2002(Wa) št. 514)). V tej zadevi je uradnik obrambne agencije pripravil, hranil in razširjal seznam posameznikov, ki so pri obrambni agenciji vložili zahtevke za razkritje upravnih dokumentov. Na tem seznamu so bili opisi tožnikovih osebnih informacij. Tožnik je vztrajal pri tem, da je bila kršena njegova zasebnost, pravica do seznanitve itd., ter zahteval, da toženec plača odškodnino v skladu s členom 1(1) zakona o nadomestilih države. Sodišče je temu zahtevku delno ugodilo in tožniku dodelilo delno nadomestilo.

⁽²⁰⁾ Sklep vrhovnega sodišča z dne 5. aprila 1910 (1910(O) št. 71).

- 3) Pravna sredstva posameznikov zoper nezakonite/nepravilne preiskave policije: pritožba prefekturni komisiji za javno varnost (člen 79 zakona o policiji)

V skladu s členom 79 zakona o policiji ⁽²¹⁾, kot je podrobneje pojasnjeno v navodilih vodje nacionalne policijske agencije prefekturni policiji in prefekturnim komisijam za javno varnost ⁽²²⁾, lahko posamezniki vložijo pisno pritožbo ⁽²³⁾ pri pristojni prefekturni komisiji za javno varnost v primeru nezakonitega ravnanja ali neprimerne ravnanja policista pri opravljanju njegovih nalog; to vključuje naloge v zvezi z zbiranjem in uporabo osebnih informacij. Komisija natančno obravnava take pritožbe v skladu z zakoni in lokalnimi odloki ter o rezultatu preiskave pisno obvesti pritožnika.

Prefekturna komisija za javno varnost na podlagi svojih nadzornih pristojnosti v skladu s členom 38(3) zakona o policiji prefekturni policiji izda navodilo, da razišče dejstva, izvede potrebne ukrepe glede na rezultate pregleda in rezultate sporoči komisiji. Kadar komisija meni, da je to potrebno, lahko izda tudi navodilo o obravnavi pritožbe, na primer, če je preiskava, ki jo je izvedla policija, po njenem mnenju nezadostna. To izvajanje je opisano v obvestilu, ki ga nacionalna policijska agencija izda vodjem prefekturne policije.

Pritožnika se o rezultatih preiskave obvesti tudi glede na poročila policije v zvezi s preiskavo in ukrepi, sprejetimi na zahtevo komisije.

- 4) Pravna sredstva posameznikov v skladu z zakonom o varstvu osebnih informacij, ki jih hranijo upravni organi, in zakonikom o kazenskem postopku

a) Zakon o varstvu osebnih informacij, ki jih hranijo upravni organi

V skladu s členom 48 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, si morajo upravni organi prizadevati za ustrezno in hitro obravnavo vseh pritožb v zvezi z obravnavanjem osebnih informacij. Ministrstvo za notranje zadeve in komunikacije je za zagotavljanje celovitih informacij posameznikom (npr. o razpoložljivih pravicah do razkritja, popravka in začasnega prenehanja uporabe v okviru zakona o varstvu osebnih informacij, ki jih hranijo upravni organi) in kot kontaktna točka za poizvedbe vzpostavilo celovite informacijske centre za razkritje informacij / varstvo osebnih informacij v vsaki prefekturi na podlagi člena 47(2) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi. Možne so tudi poizvedbe nerezidentov. Na primer, v poslovnem letu 2017 (od aprila 2017 do marca 2018) so celoviti informacijski centri odgovorili na poizvedbe itd. v 5 186 primerih.

Člena 12 in 27 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, posameznikom zagotavljata pravico, da zahtevajo razkritje in popravek hranjenih osebnih informacij. Poleg tega lahko posamezniki v skladu s členom 36 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, zahtevajo začasno prenehanje uporabe ali izbris hranjenih osebnih informacij, če upravni organ hranjenih osebnih informacij ni pridobil zakonito ali če s hrambo ali uporabo takih informacij krši zakon.

Kar zadeva osebne informacije, ki se zbirajo (na podlagi naloga ali prek „lista za poizvedbo“) in hranijo za kazenske preiskave ⁽²⁴⁾, pa se takšne informacije na splošno uvrščajo v kategorijo „osebnih informacij, ki jih vsebujejo dokumenti, ki se nanašajo na sojenja in zasežene predmete“. Take osebne informacije so zato izključene iz področja uporabe individualnih pravic iz poglavja 4 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, v skladu s členom 53-2 zakonika o kazenskem postopku ⁽²⁵⁾. Namesto tega se za obdelavo takih osebnih informacij in pravic posameznika

⁽²¹⁾ Člen 79 zakona o policiji (izvleček):

1. Kdor vloži pritožbo proti opravljanju nalog s strani osebja prefekture policije, lahko vloži pritožbo v pisni obliki pri prefekturni komisiji za javno varnost po postopku, predpisanem v odloku nacionalne komisije za javno varnost.
2. Prefekturna komisija za javno varnost, ki je prejela pritožbo iz prejšnjega odstavka, to natančno obravnava v skladu z zakoni in lokalnimi odloki ter o rezultatih pisno obvesti pritožnika, razen v naslednjih primerih:
 - (1) ugotoviti je mogoče, da je bila pritožba vložena z namenom oviranja zakonitega opravljanja nalog prefekturne policije;
 - (2) trenutno prebivališče pritožnika ni znano;
 - (3) ugotoviti je mogoče, da je bila pritožba vložena skupaj z drugimi pritožniki, ki so bili že obveščeni o rezultatu skupne pritožbe.

⁽²²⁾ Obvestilo nacionalne policijske agencije o ustrezni obravnavi pritožb v zvezi z opravljanjem nalog policistov z dne 13. aprila 2001 z Dodatkom 1 „Standardi za razlago/izvajanje člena 79 zakona o policiji“.

⁽²³⁾ V skladu z obvestilom nacionalne policijske agencije (glej prejšnjo opombo) so posamezniki, ki imajo težave pri pripravi pisne pritožbe, deležni pomoči. To izrecno vključuje primer tujcev.

⁽²⁴⁾ Po drugi strani pa obstajajo dokumenti, ki niso razvrščeni kot „dokumenti, ki se nanašajo na sojenja“, saj sami niso informacije, pridobljene z nalogom ali pisnimi poizvedbami v zvezi s preiskovalnimi zadevami, temveč nastanejo na podlagi takih dokumentov. To bi veljalo v primeru, ko za zasebne informacije ne velja člen 45(1) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, zato take informacije ne bi bile izključene iz uporabe poglavja 4 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi.

⁽²⁵⁾ Člen 53-2(2) zakonika o kazenskem postopku določa, da se določbe poglavja IV zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, ne uporabljajo za osebne informacije, ki jih vsebujejo dokumenti, ki se nanašajo na sojenja in zasežene predmete.

do dostopa in popravka uporabljajo posebna pravila iz zakonika o kazenskem postopku in zakona o spisih pravnomočnih kazenskih zadev (glej v nadaljevanju) ⁽²⁶⁾. Ta izključitev je utemeljena z različnimi dejavniki, kot so varstvo zasebnosti zadevnih oseb, tajnost preiskav in ustrezno vodenje kazenskega sodnega postopka. Ob tem je treba poudariti, da se določbe iz poglavja 2 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, v zvezi z načeli za obravnavo takih informacij še naprej uporabljajo.

b) Zakonik o kazenskem postopku

V skladu z zakonikom o kazenskem postopku so možnosti za dostop do osebnih informacij, zbranih za namene kazenske preiskave, odvisne tako od faze postopka kot tudi od vloge posameznika v preiskavi (osumljenec, obtoženec, žrtev itd.).

Kot izjema od pravila iz člena 47 zakonika o kazenskem postopku, da se dokumenti, ki se nanašajo na sojenje, ne objavijo pred začetkom sojenja (ker bi to lahko škodovalo časti in/ali kršilo pravico do zasebnosti zadevnih posameznikov in oviralo preiskavo/sojenje), se žrtvam kaznivega dejanja načeloma dovoli vpogled v take informacije, če se to šteje za razumno ob upoštevanju namena določb člena 47 zakonika o kazenskem postopku ⁽²⁷⁾.

Kar zadeva osumljence, se z dejstvom, da so predmet kazenske preiskave, običajno seznanijo na zaslišanju s strani pravosodnega policista ali državnega tožilca. Če se državni tožilec nato odloči, da ne bo začel kazenskega pregona, o tem nemudoma obvesti osumljenca na njegovo zahtevo (člen 259 zakonika o kazenskem postopku).

Poleg tega državni tožilec po začetku kazenskega pregona obtožencu ali njegovemu zagovorniku zagotovi možnost, da vnaprej pregleda dokaze, preden za njihov pregled zaprosi sodišče (člen 299 zakonika o kazenskem postopku). Tako se obtožencu omogoči, da preveri svoje osebne informacije, zbrane v kazenski preiskavi.

Varstvo osebnih informacij, zbranih v okviru kazenske preiskave, se ne glede na to, ali je zadevna oseba osumljenec, obtoženec ali katera koli druga oseba (npr. žrtev kaznivega dejanja), zagotovi z obveznostjo varovanja zaupnosti (člen 100 zakona o državni javni službi) in grožnjo s kaznijo v primeru uhajanja zaupnih informacij v okviru izvajanja nalog javne službe (člen 109 (xii) zakona o državni javni službi).

5) Pravna sredstva posameznikov zoper nezakonite/neustrezne preiskave s strani javnih organov: pritožba na komisijo za varstvo osebnih informacij

V skladu s členom 6 zakona o varstvu osebnih informacij vlada v sodelovanju z vladami tretjih držav sprejme potrebne ukrepe za vzpostavitev mednarodno skladnega sistema za osebne informacije prek spodbujanja sodelovanja z mednarodnimi organizacijami in drugimi mednarodnimi okviri. Na podlagi te določbe se v skladu z osnovno politiko o varstvu osebnih informacij (sprejeta s sklepom vlade) komisiji za varstvo osebnih informacij, ki ima nalogo splošnega upravljanja zakona o varstvu osebnih informacij, podeljuje pooblastilo za sprejetje potrebnih ukrepov za premoščanje razlik med japonskim sistemom in njegovim delovanjem ter sistemi zadevnih tujih držav in njihovim delovanjem, da se tako zagotovi ustrezna obravnavo osebnih informacij, prejetih iz take države.

Poleg tega sta komisiji za varstvo osebnih informacij v skladu s točkama (i) in (ii) člena 61 zakona o varstvu osebnih informacij zaupana naloga oblikovanja in spodbujanja osnovne politike ter izvedba mediacije v primerih pritožb, vloženih zoper poslovne subjekte. Upravni organi tudi tesno komunicirajo in sodelujejo med seboj (člen 80 zakona o varstvu osebnih informacij).

Na podlagi teh določb komisija za varstvo osebnih informacij obravnava pritožbe, ki jih vložijo posamezniki, in sicer:

- a) Posameznik, ki sumi, da so javni organi na Japonskem zbrali ali uporabili njegove podatke, prenesene iz EU, vključno z organi, odgovornimi za dejavnosti iz poglavja II in poglavja III tega dokumenta, v nasprotju s pravili, ki se uporabljajo, vključno s tistimi, ki so predmet tega dokumenta, lahko vloži pritožbo pri komisiji za varstvo osebnih informacij (posamično ali prek pristojnega organa za varstvo podatkov).
- b) Komisija za varstvo osebnih informacij obravnava pritožbo, vključno z uporabo svojih pooblastil iz členov 6, 61(ii) in 80 zakona o varstvu osebnih informacij, ter o njej obvesti pristojne javne organe, vključno z ustreznimi nadzornimi organi.

⁽²⁶⁾ V skladu z zakonikom o kazenskem postopku in zakonom o spisih pravnomočnih kazenskih zadev za dostop do zaseženih predmetov in njihov popravek ter za dokumente / osebne informacije v zvezi s sojenji v kazenskih zadevah velja edinstven in poseben sistem pravil, katerega cilj je varovanje zasebnosti zadevnih oseb, tajnost preiskav ter ustrezno vodenje kazenskega sodnega postopka itd.

⁽²⁷⁾ Natančneje, žrtvam kaznivih dejanj se načeloma dovoli vpogled v informacije glede objektivnih dokazov v zvezi z evidencami v zadevah, ki niso v kazenskem postopku, pri katerih žrtev sodeluje v skladu s členom 316-33 zakonika o kazenskem postopku, da se zagotovi boljša zaščita žrtev kaznivih dejanj.

Navedeni organi morajo v skladu s členom 80 zakona o varstvu osebnih informacij sodelovati s komisijo za varstvo osebnih informacij, in sicer tudi z zagotavljanjem potrebnih informacij in ustreznega gradiva, da lahko navedena komisija presodi, ali je bilo zbiranje oziroma nadaljnja uporaba osebnih informacij v skladu s pravili, ki se uporabljajo. Komisija za varstvo osebnih informacij pri presoji sodeluje z ministrstvom za notranje zadeve in komunikacije.

- c) Če se v okviru presoje izkaže, da so bila kršena pravila, ki se uporabljajo, sodelovanje zadevnih javnih organov s komisijo za varstvo osebnih informacij zajema obveznost odprave kršitve.

V primeru nezakonitega zbiranja osebnih informacij na podlagi pravil, ki se uporabljajo, to vključuje izbris zbranih osebnih informacij.

V primeru kršitve pravil, ki se uporabljajo, komisija za varstvo osebnih informacij pred zaključkom presoje potrdi, da je kršitev v celoti odpravljena.

- d) Po zaključku presoje komisija za varstvo osebnih informacij posameznika v razumnem roku obvesti o rezultatu presoje in o morebitnih popravnihi ukrepih, če je ustrezno. S tem obvestilom hkrati obvesti posameznika o možnosti zahtevati potrditev rezultata od pristojnega javnega organa in navede organ, pri katerem se vloži taka zahteva za potrditev.

Podrobne informacije o rezultatu presoje se lahko omejijo, če obstajajo utemeljeni razlogi, da bi lahko razkritje takih informacij pomenilo tveganje za potekajočo preiskavo.

Če se pritožba nanaša na zbiranje in uporabo osebnih informacij na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, komisija za varstvo osebnih informacij v primeru, da se v okviru presoje izkaže, da je bila zadeva v zvezi z osebnimi informacijami posameznika obravnavana in zaključena, obvesti posameznika, da lahko vpogleda v spis zadeve na podlagi člena 53 zakonika o kazenskem postopku in člena 4 zakona o spisih pravnomočnih kazenskih zadev.

Kadar se v okviru presoje izkaže, da je posameznik osumljenec v kazenski zadevi, komisija za varstvo osebnih informacij o tem obvesti posameznika, obvesti pa ga tudi o možnosti, da na podlagi člena 259 zakonika o kazenskem postopku vloži zahtevo.

- e) Če posameznik še vedno ni zadovoljen z rezultatom tega postopka, se lahko obrne na komisijo za varstvo osebnih informacij, ki ga seznani z različnimi možnostmi in podrobnimi postopki v zvezi s pravnimi sredstvi v skladu z japonskimi zakoni in predpisi. Komisija za varstvo osebnih informacij posamezniku zagotovi podporo, kar vključuje tudi svetovanje in pomoč pri vložitvi nadaljnjih vlog zadevnim upravnim ali pravosodnim organom.

III. Vladni dostop za namene nacionalne varnosti

A. Pravne podlage in omejitve glede zbiranja osebnih informacij

1) Pravne podlage za zbiranje informacij s strani zadevnega ministrstva/agencije

Kot je navedeno zgoraj, mora biti zbiranje osebnih informacij s strani upravnih organov za namene nacionalne varnosti v okviru njihove upravne pristojnosti.

Japonska nima zakona, ki bi omogočal zbiranje informacij z obveznimi sredstvi zgolj za namene nacionalne varnosti. V skladu s členom 35 ustave je prisilno zbiranje osebnih informacij mogoče samo na podlagi naloga, ki ga izda sodišče za preiskavo kaznivih dejanj. Tak nalog se torej lahko izda samo za namene kazenske preiskave. To pomeni, da v japonskem pravnem sistemu zbiranje oziroma dostop do informacij z obveznimi sredstvi iz razlogov nacionalne varnosti ni dovoljen. Na področju nacionalne varnosti lahko zadevna ministrstva ali agencije pridobijo informacije samo iz virov, do katerih je mogoče prosto dostopati, ali od poslovnih subjektov ali posameznikov s prostovoljnim razkritjem. Poslovni subjekti, ki prejmejo prošnjo za prostovoljno sodelovanje, niso z ničemer pravno zavezani k zagotavljanju takih informacij in zato ne trpijo negativnih posledic, če sodelovanje zavrnejo.

Na področju nacionalne varnosti je pristojnih več oddelkov ministrstev in agencij.

(1) Sekretariat vlade

Sekretariat vlade zbira in raziskuje informacije o pomembnih politikah vlade⁽²⁸⁾, določenih v členu 12-2 zakona o vladi⁽²⁹⁾. Vendar pa sekretariat vlade nima pristojnosti za zbiranje osebnih informacij neposredno od poslovnih subjektov. Zbira, vključuje, analizira in ocenjuje informacije iz odprtih virov, drugih javnih organov itd.

(2) Nacionalna policijska agencija / prefekturna policija

Prefekturna policija je v vseh prefekturah pristojna za zbiranje informacij v okviru svoje pristojnosti na podlagi člena 2 zakona o policiji. Lahko se zgodi, da nacionalna policijska agencija neposredno zbira informacije v okviru svoje pristojnosti na podlagi zakona o policiji. To velja zlasti za dejavnosti varnostnega urada nacionalne policijske agencije ter službe za zunanje zadeve in obveščevanje. V skladu s členom 24 zakona o policiji je varnostni urad zadolžen za zadeve, ki se nanašajo na varnostno policijo⁽³⁰⁾, služba za zunanje zadeve in obveščevanje pa za zadeve, ki se nanašajo na tuje državljane in na japonske državljane s sedežem dejavnosti v tuji državi.

(3) Obveščevalna agencija za javno varnost

Uporaba zakona o preprečevanju subverzivnih dejavnosti in zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora, je v glavnem v pristojnosti obveščevalne agencije za javno varnost. Ta agencija spada pod ministrstvo za pravosodje.

Zakon o preprečevanju subverzivnih dejavnosti in zakon o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora, določata, da se lahko pod strogimi pogoji sprejmejo upravni ukrepi (tj. ukrepi, s katerimi se odredi omejitev dejavnosti takih organizacij, njihova razpustitev itd.) proti organizacijam, ki so storile nekatera huda dejanja („teroristična subverzivna dejavnost“ ali „dejanje vsesplošnega množičnega umora“) in s tem kršile z ustavo določeno „javno varnost“ ali „temeljni družbeni sistem“. Izraz „teroristična subverzivna dejavnost“ spada na področje zakona o preprečevanju subverzivnih dejavnosti (glej člen 4, ki zajema dejavnosti, kot so upor, napad tujih sil, uboj s političnim namenom itd.), zakon o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora, pa se nanaša na „dejanja vsesplošnega množičnega umora“ (glej člen 4 zakona). Predmet določb zakona o preprečevanju subverzivnih dejavnosti in zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora, so lahko samo natančno opredeljene organizacije, ki predstavljajo posebno notranjo ali zunanjo grožnjo javni varnosti.

V ta namen zakon o preprečevanju subverzivnih dejavnosti in zakon o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora, zagotavljata pravno podlago za preiskave. Temeljna preiskovalna pooblastila uradnih oseb obveščevalne agencije za javno varnost so določena v členu 27 zakona o preprečevanju subverzivnih dejavnosti in členu 29 zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora. Preiskave s strani obveščevalne agencije za javno varnost se v skladu s temi določbami izvajajo, če so potrebne glede na zgornje določbe o nadzoru organizacij (predmet preiskave so že bile na primer radikalne levičarske skupine, sekta *Aum Shinrikyo* in nekatere domače skupine, ki so tesno povezane s Severno Korejo). Vendar se te preiskave ne morejo zanašati na obvezna sredstva, zato organizacij, ki imajo osebne informacije, ni mogoče prisiliti, da bi te informacije posredovale.

Za zbiranje in uporabo informacij, ki se prostovoljno razkrijejo obveščevalni agenciji za javno varnost, veljajo ustrezni zaščitni ukrepi in omejitve, ki jih določa zakon, med drugim tajnost komunikacijskih sredstev, ki jo zagotavlja ustava, in pravila o ravnanju z osebnimi informacijami na podlagi zakona o varstvu osebnih informacij, ki jih hranijo upravni organi.

(4) Ministrstvo za obrambo

Ministrstvo za obrambo zbira informacije na podlagi člena 3 in 4 zakona o ustanovitvi ministrstva za obrambo, če je to potrebno za izvajanje njegove upravne pristojnosti, vključno v zvezi z obrambo in zaščito, ukrepi, ki jih sprejmejo vojaške sile, ter napotitvijo kopenskih, pomorskih in zračnih vojaških sil. Ministrstvo za obrambo lahko informacije za te namene zbira samo prek prostovoljnega sodelovanja in iz prosto dostopnih virov. Informacij o širši javnosti ne zbira.

2) Omejitve in zaščitni ukrepi

a) Zakonske omejitve

(1) Splošne omejitve na podlagi zakona o varstvu osebnih informacij, ki jih hranijo upravni organi

Zakon o varstvu osebnih informacij, ki jih hranijo upravni organi je splošni zakon, ki se uporablja za zbiranje in obdelavo osebnih informacij s strani upravnih organov na vseh področjih dejavnosti teh organov. Zato omejitve in zaščitni ukrepi iz oddelka II.A.1)b)(2) veljajo tudi za hrambo, uporabo itd. osebnih informacij na področju nacionalne varnosti.

⁽²⁸⁾ Vodi ga urad vlade za obveščevalno dejavnost in raziskave na podlagi člena 4 odredbe o sekretariatu vlade.

⁽²⁹⁾ To vključuje zbiranje in raziskovanje informacij o pomembnih politikah vlade.

⁽³⁰⁾ Varnostna policija je odgovorna za dejavnosti boja proti kriminaliteti, ki so povezane z javno varnostjo in v državnem interesu. To vključuje boj proti kriminaliteti in zbiranje informacij o nezakonitih dejanjih, povezanih z ekstremnimi levičarskimi in desničarskimi skupinami ter škodljivimi protijaponskimi dejavnostmi.

(2) Posebne omejitve, ki veljajo za policijo (tako za nacionalno policijsko agencijo kot tudi prefekturno policijo)

Kot je navedeno zgoraj v oddelku, ki obravnava zbiranje informacij za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, lahko policija zbira informacije samo v okviru svoje pristojnosti, in sicer so v skladu s členom 2(2) zakona o policiji te dejavnosti „strogo omejene“ na opravljanje nalog policije na način, ki je „nepistranski, neopredeljen, brez predsodkov in pošten“. Poleg tega „nikoli ne zlorablja svojih pooblastil na noben način, ki bi posegal v pravice in svoboščine posameznika, kot so zagotovljene v ustavi Japonske“.

(3) Posebne omejitve, ki se uporabljajo za obveščevalno agencijo za javno varnost

Člen 3 zakona o preprečevanju subverzivnih dejavnosti in člen 3 zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora, določata, da se preiskave, ki se izvajajo v skladu s tema aktoma, izvajajo samo v najmanjšem potrebnem obsegu, da se doseže zastavljeni cilj, in se ne izvajajo tako, da bi neupravičeno omejevale temeljne človekove pravice. Poleg tega je v skladu s členom 45 zakona o preprečevanju subverzivnih dejavnosti in členom 42 zakona o nadzoru organizacij, ki so zagrešile dejanja vsesplošnega množičnega umora, zloraba pooblastil s strani uradne osebe obveščevalne agencije za javno varnost kaznivo dejanje, ki se kaznuje s strožjimi kazenskimi sankcijami kot „splošna“ zloraba pooblastil na drugih področjih javnega sektorja.

(4) Posebne omejitve, ki se uporabljajo za ministrstvo za obrambo

Kar zadeva zbiranje/organizacijo informacij s strani ministrstva za obrambo, kot je navedeno v členu 4 zakona o ustanovitvi ministrstva za obrambo, je zbiranje informacij s strani ministrstva omejeno na tisto, kar je „potrebno“ za izvajanje njegovih nalog na področju (1) obrambe in varovanja, (2) ukrepov vojaških sil ter (3) organizacije, števila osebja, strukture, opreme in napotitve kopenskih, pomorskih in zračnih vojaških sil.

b) Druge omejitve

Kot je pojasnjeno v oddelku II.A.2(b)(1) v zvezi s kazenskimi preiskavami, iz sodne prakse vrhovnega sodišča izhaja, da mora biti za obravnavo prošnje za prostovoljno sodelovanje s poslovnim subjektom ta prošnja potrebna za preiskavo domnevnega kaznivega dejanja in razumna, da bi se dosegel namen preiskave.

Čeprav se preiskave, ki jih izvajajo preiskovalni organi na področju nacionalne varnosti, razlikujejo od preiskav, ki jih izvajajo preiskovalni organi na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, v smislu njihove pravne podlage in namena, se na področju nacionalne varnosti podobno uporabljajo osrednja načela „potrebnosti preiskave“ in „ustreznosti metode“, ki jih je treba upoštevati, pri tem pa ustrezno upoštevati tudi posebne okoliščine vsake zadeve.

S kombinacijo navedenih omejitev se zagotovi, da zbiranje in obdelava informacij potekata le v obsegu, ki je potreben za izvajanje posebnih nalog pristojnega javnega organa, in na podlagi posebnih groženj. Sem ne spada množično in neselektivno zbiranje osebnih informacij ali dostop do njih iz razlogov nacionalne varnosti.

B. Nadzor

1) Nadzor na podlagi zakona o varstvu osebnih informacij, ki jih hranijo upravni organi

Kot je pojasnjeno v oddelku II.B.2), imajo v japonskem javnem sektorju ministri in vodje ministrstev in agencij pooblastilo, da v svojem ministrstvu ali agenciji nadzorujejo in zagotavljajo skladnost z zakonom o varstvu osebnih informacij, ki jih hranijo upravni organi. Poleg tega lahko minister za notranje zadeve in komunikacije preveri izvajanje tega zakona, od vsakega ministra zahteva predložitev gradiva in pojasnil na podlagi člena 49 in 50 zakona ter na vse ministre naslovi mnenje na podlagi člena 51 zakona. Lahko na primer zahteva revizijo ukrepov z ukrepi na podlagi člena 50 in 51 zakona.

2) Nadzor policije s strani komisij za javno varnost

Kot je pojasnjeno v oddelku „II. Zbiranje informacij za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj“, neodvisna prefekturna komisija za javno varnost nadzoruje dejavnosti prefekturne policije.

Nacionalno policijsko agencijo nadzoruje nacionalna komisija za javno varnost. V skladu s členom 5 zakona o policiji je ta komisija odgovorna zlasti za „varstvo pravic in svoboščin posameznika“. V ta namen oblikuje celovite politike, ki določajo predpise za upravljanje zadev iz vsake točke člena 5(4) zakona o policiji, in določa druge temeljne usmeritve ali ukrepe, ki bi morali biti podlaga za izvajanje navedenih dejavnosti. Nacionalna komisija za javno varnost ima enako stopnjo neodvisnosti kot prefekturna komisija za javno varnost.

3) Nadzor ministrstva za obrambo s strani urada generalnega inšpektorja za pravno skladnost

Urad generalnega inšpektorja za pravno skladnost je neodvisen urad ministrstva za obrambo, ki je pod neposrednim nadzorom ministra za obrambo v skladu s členom 29 zakona o ustanovitvi ministrstva za obrambo. Urad generalnega inšpektorja za pravno skladnost lahko preverja, ali uradniki ministrstva za obrambo spoštujejo zakone in predpise. Tako preverjanje se imenuje „obrambni inšpekcijski pregled“.

Urad generalnega inšpektorja za pravno skladnost opravlja inšpekcijske preglede s pozicije neodvisnega urada, da se zagotovi pravna skladnost celotnega ministrstva, vključno z vojaškimi silami. Svoje naloge opravlja neodvisno od operativnih oddelkov ministrstva za obrambo. Rezultate inšpekcijskih pregledov skupaj s potrebnimi izboljševalnimi ukrepi takoj posreduje neposredno ministru za obrambo. Minister za obrambo lahko na podlagi poročila urada generalnega inšpektorja za pravno skladnost izdaja odredbe za izvajanje ukrepov, potrebnih za izboljšanje stanja. Za izvajanje teh ukrepov je odgovoren namestnik pomočnika ministra, ki o izvajanju poroča ministru za obrambo.

Kot prostovoljen ukrep za preglednost se ugotovitve obrambnih inšpekcijskih pregledov zdaj objavljajo na spletišču ministrstva za obrambo (čeprav zakon tega ne zahteva).

Obrambni inšpekcijski pregledi se razdelijo v tri kategorije:

- (i) redni obrambni inšpekcijski pregledi, ki se izvajajo v rednih časovnih presledkih ⁽³¹⁾;
- (ii) obrambni inšpekcijski pregledi, s katerimi se preverja, ali so se izvedli izboljševalni ukrepi, ter
- (iii) posebni obrambni inšpekcijski pregledi, ki se izvajajo v zvezi s posebnimi vprašanji, ki jih odredi minister za obrambo.

Generalni inšpektor lahko pri teh inšpekcijskih pregledih zahteva poročila od zadevnega urada, zahteva predložitev dokumentov, vstopi v objekte, da bi opravil inšpekcijski pregled, zahteva pojasnila namestnika pomočnika ministra itd. Zaradi narave inšpekcijskih nalog urada generalnega inšpektorja za pravno skladnost urad vodijo visoki pravni strokovnjaki (nekdanji nadrejeni tožilec).

4) Nadzor nad obveščevalno agencijo za javno varnost

Obveščevalna agencija za javno varnost izvaja redne in posebne inšpekcijske preglede dejavnosti svojih služb in uradov (obveščevalna služba za javno varnost, obveščevalni urad za javno varnost in poduradi itd.). Za namene rednih inšpekcijskih pregledov se za inšpektorja imenuje pomočnik generalnega direktorja in/ali direktor. Taki inšpekcijski pregledi se nanašajo tudi na upravljanje osebnih informacij.

5) Nadzor s strani parlamenta

Kar zadeva zbiranje informacij za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, lahko parlament prek svojega pristojnega odbora prouči zakonitost zbiranja informacij na področju nacionalne varnosti. Preiskovalna pooblastila parlamenta temeljijo na členu 62 ustave ter členih 74 in 104 zakona o parlamentu.

C. Pravna sredstva posameznikov

Pravna sredstva posameznikov se uveljavljajo na enak način kot na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. To vključuje tudi nov mehanizem pravnih sredstev, ki ga upravlja in nadzoruje komisija za varstvo osebnih informacij, za obravnavo in reševanje pritožb, ki jih vložijo posamezniki iz EU. V zvezi s tem glej ustrezne dele oddelka II.C.

Poleg tega so na področju nacionalne varnosti posameznikom na voljo posebna pravna sredstva.

Za osebne informacije, ki jih zbere upravni organ za namene nacionalne varnosti, se uporabljajo določbe poglavja 4 zakona o varstvu osebnih informacij, ki jih hranijo upravni organi. To vključuje pravico zahtevati razkritje (člen 12) ali popravek (vključno z dodatkom ali izbrisom) (člen 27) shranjenih osebnih informacij posameznika ter pravico zahtevati začasno prekinitev uporabe osebnih informacij, če je upravni organ zadevne informacije pridobil nezakonito (člen 36). Vendar za uveljavljanje teh pravic na področju nacionalne varnosti veljajo nekatere omejitve: zahteve po razkritju,

⁽³¹⁾ Primer inšpekcijskega pregleda v zvezi z vprašanji, ki jih zajema ta dokument, je redni obrambni inšpekcijski pregled iz leta 2016 v zvezi z „ozaveščanjem/pripravljanjem za pravno skladnost“, saj je bilo varstvo osebnih informacij ena od osrednjih točk pregleda. Natančneje, inšpekcijski pregled je obsegal upravljanje, hrambo itd. osebnih informacij. Urad generalnega inšpektorja za pravno skladnost je v svojem poročilu opredelil več neustreznosti pri upravljanju osebnih informacij, ki bi jih bilo treba odpraviti, na primer to, da informacije niso bile zaščitene z geslom. Poročilo je na voljo na spletišču ministrstva za obrambo.

popravku ali začasni prekinitvi se ne odobrijo, če zadevajo „informacije, v zvezi s katerimi obstajajo utemeljeni razlogi, da lahko vodja upravnega organa domneva, da bi razkritje lahko škodovalo nacionalni varnosti, uničilo odnos zaupanja s tujo državo ali mednarodno organizacijo ali škodovalo pogajanjem s tujo državo ali mednarodno organizacijo“ (člen 14(iv)). Zato ta izjema ne velja za vsako prostovoljno zbiranje informacij v zvezi z nacionalno varnostjo, saj vedno zahteva konkretno oceno tveganj, povezanih z njihovim razkritjem.

Poleg tega lahko v primeru, da se zahteva posameznika zavrne z utemeljitvijo, da zadevnih informacij v skladu s členom 14(iv) ni mogoče razkriti, posameznik vloži upravno pritožbo za pregled te odločitve, pri čemer lahko na primer trdi, da pogoji iz člena 14(iv) v zadevnem primeru niso izpolnjeni. V tem primeru se vodja zadevnega upravnega organa pred sprejetjem odločitve posvetuje z odborom za razkritje informacij in varstvo osebnih informacij. Odbor pritožbo obravnava z neodvisnega stališča. Odbor je visoko specializiran in neodvisen organ, katerega člane imenuje predsednik vlade s soglasjem obeh domov parlamenta izmed strokovnjakov⁽³²⁾. Odbor ima močna preiskovalna pooblastila, vključno z možnostjo, da zahteva dokumente in razkritje zadevnih osebnih informacij, razpravlja brez navzočnosti javnosti in uporabi postopek z indeksom Vaughn⁽³³⁾. Nato pripravi pisno poročilo, ki se posreduje zadevnemu posamezniku⁽³⁴⁾. Ugotovitve iz poročila se objavijo. Čeprav poročilo formalno gledano ni pravno zavezujoče, zadevni upravni organ upošteva skoraj vsa poročila⁽³⁵⁾.

V skladu s členom 3(3) zakona o upravnem sporu lahko posameznik vloži tožbo za razveljavitev odločbe upravnega organa, da se osebnih informacij ne razkrije.

IV. Redni pregled

V okviru rednega pregleda sklepa o ustreznosti si komisija za varstvo osebnih informacij in Evropska komisija izmenjujeta informacije o obdelavi podatkov pod pogoji iz ugotovitev glede ustreznosti, vključno s tistimi iz teh navedb.

⁽³²⁾ Glej člen 4 zakona o ustanovitvi nadzornega odbora za razkritje informacij in varstvo osebnih informacij.

⁽³³⁾ Glej člen 9 zakona o ustanovitvi nadzornega odbora za razkritje informacij in varstvo osebnih informacij.

⁽³⁴⁾ Glej člen 16 zakona o ustanovitvi nadzornega odbora za razkritje informacij in varstvo osebnih informacij.

⁽³⁵⁾ V zadnjih treh letih ni bilo primera, da bi zadevni upravni organ sprejel odločitev, ki bi se razlikovala od sklepov odbora. Pred tem sta bila od leta 2005 (leto, ko je začel veljati zakon o varstvu osebnih informacij, ki jih hranijo upravni organi) med 2 000 zadevami samo dva taka primera. Kadar upravni organ sprejme odločitev, ki se razlikuje od sklepov odbora, v skladu s točko 4 člena 50(1) zakona o pritožbah na upravne odločbe, ki se uporablja z nadomestitvijo člena 42(2) zakona o varstvu osebnih informacij, ki jih hranijo upravni organi, jasno navede razloge za to.

ISSN 1977-0804 (elektronska različica)
ISSN 1725-5155 (tiskana različica)



Urad za publikacije Evropske unije
2985 Luxembourg
LUKSEMBURG

SL