II

(Nezakonodajni akti)

SKLEPI

IZVEDBENI SKLEP KOMISIJE (EU) 2022/254

z dne 17. decembra 2021

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

(notificirano pod dokumentarno številko C(2021) 9316)

(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 člena 45(3) Uredbe,

ob upoštevanju naslednjega:

1. UVOD

(1) Uredba (EU) 2016/679 določa pravila o prenosu osebnih podatkov od upravljavcev ali obdelovalcev v Uniji v tretje države in mednarodne organizacije, če taki prenosi spadajo na področje uporabe navedene uredbe. Pravila o mednarodnem prenosu podatkov vsebuje poglavje V navedene uredbe (členi 44 do 50). Čeprav je pretok osebnih podatkov v države zunaj Evropske unije in iz njih ključen za širitev čezmejne trgovine in mednarodnega sodelovanja, je treba zagotoviti, da zaradi takih prenosov v tretje države ni ogrožena raven varstva osebnih podatkov, ki se zagotavlja v Uniji ([2]).

(2) V skladu s členom 45(3) Uredbe (EU) 2016/679 lahko Komisija z izvedbenim aktom odloči, da tretja država, ozemlje ali en oziroma več določenih sektorjev v tretji državi ali mednarodna organizacija zagotavlja ustrezno raven varstva. Pod tem pogojem se lahko osebni podatki v tretjo državo prenašajo brez dodatnega dovoljenja, kot je določeno v členu 45(1) in uvodni izjavi 103 Uredbe (EU) 2016/679.

(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, kar vključuje pravila, ki se uporabljajo glede uvoznikov podatkov, ter omejitve in zaščitne ukrepe glede dostopa javnih organov do osebnih podatkov. Komisija mora v oceni ugotoviti, ali zadevna tretja država zagotavlja raven varstva, ki je „v osnovi enakovredna“ tisti, zagotovljeni v Evropski uniji (uvodna izjava 104 Uredbe (EU) 2016/679). Ali je tako, je treba oceniti glede na zakonodajo Unije, predvsem Uredbo (EU) 2016/679, in sodno prakso Sodišča Evropske unije ([3]).

([1]) UL L 119, 4.5.2016, str. 1.
([2]) Glej uvodno izjavo 101 Uredbe (EU) 2016/679.
([3]) Glej, nazadnje, sodbo z dne 16. julija 2020, Facebook Ireland in Schrems (v nadaljnjem besedilu: Schrems II), C-311/18, EU:C:2020:559.

(4) Kot je pojasnilo Sodišče Evropske unije, v ta namen ni nujno, da se ugotovi identična raven varstva ([4]). To pomeni zlasti, da se lahko sredstva, ki jih zadevna tretja država uporablja za varstvo osebnih podatkov, razlikujejo od tistih, ki jih uporablja Unija, če se v praksi izkaže, da so učinkovita pri zagotavljanju ustrezne ravni varstva ([5]). Standard ustreznosti torej ne zahteva doslednega posnemanja pravil Unije. Pač pa se prouči, ali tuji sistem kot celota z vsebino pravic do zasebnosti ter njihovim učinkovitim izvajanjem, nadzorom in izvrševanjem zagotavlja zahtevano raven varstva ([6]). Smernice v zvezi s tem zagotavlja tudi referenčni dokument o ustreznosti, ki ga je izdal Evropski odbor za varstvo podatkov in v katerem je nadalje pojasnjen ta standard ([7]).

(5) Komisija je skrbno proučila korejsko zakonodajo in prakso. Na podlagi ugotovitev iz uvodnih izjav (8) do (208) Komisija ugotavlja, da Republika Koreja zagotavlja ustrezno raven varstva osebnih podatkov, ki se od upravljavca oziroma obdelovalca v Uniji ([8]) prenašajo k subjektom (npr. fizičnim ali pravnim osebam, organizacijam, javnim organom) v Koreji, ki spadajo na področje uporabe zakona o varstvu osebnih podatkov (zakon št. 10465 z dne 29. marca 2011, kakor je bil nazadnje spremenjen z zakonom št. 16930 z dne 4. februarja 2020). To vključuje upravljavce in obdelovalce (tako imenovane zunanje izvajalce ([9])) v smislu Uredbe (EU) 2016/679. Ugotovitev o ustreznosti ne zajema obdelave osebnih podatkov za misijonarske dejavnosti verskih organizacij in imenovanja kandidatov s strani političnih strank, niti obdelave osebnih kreditnih informacij na podlagi zakona o kreditnih informacijah s strani upravljavcev, ki so pod nadzorom komisije za finančne storitve.

(6) V teh sklepnih ugotovitvah se upoštevajo dodatni zaščitni ukrepi iz Uradnega obvestila št. 2021-5 (Priloga I) ter uradne navedbe, zagotovila in zaveze, ki jih je korejska vlada dala Komisiji (Priloga II).

(7) Ta sklep pomeni, da za prenos osebnih podatkov upravljavcem in obdelovalcem v Republiki Koreji ni treba pridobiti nobenega dodatnega dovoljenja. Ne vpliva na neposredno uporabo Uredbe (EU) 2016/679 za take subjekte, če so izpolnjeni pogoji glede ozemeljske veljavnosti navedene uredbe iz njenega člena 3.

2. PRAVILA, KI SE UPORABLJAJO ZA OBDELAVO OSEBNIH PODATKOV

2.1 Okvir varstva osebnih podatkov v Republiki Koreji

(8) Pravni sistem, ki v Koreji ureja varstvo zasebnosti in podatkov, temelji na korejski ustavi, razglašeni 17. julija 1948. Čeprav pravica do varstva osebnih podatkov v ustavi ni izrecno navedena, pa je kljub temu priznana kot temeljna pravica, ki izhaja iz ustavnih pravic do človekovega dostojanstva in prizadevanja za srečo (člen 10), zasebnega življenja (člen 17) in zasebnosti komunikacij (člen 18). To sta potrdili vrhovno sodišče ([10]) in ustavno sodišče ([11]). Omejitve temeljnih pravic in svoboščin (vključno s pravico do zasebnosti) se lahko naložijo le z zakonom, kadar je to potrebno za nacionalno varnost ali vzdrževanje javnega reda in miru zaradi javne blaginje, in ne smejo vplivati na bistvo zadevne pravice ali svoboščine (člen 37(2)).

([4]) Sodba z dne 6. oktobra 2015, Maximillian Schrems/Data Protection Commissioner (v nadaljnjem besedilu: sodba v zadevi Schrems), C-362/14, EU:C:2015:650, točka 73.

([5]) Sodba v zadevi Schrems, točka 74.

([6]) Glej Sporočilo Komisije Evropskemu parlamentu in Svetu: Izmenjava in varstvo osebnih podatkov v globaliziranem svetu (COM(2017) 7 z dne 10. januarja 2017, oddelek 3.1, str. 6 in 7.

([7]) Evropski odbor za varstvo podatkov, Referenčni dokument o ustreznosti, WP 254 rev. 01, na voljo na povezavi: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([8]) 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, veljati pa je začel 20. julija 2018. Navedeni sporazum torej vključuje tudi Uredbo. Za namene sklepa se torej šteje, da sklici na EU in države članice EU vključujejo tudi države EGP.

([9]) Glej oddelek 2.2.3 tega sklepa.

([10]) Glej na primer odločbo vrhovnega sodišča št. 2014Da77970 z dne 15. oktobra 2015 (angleški povzetek je na voljo na povezavi z naslovom *Lawmaker's disclosure of teachers' trade union members case* (Zadeva: razkritje članov učiteljskega sindikata s strani zakonodajalca): https://www.privacy.go.kr/eng/enforcement_01.do) in v njej navedeno sodno prakso, vključno z odločbo št. 2012Da49933 z dne 24. julija 2014.

([11]) Glej zlasti odločbo ustavnega sodišča št. 99Hun-ma513 z dne 26. maja 2005 (angleški povzetek je na voljo na povezavi: http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) in odločbo št. 2014JHun-ma449 2013 Hun-Ba68 (prečiščena različica) z dne 23. decembra 2015 (angleški povzetek je na voljo na povezavi z naslovom *Change of resident registration number case* (Zadeva: sprememba registrske številke prebivalca): https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Čeprav se ustava na več mestih sklicuje na pravice korejskih državljanov, je ustavno sodišče odločilo, da temeljne pravice veljajo tudi za tujce ([12]). Natančneje, sodišče je odločilo, da ima vsak človek, ne le vsak državljan, pravico do varstva svojega dostojanstva in vrednosti ter pravico, da si prizadeva za srečo ([13]). Poleg tega je glede na uradne navedbe korejske vlade ([14]) splošno priznano, da členi 12 do 22 ustave (ki vključujejo tudi pravice do zasebnosti) zagotavljajo temeljne človekove pravice ([15]). Čeprav še ne obstaja sodna praksa, ki bi se nanašala posebej na pravico do zasebnosti tujih državljanov, pa dejstvo, da ta temelji na varstvu človekovega dostojanstva in prizadevanja za srečo, podpira tako ugotovitev ([16]).

(10) Poleg tega je Koreja sprejela več zakonov na področju varstva podatkov, ki določajo zaščitne ukrepe za vse posameznike, ne glede na njihovo državljanstvo ([17]). Za namene tega sklepa so relevantni naslednji zakoni:

— zakon o varstvu osebnih podatkov;

— zakon o uporabi in varstvu kreditnih informacij ([18]);

— zakon o varstvu zasebnosti komunikacij.

(11) Zakon o varstvu osebnih podatkov določa splošni pravni okvir za varstvo podatkov v Republiki Koreji. Dopolnjuje ga uredba o izvajanju (predsedniška uredba št. 23169 z dne 29. septembra 2011, nazadnje spremenjena s predsedniško uredbo št. 30892 z dne 4. avgusta 2020; v nadaljnjem besedilu: uredba o izvajanju zakona o varstvu osebnih podatkov), ki je tako kot zakon o varstvu osebnih podatkov pravno zavezujoča in izvršljiva.

(12) Prav tako regulativna uradna obvestila, ki jih sprejema komisija za varstvo osebnih podatkov, določajo nadaljnja pravila glede razlage in uporabe zakona o varstvu osebnih podatkov. Komisija za varstvo osebnih podatkov je na podlagi člena 5 (obveznosti države) zakona o varstvu osebnih podatkov in člena 14 (mednarodno sodelovanje) istega zakona sprejela uradno obvestilo št. 2021-5 z dne 1. septembra 2020 (kakor je bilo spremenjeno z obvestilom št. 2021-1 z dne 21. januarja 2021 in obvestilom št. 2021-5 z dne 16. novembra 2021, v nadaljnjem besedilu: uradno obvestilo št. 2021-5) o razlagi, uporabi in izvrševanju nekaterih določb zakona o varstvu osebnih podatkov. Navedeno uradno obvestilo vsebuje pojasnila, ki se uporabljajo za vsakršno obdelavo osebnih podatkov na podlagi zakona o varstvu osebnih podatkov, ter dodatne zaščitne ukrepe za osebne podatke, ki se v Korejo prenašajo na podlagi tega sklepa. Uradno obvestilo je pravno zavezujoče za obdelovalce osebnih podatkov, izvršujejo pa ga lahko komisija za varstvo osebnih podatkov in sodišča ([19]). Kršitev pravil iz uradnega obvestila pomeni kršitev zadevnih določb zakona o varstvu osebnih podatkov, ki jih dopolnjujejo. Vsebina dodatnih zaščitnih ukrepov je torej analizirana v okviru ocene zadevnih členov zakona o varstvu osebnih podatkov. Nazadnje, nadaljnje smernice o zakonu o varstvu osebnih podatkov in uredbi o njegovem izvajanju, na katerih temeljita uporaba in izvrševanje pravil o varstvu podatkov s strani komisije za varstvo osebnih podatkov, vsebujejo priročnik in smernice o zakonu o varstvu osebnih podatkov, ki jih je sprejela komisija za varstvo osebnih podatkov ([20]).

([12]) Odločba ustavnega sodišča št. 93 Hun-MA120 z dne 29. decembra 1994.
([13]) Odločba ustavnega sodišča št. 99HeonMa494 z dne 29. novembra 2001.
([14]) Glej Prilogo II, oddelek 1.1.
([15]) Glej tudi člen 1 zakona o varstvu osebnih podatkov, ki se izrecno sklicuje na „svoboščine in pravice posameznikov“. Natančneje, določa, da je namen takega zakona „zagotoviti obdelavo in varstvo osebnih podatkov s ciljem varstva svoboščin in pravic posameznikov ter uresničevanja osebnega dostojanstva in vrednosti posameznikov“. Podobno tudi člen 5(1) zakona o varstvu osebnih podatkov določa obveznost države, da „oblikuje politike za preprečevanje škodljivih posledic zbiranja, ki presega namen, zlorabe in nepravilne uporabe osebnih podatkov, nediskretnega nadzora in sledenja itd. ter krepitev dostojanstva ljudi in njihove zasebnosti“.
([16]) Poleg tega člen 6(2) ustave določa, da status tujcev zagotavljajo mednarodno pravo in mednarodne pogodbe. Koreja je podpisnica več mednarodnih sporazumov, ki zagotavljajo pravico do zasebnosti, na primer Mednarodnega pakta o državljanskih in političnih pravicah (člen 17), Konvencije o pravicah invalidov (člen 22) in Konvencije o otrokovih pravicah (člen 16).
([17]) To vključuje pravila, ki so pomembna za varstvo osebnih podatkov, vendar se ne uporabljajo, kadar se osebni podatki zbirajo v Uniji in prenašajo v Korejo na podlagi Uredbe (EU) 2016/679, na primer v zakonu o varstvu, uporabi itd. podatkov o lokaciji.
([18]) Namen tega zakona je omogočati zanesljivo poslovanje s kreditnimi informacijami, spodbujati učinkovito uporabo in sistematično upravljanje kreditnih informacij ter varovati zasebnost pred nepravilno uporabo in zlorabo kreditnih informacij (člen 1 zakona).
([19]) Na primer, korejska sodišča so v številnih primerih razsodila o skladnosti z regulativnimi uradnimi obvestili, tudi tako, da so korejski nadzorniki odgovorni za kršitve obvestila (glej npr. odločbo vrhovnega sodišča št. 2018Da219406 z dne 25. oktobra 2018, v kateri je sodišče upravljavcu naložilo, naj posameznikom plača nadomestilo za škodo, ki so jo utrpeli zaradi kršitve Uradnega obvestila glede standarda za ukrepe za zagotovitev varnosti osebnih podatkov; glej tudi odločbo vrhovnega sodišča št. 2018Da219352 t dne 25. oktobra 2018; odločbo vrhovnega sodišča št. 2011Da24555 z dne 16. maja 2016; odločbo osrednjega okrožnega sodišča v Seulu št. 2014Gahap511956 z dne 13. oktobra 2016; odločbo osrednjega okrožnega sodišča v Seulu št. 2009Gahap43176 t dne 26. januarja 2010).
([20]) Člen 12(1) zakona o varstvu osebnih podatkov.

(13) Poleg tega zakon o uporabi in varstvu kreditnih informacij določa posebna pravila, ki se uporabljajo za „navadne“ gospodarske subjekte in specializirane subjekte v finančnem sektorju, kadar ti obdelujejo osebne kreditne informacije, tj. podatke, ki so potrebni za določitev kreditne sposobnosti strank v finančnih ali poslovnih transakcijah. To zlasti vključuje ime, kontaktne podatke, finančne transakcije, bonitetno oceno, zavarovalni status ali preostali znesek posojila, kadar se taki podatki uporabljajo za določitev posameznikove kreditne sposobnosti ([21]). Kadar pa se taki podatki uporabljajo za druge namene (npr. kadrovske), se zakon o varstvu osebnih podatkov uporablja v celoti. Skladnost s posebnimi določbami o varstvu podatkov iz zakona o uporabi in varstvu kreditnih informacij deloma nadzoruje komisija za varstvo osebnih podatkov (glede gospodarskih subjektov glej člen 45-3 zakona o uporabi in varstvu kreditnih informacij) in deloma komisija za finančne storitve ([22]) (glede finančnega sektorja, vključno z bonitetnimi agencijami, bankami, zavarovalnicami, vzajemnimi hranilnicami, specializiranimi kreditnimi finančnimi družbami, družbami za storitve finančnih naložb, finančnimi družbami za vrednostne papirje, kreditnimi zadrugami itd. glej člen 45(1) zakona o uporabi in varstvu kreditnih informacij v povezavi s členom 36-2 uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij in členom 38 zakona o komisiji za finančne storitve). V tem smislu je področje uporabe tega sklepa omejeno na gospodarske subjekte, ki jih nadzoruje komisija za varstvo osebnih podatkov ([23]). Posebna pravila zakona o uporabi in varstvu kreditnih informacij, ki se uporabljajo v tem okviru (splošna pravila zakona o varstvu osebnih podatkov se uporabljajo, če ni posebnih pravil), so opisana v oddelku 2.3.11.

2.2 **Materialno in osebno področje uporabe zakona o varstvu osebnih podatkov**

(14) Varstvo osebnih podatkov ureja zakon o varstvu osebnih podatkov, razen če je v drugih zakonih izrecno določeno drugače (člen 6). Materialno in osebno področje uporabe določajo opredelitve pojmov „osebni podatek“, „obdelava“ in „obdelovalec osebnih podatkov“.

2.2.1 *Opredelitev pojma osebni podatki*

(15) Člen 2(1) zakona o varstvu osebnih podatkov te opredeljuje kot podatke, ki se nanašajo na živečega posameznika in s katerimi je mogoče posameznika identificirati neposredno, na primer z imenom, registrsko številko prebivalca ali sliko, ali posredno, in sicer kadar je mogoče podatke, s katerimi ni mogoče identificirati določenega posameznika, brez težav združiti z drugimi podatki. Ali je mogoče podatke „brez težav“ združiti, je odvisno od tega, ali je tako združevanje razumno verjetno, pri čemer se upoštevajo verjetnost za pridobitev drugih podatkov ter čas, stroški in tehnologija, ki so potrebni za identifikacijo posameznika.

(16) Poleg tega se na podlagi zakona o varstvu osebnih podatkov (člen 2(1), točka (c)) psevdonimizirani podatki (tj. podatki, s katerimi posameznika ni mogoče identificirati brez uporabe dodatnih informacij ali združevanja z njimi za obnovitev podatkov v prvotno stanje) štejejo za osebne podatke. Nasprotno pa se zakon o varstvu osebnih podatkov ne uporablja za informacije, ki so povsem anonimizirane (člen 58-2 navedenega zakona). To velja za informacije, s katerimi ni mogoče identificirati določenega posameznika, niti v povezavi z drugimi informacijami, ob upoštevanju časa, stroškov in tehnologije, ki so razumno potrebni za tako identifikacijo.

(17) To ustreza materialnemu področju uporabe Uredbe (EU) 2016/679 in njenim pojmom „osebni podatki“, „psevdonimizacija“ ([24]) in „anonimizirane informacije“ ([25]).

([21]) Člen 2(1) zakona o uporabi in varstvu kreditnih informacij.

([22]) Komisija za finančne storitve je korejski nadzorni organ za finančni sektor, ki v tej vlogi tudi izvršuje zakon o uporabi in varstvu kreditnih informacij.

([23]) Če bi se to v prihodnosti spremenilo, na primer z razširitvijo pristojnosti komisije za varstvo osebnih podatkov na vse primere obdelave osebnih kreditnih informacij na podlagi zakona o uporabi in varstvu kreditnih informacij, bi se lahko proučila možnost spremembe sklepa o ustreznosti, tako da bi vključeval tudi subjekte, ki jih trenutno nadzoruje komisija za finančne storitve.

([24]) Zakon o varstvu osebnih podatkov določa, da se za „psevdonimizirano obdelavo“ šteje obdelava z uporabo metod, kot je delni izbris osebnih podatkov ali delna oziroma popolna nadomestitev osebnih podatkov tako, da brez dodatnih informacij ni mogoče prepoznati konkretnega posameznika (člen 2(1-2) zakona o varstvu osebnih podatkov). To ustreza opredelitvi psevdonimizacije v členu 4(5) Uredbe (EU) 2016/679, ki se nanaša na „obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku“.

([25]) Natančneje, v uvodni izjavi 26 Uredbe (EU) 2016/679 je pojasnjeno, da se uredba ne uporablja za anonimizirane informacije, tj. informacije, ki se ne nanašajo na določeno ali določljivo fizično osebo. To pa je odvisno od vseh sredstev, za katera se razumno pričakuje, da jih bo upravljavec ali druga oseba uporabila za neposredno ali posredno identifikacijo posameznika. Da bi ugotovili, ali se za ta sredstva lahko razumno pričakuje, da bodo uporabljena, je treba upoštevati vse objektivne dejavnike, kot so stroški identifikacije in čas, potreben zanjo, ter pri tem upoštevati razpoložljivo tehnologijo in tehnološki razvoj v času obdelave.

2.2.2 *Opredelitev obdelave*

(18) Pojem „obdelava“ je v zakonu o varstvu osebnih podatkov široko opredeljen kot „zbiranje, ustvarjanje, povezovanje, beleženje, shranjevanje, hramba, obdelava z dodano vrednostjo, urejanje, priklic, dajanje na voljo, popravljanje, obnavljanje, uporaba, zagotavljanje, razkrivanje in uničenje osebnih podatkov ter druge podobne dejavnosti“ ([26]). Čeprav se nekatere določbe zakona o varstvu osebnih podatkov nanašajo le na posebne vrste obdelave, kot so „uporaba“, „zagotavljanje“ ali „zbiranje“ ([27]), pa se pojem „uporaba“ razlaga tako, da vključuje vse vrste obdelave, razen „zbiranja“ ali „zagotavljanja“ (tretjim osebam). Ta široka razlaga pojma „uporaba“ torej zagotavlja, da v varstvu ni vrzeli pri posameznih dejavnostih obdelave. Pojem obdelave torej ustreza istemu pojmu iz Uredbe (EU) 2016/679.

2.2.3 *Upravljavec osebnih podatkov in „zunanji izvajalec“*

(19) Zakon o varstvu osebnih podatkov se uporablja za „upravljavce osebnih podatkov“ (v nadaljnjem besedilu: upravljavec). Podobno kot v Uredbi (EU) 2016/679 ta izraz vključuje vsak javni organ, pravno osebo, organizacijo ali posameznika, ki kot del svojih dejavnosti obdeluje osebne podatke neposredno ali posredno za delo z datotekami z osebnimi podatki ([28]). V tem smislu „datoteka z osebnimi podatki“ pomeni kateri koli „niz ali več nizov osebnih podatkov, ki so sistematično urejeni ali organizirani po določenem pravilu, da se omogoči preprost dostop do osebnih podatkov“ (člen 2(4) zakona o varstvu podatkov) ([29]). Upravljavec mora v okviru svoje organizacije usposobiti osebe, ki pod njegovim vodstvom sodelujejo pri obdelavi, na primer uslužbence ali zaposlene v družbi, ter izvajati ustrezen nadzor (člen 28(1) zakona o varstvu osebnih podatkov).

(20) Posebne obveznosti veljajo, kadar upravljavec odda obdelavo osebnih podatkov tretji osebi (zunanjemu izvajalcu). Taka oddaja zunanjemu izvajalcu mora biti zlasti urejena s pravno zavezujočim dogovorom (običajno s pogodbo) ([30]), ki opredeljuje obseg dela, oddanega zunanjemu izvajalcu, namen obdelave, tehnične in upravljavske standarde, ki se morajo uporabljati, nadzor s strani upravljavca, odgovornost (npr. odškodnino za škodo zaradi kršitve pogodbenih obveznosti) in omejitve morebitne podobdelave ([31]) (člen 26(1) in (2) zakona o varstvu osebnih podatkov v povezavi s členom 28(1) uredbe o izvajanju) ([32]).

(21) Poleg tega mora upravljavec objaviti in stalno posodabljati informacije o delu, oddanem v zunanje izvajanje, ter o zunanjih izvajalcih; če se obdelava, oddana v zunanje izvajanje, nanaša na dejavnosti neposrednega trženja, pa mora zadevne informacije zagotoviti neposredno posamezniku (člen 26(2) in (3) zakona o varstvu osebnih podatkov v povezavi s členom 28(2)-(5) uredbe o izvajanju) ([33]).

(22) Prav tako mora v skladu s členom 26(4) zakona o varstvu osebnih podatkov v povezavi s členom 28(6) uredbe o izvajanju upravljavec zunanjega izvajalca „podučiti“ o potrebnih varnostnih ukrepih in nadzirati, med drugim z inšpekcijskimi pregledi, ali zagotavlja skladnost z vsemi obveznostmi upravljavca na podlagi zakona o varstvu osebnih podatkov ([34]) in na podlagi pogodbe o zunanjem izvajanju. Če zunanji izvajalec povzroči škodo zaradi kršitev zakona o varstvu osebnih podatkov, se za namene odgovornosti njegova dejanja ali opustitve pripišejo upravljavcu, tako kot v primeru zaposlenega (člen 26(6) zakona o varstvu osebnih podatkov).

([26]) Člen 2(2) zakona o varstvu osebnih podatkov.
([27]) Členi 15 do 19 zakona o varstvu osebnih podatkov se torej nanašajo le na zbiranje, uporabo in zagotavljanje osebnih podatkov.
([28]) Člen 2(5) zakona o varstvu osebnih podatkov. Izraz javni organ v smislu zakona o varstvu osebnih podatkov vključuje vse osrednje upravne oddelke ali organe in njihove pridružene organe, lokalno upravo, šole in javna podjetja, v katera vlaga lokalna vlada, upravne organe parlamenta in sodstvo (vključno z ustavnim sodiščem) (člen 2(6) zakona o varstvu osebnih podatkov v povezavi s členom 2 uredbe o izvajanju zakona o varstvu osebnih podatkov).
([29]) To ustreza materialnemu področju uporabe Uredbe (EU) 2016/679. Člen 2(1) Uredbe (EU) 2016/679 določa, da se uredba uporablja za „obdelavo osebnih podatkov, ki se v celoti ali delno izvaja z avtomatiziranimi sredstvi, in za obdelavo osebnih podatkov, ki so del zbirke ali so namenjeni oblikovanju dela zbirke, ki se ne izvaja z avtomatiziranimi sredstvi“. V členu 4(6) Uredbe (EU) 2016/679 je „zbirka“ opredeljena kot „vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili“. V skladu s tem je v uvodni izjavi 15 pojasnjeno, da bi se moralo varstvo posameznikov uporabljati za „obdelavo osebnih podatkov z avtomatiziranimi sredstvi in za ročno obdelavo, če so osebni podatki del zbirke ali so namenjeni, da postanejo del zbirke. Zapisi ali nizi zapisov – kot tudi njihove naslovnice –, ki niso strukturirani v skladu s posebnimi merili, ne bi smeli spadati na področje uporabe te uredbe.“
([30]) Glej priročnik o zakonu o varstvu osebnih podatkov, poglavje III, oddelek 2, o členu 26 (str. 203 do 212), v katerem je pojasnjeno, da se člen 26(1) zakona o varstvu osebnih podatkov nanaša na zavezujoče dogovore, kot so pogodbe ali podobni dogovori.
([31]) Člen 26(5) zakona o varstvu osebnih podatkov določa, da obdelovalec ne sme nobenih osebnih podatkov uporabljati zunaj obsega dela, oddanega v zunanje izvajanje, ali zagotavljati osebnih podatkov tretji osebi. Za kršitev te zahteve se lahko izreče kazenska sankcija na podlagi člena 71, točka 2, zakona o varstvu osebnih podatkov.
([32]) Za kršitev te zahteve se lahko izreče globa, glej člen 75(4), točka 4, zakona o varstvu osebnih podatkov.
([33]) Za kršitev te zahteve se lahko izreče globa, glej člen 75(2), točka 1, in člen 75(4), točka 5, zakona o varstvu osebnih podatkov.
([34]) Glej tudi člen 26(7) zakona o varstvu osebnih podatkov, v skladu s katerim se členi 15 do vključno 25, 27 do vključno 31, 33 do vključno 38 in 50 smiselno uporabljajo tudi za obdelovalca.

(23) Čeprav zakon o varstvu osebnih podatkov torej ne razlikuje med pojmoma „upravljavec“ in „obdelovalec“, pa pravila o oddaji del v zunanje izvajanje zagotavljajo v osnovi enakovredne obveznosti in zaščitne ukrepe kot pravila, ki urejajo razmerje med upravljavcem in obdelovalcem na podlagi Uredbe (EU) 2016/679.

2.2.4 *Posebne določbe, ki se nanašajo na ponudnike informacijskih in komunikacijskih storitev*

(24) Čeprav se zakon o varstvu osebnih podatkov uporablja za obdelavo osebnih podatkov s strani katerega koli upravljavca, pa nekatere določbe vsebujejo posebna pravila (kot *lex specialis*) glede obdelave osebnih podatkov „uporabnikov“ s strani „ponudnikov informacijskih in komunikacijskih storitev“ ([35]). Pojem „uporabniki“ vključuje posameznike, ki uporabljajo informacijske in komunikacijske storitve (člen 2(1), točka 4, zakona o spodbujanju uporabe informacijskih in komunikacijskih omrežij in varstva podatkov, v nadaljnjem besedilu: zakon o omrežjih). To pomeni, da mora posameznik bodisi neposredno uporabljati telekomunikacijske storitve, ki jih zagotavlja korejski telekomunikacijski operater, bodisi uporabljati informacijske storitve ([36]), ki jih komercialno (tj. za dobiček) zagotavlja subjekt, ki se sam zanaša na storitve telekomunikacijskega operaterja, ki ima dovoljenje za opravljanje storitev ali je registriran v Koreji ([37]). V obeh primerih je subjekt, ki ga zavezujejo specifične določbe zakona o varstvu osebnih podatkov, tisti, ki ponuja spletno storitev neposredno posamezniku (tj. uporabniku).

(25) Nasprotno pa se ugotavljanje ustreznosti nanaša izključno na raven varstva pri prenosu osebnih podatkov od upravljavca/obdelovalca v Uniji k subjektu v tretji državi (v tem primeru: v Republiki Koreji). V slednjem primeru bodo imeli posamezniki v Uniji običajno neposreden odnos le z „izvoznikom podatkov“ v Uniji, ne pa tudi s korejskim ponudnikom informacijskih in komunikacijskih storitev ([38]). Zato se bodo posebne določbe zakona o varstvu osebnih podatkov, ki se nanašajo na osebne podatke uporabnikov informacijskih in komunikacijskih storitev, uporabljale le v omejenih primerih za osebne podatke, ki se prenašajo na podlagi tega sklepa.

2.2.5 *Izvzetje iz nekaterih določb zakona o varstvu osebnih podatkov*

(26) Člen 58(1) zakona o varstvu osebnih podatkov izključuje uporabo dela navedenega zakona (tj. členov 15 do 57) za štiri vrste obdelave podatkov ([39]). Zlasti se ne uporabljajo deli zakona o varstvu osebnih podatkov, ki se nanašajo na posebno podlago za obdelavo, nekatere obveznosti glede varstva podatkov, podrobna pravila glede uresničevanja pravic posameznikov in pravila, ki urejajo reševanje sporov v okviru odbora za mediacijo v primeru sporov v zvezi z osebnimi podatki. Druge temeljne določbe zakona o varstvu osebnih podatkov se uporabljajo, zlasti splošne določbe o načelih glede varstva podatkov (člen 3 zakona o varstvu osebnih podatkov) – kar vključuje na primer načela zakonitosti, opredelitve in omejitve namena, najmanjšega obsega podatkov ter točnosti in varnosti podatkov – in pravic posameznikov (do dostopa, popravka, izbrisa in prenehanja obdelave, glej člen 4 zakona o varstvu osebnih podatkov). Poleg tega člen 58(4) zakona o varstvu osebnih podatkov uvaja posebne obveznosti glede takih dejavnosti obdelave, in sicer glede najmanjšega obsega podatkov, omejene hrambe podatkov, varnostnih ukrepov in obravnave pritožb ([40]). Posledično lahko posamezniki še vedno vložijo pritožbo pri komisiji za varstvo osebnih podatkov, če se ta načela in obveznosti ne upoštevajo, navedena komisija pa lahko v primeru neskladnosti sprejme izvršilne ukrepe.

([35]) Glej zlasti člen 18(2) in poglavje VI zakona o varstvu osebnih podatkov.

([36]) Informacijske storitve vključujejo zagotavljanje informacij in posredniške storitve za zagotavljanje informacij.

([37]) Glej člen 2(1), točka 3, (v povezavi s členom 2(1), točki 2 in 4) zakona o omrežjih ter člen 2(6) in (8) zakona o zagotavljanju telekomunikacijskih storitev.

([38]) Če bi imeli korejski ponudniki informacijskih in komunikacijskih storitev neposreden odnos s posamezniki v EU (s ponujanjem spletnih storitev), bi se lahko neposredno uporabljala Uredba (EU) 2016/679, in sicer na podlagi člena 3(2), točka (a).

([39]) Člen 58(2) zakona o varstvu osebnih podatkov nadalje določa, da se člena 15 in 22, člen 27(1) - (2) ter člena 34 in 37 ne uporabljajo za osebne podatke, ki se obdelujejo z napravami za obdelavo vizualnih podatkov, ki so nameščene in delujejo na prostem. Ker se ta določba nanaša na uporabo video nadzora v Koreji, tj. neposredno zbiranje osebnih podatkov od posameznikov v Koreji, ni relevantna za namene tega sklepa, ki se nanaša na prenose osebnih podatkov od upravljavcev/obdelovalcev v EU k subjektom v Koreji. Poleg tega se v skladu s členom 58(3) zakona o varstvu osebnih podatkov člen 15 (zbiranje in uporaba osebnih podatkov), člen 30 (obveznost sprejetja javne politike zasebnosti) in člen 31 (obveznost imenovanja pooblaščene osebe za varstvo zasebnosti) ne uporabljajo za osebne podatke, ki se obdelujejo za vodenje prijateljskih skupin ali združenj (npr. klubov za prostočasne dejavnosti). Ker se šteje, da so take skupine po naravi zasebne in niso povezane s poklicno ali gospodarsko dejavnostjo, za zbiranje in uporabo podatkov v tem okviru ni potrebna posebna pravna podlaga (kot je privolitev zadevnih posameznikov). Vse ostale določbe zakona o varstvu osebnih podatkov (npr. najmanjši obseg podatkov, omejitev namena, zakonitost obdelave, varnost in pravice posameznikov) se uporabljajo. Še več, za kakršno koli obdelavo osebnih podatkov, ki presega namen, za katerega je bila družbena skupina ustanovljena, navedena izjema ne velja.

([40]) Natančneje, člen 58(4) zakona o varstvu osebnih podatkov določa, da je treba osebne podatke obdelovati v najmanjšem možnem obsegu, da se doseže namen obdelave, da jih je treba obdelovati čim krajši čas ter da je treba zagotoviti varno upravljanje in ustrezno obdelavo takih osebnih podatkov. Slednje vključuje tehnične, upravljavske in fizične zaščitne ukrepe ter ukrepe za zagotovitev ustrezne obravnave posameznih pritožb.

(27) Prvič, delna izjema se nanaša na osebne podatke, ki jih z namenom obdelave in na podlagi zakona o statističnih podatkih zbirajo javni organi. Iz pojasnil korejske vlade izhaja, da se osebni podatki, ki se obdelujejo v tem okviru, običajno nanašajo na korejske državljane in le izjemoma vključujejo podatke o tujcih, namreč v primeru statističnih podatkov o vstopu na ozemlje in izstopu z njega ali o tujih naložbah. Vendar pa se tudi v takih primerih podatki običajno ne prenašajo od upravljavcev/obdelovalcev v Uniji, ampak jih neposredno zbirajo javni organi v Koreji ([41]). Poleg tega podobno kot je navedeno v uvodni izjavi 162 Uredbe (EU) 2016/679 za obdelavo podatkov na podlagi zakona o statistiki velja več pogojev in zaščitnih ukrepov. Zakon o statistiki nalaga zlasti posebne obveznosti, kot so zagotavljanje točnosti, doslednosti in nepristranskosti; da se posameznikom zagotovi zaupnost, da se varujejo podatki anketirancev pri izvajanju statističnih anket, da se med drugim prepreči uporaba takih podatkov za kateri koli drug namen, razen za zbiranje statističnih podatkov, in da se osebje zaveže k varovanju zaupnosti ([42]). Javni organi, ki obdelujejo statistične podatke, morajo med drugim upoštevati tudi načela najmanjšega obsega podatkov, omejitve namena in varnosti (člen 3 in člen 58(4) zakona o varstvu osebnih podatkov) ter posameznikom omogočiti uveljavljanje njihovih pravic (dostop, popravek, izbris in prenehanje obdelave, glej člen 4 zakona o varstvu osebnih podatkov). Nazadnje, podatke je treba obdelovati v anonimizirani ali psevdonimizirani obliki, če to omogoča izpolnitev namena obdelave (člen 3(7) PIPA).

(28) Drugič, člen 58(1) zakona o varstvu osebnih podatkov se nanaša na osebne podatke, zbrane ali zahtevane zaradi analize informacij, povezanih z nacionalno varnostjo. Področje uporabe in posledice te delne izjeme so podrobneje opisani v uvodni izjavi (149).

(29) Tretjič, delna izjema se nanaša na začasno obdelavo osebnih podatkov, kadar je to nujno potrebno zaradi javne varnosti, vključno z javnim zdravjem. Komisija za varstvo osebnih podatkov to kategorijo razlaga ozko in po prejetih informacijah ni bila nikoli uporabljena. Uporablja se le v nujnih primerih, ko je potrebno takojšnje ukrepanje, na primer pri sledenju povzročiteljem nalezljivih bolezni ali pri reševanju žrtev naravnih nesreč in zagotavljanju pomoči tem žrtvam ([43]). Tudi v teh primerih se delno izvzetje nanaša le na obdelavo osebnih podatkov za omejeno časovno obdobje za izvedbo takega ukrepa. Primeri, ko bi to lahko veljalo za prenose podatkov, na katere se nanaša ta sklep, so še bolj omejeni, saj je malo verjetno, da bi bili osebni podatki, ki se iz Unije prenašajo h korejskim subjektom, take vrste, da bi bila njihova obdelava v takih nujnih primerih „nujno potrebna“.

(30) Nazadnje, delna izjema velja za osebne podatke, ki jih zbirajo ali uporabljajo mediji, verske organizacije za misijonarske dejavnosti ali politične stranke za imenovanje kandidatov. Izjema velja le, kadar mediji, verske organizacije ali politične stranke osebne podatke obdelujejo za navedene posebne namene (tj. novinarsko dejavnost, misijonarsko delo in imenovanje političnih kandidatov). Kadar navedeni subjekti obdelujejo osebne podatke za druge namene, na primer kadrovske zadeve ali notranje upravljanje, se zakon o varstvu osebnih podatkov v celoti uporablja.

(31) Pri obdelavi osebnih podatkov s strani medijev za namene novinarske dejavnosti uravnoteženost med svobodo izražanja in drugimi pravicami (vključno s pravico do zasebnosti) zagotavlja zakon o arbitraži in pravnih sredstvih itd. zaradi škode, ki jo povzroči poročanje medijev (v nadaljnjem besedilu: zakon o medijih) ([44]). Zlasti člen 5 zakona o medijih določa, da mediji (tj. katera koli organizacija za radiofuzijo, časopis, revija ali spletni časopis), spletne novičarske storitve ali spletne multimedijske organizacije za radiofuzijo ne smejo kršiti zasebnosti posameznikov. Če kljub temu pride do kršitve zasebnosti, jo je treba takoj odpraviti v skladu s posebnimi postopki iz navedenega zakona. V tem smislu zakon o medijih posameznikom, ki so utrpeli škodo zaradi medijskega poročanja, zagotavlja več pravic, na primer do objave popravka neresnične izjave, popravka v obliki nasprotne izjave ali nadaljnjega poročanja (kadar se medijsko poročanje nanaša na domnevno kaznivo dejanje, ki

([41]) V tem smislu člen 33 zakona o statističnih podatkih od javnih organov zahteva, da varujejo podatke anketirancev pri izvajanju statističnih anket, da se med drugim prepreči uporaba takih podatkov za kateri koli drug namen, razen za zbiranje statističnih podatkov.

([42]) Člen 2(2)-(3), člen 30(2) ter člena 33 in 34 zakona o statističnih podatkih.

([43]) Priročnik o zakonu o varstvu osebnih podatkov, oddelek o členu 58.

([44]) Člen 4 zakona o medijih na primer določa, da mora biti medijsko poročanje nepristransko in objektivno, da mora biti v javnem interesu, da mora spoštovati človekovo dostojanstvo in vrednost ter da ne sme škoditi ugledu drugih ali posegati v njihove pravice oziroma kršiti javne morale ali družbene etike.

ga je posameznik pozneje oproščen) ([45]). Pritožbe posameznikov lahko neposredno obravnava medijska hiša (prek varuha pravic) ([46]), lahko se obravnavajo v okviru spravnega postopka oziroma arbitraže (pred posebno komisijo za arbitražo na področju medijev) ([47]) ali pred sodišči. Posamezniki lahko prejmejo tudi odškodnino, če zaradi nezakonitega dejanja medija (namerno ali iz malomarnosti) utrpijo denarno škodo, poseg v osebnostne pravice ali druge duševne bolečine ([48]). Na podlagi zakona so mediji oproščeni odgovornosti, če njihovo poročanje, ki posega v pravice posameznika, ni v nasprotju z družbenimi vrednotami in če je objavljeno s privolitvijo zadevnega posameznika ali v javnem interesu (in če obstaja dovolj razlogov za sklepanje, da poročanje ustreza resnici) ([49]).

(32) Medtem ko za obdelavo osebnih podatkov s strani medijev za namene novinarske dejavnosti torej veljajo posebni zaščitni ukrepi, ki izhajajo iz zakona o medijih, pa ni takih dodatnih zaščitnih ukrepov, ki bi določali uporabo izjem za dejavnosti obdelave s strani verskih organizacij ali političnih strank ter bi bili primerljivi s členi 85, 89 in 91 Uredbe (EU) 2016/679. Komisija torej meni, da je ustrezno, da se s področja uporabe tega sklepa izključijo verske organizacije, kadar obdelujejo osebne podatke za misijonarsko dejavnost, in politične stranke, kadar obdelujejo osebne podatke v okviru imenovanja kandidatov.

2.3 **Zaščitni ukrepi, pravice in obveznosti**

2.3.1 *Zakonitost in poštenost obdelave*

(33) Osebni podatki bi se morali obdelovati zakonito in pošteno.

(34) To načelo določa člen 3(1) in (2) zakona o varstvu osebnih podatkov, utrjuje pa ga člen 59 navedenega zakona, ki prepoveduje obdelavo osebnih podatkov „na podlagi goljufije ali z neprimernimi oziroma nepoštenimi sredstvi“, „brez zakonskega pooblastila“ ali „s prekoračitvijo takega pooblastila“ ([50]). Ta splošna načela zakonite obdelave so podrobneje opredeljena v členih 15 do 19 zakona o varstvu osebnih podatkov, ki določajo različne pravne podlage za obdelavo (zbiranje, uporaba in zagotavljanje tretjim osebam), med drugim v okoliščinah, v katerih se lahko namen spremeni (člen 18 zakona o varstvu osebnih podatkov).

([45]) Členi 15 do 17 zakona o medijih.

([46]) Vsak medij ali medijska hiša mora imeti svojega varuha pravic, da se prepreči in odpravi morebitna škoda, ki jo povzroči medij (npr. s priporočilom za popravek neresničnega medijskega poročanja ali medijskega poročanja, ki škoduje ugledu drugih), člen 6 zakona o medijih.

([47]) Komisijo sestavlja med 40 in 90 arbitrov, ki jih minister za kulturo, šport in turizem imenuje izmed sodnikov, odvetnikov, oseb, ki že vsaj 10 let delajo na področju zbiranja novic ali poročanja o novicah, ali drugih oseb, ki imajo strokovno znanje s področja medijev. Navedeni arbitri ne morejo hkrati biti javni uslužbenci, člani političnih strank ali novinarji. V skladu s členom 8 zakona o medijih morajo navedeni arbitri svoje naloge opravljati neodvisno ter ne smejo prejemati nobenih usmeritev ali navodil. Poleg tega so uvedena posebna pravila, ki preprečujejo navzkrižje interesov, tako na primer posamezni arbiter ne sme obravnavati zadeve, v kateri kot stranka nastopa njegov zakonec ali sorodnik (člen 10 zakona o medijih). Komisija lahko spore obravnava v spravnem ali arbitražnem postopku, lahko pa tudi daje priporočila za odpravo kršitev (oddelek 5 zakona o medijih).

([48]) Člen 30 zakona o medijih.

([49]) Člen 5 zakona o medijih.

([50]) Člen 59 zakona o varstvu osebnih podatkov vsem osebam, „ki obdelujejo ali so kdaj obdelovale osebne podatke“, prepoveduje „pridobivanje osebnih podatkov ali privolitve za obdelavo osebnih podatkov na podlagi goljufije oziroma z neustreznimi ali nepoštenimi sredstvi“, „razkrivanje osebnih podatkov, pridobljenih v okviru poslovanja, ali njihovo zagotavljanje tretjim osebam brez pooblastila“ oziroma „poškodovanje, uničenje, spreminjanje, ponarejanje ali razkrivanje osebnih podatkov drugih oseb brez zakonskega pooblastila ali s prekoračitvijo takega pooblastila“. Za kršitev te prepovedi se lahko izreče kazenska sankcija (glej člen 71(5) in (6) ter člen 72(2) zakona o varstvu osebnih podatkov). Člen 70(2) zakona o varstvu osebnih podatkov nadalje omogoča izrek kazenske sankcije za pridobivanje osebnih podatkov, ki jih obdelujejo tretje osebe, in sicer na podlagi goljufije ali z drugimi nepoštenimi sredstvi ali metodami, ali za zagotavljanje osebnih podatkov tretji osebi za dobiček ali nepoštene namene, pa tudi za napeljevanje k takemu ravnanju ali za organizacijo takega ravnanja.

(35) V skladu s členom 15(1) zakona o varstvu osebnih podatkov lahko upravljavec osebne podatke (v okviru obsega namena zbiranja) zbira le na podlagi omejenega števila pravnih podlag. Te so (1) privolitev posameznika, na katerega se nanašajo osebni podatki ([51]) (točka 1); (2) potreba po sklenitvi in izpolnitvi pogodbe s posameznikom, na katerega se nanašajo osebni podatki (točka 4); (3) posebno pooblastilo v zakonu ali potreba po izpolnitvi pravne obveznosti (točka 2); obveznost ([52]) javnega organa, da izvaja naloge v okviru svoje pristojnosti, kot to določa zakon; (4) očitna potreba po zaščiti življenja, telesa ali premoženja posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe pred neposredno nevarnostjo (le če posameznik, na katerega se nanašajo osebni podatki, ne more izraziti svojega namena, ali če predhodne privolitve ni mogoče pridobiti) (točka 5); (5) potreba po uresničitvi „upravičenega interesa“ upravljavca, če ta „očitno prevlada“ nad interesi posameznika, na katerega se nanašajo osebni podatki (in le kadar je obdelava „pomembno povezana“ z zakonitim interesom in ne presega tega, kar je razumno) (točka 6) ([53]). Te podlage za obdelavo so v osnovi enakovredne tistim iz člena 6 Uredbe (EU) 2016/679, vključno s podlago „upravičenega interesa“, ki je enakovredna podlagi „zakonitega interesa“ iz člena 6(1), točka f, Uredbe (EU) 2016/679.

(36) Zbrani osebni podatki se lahko uporabljajo v okviru namena zbiranja (člen 15(1) zakona o varstvu osebnih podatkov) ali „v okviru obsega, ki je razumno povezan“ z namenom zbiranja, pri čemer se upoštevajo morebitne težave za posameznika, na katerega se nanašajo osebni podatki, sprejeti pa morajo biti tudi potrebni varnostni ukrepi (npr. šifriranje) (člen 15(3) zakona o varstvu osebnih podatkov). Za ugotovitev, ali je namen uporabe „razumno povezan“ z izvirnim namenom zbiranja, uredba o izvajanju določa posebna merila, ki so podobna tistim iz člena 6(4) Uredbe (EU) 2016/679. Zlasti velja, da mora obstajati pomembna povezava z izvirnim namenom, da mora biti dodatna uporaba predvidljiva (npr. glede na okoliščine, v katerih so bile informacije zbrane) in da morajo biti podatki psevdonimizirani, če je to mogoče ([54]). Posebna merila, ki jih upravljavec uporablja pri tej oceni, morajo biti vnaprej navedena v politiki zasebnosti ([55]). Poleg tega se izrecno zahteva, da pooblaščena oseba za varstvo zasebnosti (glej uvodno izjavo (94)) preveri, ali nadaljnja uporaba spada v navedene parametre.

([51]) Privolitev mora biti dana svobodno, biti mora premišljena, specifična in izražena na enega od načinov, ki jih predvideva zakon. V nobenem primeru ne sme biti privolitev pridobljena z goljufijo, neprimernimi ali kako drugače nepoštenimi sredstvi (člen 59(1) zakona o varstvu osebnih podatkov). Prvič, na podlagi člena 4, točka 2, zakona o varstvu osebnih podatkov imajo posamezniki, na katere se nanašajo osebni podatki, pravico „dati ali odreči privolitev“ in „izbrati obseg privolitve“, pri čemer jih je treba seznaniti s to pravico (člen 15(2), člen 16(2) in (3), člen 17(2) in člen 18(3) zakona o varstvu osebnih podatkov). Člen 22(5) zakona o varstvu osebnih podatkov vsebuje nadaljnji zaščitni ukrep, saj upravljavcu prepoveduje, da bi posamezniku odrekel zagotavljanje blaga ali storitev, kadar bi to lahko omejilo posameznikovo svobodno izbiro glede privolitve. To vključuje primere, ko je privolitev potrebna le za nekatere vrste obdelave (druge pa temeljijo na pogodbi), in nadaljnjo obdelavo osebnih podatkov, zbranih v okviru zagotavljanja blaga ali storitev. Drugič, v skladu s členom 15(2), člena 17(2) in (3) ter člena 18(3) zakona o varstvu osebnih podatkov mora upravljavec, kadar zaprosi za privolitev, posameznika, na katerega se nanašajo osebni podatki, obvestiti o „podrobnostih“ zadevnih osebnih podatkov (npr. da se to nanaša na občutljive podatke, glej člen 17(2), točka 2(a), uredbe o izvajanju zakona o varstvu osebnih podatkov), namenu obdelave, obdobju hrambe in vseh morebitnih prejemnikih podatkov. Vsaka taka prošnja se izrazi „na očitno prepoznaven način“, tako da so zadeve, glede katerih je potrebna privolitev, ločene od drugih zadev (člen 22(1) do (4) zakona o varstvu osebnih podatkov). Tretjič, člen 17(1), tč. 1-6, uredbe o izvajanju zakona o varstvu osebnih podatkov določa posebne metode, s katerimi upravljavec pridobi privolitev, na primer pisna privolitev s podpisom posameznika, na katerega se nanašajo osebni podatki, ali privolitev s (povratnim) elektronskim sporočilom. Čeprav zakon o varstvu osebnih podatkov posameznikom ne zagotavlja izrecno splošne pravice do umika privolitve, imajo posamezniki pravico do prenehanja obdelave podatkov, ki se nanašajo nanje, kar bo v primeru uveljavljanja privedlo do prekinitve obdelave in izbrisa podatkov (glej uvodno izjavo 78 o pravici do prenehanja obdelave).

([52]) Glede na informacije komisije za varstvo osebnih podatkov se lahko javni organi na to podlago sklicujejo le, če se obdelavi osebnih podatkov ni mogoče izogniti, tj. organ brez obdelave podatkov ne more opravljati svojih nalog ali jih opravlja nerazumno težko.

([53]) Člen 39-3 zakona o varstvu osebnih podatkov določa posebne (strožje) obveznosti ponudnikov informacijskih in komunikacijskih storitev glede zbiranja in uporabe osebnih podatkov njihovih uporabnikov. Zlasti določa, da mora ponudnik pridobiti privolitev uporabnika, potem ko mu zagotovi informacije o namenu zbiranja/uporabe, vrstah osebnih podatkov, ki se zbirajo, in obdobju obdelave podatkov (člen 39-3(1) zakona o varstvu osebnih podatkov). Enako velja, ko se kateri koli od teh vidikov spremeni. Če se ne pridobi soglasje za zbiranje podatkov, se lahko izreče kazenska sankcija (člen 71(4-5) zakona o varstvu osebnih podatkov). Izjemoma lahko ponudniki informacijskih in komunikacijskih storitev zbirajo ali uporabljajo osebne podatke uporabnikov brez predhodne privolitve. Tako je, (1) kadar je iz ekonomskih in tehnoloških razlogov očitno težko pridobiti običajno privolitev glede osebnih podatkov, ki so potrebni za izvajanje pogodbe o zagotavljanju informacijskih in komunikacijskih storitev (npr. kadar se osebni podatki neizogibno ustvarjajo zaradi izvajanja pogodbe, kot so podatki za izdajo računa, dnevniki dostopov in evidence plačil); (2) kadar je to potrebno za plačilo informacijskih in komunikacijskih storitev; ali (3) če to dopušča drug zakon (npr. člen 21 (1), točka 6, zakona o varstvu potrošnikov pri elektronskem poslovanju, ki določa, da lahko poslovni subjekti zbirajo osebne podatke o pravnih zastopnikih mladoletnikov, da preverijo, ali je bila privolitev mladoletnika veljavno pridobljena) (člen 39-3(2) zakona o varstvu osebnih podatkov). Vsekakor ponudniki informacijskih in komunikacijskih storitev ne morejo zavrniti zagotavljanja storitev le zato, ker uporabnik ne zagotovi več osebnih podatkov, kot se minimalno zahteva (tj. kot so potrebni za izvajanje bistvenih elementov zadevne storitve), glej člen 39-3(3) zakona o varstvu osebnih podatkov.

([54]) Glej člen 14-2 uredbe o izvajanju zakona o varstvu osebnih podatkov.

([55]) Člen 14-2(2) uredbe o izvajanju zakona o varstvu osebnih podatkov.

(37) Podobna (vendar nekoliko strožja) pravila se uporabljajo za zagotavljanje podatkov tretjim osebam. Člen 71(1) zakona o varstvu osebnih podatkov določa, da se lahko osebni podatki zagotavljajo tretjim osebam na podlagi privolitve ([56]) ali v okviru namena zbiranja, če so bili podatki zbrani sklicujoč se na eno od pravnih podlag iz člena 15(1), točke 2, 3 in 5, zakona o varstvu osebnih podatkov. To zlasti izključuje vsako razkritje na podlagi „upravičenega interesa“ upravljavca. Zunaj tega okvira člen 17(4) zakona o varstvu osebnih podatkov omogoča zagotavljanje podatkov tretji osebi „v okviru obsega, ki je razumno povezan“ z namenom zbiranja, pri čemer je treba prav tako upoštevati morebitne težave za posameznika, na katerega se nanašajo osebni podatki, sprejeti pa morajo biti tudi potrebni varnostni ukrepi (npr. šifriranje). Pri oceni, ali zagotavljanje podatkov spada v obseg, ki je razumno povezan z namenom zbiranja, in ali se uporabljajo enaki zaščitni ukrepi (tj. glede preglednosti na podlagi politike zasebnosti in vključevanja pooblaščene osebe za varstvo zasebnosti), je treba upoštevati enake dejavnike, kot so opisani v uvodni izjavi (36).

(38) Če korejski upravljavec podatkov prejme osebne podatke iz Unije, se to šteje za „zbiranje“ v smislu člena 15 zakona o varstvu osebnih podatkov. V uradnem obvestilu št. 2021-5 (Priloga I, oddelek I, k temu sklepu) je pojasnjeno, da je namen, za katerega zadevni subjekt EU prenese podatke, tudi namen zbiranja za korejskega upravljavca podatkov. Posledično morajo korejski upravljavci podatkov, ki prejmejo osebne podatke iz Unije, načeloma obdelovati te podatke v okviru namena prenosa, in sicer v skladu s členom 17 zakona o varstvu osebnih podatkov.

(39) Posebne omejitve veljajo, kadar upravljavec želi osebne podatke uporabiti ali jih zagotoviti tretji osebi za namen, ki se razlikuje od namena zbiranja ([57]). V skladu s členom 18(2) zakona o varstvu osebnih podatkov lahko zasebni upravljavec izjemoma ([58]) uporabi osebne podatke ali jih zagotovi tretji osebi za drug namen: (1) na podlagi dodatne (torej ločene) privolitve posameznika, na katerega se nanašajo osebni podatki; (2) kadar tako določajo posebne zakonske določbe; ali (3) kadar je to očitno nujno za zaščito življenja, telesa ali premoženja posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe pred neposredno nevarnostjo (le če posameznik, na katerega se nanašajo osebni podatki, ne more izraziti svojega namena in če predhodne privolitve ni mogoče pridobiti) ([59]).

(40) Javni organi lahko v nekaterih okoliščinah osebne podatke uporabljajo ali jih zagotavljajo tretjim osebam tudi za drug namen. To vključuje primere, ko javni organi drugače ne bi mogli opravljati svojih zakonskih dolžnosti, za kar je potrebno dovoljenje komisije za varstvo osebnih podatkov. Poleg tega lahko javni organi osebne podatke zagotovijo drugemu organu ali sodišču, kadar je to potrebno zaradi preiskave in pregona kaznivih dejanj ali za vložitev obtožnice, če jih sodišče potrebuje za opravljanje svojih nalog v zvezi s tekočim sodnim postopkom ali kadar je to potrebno zaradi izvršitve kazenske sankcije oziroma odredbe o varstvu in vzgoji ([60]). Osebne podatke lahko zagotovijo tudi tuji vladi ali mednarodni organizaciji, da izpolnijo pravno obveznost iz mednarodne pogodbe ali konvencije – v takem primeru morajo izpolniti tudi zahteve za čezmejni prenos podatkov (glej uvodno izjavo (90)).

(41) Načeli zakonitosti in poštenosti obdelave se torej v korejskem pravnem sistemu izvajata na v osnovi enakovreden način kot v Uredbi (EU) 2016/679, saj dovoljujeta obdelavo le iz zakonitih in jasno opredeljenih razlogov. Poleg tega je v vseh navedenih primerih obdelava dovoljena le, če ni verjetno, da bi „nepošteno posegala“ v interese posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe, zaradi česar je treba tehtati različne interese. Poleg tega člen 18(5) zakona o varstvu osebnih podatkov določa dodatne zaščitne ukrepe, kadar upravljavec zagotavlja osebne podatke tretji osebi, kar lahko vključuje zahtevo za omejitev namena in metode uporabe ali uvedbo posebnih varnostnih ukrepov. Tretja oseba pa mora nato v takem primeru izvesti zahtevane ukrepe.

([56]) Za kršitve člena 17(1), točka 1, zakona o varstvu osebnih podatkov se lahko izreče kazenska sankcija (člen 71(1) zakona o varstvu osebnih podatkov).

([57]) „Nameravani namen“ je namen, za katerega so se podatki zbrali. Kadar se podatki zberejo na primer na podlagi privolitve zadevnega posameznika, je nameravani namen tisti, ki je posamezniku sporočen na podlagi člena 15(2) zakona o varstvu osebnih podatkov.

([58]) Glej člen 18(1) zakona o varstvu osebnih podatkov. Za kršitve člena 18(1) in (2) se lahko izrečejo kazenske sankcije (člen 71(2) zakona o varstvu osebnih podatkov).

([59]) Ponudniki informacijskih in komunikacijskih storitev lahko osebne podatke uporabijo ali jih zagotovijo tretji osebi za namen, ki se razlikuje od prvotnega, le pod pogoji iz člena 18(2), točki 1 in 2, zakona o varstvu osebnih podatkov (tj. če se pridobi dodatna privolitev ali če zakon vsebuje posebne določbe). Glej člen 18(2) zakona o varstvu osebnih podatkov.

([60]) Razen kadar je obdelava potrebna zaradi preiskovanja kaznivih dejanj, vložitve obtožnice ali pregona, morajo javni organi, ki uporabljajo osebne podatke ali jih zagotavljajo tretjim osebam za namen, ki se razlikuje od tistega, za katerega so bili zbrani (npr. kadar je to izrecno dovoljeno po zakonu ali potrebno za izpolnitev mednarodne pogodbe), na svojem spletnem mestu ali v uradnem listu objaviti pravno podlago za obdelavo, namen in obseg obdelave ter voditi evidence (člen 18(4) zakona o varstvu osebnih podatkov v povezavi s členom 15 uredbe o izvajanju zakona o varstvu osebnih podatkov).

(42) Nazadnje, člen 28-2 zakona o varstvu osebnih podatkov omogoča (nadaljnjo) obdelavo psevdonimiziranih podatkov brez privolitve zadevnega posameznika za namene statistične obdelave, znanstvenih raziskav ([61]) in arhiviranja v javnem interesu, pri čemer se uporabljajo posebni zaščitni ukrepi. Podobno kot Uredba (EU) 2016/679 ([62]) torej zakon o varstvu osebnih podatkov omogoča (nadaljnjo) obdelavo osebnih podatkov za take namene, če so zagotovljeni ustrezni zaščitni ukrepi za varstvo pravic posameznikov. Namesto sklicevanja na psevdonimizacijo kot možen zaščitni ukrep je z zakonom o varstvu osebnih podatkov psevdonimizacija določena kot osnovni pogoj za izvajanje nekaterih dejavnosti obdelave za namene statistične analize, znanstvenih raziskav in arhiviranja v javnem interesu (npr. da se omogoči obdelava podatkov brez privolitve ali da se združijo različni nabori podatkov).

(43) Poleg tega zakon o varstvu osebnih podatkov določa več posebnih zaščitnih ukrepov, zlasti glede zahtevanih tehničnih in organizacijskih ukrepov, vodenja evidenc, omejitev pri izmenjavi podatkov in obravnave morebitnih tveganj za ponovno identifikacijo. Kombinacija različnih zaščitnih ukrepov, opisanih v uvodnih izjavah (44) do (48), zagotavlja, da se za obdelavo osebnih podatkov v tem okviru uporablja v osnovi enakovredno varstvo, kot bi se zahtevalo v skladu z Uredbo (EU) 2016/679.

(44) Prvič, in kar je najpomembneje, člen 28-5(1) zakona o varstvu osebnih podatkov prepoveduje obdelavo psevdonimiziranih podatkov z namenom identifikacije določenega posameznika. Če bi se med obdelavo psevdonimiziranih podatkov kljub temu ustvarile informacije, na podlagi katerih bi bilo mogoče identificirati posameznika, mora upravljavec takoj prenehati obdelovati take podatke in jih uničiti (člen 28-5(2) zakona o varstvu osebnih podatkov). Za kršitev teh določb se lahko izreče upravna globa, pomeni pa tudi kaznivo dejanje ([63]). To pomeni, da je taka ponovna identifikacija *zakonsko* prepovedana tudi, kadar bi bilo *praktično* mogoče ponovno identificirati posameznika.

(45) Drugič, kadar upravljavec (nadalje) obdeluje psevdonimizirane podatke za take namene, mora sprejeti določene tehnološke, upravljavske in fizične ukrepe, da se zagotovi varnost podatkov (vključno z ločeno hrambo in upravljanjem podatkov, ki so potrebni za obnovitev psevdonimiziranih podatkov nazaj v izvirno obliko) ([64]). Poleg tega je treba voditi evidence o psevdonimiziranih podatkih, ki se obdelujejo, namenu obdelave, zgodovini uporabe in vseh morebitnih tretjih osebah, ki so jih prejele (člen 29-5(2) uredbe o izvajanju zakona o varstvu osebnih podatkov).

(46) Tretjič in nazadnje, zakon o varstvu osebnih podatkov določa posebne zaščitne ukrepe, ki tretjim osebam preprečujejo identifikacijo posameznikov v primeru izmenjave podatkov. To zlasti pomeni, da kadar upravljavci zagotavljajo psevdonimizirane podatke tretjim osebam za namene statistične obdelave, znanstvenih raziskav ali arhiviranja v javnem interesu, ne smejo vključiti podatkov, ki bi jih bilo mogoče uporabiti za identifikacijo določenega posameznika (člen 28-2(2) zakona o varstvu osebnih podatkov) ([65]).

(47) Natančneje, čeprav zakon o varstvu osebnih podatkov omogoča združevanje psevdonimiziranih podatkov (ki jih obdelujejo različni upravljavci) za namene statistične analize, znanstvenih raziskav ali arhiviranja v javnem interesu, pa to pristojnost omejuje na specializirane subjekte, ki so vzpostavili posebno varnostno infrastrukturo (člen 28-3(1) zakona o varstvu osebnih podatkov) ([66]). Upravljavec mora ob vložitvi vloge za združevanje psevdonimiziranih podatkov med drugim predložiti dokumentacijo o podatkih, ki se bodo združevali, namenu

([61]) Znanstvene raziskave so v členu 2(8) zakona o varstvu osebnih podatkov opredeljene kot „raziskave, pri katerih se uporabljajo znanstvene metode, na primer tehnološki razvoj, predstavitvene dejavnosti, temeljne raziskave, uporabne raziskave in zasebno financirane raziskave“. Te kategorije ustrezajo tistim iz uvodne izjave 159 Uredbe (EU) 2016/679.

([62]) Glej člen 5(1), točka b, člen 89(1) in (2) ter uvodni izjavi 50 in 157 Uredbe (EU) 2016/679.

([63]) Gej člen 28-6(1), člen 71(4-3) in člen 75(2), točka 4-4, zakona o varstvu osebnih podatkov.

([64]) Člen 28-4 zakona o varstvu osebnih podatkov in člen 29-5 uredbe o izvajanju zakona o varstvu osebnih podatkov. Za kršitev te obveznosti se lahko izrečejo upravne in kazenske sankcije, glej člen 73(1) in člen 75(2), točka 6, zakona o varstvu osebnih podatkov.

([65]) Za kršitve teh zahtev se lahko izrečejo kazenske sankcije (člen 71(2) zakona o varstvu osebnih podatkov). Komisija za varstvo osebnih podatkov je ta nova pravila takoj začela izvrševati, na primer v odločbi z dne 28. aprila 2021, v kateri je izrekla globo in popravne ukrepe družbi, ki med drugimi kršitvami zakona o varstvu osebnih podatkov ni zagotovila skladnosti z zahtevo iz člena 28-2(2) navedenega zakona; glej: https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([66]) Za imenovanje za specializirani subjekt (strokovna agencija za združevanje podatkov) je treba komisiji za varstvo osebnih podatkov predložiti vlogo, ki se ji priložijo tudi dokazila, iz katerih sta med drugim razvidni infrastruktura in oprema za varno združevanje psevdonimiziranih podatkov ter ki potrjujejo, da ima vložnik med svojim osebjem vsaj tri zaposlene za polni delovni čas, ki imajo ustrezne kvalifikacije ali izkušnje s področja varstva osebnih podatkov (člen 29-2(1)-(2) uredbe o izvajanju zakona o varstvu osebnih podatkov). Podrobne zahteve, na primer glede kvalifikacij osebja, razpoložljivih prostorov, varnostnih ukrepov, notranjih politik in postopkov, ter finančne zahteve so navedene v uradnem obvestilu komisije za varstvo osebnih podatkov št. 2020-9 o združevanju in sproščanju psevdonimiziranih podatkov (Priloga I). Komisija za varstvo osebnih podatkov lahko iz določenih razlogov prekliče imenovanje strokovne agencije za združevanje podatkov (na podlagi opravljene obravnave), na primer če agencija ne dosega več varnostnih standardov, ki so potrebni za imenovanje, ali če je pri združevanju podatkov prišlo do kršitve varstva podatkov (člen 29-2(5)-(6) uredbe o izvajanju zakona o varstvu osebnih podatkov). Komisija za varstvo osebnih podatkov mora objaviti vsako imenovanje (ali preklic imenovanja) strokovne agencije za združevanje podatkov (člen 29-2(7) uredbe o izvajanju zakona o varstvu osebnih podatkov).

združevanja in predlaganih varnostnih ukrepih za obdelavo združenih podatkov ([67]). Če želi pridobiti dovoljenje za združevanje, mora upravljavec podatke, ki se bodo združevali, poslati specializiranemu subjektu ter korejski agenciji za splet in varnost ([68]) predložiti „kombinacijski ključ“ (tj. informacije, ki so bile uporabljene za psevdonimizacijo). Slednja ustvari povezovalne podatke med kombinacijskimi ključi (kar omogoča povezovanje kombinacijskih ključev različnih vložnikov, da se omogoči združevanje naborov podatkov) in jih predloži specializiranemu subjektu ([69]).

(48) Upravljavec, ki prosi za dovoljenje za združevanje, lahko združene informacije analizira v prostorih specializiranega subjekta, kjer se izvajajo posebni tehnični, fizični in upravni varnostni ukrepi (člen 29-3 uredbe o izvajanju zakona o varstvu osebnih podatkov). Upravljavci, ki prispevajo nabor podatkov za tako združevanje, lahko združene podatke odnesejo iz specializiranega subjekta šele po opravljeni nadaljnji psevdonimizaciji ali anonimizaciji združenih podatkov ter s soglasjem navedenega subjekta (člen 28-3(2) zakona o varstvu osebnih podatkov) ([70]). Zadevni subjekt pri oceni, ali naj izda tako soglasje ali ne, preveri povezavo med združenimi podatki in namenom obdelave ter obstoj posebnega varnostnega načrta za uporabo takih podatkov ([71]). Izvoz združenih podatkov iz subjekta ni dovoljen, če podatki vsebujejo podatke, ki omogočajo identifikacijo posameznika ([72]). Nazadnje, združevanje in sproščanje psevdonimiziranih podatkov s strani specializiranega subjekta nadzoruje komisija za varstvo osebnih podatkov (člen 29-4(3) uredbe o izvajanju zakona o varstvu osebnih podatkov).

2.3.2 *Obdelava posebnih vrst osebnih podatkov*

(49) Pri obdelavi posebnih vrst podatkov bi morali veljati posebni zaščitni ukrepi.

(50) Zakon o varstvu osebnih podatkov vsebuje posebna pravila glede obdelave občutljivih podatkov ([73]), ki so opredeljeni kot osebni podatki, ki razkrivajo informacije o ideologiji, prepričanju, včlanitvi v sindikat ali politično stranko ali izstopu iz take organizacije, političnem stališču, zdravju in spolnem življenju posameznika, ter drugi osebni podatki, ki bi verjetno „pomembno“ ogrozili zasebnost posameznika, na katerega se nanašajo osebni podatki, in ki so kot občutljivi podatki opredeljeni v predsedniški uredbi ([74]). Glede na pojasnila komisije za varstvo osebnih podatkov se spolno življenje razlaga tako, da vključuje tudi posameznikovo spolno usmerjenost ali nagnjenja ([75]). Poleg tega člen 18 uredbe o izvajanju opredeljuje dodatne vrste občutljivih podatkov, zlasti informacije o DNK, pridobljene z genskim testiranjem, in podatke, ki so del kazenske evidence. Z nedavno spremembo uredbe o izvajanju zakona o varstvu osebnih podatkov se je pojem občutljivih podatkov še razširil, saj vključuje tudi osebne podatke, ki razkrivajo rasno ali etnično poreklo, in biometrične podatke ([76]). Po navedeni spremembi je pojem občutljivih podatkov na podlagi zakona o varstvu osebnih podatkov v osnovi enakovreden tistemu iz člena 9 Uredbe (EU) 2016/679.

(51) V skladu s členom 23(1) zakona o varstvu osebnih podatkov in podobno kot določa člen 9(1) Uredbe (EU) 2016/679, je obdelava občutljivih podatkov na splošno prepovedana, razen če se uporablja ena od naštetih izjem ([77]). Z njimi je obdelava omejena na primere, ko upravljavec obvesti posameznika, na katerega se nanašajo osebni podatki, v skladu s členoma 15 in 17 zakona o varstvu osebnih podatkov ter pridobi ločeno privolitev (tj. ločeno od privolitve za obdelavo drugih osebnih podatkov), ali kadar je obdelava potrebna ali dovoljena na podlagi zakona. Javni organi lahko obdelujejo tudi biometrične podatke, podatke o DNK, pridobljene z genetskim testiranjem, osebne podatke, ki razkrivajo rasno ali etnično poreklo, in podatke, ki so del kazenske evidence,

([67]) Člen 8(1)–(2) uradnega obvestila št. 2020-9 o združevanju in sproščanju psevdonimiziranih podatkov.
([68]) Člen 2(3) in (6) ter člen 9(1) uradnega obvestila št. 2020-9 o združevanju in sproščanju psevdonimiziranih podatkov.
([69]) Člen 2(4) ter člen 9(2)–(3) uradnega obvestila št. 2020-9 o združevanju in sproščanju psevdonimiziranih informacij. Specializirani subjekt mora takoj po končanem združevanju uničiti povezovalne podatke med kombinacijskimi ključi (člen 9(4) uradnega obvestila).
([70]) Za kršitve zahtev glede združevanja naborov podatkov se lahko izrečejo kazenske sankcije (člen 71(4-2) zakona o varstvu osebnih podatkov). Glej tudi člen 29-2(4) uredbe o izvajanju zakona o varstvu osebnih podatkov.
([71]) Postopek soglasja za sprostitev združenih podatkov je določen v členu 11 uradnega obvestila št. 2020-9 o združevanju in sproščanju psevdonimiziranih podatkov. Specializirani subjekt mora zlasti ustanoviti odbor za preverjanje sproščanja, ki ga sestavljajo člani z obsežnim znanjem in izkušnjami na področju varstva podatkov.
([72]) Člen 29-2(4) uredbe o izvajanju zakona o varstvu osebnih podatkov in uradno obvestilo št. 2020-9, člen 11.
([73]) Potrebo po zagotovitvi posebnega varstva pri obdelavi občutljivih podatkov, na primer podatkov o zdravju ali spolnem vedenju, je prepoznalo tudi korejsko ustavno sodišče, glej odločbo ustavnega sodišča HunMa 1139 z dne 31. maja 2007.
([74]) Člen 23(1) zakona o varstvu osebnih podatkov.
([75]) Glej tudi priročnik o zakonu o varstvu osebnih podatkov, poglavje III, oddelek 2, o členu 23 (str. 157 do 164).
([76]) To so osebni podatki, ki izhajajo iz posebne tehnične obdelave podatkov v zvezi s telesnimi, psihološkimi ali vedenjskimi značilnostmi posameznika z namenom edinstvene identifikacije takega posameznika.
([77]) Za neskladnost s temi zahtevami se lahko izrečejo sankcije na podlagi člena 71, točka 3, zakona o varstvu osebnih podatkov.

vendar le iz razlogov, ki so jim izključno na voljo (npr. kadar je to potrebno za preiskavo kaznivih dejanj ali da lahko sodišče obravnava zadevo) ([78]). Pravne podlage za obdelavo občutljivih podatkov so torej bolj omejene kot pravne podlage za druge vrste osebnih podatkov in so po korejskem pravu še celo bolj omejevalne kot na podlagi člena 9(2) Uredbe (EU) 2016/679.

(52) Poleg tega je v členu 23(2) zakona o varstvu osebnih podatkov (za neupoštevanje katerega se lahko izrečejo sankcije ([79])) poudarjen posebni pomen zagotavljanja ustrezne varnosti pri ravnanju z občutljivimi podatki, da „se ne izgubijo, niso ukradeni, se ne razkrijejo, ponaredijo, spremenijo ali poškodujejo“. Medtem ko je navedeno splošna zahteva na podlagi člena 29 zakona o varstvu osebnih podatkov, pa člen 3(4) jasno določa, da je treba raven varnosti prilagoditi vrsti osebnih podatkov, ki se obdelujejo, kar pomeni, da je treba upoštevati posebna tveganja pri obdelavi občutljivih podatkov. Poleg tega se podatki vedno obdelujejo „tako, da se čim bolj zmanjša možnost kršitve“ zasebnosti posameznika, na katerega se nanašajo osebni podatki, in po možnosti „anonimno“ (člen 3(6) in (7) zakona o varstvu osebnih podatkov). Te zahteve so še posebno pomembne pri obdelavi občutljivih podatkov.

2.3.3 *Omejitev namena*

(53) Osebni podatki bi se morali zbirati za določen namen in tako, da to ni nezdružljivo z namenom obdelave.

(54) To načelo vsebuje člen 3(1) in (2) zakona o varstvu osebnih podatkov, v skladu s katerim upravljavec „jasno opredeli“ namen obdelave, obdeluje osebne podatke na način, ki ustreza namenu, in jih ne uporablja tako, da bi bil tak namen presežen. Splošno načelo omejitve namena je potrjeno tudi v členu 15(1), členu 18(1) in členu 19, za obdelovalce (tako imenovane zunanje izvajalce) pa v členu 26(1), točka 1, ter členu 26(5) in (7) zakona o varstvu osebnih podatkov. Zlasti velja, da se lahko osebni podatki načeloma uporabljajo in zagotavljajo tretjim osebam le v okviru namena, za katerega so bili zbrani (člen 15(1) in člen 17(1), točka 2). Obdelava za skladen namen, tj. „v obsegu, ki je razumno povezan s prvotnim namenom zbiranja“, se lahko izvaja le, če nima negativnega učinka na zadevne posameznike, na katere se nanašajo osebni podatki, in če so sprejeti potrebni varnostni ukrepi (kot je šifriranje) (člen 15(3) in člen 17(4) zakona o varstvu osebnih podatkov). Za ugotovitev, ali gre pri nadaljnji obdelavi za skladen namen, uredba o izvajanju zakona o varstvu osebnih podatkov določa posebna merila, ki so podobna tistim iz člena 6(4) Uredbe (EU) 2016/679, glej uvodno izjavo (36).

(55) Kot je pojasnjeno v uvodni izjavi (38), je namen zbiranja v primeru korejskih upravljavcev, ki prejemajo osebne podatke iz Unije, namen, za katerega so podatki preneseni. Upravljavec lahko namen spremeni le izjemoma, v posebnih (izrecno navedenih) primerih (člen 18(2), tč. 1-3, zakona o varstvu osebnih podatkov, glej tudi uvodno izjavo (39)). Če je sprememba namena dovoljena z zakonom, morajo taki zakoni spoštovati temeljno pravico do zasebnosti in varstva podatkov ter načeli nujnosti in sorazmernosti iz korejske ustave. Poleg tega člen 18(2) in (5) zakona o varstvu osebnih podatkov določa dodatne zaščitne ukrepe, zlasti zahtevo, da taka sprememba namena ne sme „nepošteno posegati v interese posameznika, na katerega se nanašajo osebni podatki“, zaradi česar je vedno potrebno tehtanje interesov. To zagotavlja raven varstva, ki je v osnovi enakovredna tisti iz člena 5(1), točka (b), in člena 6 v povezavi z uvodno izjavo 50 Uredbe (EU) 2016/679.

2.3.4 *Točnost podatkov in načelo najmanjšega obsega*

(56) Osebni podatki bi morali biti točni in po potrebi posodobljeni. Prav tako bi morali biti ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo.

([78]) Člen 18 uredbe o izvajanju zakona o varstvu osebnih podatkov določa, da se za v njem navedene vrste podatkov ne uporablja določba člena 23(1) navedenega zakona, če jih obdeluje javni organ na podlagi člena 18(2), točke 5–9, zakona o varstvu osebnih podatkov.

([79]) Glej člen 73, točka 1, in člen 75(2), točka 6, zakona o varstvu osebnih podatkov.

(57) Načelo točnosti je podobno priznano v členu 3(3) zakona o varstvu osebnih podatkov, s katerim se zahteva, da so osebni podatki „točni, popolni in posodobljeni, kolikor je to potrebno glede na namene“, za katere se obdelujejo. Najmanjši obseg podatkov se zahteva s členom 3(1) in (6) ter členom 16(1) zakona o varstvu osebnih podatkov, ki določata, da upravljavec zbira osebne podatke (le) „v najmanjšem možnem obsegu, ki je potreben“ za nameravani namen, ter da nosi dokazno breme v zvezi s tem. Če je namen zbiranja mogoče doseči z obdelavo anonimiziranih informacij, si morajo upravljavci za to prizadevati (člen 3(7) zakona o varstvu osebnih podatkov).

2.3.5 *Omejitev hrambe*

(58) Osebni podatki se načeloma ne smejo hraniti dlje, kot je potrebno za namene, za katere se obdelujejo.

(59) Načelo omejitve hrambe podobno določa člen 21(1) zakona o varstvu osebnih podatkov ([80]), s katerim se zahteva, da upravljavec brez odlašanja „uniči“ ([81]) osebne podatke, ko se izpolni namen obdelave ali ko se izteče obdobje hrambe (kar koli nastopi prej), razen če se nadaljnja hramba zahteva z zakonom ([82]). V slednjem primeru se zadevni osebni podatki „hranijo in upravljajo ločeno od drugih osebnih podatkov“ (člen 21(3) zakona o varstvu osebnih podatkov).

(60) Člen 21(1) zakona o varstvu osebnih podatkov se ne uporablja, če se psevdonimizirani podatki obdelujejo za statistične namene, znanstvene raziskave ali arhiviranje v javnem interesu ([83]). Da se tudi v takem primeru zagotovi upoštevanje načela omejene hrambe podatkov, uradno obvestilo št. 2021-5 upravljavcem nalaga anonimizacijo informacij v skladu s členom 58-2 zakona o varstvu osebnih podatkov, če podatki niso bili uničeni ob izpolnitvi posebnega namena obdelave ([84]).

2.3.6 *Varnost podatkov*

(61) Osebni podatki se morajo obdelovati tako, da je zagotovljena njihova varnost, vključno z varstvom pred nepooblaščeno ali nezakonito obdelavo in pred nenamerno izgubo, uničenjem ali poškodovanjem. Zato bi morali poslovni subjekti sprejeti ustrezne tehnične ali organizacijske ukrepe za varstvo osebnih podatkov pred morebitnimi grožnjami. Pri ocenjevanju teh ukrepov bi bilo treba upoštevati najnovejše znanstvene dosežke, s tem povezane stroške ter naravo, obseg, kontekst in namen obdelave, pa tudi tveganja za pravice posameznikov.

(62) Podobno načelo o varnosti je določeno v členu 3(4) zakona o varstvu osebnih podatkov, ki določa, da morajo upravljavci „z osebnimi podatki ravnati varno, v skladu z metodami, vrstami itd. obdelave osebnih podatkov, pri tem pa upoštevati možnost poseganja v pravice posameznikov, na katere se nanašajo osebni podatki, in stopnjo zadevnih tveganj“. Poleg tega upravljavec „obdeluje osebne podatke tako, da se čim bolj zmanjša možnost kršitve zasebnosti posameznika, na katerega se nanašajo osebni podatki,“ in si v tem okviru prizadeva za obdelavo osebnih podatkov v anonimizirani ali psevdonimizirani obliki, če je to mogoče (člen 3(6) in (7) zakona o varstvu osebnih podatkov).

(63) Te splošne zahteve so podrobneje opredeljene v členu 29 zakona o varstvu osebnih podatkov, ki določa, da vsak upravljavec „sprejme take tehnične, upravljavske in fizične ukrepe (kot sta priprava notranjega načrta upravljanja in hramba evidenc o dostopu itd.), ki so potrebni za zagotavljanje varnosti v skladu s predsedniško uredbo, da se preprečijo izguba, kraja, razkritje, ponarejanje, spreminjanje ali poškodovanje osebnih podatkov“. Člen 30(1) uredbe o izvajanju zakona o varstvu osebnih podatkov podrobno določa navedene, pri čemer se sklicuje na (1) pripravo in izvajanje notranjega načrta upravljanja za varno obdelavo osebnih podatkov, (2) nadzor in

([80]) Člen 8 (v povezavi s členom 8-2 uredbe o izvajanju) in člen 11 (v povezavi s členom 12(2) uredbe o izvajanju).

([81]) Glede načinov uničenja osebnih podatkov glej člen 16 uredbe o izvajanju zakona o varstvu osebnih podatkov. V členu 21(2) zakona o varstvu osebnih podatkov je pojasnjeno, da to vključuje „ukrepe, ki so potrebni za preprečitev obnovitve in ponovnega priklica“.

([82]) Za kršitve teh zahtev se lahko izrečejo kazenske sankcije (člen 73(1-2) zakona o varstvu osebnih podatkov). Člen 39-6 zakona o varstvu osebnih podatkov dodatno določa, da morajo ponudniki informacijskih in komunikacijskih storitev izbrisati osebne podatke uporabnikov, ki že vsaj leto dni ne uporabljajo ponujenih informacijskih in komunikacijskih storitev (razen če je nadaljnja hramba potrebna na podlagi zakona ali na zahtevo posameznika). Posameznike je treba o nameravanem izbrisu njihovih podatkov obvestiti 30 dni pred iztekom enoletnega roka (člen 39-6(2) zakona o varstvu osebnih podatkov in člen 48-5(3) uredbe o izvajanju zakona o varstvu osebnih podatkov). Če je nadaljnja hramba potrebna na podlagi zakona, morajo biti taki podatki shranjeni ločeno od drugih informacij o uporabnikih in se smejo uporabiti ali razkriti le v skladu z navedenim zakonom (člen 48-5(1)-(2) uredbe o izvajanju zakona o varstvu osebnih podatkov).

([83]) Člen 28-7 zakona o varstvu osebnih podatkov.

([84]) Uradno obvestilo št. 2021-5 (Priloga I), oddelek 4.

omejitve dostopa, (3) uporabo tehnologije šifriranja za varno shranjevanje in prenos osebnih podatkov, (4) evidence vstopa, (5) varnostne programe in (6) fizične ukrepe, kot je sistem varnega shranjevanja ali zaklepanja ([85]).

(64) Poleg tega veljajo posebne obveznosti v primeru kršitve varstva podatkov (člen 34 zakona o varstvu osebnih podatkov v povezavi s členoma 39 in 40 uredbe o izvajanju zakona o varstvu osebnih podatkov) ([86]). Zlasti velja, da mora upravljavec prizadete posameznike, na katere se nanašajo osebni podatki, brez odlašanja uradno obvestiti o podrobnostih kršitve ([87]), med drugim jim zagotoviti informacije o (obveznih) protiukrepih, ki jih je sprejel upravljavec, in o tem, kako lahko zmanjšajo tveganje nastanka škode (člen 34(1) in (2) zakona o varstvu osebnih podatkov) ([88]). Kadar kršitev varstva podatkov prizadene najmanj 1 000 posameznikov, na katere se nanašajo osebni podatki, upravljavec o kršitvi in sprejetih protiukrepih brez odlašanja poroča tudi komisiji za varstvo osebnih podatkov in korejski agenciji za splet in varnost, ki lahko zagotovita tehnično pomoč (člen 34(3) zakona o varstvu osebnih podatkov v povezavi s členom 39 uredbe o izvajanju zakona o varstvu osebnih podatkov). Upravljavci so odgovorni za škodo, ki nastane zaradi kršitev varnosti podatkov, in sicer v skladu z določbami zakona o civilni odškodninski odgovornosti (glej tudi oddelek 2.5 o pravnem varstvu) ([89]).

(65) Pri izpolnjevanju obveznosti glede varnosti mora upravljavcu pomagati pooblaščena oseba za varstvo zasebnosti, katere naloge med drugim vključujejo vzpostavitev sistema notranjega nadzora „za preprečitev razkrivanja, zlorabe in nepravilne uporabe osebnih podatkov“ (člen 31(2), točka 4, zakona o varstvu osebnih podatkov). Poleg tega mora upravljavec zagotavljati „ustrezno preverjanje in nadzor“ osebja, ki obdeluje osebne podatke, tudi glede varnega upravljanja teh podatkov, to pa vključuje potrebno usposabljanje („izobraževanje“) zaposlenih (člen 28(1) in (2) zakona o varstvu osebnih podatkov). Nazadnje, v primeru podobdelave mora upravljavec zunanjemu izvajalcu naložiti določene obveznosti, med drugim glede varnega upravljanja osebnih podatkov („tehnični in upravljavski zaščitni ukrepi“), in nadzorovati njihovo izpolnjevanje v okviru inšpekcijskih pregledov (člen 26(1) in (4) zakona o varstvu osebnih podatkov v povezavi s členom 28(1), točki 3 in 4, ter členom 28(6) uredbe o izvajanju zakona o varstvu osebnih podatkov).

2.3.7 *Preglednost*

(66) Posamezniki, na katere se nanašajo osebni podatki, morajo biti obveščeni o glavnih značilnostih obdelave svojih osebnih podatkov.

([85]) Glede obdelave osebnih podatkov s strani ponudnikov informacijskih in komunikacijskih storitev člen 39-5 zakona o varstvu osebnih podatkov izrecno določa, da z osebnimi podatki ravna čim manj oseb. Poleg tega ponudniki informacijskih in komunikacijskih storitev zagotovijo, da se osebni podatki uporabnikov ne razkrijejo javnosti prek informacijskih in komunikacijskih omrežij (člen 39-10(1) zakona o varstvu osebnih podatkov). Razkrite podatke je treba na zahtevo komisije za varstvo osebnih podatkov izbrisati ali blokirati (člen 39-10(2) zakona o varstvu osebnih podatkov). Splošneje, za ponudnike informacijskih in komunikacijskih storitev (in tretje osebe, ki prejmejo osebne podatke uporabnikov) veljajo dodatne obveznosti glede varnosti, navedene v členu 48-2 uredbe o izvajanju zakona o varstvu osebnih podatkov, na primer priprava in izvajanje notranjega načrta upravljanja glede varnostnih ukrepov, ukrepov za zagotavljanje nadzora nad dostopom, šifriranja, uporabe programske opreme za zaznavanje zlonamernih programov itd.

([86]) Poleg tega velja splošna prepoved poškodovanja, uničenja, spreminjanja, ponarejanja ali razkrivanja osebnih podatkov brez pravnega pooblastila, glej člen 59, točka 3, zakona o varstvu osebnih podatkov.

([87]) Obveznost uradnega obveščanja posameznika ne velja, če se kršitev varnosti podatkov nanaša na psevdonimizirane podatke, ki se obdelujejo za namene statistične analize, znanstvenih raziskav ali arhiviranja v javnem interesu (člen 28-7 zakona o varstvu osebnih podatkov, ki določa izjemo od člena 34(1) in člena 39-4 zakona o varstvu osebnih podatkov). Za zagotovitev uradnega obveščanja posameznikov bi moral zadevni upravljavec identificirati posameznike iz psevdonimiziranega nabora podatkov, kar pa je izrecno prepovedano s členom 28-5 zakona o varstvu osebnih podatkov. Kljub temu pa se še naprej uporablja splošna zahteva glede obveščanja (komisije za varstvo osebnih podatkov) o kršitvi varnosti podatkov.

([88]) Zahteve glede uradnega obveščanja, vključno z roki in možnostjo obveščanja v več fazah, so podrobneje opredeljene v členu 40 uredbe o izvajanju zakona o varstvu osebnih podatkov. Strožja pravila veljajo za ponudnike informacijskih in komunikacijskih storitev, ki morajo posameznika, na katerega se nanašajo osebni podatki, in komisijo za varstvo osebnih podatkov uradno obvestiti v 24 urah po tem, ko izvedo, da so bili osebni podatki izgubljeni, ukradeni ali razkriti (člen 39-4(1) zakona o varstvu osebnih podatkov). Tako uradno obvestilo mora vključevati podrobnosti o osebnih podatkih, ki so bili razkriti, trenutku, ko se je to zgodilo, ukrepih, ki jih lahko sprejme uporabnik, ukrepih, ki jih je v odziv na to sprejel ponudnik, in kontaktnih podatkih oddelka, na katerega se lahko uporabnik obrne z vprašanji (člen 39-4(1)1-5 zakona o varstvu osebnih podatkov). Če obstaja upravičen razlog za to, na primer če ponudnik nima kontaktnih podatkov uporabnika, se lahko uporabijo drugi načini obveščanja, na primer z javno objavo obvestila na spletnem mestu (člen 39-4(1) zakona o varstvu osebnih podatkov v povezavi s členom 48-4(4) in naslednjimi uredbe o izvajanju zakona o varstvu osebnih podatkov). V takem primeru je treba o razlogih obvestiti komisijo za varstvo osebnih podatkov (člen 34-4(3) zakona o varstvu osebnih podatkov).

([89]) Glej na primer odločbe vrhovnega sodišča št. 2011Da59834, 2011Da59858 in 2011Da59841 z dne 26. decembra 2012. Povzetek v angleščini je na voljo na tej povezavi: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) Korejski sistem to zagotavlja na različne načine. Zakon o varstvu osebnih podatkov poleg pravice do obveščanja na podlagi člena 4, točka 1, (na splošno) in člena 20(1) (za osebne podatke, ki se zbirajo od tretjih oseb) ter pravice do dostopa na podlagi člena 35 vsebuje tudi splošno zahtevo glede preglednosti v zvezi z namenom obdelave (člen 3(1) zakona o varstvu osebnih podatkov) in posebne zahteve glede preglednosti, kadar se podatki obdelujejo na podlagi privolitve (člen 15(2), člen 17(2) in člen 18(3) zakona o varstvu osebnih podatkov) ([90]). Poleg tega člen 20(2) zakona o varstvu osebnih podatkov določa, da morajo nekateri upravljavci – tisti, katerih obdelava presega določen prag ([91])– uradno obvestiti posameznika, katerega osebne podatke so prejeli od tretje osebe, o viru teh podatkov, namenu obdelave in posameznikovi pravici, da zahteva prenehanje obdelave, razen če tako obveščanje ni mogoče zaradi neobstoja kontaktnih podatkov. Izjeme veljajo za nekatere datoteke z osebnimi podatki, ki jih imajo javni organi, zlasti datoteke s podatki, ki se obdelujejo zaradi nacionalne varnosti, drugih posebno pomembnih („resnih“) nacionalnih interesov ali za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ali kadar bi uradno obveščanje verjetno povzročilo škodo življenju in telesu druge osebe ali nepošteno škodilo premoženju in drugim interesom druge osebe, vendar le, če zadevni javni ali zasebni interesi „očitno prevladajo“ nad pravicami zadevnih posameznikov, na katere se nanašajo osebni podatki (člen 20(4) zakona o varstvu osebnih podatkov). To zahteva tehtanje interesov.

(68) Poleg tega člen 3(5) zakona o varstvu osebnih podatkov določa, da morajo upravljavci javno objaviti svojo politiko zasebnosti (in druge zadeve, ki se nanašajo na obdelavo osebnih podatkov). Ta zahteva je nadalje opredeljena v členu 30 zakona o varstvu osebnih podatkov v povezavi s členom 31 uredbe o izvajanju zakona o varstvu osebnih podatkov. V skladu z navedenimi določbami mora javna politika zasebnosti med drugim vključevati (1) vrste osebnih podatkov, ki se obdelujejo, (2) namen obdelave, (3) obdobje hrambe, (4) ali se osebni podatki zagotavljajo tretjim osebam ([92]), (5) morebitno podobdelavo, (6) informacije o pravicah posameznikov, na katere se nanašajo osebni podatki, in kako jih uresničevati, ter (7) kontaktne podatke (vključno z imenom pooblaščene osebe za varstvo zasebnosti ali nazivom notranjega oddelka, ki je odgovoren za zagotavljanje skladnosti s pravili o varstvu podatkov in obravnavo pritožb). Politika zasebnosti mora biti javno dostopna tako, da jo posamezniki, na katere se nanašajo osebni podatki, „zlahka prepoznajo“ (člen 30(2) zakona o varstvu osebnih podatkov) ([93]), in jo je treba stalno posodabljati (člen 31(2) uredbe o izvajanju zakona o varstvu osebnih podatkov).

(69) Za javne organe velja dodatna obveznost, da komisiji za varstvo osebnih podatkov prijavijo zlasti naslednje: (1) ime javnega organa, (2) podlago in namene obdelave datotek z osebnimi podatki, (3) podrobnosti osebnih podatkov, ki se beležijo, (4) metodo obdelave, (5) obdobje hrambe, (6) število posameznikov, katerih osebni podatki se hranijo, (7) naziv oddelka, ki obravnava zahteve posameznikov, na katere se nanašajo osebni podatki, ter (8) prejemnike osebnih podatkov, če se ti zagotavljajo redno ali večkrat (člen 32(1) zakona o varstvu osebnih podatkov) ([94]). Komisija za varstvo osebnih podatkov javno objavi prijavljene datoteke z osebnimi podatki, javni organi pa jih morajo navesti tudi v svojih politikah zasebnosti (člen 30(1) in člen 32(4) zakona o varstvu osebnih podatkov).

(70) Da bi se povečala preglednost za posameznike v Uniji, na katere se nanašajo osebni podatki, ki se prenašajo v Korejo na podlagi tega sklepa, oddelek 3(i) in (ii) uradnega obvestila 2021-5 (Priloga I) določa dodatne zahteve glede preglednosti. Prvič, ko korejski upravljavci prejmejo osebne podatke iz Unije na podlagi tega sklepa, morajo zadevnim posameznikom, na katere se nanašajo osebni podatki, brez nepotrebnega odlašanja (vsekakor pa najpozneje en mesec po prenosu) sporočiti nazive in kontaktne podatke subjektov, ki podatke prenašajo in prejemajo, ter jih obvestiti o tem, kateri osebni podatki (ali vrste teh podatkov) se prenašajo, o namenu, za katerega jih zbira korejski upravljavec, obdobju hrambe in pravicah, ki jih imajo na podlagi zakona o varstvu osebnih podatkov. Drugič, kadar se osebni podatki, prejeti iz Unije na podlagi tega sklepa, zagotavljajo tretjim

([90]) Zlasti kadar se osebni podatki obdelujejo na podlagi privolitve posameznika, mora upravljavec takega posameznika obvestiti o namenu obdelave, podrobnostih podatkov, ki se obdelujejo, prejemniku podatkov, obdobju hrambe in uporabe osebnih podatkov ter o pravici posameznika, da privolitev umakne (ter o vseh slabostih takega umika).

([91]) V skladu s členom 15-2(1) uredbe o izvajanju zakona o varstvu osebnih podatkov se to nanaša na upravljavce, ki obdelujejo občutljive podatke najmanj 50 000 posameznikov, na katere se nanašajo osebni podatki, ali „običajne“ osebne podatke najmanj enega milijona posameznikov. Člen 15-2(2) uredbe o izvajanju zakona o varstvu osebnih podatkov določa metode in roke za uradno obveščanje, člen 15-2(3) pa zahtevo glede vodenja nekaterih evidenc o tem. Poleg tega za določene vrste ponudnikov informacijskih in komunikacijskih storitev veljajo posebna pravila (za tiste, ki so v preteklem letu ustvarili vsaj 10 milijonov KRW prihodkov iz prodaje, ali tiste, ki so v treh mesecih pred koncem preteklega leta v povprečju shranjevali/upravljali osebne podatke najmanj enega milijona uporabnikov na dan): taki ponudniki morajo uporabnike redno obveščati o zgodovini uporabe njihovih osebnih podatkov, razen če to ni mogoče zaradi neobstoja vseh kontaktnih podatkov (člen 39-8 zakona o varstvu osebnih podatkov in člen 48-6 uredbe o izvajanju zakona o varstvu osebnih podatkov).

([92]) Glede na informacije korejske vlade to vključuje obveznost poimenske navedbe prejemnikov v javni politiki zasebnosti.

([93]) Nadaljnje podrobnosti so določene v členu 31(3) uredbe o izvajanju zakona o varstvu osebnih podatkov.

([94]) Obveznost prijave se ne uporablja za nekatere vrste datotek z osebnimi podatki, na primer kadar se nanašajo na nacionalno varnost, diplomatske skrivnosti, kazenske preiskave, pregon, kaznovanje, preiskave kaznivih dejanj, povezanih z obdavčenjem, ali za datoteke, ki se izključno nanašajo na izpolnjevanje internih nalog (člen 32(2) zakona o varstvu osebnih podatkov).

osebam, morajo biti posamezniki, na katere se nanašajo osebni podatki, med drugim obveščeni o prejemniku, o tem, kateri osebni podatki oziroma katere vrste teh podatkov se zagotavljajo, o državi, v katero se podatki zagotavljajo (če je ustrezno), in o pravicah, ki jih ima posameznik na podlagi zakona o varstvu osebnih podatkov ([95]). Uradno obvestilo tako zagotavlja, da so posamezniki iz EU še naprej obveščeni o posameznih upravljavcih, ki obdelujejo njihove podatke, in lahko svoje pravice uresničujejo pri ustreznih subjektih.

(71) Oddelek 3(iii) uradnega obvestila (Priloga I) omogoča nekatere omejene in kvalificirane izjeme od teh dodatnih obveznosti glede preglednosti, ki so v osnovi enakovredne tistim iz Uredbe (EU) 2016/679. Uradno obveščanje posameznikov v Uniji, na katere se nanašajo osebni podatki, se zlasti ne zahteva, (1) kadar in dokler je treba omejiti obveščanje iz določenih razlogov v javnem interesu (npr. kadar se podatki obdelujejo za namene nacionalne varnosti ali tekočih kazenskih preiskav), če ti cilji v javnem interesu očitno prevladajo nad pravico posameznika, na katerega se nanašajo osebni podatki; (2) kadar posameznik, na katerega se nanašajo osebni podatki, te informacije že ima; (3) če in kolikor bi uradno obvestilo verjetno povzročilo škodo življenju ali telesu posameznika ali druge osebe ali neupravičeno poseglo v premoženjske interese druge osebe, kadar te pravice ali interesi očitno prevladajo nad pravicami posameznika, na katerega se nanašajo osebni podatki, ali (4) če ni kontaktnih podatkov o zadevnem posamezniku ali če bi bil za njegovo uradno obveščanje potreben nesorazmeren napor. Pri ugotavljanju, ali je mogoče stopiti v stik s posameznikom, na katerega se nanašajo osebni podatki, ali ne in ali je za to potreben čezmeren napor, se upošteva možnost sodelovanja z izvoznikom podatkov v Uniji.

(72) Pravila iz uvodnih izjav (67) do (71) torej zagotavljajo v osnovi enakovredno raven varstva glede preglednosti, kot je zagotovljena v Uredbi (EU) 2016/679.

2.3.8 *Pravice posameznikov*

(73) Posamezniki, na katere se nanašajo osebni podatki, bi morali imeti določene pravice, ki jih lahko uresničujejo zoper upravljavca ali obdelovalca, zlasti pravico do dostopa do podatkov, pravico do popravka, pravico do ugovora obdelavi in pravico do izbrisa podatkov. Hkrati so te pravice lahko omejene, če so take omejitve potrebne in sorazmerne za zaščito pomembnih ciljev v splošnem javnem interesu.

(74) Člen 3(5) zakona o varstvu osebnih podatkov določa, da upravljavec posamezniku, na katerega se nanašajo osebni podatki, zagotavlja pravice, ki so navedene v členu 4 navedenega zakona ter podrobneje opredeljene v členih 35 do 37, členu 39 in členu 39-2 zakona o varstvu osebnih podatkov.

(75) Prvič, posamezniki imajo pravico do obveščanja in dostopa. Če upravljavec zbira osebne podatke od tretje osebe (tako je v vseh primerih, ko se podatki prenašajo iz Unije), imajo posamezniki, na katere se nanašajo osebni podatki, na splošno pravico do obveščanja o (1) viru zbranih osebnih podatkov (tj. subjektu, ki jih je prenesel), (2) namenu obdelave in (3) dejstvu, da lahko zahtevajo prenehanje obdelave (člen 20(1) zakona o varstvu osebnih podatkov). Uporabljajo se omejene izjeme, in sicer kadar bi tako uradno obveščanje verjetno povzročilo škodo življenju ali telesu druge osebe ali če „neupravičeno škoduje premoženju in drugim interesom“ druge osebe, vendar le če taki interesi tretje osebe „izrecno prevladajo“ nad pravicami posameznika, na katerega se nanašajo osebni podatki (člen 20(4), točka 2, zakona o varstvu osebnih podatkov).

(76) Poleg tega člen 35(1) in (3) zakona o varstvu osebnih podatkov v povezavi s členom 41(4) uredbe o izvajanju zakona o varstvu osebnih podatkov posameznikom, na katere se nanašajo osebni podatki, priznava pravico do dostopa do njihovih osebnih podatkov ([96]). Pravica do dostopa vključuje potrditev obdelave, obveščanje o vrsti podatkov, ki se obdelujejo, namenu obdelave, obdobju hrambe ter morebitnem razkritju podatkov tretjim osebam, pa tudi zagotovitev kopije osebnih podatkov, ki se obdelujejo (člen 4, točka 3, zakona o varstvu osebnih

([95]) Uradno obvestilo 2021-5, oddelek 3(ii) (Priloga I).

([96]) Na podlagi člena 35(3) zakona o varstvu osebnih podatkov v povezavi s členom 42(2) uredbe o izvajanju zakona o varstvu osebnih podatkov lahko upravljavec iz „dobrih razlogov“ odloži dostop (tj. iz upravičenih razlogov, npr. če je potrebnega več časa za oceno, ali je dostop mogoč), vendar mora posameznika, na katerega se nanašajo osebni podatki, o tem uradno obvestiti v desetih dneh in ga poučiti, kako se lahko na tako odločitev pritoži; takoj ko razlogi za odlog prenehajo, je treba dostop zagotoviti.

podatkov v povezavi s členom 41(1) uredbe o izvajanju zakona o varstvu osebnih podatkov) ([97]). Dostop se lahko omeji (delni dostop) ([98]) ali zavrne le, če tako določa zakon ([99]), če bi zaradi tega verjetno nastala škoda za življenje ali telo tretje osebe oziroma če bi to pomenilo neupravičen poseg v premoženjske in druge interese druge osebe (člen 35(4) zakona o varstvu osebnih podatkov) ([100]). Slednje pomeni, da je treba tehtati med ustavno zaščitenimi pravicami in svoboščinami posameznika na eni strani ter drugih oseb na drugi strani. Če se dostop omeji ali zavrne, mora upravljavec posameznika, na katerega se nanašajo osebni podatki, uradno obvestiti o razlogih za to in o tem, kako se lahko na tako odločitev pritoži (člen 41(5) in člen 42(2) uredbe o izvajanju zakona o varstvu osebnih podatkov).

(77) Drugič, posamezniki, na katere se nanašajo osebni podatki, imajo pravico do popravka ali izbrisa ([101]) svojih osebnih podatkov, „razen če drugi predpisi izrecno določajo drugače“ (člen 36(1) in (2) zakona o varstvu osebnih podatkov) ([102]). Ob prejemu zahteve mora upravljavec zadevo obravnavati brez odlašanja, sprejeti potrebne ukrepe ([103]) in o njih v desetih dneh uradno obvestiti posameznika, na katerega se nanašajo osebni podatki. Če pa zahtevi ni mogoče ugoditi, je treba posameznika uradno obvestiti o razlogih za zavrnitev in ga poučiti o možnosti pritožbe (glej člen 36(4) zakona o varstvu osebnih podatkov v povezavi s členom 43(3) uredbe o izvajanju zakona o varstvu osebnih podatkov) ([104]).

(78) Nazadnje, posamezniki, na katere se nanašajo osebni podatki, imajo pravico do takojšnjega prenehanja obdelave njihovih osebnih podatkov ([105]), razen če velja ena od naštetih izjem (člen 37(1) in (2) zakona o varstvu osebnih podatkov) ([106]). Upravljavec lahko zahtevo zavrne, (1) če to izrecno dovoljuje zakon ali če je to potrebno („neizogibno“) za izpolnjevanje pravnih obveznosti, (2) če bi prenehanje obdelave verjetno povzročilo škodo za življenje ali telo tretje osebe oziroma neupravičeno posegla v premoženjske in druge interese druge osebe, (3) če javni organ brez obdelave takih podatkov ne bi mogel opravljati svojih nalog, kot jih določa zakon, ali (4) če posameznik, na katerega se nanašajo osebni podatki, izrecno ne odpove zadevne pogodbe z upravljavcem, pri čemer bi bilo nepraktično izvajati pogodbo brez take obdelave podatkov. V takem primeru mora upravljavec posameznika, na katerega se nanašajo osebni podatki, brez odlašanja uradno obvestiti o razlogih za zavrnitev in ga poučiti o možnostih pritožbe (člen 37(2) zakona o varstvu osebnih podatkov v povezavi s členom 44(2) uredbe o izvajanju zakona o varstvu osebnih podatkov). Člen 37(4) zakona o varstvu osebnih podatkov določa, da mora upravljavec, kadar ugodi zahtevi za prenehanje obdelave, brez odlašanja „sprejeti potrebne ukrepe, vključno z uničenjem zadevnih osebnih podatkov“ ([107]).

(79) Pravica do prenehanja obdelave se uporablja tudi, kadar se osebni podatki uporabljajo za namene neposrednega trženja, tj. za promocijo blaga in storitev ali za spodbujanje k njihovemu nakupu. Poleg tega je za tako nadaljnjo obdelavo na splošno potrebna posebna (dodatna) privolitev posameznika, na katerega se nanašajo osebni podatki (glej člen 15(1), točka 1, in člen 17(2), točka 1, zakona o varstvu osebnih podatkov) ([108]). Kadar upravljavec zaprosi za tako privolitev, mora posameznika, na katerega se nanašajo osebni podatki, obvestiti zlasti o

([97]) Dostop do osebnih podatkov, ki jih obdeluje javni organ, lahko zagotovi neposredno organ ali se zagotovi posredno z vložitvijo zahteve pri komisiji za varstvo osebnih podatkov, ki tako zahtevo brez odlašanja posreduje naprej (člen 35(2) zakona o varstvu osebnih podatkov in člen 41(3) uredbe o izvajanju zakona o varstvu osebnih podatkov).

([98]) Člen 42(1) uredbe o izvajanju zakona o varstvu osebnih podatkov določa, da mora upravljavec zagotoviti delni dostop, kadar se razlogi za zavrnitev ne nanašajo na vse podatke, ampak le na njihov del.

([99]) Tak zakon mora spoštovati temeljno pravico do zasebnosti in varstva podatkov ter načeli nujnosti in sorazmernosti iz korejske ustave.

([100]) Poleg tega lahko javni organi zavrnejo dostop, če bi ta povzročil velike težave pri izvajanju nekaterih nalog, vključno s tekočimi revizijami ali z naložitvijo, pobiranjem ali poplačilom davkov (člen 35(4) zakona o varstvu osebnih podatkov).

([101]) V takem primeru mora upravljavec sprejeti ukrepe, ki preprečujejo obnovitev osebnih podatkov (glej člen 36(3) zakona o varstvu osebnih podatkov).

([102]) Taki predpisi morajo izpolnjevati ustavne zahteve, da je temeljno pravico mogoče omejiti le, če je to potrebno zaradi nacionalne varnosti ali ohranjanja javnega reda in miru v javno dobro, pri tem pa se ne sme posegati v bistvo svoboščine ali pravice (člen 37 (2) ustave).

([103]) Člen 43(2) uredbe o izvajanju zakona o varstvu osebnih podatkov določa poseben postopek v primeru, ko upravljavec obdeluje datoteke z osebnimi podatki, ki mu jih je zagotovil drug upravljavec.

([104]) Za nesprejetje potrebnih ukrepov za popravek ali izbris osebnih podatkov in za nadaljnjo uporabo takih podatkov ali njihovo zagotavljanje tretji osebi se lahko izrečejo kazenske sankcije (člen 73(2) zakona o varstvu osebnih podatkov).

([105]) Člen 44(2) uredbe o izvajanju zakona o varstvu osebnih podatkov določa, da upravljavec v desetih dneh od prejetja zahteve obvesti posameznika, na katerega se nanašajo osebni podatki, da je ustrezno prenehal obdelovati podatke.

([106]) V primeru javnih organov se pravica do prenehanja obdelave lahko uresničuje v zvezi s podatki, ki jih vsebujejo prijavljene datoteke z osebnimi podatki (člen 37 v povezavi s členom 32 zakona o varstvu osebnih podatkov). Taka prijava ni potrebna v omejenih primerih, na primer kadar se datoteke z osebnimi podatki nanašajo na nacionalno varnost, kazenske preiskave, diplomatske odnose itd. (člen 32(2) zakona o varstvu osebnih podatkov).

([107]) Za kršitev obveznosti prenehanja obdelave se lahko izrečejo kazenske sankcije (člen 73(3) zakona o varstvu osebnih podatkov).

([108]) Odbor za mediacijo v primeru sporov (glej uvodno izjavo 133) je obravnaval več primerov, ko so se posamezniki pritožili glede uporabe njihovih podatkov za namene neposrednega trženja brez privolitve, na podlagi tega pa je na primer zadevni upravljavec plačal nadomestilo in izbrisal osebne podatke (glej npr. Odbor za mediacijo v primeru sporov 20R10-024(2020.11.18), 20R08-015(2020.8.28) in 20R07-031(2020.9.1)).

nameravani uporabi podatkov za namene neposrednega trženja (tj. na dejstvo, da bodo lahko uporabljeni za vzpostavitev stika z njim za promocijo blaga in storitev ali spodbujanje k njihovemu nakupu) „na očitno prepoznaven način“ (člen 22(2) in (4) zakona o varstvu osebnih podatkov v povezavi s členom 17(2), točka 1, uredbe o izvajanju zakona o varstvu osebnih podatkov).

(80) Za lažje uresničevanje pravic posameznikov mora upravljavec vzpostaviti namenske postopke in jih javno objaviti (člen 38(4) zakona o varstvu osebnih podatkov) ([109]). To vključuje postopke za vložitev ugovorov zoper zavrnitev zahteve (člen 38(5) zakona o varstvu osebnih podatkov). Upravljavec mora zagotoviti, da je postopek za uresničevanje pravic „prijazen do posameznika, na katerega se nanašajo osebni podatki,“ in ni zahtevnejši od postopka, ki omogoča zbiranje osebnih podatkov; to vključuje tudi obveznost zagotavljanja informacij o postopku na spletnem mestu upravljavca (člen 41(2), člen 43(1) in člen 44(1) uredbe o izvajanju zakona o varstvu osebnih podatkov) ([110]). Posamezniki lahko za vložitev take zahteve pooblastijo zastopnika (člen 38(1) zakona o varstvu osebnih podatkov v povezavi s členom 45 uredbe o izvajanju zakona o varstvu osebnih podatkov). Upravljavec lahko za to zaračuna pristojbino (v primeru zahteve za pošiljanje kopij osebnih podatkov po pošti pa tudi poštnino), vendar mora biti znesek te pristojbine določen „v okviru dejanskih izdatkov, potrebnih za obdelavo [zahteve]“; če je zahteva vložena zaradi ravnanja upravitelja, se pristojbina (ali poštnina) ne sme zaračunati (člen 38(3) zakona o varstvu osebnih podatkov v povezavi s členom 47 uredbe o izvajanju zakona o varstvu osebnih podatkov).

(81) Zakon o varstvu osebnih podatkov in uredba o njegovem izvajanju ne vsebujeta splošnih določb glede odločitev, ki vplivajo na posameznika, na katerega se nanašajo osebni podatki, in ki temeljijo izključno na samodejni obdelavi osebnih podatkov. Vendar glede osebnih podatkov, zbranih v Uniji, velja, da vse odločitve, ki temeljijo na samodejni obdelavi, po navadi sprejme upravljavec v Uniji (ki ima neposredno razmerje z zadevnim posameznikom, na katerega se nanašajo osebni podatki), zato se zanj uporablja Uredba (EU) 2016/679 ([111]). To vključuje tudi primere prenosa, ko obdelavo izvaja tuji (npr. korejski) poslovni subjekt, ki deluje kot zastopnik (obdelovalec) v imenu upravljavca iz Unije (ali kot podobdelovalec, ki deluje v imenu obdelovalca iz Unije, ta pa je podatke prejel od upravljavca podatkov iz Unije, ki jih je zbral) in nato na tej podlagi sprejme odločitev. Dejstvo, da zakon o varstvu osebnih podatkov ne vsebuje posebnih pravil o samodejnem odločanju, torej najverjetneje ne bo vplivalo na raven varstva osebnih podatkov, ki se prenašajo na podlagi tega sklepa.

(82) Izjemoma pa se določbe o preglednosti na zahtevo (člen 20) in pravicah posameznika (členi 35 do 37) ter obveznosti ponudnikov informacijskih in komunikacijskih storitev glede uradnega obveščanja posameznika (člen 39-8 zakona o varstvu osebnih podatkov) ne uporabljajo v zvezi s psevdonimiziranimi podatki, kadar se ti obdelujejo za namene statistične analize, znanstvenih raziskav ali arhiviranja v javnem interesu (člen 28-7 zakona o varstvu osebnih podatkov) ([112]). V skladu s pristopom iz člena 11(2) (v povezavi z uvodno izjavo 57) Uredbe (EU) 2016/679 je to upravičeno z dejstvom, da bi moral upravljavec za zagotovitev preglednosti ali podelitev individualnih pravic ugotoviti, ali so kateri koli podatki (in, če da, kateri) povezani s posameznikom, ki je vložil zahtevo, kar je izrecno prepovedano z zakonom o varstvu osebnih podatkov (člen 28-5(1) zakona o varstvu osebnih podatkov). Poleg tega bi taka ponovna identifikacija, če bi pomenila izničenje psevdonimizacije celotnega (psevdonimiziranega) niza podatkov, osebne podatke vseh drugih zadevnih posameznikov izpostavila povečanemu tveganju. Uredba (EU) 2016/679 se nanaša na primere, ko je ponovna identifikacija tako rekoč nemogoča, v zakonu o varstvu osebnih podatkov pa je uporabljen strožji pristop, saj izrecno prepoveduje ponovno identifikacijo v vseh primerih, ko se obdelujejo psevdonimizirani podatki.

(83) Korejski sistem, kot je opisan v uvodnih izjavah (74) do (82), torej vsebuje pravila o pravicah posameznika, na katerega se nanašajo osebni podatki, ki zagotavljajo v osnovi enakovredno raven varstva, kot jo zagotavlja Uredba (EU) 2016/679.

([109]) Glej tudi člen 30(1), točka 5, zakona o varstvu osebnih podatkov, ki se nanaša na politiko zasebnosti, ki med drugim vsebuje informacije o pravicah, ki jih ima na voljo posameznik, in o tem, kako jih uresničevati.

([110]) Glej tudi člen 39-7(2) zakona o varstvu osebnih podatkov glede ponudnikov informacijskih in komunikacijskih storitev.

([111]) Nasprotno pa velja, da so izjemni primeri, ko ima korejski poslovni subjekt neposreden odnos s posameznikom, na katerega se nanašajo osebni podatki, v EU, po navadi posledica tega, da se je navedeni upravljavec ciljno usmeril na posameznika v Evropski uniji s ponujanjem blaga ali storitev ali s spremljanjem njegovega vedenja. V takem primeru se tudi za korejski poslovni subjekt uporablja Uredba (EU) 2016/679 (člen 3(2)), zato mora neposredno zagotoviti skladnost s pravom EU o varstvu podatkov.

([112]) Glej tudi uradno obvestilo št. 2021-5, ki potrjuje, da se oddelek III zakona o varstvu osebnih podatkov (vključno s členom 28-7) uporablja le, kadar se psevdonimizirani podatki obdelujejo za namene znanstvenih raziskav, statistične analize ali arhiviranja v javnem interesu, glej Prilogo I, oddelek 4, k temu sklepu.

2.3.9 *Nadaljnji prenosi*

(84) Raven varstva, zagotovljena osebnim podatkom, ki se iz Unije prenesejo upravljavcem v Republiki Koreji, se z nadaljnjim prenosom takih podatkov prejemnikom v tretji državi ne sme poslabšati.

(85) Z vidika korejskega upravljavca so taki „nadaljnji prenosi“ mednarodni prenosi iz Republike Koreje. V tem smislu zakon o varstvu osebnih podatkov razlikuje med oddajo obdelave v zunanje izvajanje (tj. zunanjemu obdelovalcu) in zagotavljanjem osebnih podatkov tretjim osebam ([113]).

(86) Prvič, če se obdelava osebnih podatkov odda v zunanje izvajanje subjektu v tretji državi, mora korejski upravljavec zagotoviti skladnost z določbami zakona o varstvu osebnih podatkov o oddaji v zunanje izvajanje (člen 26 zakona o varstvu osebnih podatkov). To vključuje sprejetje pravno zavezujočega instrumenta, ki obdelavo pri zunanjem izvajalcu med drugim omejuje na namen oddaje v zunanje izvajanje, določa tehnične in upravljavske zaščitne ukrepe ter omejuje podobdelavo (glej člen 26(1) zakona o varstvu osebnih podatkov), in objavo informacij o oddaji v zunanjo obdelavo. Poleg tega mora upravljavec zunanjega izvajalca „podučiti“ o potrebnih varnostnih ukrepih ter nadzorovati, med drugim s pregledi, skladnost z vsemi obveznostmi upravljavca na podlagi zakona o varstvu osebnih podatkov ([114]) in pogodbe o oddaji v zunanje izvajanje.

(87) Če zunanji izvajalec povzroči škodo zaradi obdelave osebnih podatkov v nasprotju z zakonom o varstvu osebnih podatkov, se ta odgovornost pripiše upravljavcu, tako kot bi se v primeru upravljavčevega zaposlenega (člen 26(6) zakona o varstvu osebnih podatkov). Korejski upravljavec je torej še naprej odgovoren za osebne podatke, ki so bili poslani v obdelavo zunanjemu izvajalcu, in mora zagotoviti, da obdelovalec v tujini podatke obdeluje v skladu z zakonom o varstvu osebnih podatkov. Če zunanji izvajalec podatke obdeluje v nasprotju z zakonom o varstvu osebnih podatkov, je lahko korejski upravljavec odgovoren za neizpolnitev obveznosti zagotavljanja skladnosti z zakonom o varstvu osebnih podatkov, na primer z nadzorom nad zunanjim izvajalcem. Zaščitni ukrepi, vključeni v pogodbo o zunanjem izvajanju, in odgovornost korejskega upravljavca za dejanja zunanjega izvajalca zagotavljajo kontinuiteto varstva, kadar se obdelava osebnih podatkov odda v zunanje izvajanje subjektu zunaj Koreje.

(88) Drugič, korejski upravljavci lahko osebne podatke zagotavljajo tretji osebi zunaj Koreje. Čeprav zakon o varstvu osebnih podatkov vsebuje več pravnih podlag, ki na splošno omogočajo zagotavljanje podatkov tretjim osebam, pa mora upravljavec, če je tretja oseba zunaj Koreje, načeloma ([115]) pridobiti privolitev posameznika, na katerega se nanašajo osebni podatki ([116]), in sicer po tem, ko ga obvesti o (1) vrsti osebnih podatkov, (2) prejemniku osebnih podatkov, (3) namenu prenosa, tj. namenu obdelave, ki ga uresničuje prejemnik, (4) obdobju hrambe za namen obdelave pri prejemniku ter (5) dejstvu, da lahko posameznik, na katerega se nanašajo osebni podatki, privolitev odkloni (člen 17(2) in (3) zakona o varstvu osebnih podatkov). Uradno obvestilo št. 2021-5 v oddelku o preglednosti (glej uvodno izjavo (70)) zahteva, da so posamezniki obveščeni o tretji državi, v katero se bodo zagotavljali njihovi podatki. Tako se zagotovi, da lahko posamezniki v Uniji, na katere se nanašajo osebni podatki, sprejmejo povsem premišljeno odločitev o tem, ali privoliti v zagotavljanje podatkov v tujino ali ne. Poleg tega upravljavec s tretjo osebo (prejemnikom) ne sme skleniti pogodbe v nasprotju z zakonom o varstvu osebnih podatkov, kar pomeni, da pogodba ne sme vsebovati obveznosti, ki bi bile v nasprotju z obveznostmi upravljavca na podlagi zakona o varstvu osebnih podatkov ([117]).

([113]) Posebna pravila veljajo za ponudnike informacijskih in komunikacijskih storitev. V skladu s členom 39-12 zakona o varstvu osebnih podatkov morajo ponudniki informacijskih in komunikacijskih storitev načeloma pridobiti privolitev uporabnika za vsak prenos osebnih podatkov v tujino. Če se osebni podatki prenašajo v okviru oddaje postopkov obdelave v zunanje izvajanje, med drugim za skladiščenje, privolitev ni potrebna, če so bili zadevni posamezniki neposredno ali na podlagi zlahka dostopnega javnega obvestila vnaprej obveščeni o (1) podrobnostih podatkov, ki se bodo prenesli, (2) državi, v katero se bodo podatki prenesli (ter datumu in načinu prenosa), (3) imenu prejemnika ter (4) namenu uporabe in hrambe pri prejemniku (člen 39-12(3) zakona o varstvu osebnih podatkov). Poleg tega se v takem primeru uporabljajo splošne zahteve za oddajo v zunanje izvajanje. Pri vsakem prenosu je treba sprejeti posebne zaščitne ukrepe v zvezi z varnostjo, obravnavanjem pritožb in sporov ter drugimi ukrepi, ki so potrebni za varstvo podatkov o uporabnikih (člen 48-10 uredbe o izvajanju zakona o varstvu osebnih podatkov).

([114]) Glej tudi člen 26(7) zakona o varstvu osebnih podatkov, v skladu s katerim se členi 15 do 25, 27 do 31, 33 do 38 in 50 smiselno uporabljajo tudi za obdelovalca.

([115]) Če pa osebne podatke uporabnikov tretji osebi zagotovi ponudnik informacijskih in komunikacijskih storitev, je za to vedno potrebna privolitev uporabnika (člen 39-12(2) zakona o varstvu osebnih podatkov).

([116]) Kot je podrobneje pojasnjeno v uvodni izjavi 51, mora biti taka privolitev, da bi bila veljavna, dana prostovoljno ter biti informirana in specifična.

([117]) Glej tudi člen 39-12(1) zakona o varstvu osebnih podatkov glede ponudnikov informacijskih in komunikacijskih storitev.

(89) Brez privolitve posameznika se lahko osebni podatki zagotavljajo tretjim osebam v tujini, če namen razkritja ostaja „v okviru obsega, ki je razumno povezan“ s prvotnim namenom zbiranja (člen 17(4) zakona o varstvu osebnih podatkov, glej uvodno izjavo (36)). Vendar pa mora upravljavec pri odločanju o tem, ali razkriti (ali ne) osebne podatke za „povezan“ namen, upoštevati, ali razkritje postavlja posameznika v neugoden položaj in ali so bili sprejeti potrebni varnostni ukrepi (npr. šifriranje). Glede na to, da tretja država, v katero se prenašajo osebni podatki, morda ne zagotavlja podobnega varstva, kot ga določa zakon o varstvu osebnih podatkov, se v oddelku 2 uradnega obvestila št. 2021-5 priznava, da tak neugoden položaj lahko nastane in da se mu je mogoče izogniti le, če korejski upravljavec in prejemnik v tujini na podlagi pravno zavezujočega instrumenta (npr. pogodbe) zagotovita raven varstva, ki je enakovredna tisti iz zakona o varstvu osebnih podatkov, tudi glede pravic posameznika, na katerega se nanašajo osebni podatki.

(90) Posebna pravila se uporabljajo za razkritje, ki presega namen, tj. zagotavljanje podatkov tretji osebi za nov (nepovezan) namen, ki se lahko izvede le na eni od podlag iz člena 18(2) zakona o varstvu osebnih podatkov, kot je opisano v uvodni izjavi (39). Vendar pa je celo pod navedenimi pogoji zagotavljanje tretjim osebam izključeno, če je verjetno, da bi se s tem „nepošteno posegalo“ v interese posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe, tako da je potrebno tehtanje interesov. Poleg tega mora v skladu s členom 18(5) zakona o varstvu osebnih podatkov upravljavec sprejeti dodatne zaščitne ukrepe, med katerimi je lahko tudi zahteva, da tretja oseba omeji namen in metodo obdelave ali sprejme posebne varnostne ukrepe. Znova velja, da se, glede na to, da tretja država, v katero se prenašajo osebni podatki, morda ne zagotavlja podobnega varstva, kot ga določa zakon o varstvu osebnih podatkov, v oddelku 2 uradnega obvestila št. 2021-5 priznava, da tako „nepošteno poseganje“ v interese posameznika ali tretje osebe lahko nastane in da se mu je mogoče izogniti le, če korejski upravljavec in prejemnik v tujini na podlagi pravno zavezujočega instrumenta (npr. pogodbe) zagotovita raven varstva, ki je enakovredna tisti iz zakona o varstvu osebnih podatkov, tudi glede pravic posameznika, na katerega se nanašajo osebni podatki.

(91) Pravila iz uvodnih izjav (86) do (90) torej zagotavljajo kontinuiteto varstva pri nadaljnjem prenosu osebnih podatkov (zunanjemu izvajalcu ali tretji osebi) iz Republike Koreje, ki je v osnovi enakovredno tistemu, ki ga zagotavlja Uredba (EU) 2016/679.

2.3.10 *Odgovornost*

(92) 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 izpolnjevanje, predvsem pristojnim nadzornim organom.

(93) Člen 3(6) in (8) zakona o varstvu osebnih podatkov določa, da mora upravljavec osebne podatke obdelovati „tako, da se čim bolj zmanjša možnost kršitve“ zasebnosti posameznika, na katerega se nanašajo osebni podatki, ter si prizadeva pridobiti zaupanje takega posameznika z upoštevanjem in izpolnjevanjem nalog in obveznosti, ki jih določajo zakon o varstvu osebnih podatkov in drugi s tem povezani predpisi. To vključuje pripravo notranjega načrta upravljanja (člen 29 zakona o varstvu osebnih podatkov) ter ustrezno usposabljanje in nadzor osebja (člen 28 zakona o varstvu osebnih podatkov).

(94) Za zagotavljanje odgovornosti člen 31 zakona o varstvu osebnih podatkov v povezavi s členom 32 uredbe o izvajanju zakona o varstvu osebnih podatkov določa, da mora upravljavec imenovati pooblaščeno osebo za varstvo zasebnosti, ki „celovito prevzame nadzor nad obdelavo osebnih podatkov“. Taka pooblaščena oseba ima zlasti naslednje naloge: (1) pripravi in izvaja načrt varstva osebnih podatkov ter oblikuje politiko zasebnosti, (2) opravlja redne raziskave glede stanja in praks na področju obdelave osebnih podatkov z namenom izboljšanja morebitnih pomanjkljivosti, (3) obravnava pritožbe in priznava odškodnine, (4) vzpostavi notranji sistem nadzora za preprečevanje razkritja, zlorabe ali nepravilne uporabe osebnih podatkov, (5) pripravi in izvaja program usposabljanja, (6) zagotavlja varstvo datotek z osebnimi podatki, njihov nadzor in upravljanje ter (7) poskrbi za uničenje osebnih podatkov, ko je namen obdelave dosežen ali ko se izteče obdobje hrambe. Pri opravljanju teh nalog lahko pooblaščena oseba za varstvo zasebnosti preverja stanje na področju obdelave osebnih podatkov in s tem povezanih sistemov ter lahko zahteva informacije v zvezi s tem (člen 31(3) zakona o varstvu osebnih podatkov). Če pooblaščena oseba za varstvo zasebnosti izve za kakršno koli kršitev zakona o varstvu osebnih podatkov ali drugih zadevnih predpisov o varstvu osebnih podatkov, takoj sprejme popravne ukrepe in o njih poroča vodstvu („vodji“) upravljavca, če je potrebno (člen 31(4) zakona o varstvu osebnih podatkov). Člen 31(5) zakona o varstvu osebnih podatkov določa, da pooblaščena oseba za varstvo zasebnosti zaradi opravljanja teh nalog ne sme biti neupravičeno postavljena v neugoden položaj.

(95) Poleg tega si morajo upravljavci proaktivno prizadevati za izvedbo ocene učinka na zasebnost, kadar pri obdelavi datotek z osebnimi podatki obstaja tveganje za kršitev zasebnosti (člen 33(8) zakona o varstvu osebnih podatkov). Člen 33(1) in (2) zakona o varstvu osebnih podatkov v povezavi s členi 35, 36 in 38 uredbe o izvajanju zakona o varstvu osebnih podatkov določa, da se pri ocenjevanju stopnje tveganja za pravice posameznikov, na katere se nanašajo osebni podatki, upoštevajo dejavniki, kot so vrsta in narava podatkov, ki se obdelujejo (zlasti, ali gre za občutljive podatke), količina podatkov, obdobje hrambe in verjetnost kršitve varnosti podatkov. Namen ocene učinka na zasebnost je zagotoviti, da se analizirajo dejavniki tveganja za zasebnost in varnostni ali drugi protiukrepi ter opredelijo področja, ki jih je treba izboljšati (glej člen 33(1) zakona o varstvu osebnih podatkov v povezavi s členom 38 uredbe o izvajanju zakona o varstvu osebnih podatkov).

(96) Javni organi morajo izvesti oceno učinka, kadar obdelujejo nekatere datoteke z osebnimi podatki, ki pomenijo večje tveganje za morebitne kršitve zasebnosti (člen 33(1) zakona o varstvu osebnih podatkov). Člen 35 uredbe o izvajanju zakona o varstvu osebnih podatkov določa, da je tako med drugim v primeru datotek, ki vsebujejo občutljive podatke o najmanj 50 000 posameznikih, na katere se nanašajo osebni podatki, datotek, ki se bodo povezale z drugimi datotekami in bodo zaradi tega vsebovale podatke o najmanj 500 000 posameznikih, na katere se nanašajo osebni podatki, ali datotek, ki vsebujejo podatke o najmanj enem milijonu posameznikov, na katere se nanašajo osebni podatki. Rezultat ocene učinka, ki jo izvede javni organ, je treba sporočiti komisiji za varstvo osebnih podatkov (člen 33(1) zakona o varstvu osebnih podatkov), ki lahko izda mnenje (člen 33(3) zakona o varstvu osebnih podatkov).

(97) Nazadnje, člen 13 zakona o varstvu osebnih podatkov določa, da komisija za varstvo osebnih podatkov oblikuje politike, ki so potrebne za spodbujanje in podpiranje „samoreguliranih dejavnosti upravljavcev za varstvo podatkov“, med drugim z izobraževanjem o varstvu podatkov, spodbujanjem in podpiranjem organizacij, ki se ukvarjajo z varstvom podatkov, ter s pomočjo upravljavcem pri vzpostavljanju in izvajanju samoregulativnih pravil. Poleg tega uvede in omogoča sistem ePRIVACY Mark. Glede tega člen 32-2 zakona o varstvu osebnih podatkov v povezavi s členoma 34-2 in 34-8 uredbe o izvajanju zakona o varstvu osebnih podatkov določa možnost potrjevanja, da so upravljavčevi sistemi za obdelavo in varstvo osebnih podatkov skladni z zahtevami iz zakona o varstvu osebnih podatkov. V skladu s temi pravili se lahko izda potrdilo ([118]) (za obdobje treh let), če upravljavec izpolnjuje merila za izdajo potrdila, ki jih opredeli komisija za varstvo osebnih podatkov, vključno z vzpostavitvijo upravljavskih, tehničnih in fizičnih zaščitnih ukrepov za varstvo osebnih podatkov ([119]). Komisija za varstvo osebnih podatkov mora vsaj enkrat letno preveriti upravljavčeve sisteme, ki so pomembni za potrjevanje, da se ohrani njegova učinkovitost, pri tem pa lahko potrdilo tudi prekliče (člen 32(4) zakona o varstvu osebnih podatkov v povezavi s členom 34-5 uredbe o izvajanju zakona o varstvu osebnih podatkov; tako imenovano „nadaljnje upravljanje“).

(98) Korejski okvir torej udejanja načelo odgovornosti tako, da se zagotavlja raven varnosti, ki je v osnovi enakovredna tisti iz Uredbe (EU) 2016/679, vključno z zagotavljanjem različnih mehanizmov za zagotavljanje in dokazovanje skladnosti z zakonom o varstvu osebnih podatkov.

2.3.11 *Posebna pravila za obdelavo osebnih kreditnih informacij*

(99) Kot je opisano v uvodni izjavi (13), zakon o uporabi in varstvu kreditnih informacij določa posebna pravila za obdelavo osebnih kreditnih informacij s strani gospodarskih subjektov. Kadar gospodarski subjekti obdelujejo osebne kreditne informacije, morajo torej zagotoviti skladnost s splošnimi zahtevami iz zakona o varstvu osebnih podatkov, razen če zakon o uporabi in varstvu kreditnih informacij vsebuje podrobnejša pravila. Tako je v primeru, ko obdelujejo podatke v zvezi s kreditno kartico ali bančnim računom v okviru poslovne transakcije s posameznikom. Zakon o uporabi in varstvu kreditnih informacij kot sektorska zakonodaja za obdelavo kreditnih informacij (osebnih in neosebnih) določa posebne zaščitne ukrepe za varstvo podatkov (npr. v smislu preglednosti in varnosti), obenem pa tudi splošneje ureja posebne okoliščine, v katerih se lahko obdelujejo osebne kreditne informacije. To se še zlasti odraža v podrobnih zahtevah za uporabo podatkov, njihovo zagotavljanje tretjim osebam in hrambo takih podatkov.

(100) Tako kot zakon o varstvu osebnih podatkov tudi zakon o uporabi in varstvu kreditnih informacij odraža načeli zakonitosti in sorazmernosti. Prvič, kot splošno zahtevo člen 15(1) zakona o uporabi in varstvu kreditnih informacij določa, da je osebne kreditne informacije dovoljeno zbirati le na razumne in poštene načine in v najmanjšem možnem obsegu, ki še omogoča izpolnjevanje posameznega namena, in sicer v skladu s členom 3 (1)–(2) zakona o varstvu osebnih podatkov. Drugič, zakon o uporabi in varstvu kreditnih informacij izrecno ureja zakonitost obdelave osebnih kreditnih informacij z omejevanjem njihovega zbiranja, uporabe in zagotavljanja tretjim osebam ter na splošno z zahtevo, da se za take dejavnosti obdelave dobi privolitev zadevne osebe.

([118]) Poleg tega lahko upravljavec, če se namerava pri svojem poslovanju sklicevati na potrdilo ali ga promovirati, uporablja znak za varstvo osebnih podatkov, ki ga je uvedla komisija za varstvo osebnih podatkov. Glej člen 34-7 uredbe o izvajanju zakona o varstvu osebnih podatkov.

([119]) Novembra 2018 je bil razvit sistem za upravljanje varnosti osebnih podatkov in informacij (ISMS-P), ki potrjuje, da upravljavci uporabljajo celovit sistem upravljanja.

(101) Osebne kreditne informacije se lahko zbirajo sklicujoč se na eno od pravnih podlag iz zakona o varstvu osebnih podatkov ali na posebne pravne podlage iz zakona o uporabi in varstvu kreditnih informacij. Glede na to, da se s členom 45 Uredbe (EU) 2016/679 predpostavlja prenos osebnih podatkov od upravljavca ali obdelovalca v Uniji, ni pa zajeto neposredno zbiranje pri upravljavcu v Koreji (npr. od posameznika ali na spletnem mestu), so za ta sklep pomembne le privolitev in pravne podlage iz zakona o varstvu osebnih podatkov. Te pravne podlage vključujejo zlasti primere, ko je prenos potreben za izpolnitev pogodbe s posameznikom ali zaradi zakonitih interesov korejskega upravljavca (člen 15(1), točki 4 in 6, zakona o varstvu osebnih podatkov) ([120]).

(102) Ko so osebne kreditne informacije zbrane, se lahko uporabijo (1) za izvirni namen, za katerega jih je posameznik (neposredno) zagotovil ([121]); (2) za namen, ki je skladen z izvirnim namenom zbiranja ([122]); (3) za odločitev, ali skleniti oziroma ohraniti poslovno razmerje, za katero je zaprosil posameznik ([123]); (4) za namene statistične analize, raziskav in arhiviranja v javnem interesu ([124]), če so podatki psevdonimizirani ([125]); (5) če je pridobljena nadaljnja privolitev ali (6) v skladu z zakonom.

(103) Če gospodarski subjekt namerava razkriti osebne kreditne informacije tretji osebi, mora pridobiti posameznikovo privolitev ([126]), in sicer po tem, ko ga obvesti o prejemniku podatkov, namenu obdelave s strani prejemnika, podrobnostih podatkov, ki se bodo zagotovili, obdobju hrambe pri prejemniku in o pravici, da tako privolitev zavrne (člen 32(1) zakona o uporabi in varstvu kreditnih informacij ter člen 28(2) uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij) ([127]). Ta zahteva glede privolitve se ne uporablja v posebnih okoliščinah, in sicer kadar se osebne kreditne informacije razkrivajo ([128]): (1) zunanjemu izvajalcu za namene zunanjega izvajanja ([129]); (2) tretji osebi v primeru prenosa, delitve ali združitve poslovanja; (3) za namene statistične analize, raziskav in arhiviranja v javnem interesu, če so podatki psevdonimizirani; (4) za namen, ki je skladen z izvirnim namenom zbiranja; (5) tretji osebi, ki informacije uporabi za izterjavo dolga posameznika ([130]); (6) za izpolnitev odločbe sodišča; (7) tožilcu/pravosodnemu policistu v nujnih primerih, ko je ogroženo življenje posameznika ali

([120]) Zakon o uporabi in varstvu kreditnih informacij vsebuje še druge pravne podlage za zbiranje, tj. kadar tako zahteva zakon, kadar javni organ javno objavi informacije v skladu z zakonodajo o dostopu do informacij javnega značaja ali kadar so informacije dostopne na družbenem omrežju. Če se želi gospodarski subjekt sklicevati na zadnjenavedeno podlago, mora dokazati, da zbiranje ostaja v okviru privolitve posameznika, na katerega se nanašajo osebni podatki, in sicer na podlagi razumne („objektivne“) razlage ter ob upoštevanju narave podatkov, namena in cilja njihove objave na družbenem omrežju, vprašanja, ali je namen zbiranja „tesno povezan“ z navedenim namenom, itd. (člen 13 uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij). Vendar pa, kot je pojasnjeno v uvodni izjavi (101), te pravne podlage načeloma niso upoštevne v primeru prenosa.

([121]) Na primer kadar se kreditne informacije ustvarjajo/zagotavljajo v okviru poslovne transakcije s posameznikom. Vendar pa se na to podlago ni mogoče sklicevati pri uporabi osebnih kreditnih informacij za namene neposrednega trženja (glej člen 33(1), točka 3, zakona o uporabi in varstvu kreditnih informacij).

([122]) Pri ugotavljanju, ali je namen uporabe skladen z izvirnim namenom zbiranja, je treba upoštevati naslednje dejavnike: (1) povezavo („ustreznost“) med obema namenoma; (2) način, kako so bili podatki zbrani; (3) posledice uporabe za posameznika in (4) ali so bili izvedeni ustrezni varnostni ukrepi, kot je psevdonimizacija (glej člen 32(6), točka 9-4, zakona o uporabi in varstvu kreditnih informacij).

([123]) Upravljavec mora morda na primer upoštevati osebne kreditne informacije, ki jih je prejel od posameznika, da se lahko odloči, ali mu bo podaljšal obdobje odplačevanja kredita.

([124]) Člen 33 zakona o uporabi in varstvu kreditnih informacij v povezavi s členom 32(6), točke 9-2, 9-4 in 10, zakona o uporabi in varstvu kreditnih informacij.

([125]) Psevdonimizacija je v členu 2(15) zakona o uporabi in varstvu kreditnih informacij opredeljena kot obdelava osebnih kreditnih informacij na način, da posameznikov na podlagi takih informacij ni več mogoče identificirati, razen v kombinaciji z dodatnimi informacijami. Čeprav zakon o uporabi in varstvu kreditnih informacij vsebuje posebne zaščitne ukrepe za obdelavo psevdonimiziranih informacij za namene statistične analize, raziskav in arhiviranja v javnem interesu (člen 40-2 zakona o uporabi in varstvu kreditnih informacij), pa se ta pravila ne uporabljajo za gospodarske subjekte. Zanje še naprej veljajo posebne zahteve iz oddelka III zakona o varstvu osebnih podatkov, kot je opisano v uvodnih izjavah (42)–(48). Člen 40-3 zakona o uporabi in varstvu kreditnih informacij nadalje določa, da za obdelavo psevdonimiziranih kreditnih informacij (kadar ta poteka za namene statistične analize, znanstvenih raziskav ali arhiviranja v javnem interesu) ne veljajo zahteve glede preglednosti in pravic posameznikov, kar je podobno izjemi iz člena 28-7 zakona o varstvu osebnih podatkov, uporabljajo pa se zaščitni ukrepi iz oddelka III zakona o varstvu osebnih podatkov, kot je podrobneje opisano v uvodnih izjavah (42)–(48).

([126]) To ne velja, kadar se informacije zagotavljajo tretji osebi, da bi se ohranila točnost in posodobljenost osebnih kreditnih informacij, če tako zagotavljanje tretji osebi ostaja v okviru prvotnega namena obdelave (člen 32(1) zakona o uporabi in varstvu kreditnih informacij). Tak primer je zagotavljanje najnovejših informacij bonitetni agenciji, da se zagotovi točnost njenih evidenc.

([127]) Če zagotavljanje zgorajnavedenih informacij ni praktično, lahko zadostuje, da se posameznika po zahtevane informacije napoti k tretji osebi (prejemniku).

([128]) Ker zakon o uporabi in varstvu kreditnih informacij posebej ne ureja razkrivanja osebnih kreditnih informacij v tujino, morajo biti taka razkritja v skladu z zaščitnimi ukrepi za nadaljnje prenose, ki jih določa oddelek 2 uradnega obvestila št. 2021-5.

([129]) Obdelava osebnih kreditnih informacij se lahko odda v zunanje izvajanje le na podlagi pisne pogodbe ter v skladu z zahtevami iz člena 26(1)-(3) in člena 26(5) zakona o varstvu osebnih podatkov, kot je opisano v uvodni izjavi (20) (člen 17 zakona o uporabi in varstvu kreditnih informacij ter člen 14 uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij). Zunanji izvajalec informacij ne sme uporabiti tako, da bi to presegalo okvir njegovih nalog, družba, ki obdelavo odda v zunanje izvajanje, pa mora uvesti posebne varnostne zahteve (npr. šifriranje) in zunanjega izvajalca poučiti, kako preprečiti izgubo, krajo, razkritje in spreminjanje kreditnih informacij ali poseganje vanje.

([130]) Glej tudi člen 28(10), točke 1, 2 in 6, uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij.

če posamezniku grozi telesna poškodba in ni časa za izdajo sodne odredbe ([131]); (8) pristojnim davčnim organom za zagotovitev skladnosti z davčno zakonodajo; ali (9) v skladu z drugimi zakoni. V primeru razkritja iz enega od navedenih razlogov mora biti posameznik, na katerega se nanašajo osebni podatki, o tem vnaprej uradno obveščen (člen 32(7) zakona o uporabi in varstvu kreditnih informacij).

(104) Zakon o uporabi in varstvu kreditnih informacij tudi posebej ureja trajanje obdelave osebnih kreditnih informacij na podlagi enega od razlogov za uporabo podatkov ali njihovo zagotavljanje tretji osebi po izteku poslovnega razmerja s posameznikom ([132]). Obdržijo se lahko le informacije, ki so bile potrebne za vzpostavitev ali ohranitev navedenega razmerja, ob upoštevanju dodatnih zaščitnih ukrepov (hranjene morajo biti ločeno od kreditnih informacij, ki se nanašajo na posameznike, s katerimi poslovno razmerje še traja, zaščitene morajo biti s posebnimi varnostnimi ukrepi in dostopne le pooblaščenim posameznikom) ([133]). Vse druge podatke je treba izbrisati (člen 17-2(1), točka 2, uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij). Pri ugotavljanju, kateri podatki so bili potrebni za poslovno razmerje, je treba upoštevati različne dejavnike, tudi vprašanje, ali bi bilo mogoče razmerje vzpostaviti tudi brez teh podatkov in ali se neposredno nanašajo na blago ali storitve, ki se zagotavljajo posamezniku (člen 17-2(2) uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij).

(105) Tudi kadar se lahko osebne kreditne informacije načeloma hranijo tudi po koncu poslovnega razmerja, jih je treba izbrisati v treh mesecih po tem, ko se izpolni nadaljnji namen obdelave ([134]), vsekakor pa po petih letih (člen 20-2 zakona o uporabi in varstvu kreditnih informacij). V omejenem številu primerov se lahko osebne kreditne informacije hranijo dlje kot pet let, zlasti kadar je to potrebno za izpolnitev pravne obveznosti, če je to potrebno iz nujnih razlogov, povezanih s posameznikovim življenjem, telesom ali premoženjem, za arhiviranje psevdonimiziranih informacij (ki so bile uporabljene za namene znanstvenih raziskav, statistične analize ali arhiviranja v javnem interesu), ali za zavarovalne namene (zlasti za izplačila zavarovalnine ali za preprečitev zavarovalniških goljufij) ([135]). V teh izjemnih primerih se uporabljajo posebni zaščitni ukrepi (npr. uradno obveščanje posameznika o nadaljnji uporabi, ločitev hranjenih informacij od informacij, ki se nanašajo na posameznike, s katerimi poslovno razmerje še traja, omejitev pravic do dostopa, glej člen 17-2(1)-(2) uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij).

(106) Zakon o uporabi in varstvu kreditnih informacij tudi podrobneje določa načeli točnosti in kakovosti podatkov, saj se z njim zahteva, da se osebne kreditne informacije „registrirajo, spreminjajo in upravljajo“, da ostanejo točne in posodobljene (člen 18(1) zakona o uporabi in varstvu kreditnih informacij ter člen 15(3) uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij) ([136]). Kadar gospodarski subjekti zagotavljajo kreditne informacije nekaterim drugim subjektom (npr. bonitetnim agencijam), se tudi izrecno zahteva, da preverijo točnost informacij, s čimer se zagotovi, da prejemnik registrira in upravlja le točne informacije (člen 15(1) uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij v povezavi s členom 18(1) zakona o uporabi in varstvu kreditnih informacij). Splošneje, zakon o uporabi in varstvu kreditnih informacij določa, da je treba voditi evidence o zbiranju, uporabi, razkritju tretjim osebam in uničenju osebnih kreditnih informacij (člen 20(2) zakona o uporabi in varstvu kreditnih informacij) ([137]).

(107) Poleg tega za obdelavo osebnih kreditnih informacij veljajo posebne zahteve glede varnosti podatkov. Z zakonom o uporabi in varstvu kreditnih informacij se zlasti zahteva izvajanje tehničnih, fizičnih in organizacijskih ukrepov za preprečevanje nezakonitega dostopa do računalniških sistemov in spreminjanja, uničenja ali katerega koli drugega tveganja za podatke, ki se obdelujejo (npr. z nadzorom dostopa, glej člen 19 zakona o uporabi in varstvu kreditnih informacij ter člen 16 uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij). Poleg tega je treba pri izmenjavi osebnih kreditnih informacij s tretjo osebo skleniti sporazum, ki določa posebne varnostne ukrepe (člen 19(2) zakona o uporabi in varstvu kreditnih informacij). Če pride do kršitve osebnih kreditnih informacij, je treba sprejeti ukrepe za zmanjšanje škode in brez odlašanja uradno obvestiti zadevne posameznike (člen 39-4(1)-(2) zakona o uporabi in varstvu kreditnih informacij). Poleg tega je treba komisijo za varstvo osebnih podatkov obvestiti o tem, da so bili posamezniki uradno obveščeni, in o sprejetih ukrepih (člen 39-4(4) zakona o uporabi in varstvu kreditnih informacij).

([131]) V takem primeru je treba takoj zahtevati izdajo sodne odredbe. Če ta ni izdana v 36 urah, je treba prejete podatke brez odlašanja izbrisati (člen 32(6), točka 6, zakona o uporabi in varstvu kreditnih informacij).

([132]) Ker so bile na primer pogodbene obveznosti izpolnjene ali ker je ena od strank uveljavila svojo pravico do odpovedi itd. (glej člen 17-2(5) uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij).

([133]) Člen 20-2(1) zakona o uporabi in varstvu kreditnih informacij ter člen 17-2(1), točka 1, uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij.

([134]) Pri tem obdobju se upošteva, da izbris pogosto ni mogoč takoj, ampak je običajno za to potrebnih več korakov, za izvedbo katerih je potreben določen čas (npr. ločitev podatkov, ki jih je treba izbrisati, od drugih podatkov ter taka izvedba izbrisa, da to ne vpliva na stabilnost informacijskih sistemov).

([135]) Člen 20-2(2) zakona o uporabi in varstvu kreditnih informacij.

([136]) Člen 18(2) zakona o uporabi in varstvu kreditnih informacij ter člen 15(4) uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij določata podrobnejša pravila v zvezi s to zahtevo po evidentiranju, na primer glede evidenc o informacijah, ki bi lahko posameznika postavile v neugoden položaj, na primer informacije o kršitvah predpisov in stečaju.

([137]) Glede drugih mehanizmov odgovornosti zakon o uporabi in varstvu kreditnih informacij od nekaterih organizacij (npr. zadrug in javnih podjetij, glej člen 21(2) uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij) zahteva, da imenujejo „upravnika/skrbnika kreditnih informacij“, ki spremlja skladnost z zakonom o uporabi in varstvu kreditnih informacij ter opravlja naloge „pooblaščene osebe za varstvo zasebnosti“ v skladu z zakonom o varstvu osebnih podatkov (člen 20(3) in (4) zakona o uporabi in varstvu kreditnih informacij).

(108) Zakon o uporabi in varstvu kreditnih informacij tudi določa posebne obveznosti glede preglednosti pri pridobivanju privolitve za uporabo ali zagotavljanje osebnih kreditnih informacij (člen 32(4) in člen 34-2 zakona o uporabi in varstvu kreditnih informacij ter člen 30-3 uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij), splošneje pa tudi pred zagotavljanjem informacij tretji osebi (člen 32(7) zakona o uporabi in varstvu kreditnih informacij) ([138]). Poleg tega imajo posamezniki pravico, da na zahtevo pridobijo informacije o uporabi in zagotavljanju njihovih kreditnih informacij tretjim osebam v triletnem obdobju pred vložitvijo zahteve (vključno z namenom in datumi take uporabe/zagotavljanja) ([139]).

(109) V skladu z zakonom o uporabi in varstvu kreditnih informacij imajo posamezniki tudi pravico do dostopa do svojih osebnih kreditnih informacij (člen 38(1) zakona o uporabi in varstvu kreditnih informacij) ter pravico do popravka netočnih podatkov (člen 38(2) in (3) zakona o uporabi in varstvu kreditnih informacij) ([140]). Prav tako poleg splošne pravice do izbrisa na podlagi zakona o varstvu osebnih podatkov (glej uvodno izjavo (77)) zakon o uporabi in varstvu kreditnih informacij določa tudi posebno pravico do izbrisa osebnih kreditnih informacij, ki se hranijo tudi po izteku rokov za hrambo, navedenih v uvodni izjavi (104), tj. pet let (za osebne kreditne informacije, ki so bile potrebne za vzpostavitev ali ohranitev poslovnega razmerja) ali tri mesece (za druge vrste osebnih kreditnih informacij) ([141]). Zahteva za izbris se izjemoma lahko zavrne, če je nadaljnja hramba potrebna v okoliščinah, opisanih v uvodni izjavi (105). Če posameznik zahteva izbris, vendar se uporablja ena od izjem, je treba v zvezi z zadevnimi kreditnimi informacijami sprejeti posebne zaščitne ukrepe (člen 38-3(3) zakona o uporabi in varstvu kreditnih informacij ter člen 33-3 uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij). Informacije je na primer treba hraniti ločeno od drugih informacij, do njih ima lahko dostop le pooblaščena oseba in zanje morajo veljati posebni varnostni ukrepi.

(110) Poleg pravic, navedenih v uvodni izjavi (109), zakon o uporabi in varstvu kreditnih informacij posameznikom zagotavlja pravico, da od upravljavca zahtevajo, naj se nanje več ne obrača za namene neposrednega trženja (člen 37(2) zakona), in pravico do prenosljivosti podatkov. V zvezi s slednjim zakon o uporabi in varstvu kreditnih informacij posameznikom omogoča, da zahtevajo posredovanje svojih osebnih kreditnih informacij sebi ali nekaterim tretjim osebam (kot so finančne institucije in družbe za izdelavo bonitetnih ocen). Osebne kreditne informacije se morajo obdelovati in posredovati tretji osebi v obliki, ki omogoča obdelavo z napravo za obdelavo podatkov (kot je računalnik).

(111) Kolikor zakon o uporabi in varstvu kreditnih informacij vsebuje posebna pravila glede na zakon o varstvu osebnih podatkov, Komisija meni, da tudi ta pravila zagotavljajo raven varstva, ki je v osnovi enakovredna tisti iz Uredbe (EU) 2016/679.

2.4 **Nadzor in izvrševanje**

(112) Da se zagotovi ustrezna raven varstva podatkov v praksi, bi bilo treba vzpostaviti neodvisen nadzorni organ, pooblaščen za spremljanje in zagotavljanje skladnosti s pravili o varstvu podatkov. Ta organ bi moral pri izvajanju svojih obveznosti in pooblastil ravnati popolnoma neodvisno in nepristransko.

2.4.1 *Neodvisen nadzor*

(113) V Republiki Koreji je neodvisen organ, pristojen za spremljanje in izvrševanje zakona o varstvu osebnih podatkov, komisija za varstvo osebnih podatkov. Sestavljajo jo predsednik, podpredsednik in sedem članov. Predsednika in podpredsednika imenuje predsednik republike po priporočilu predsednika vlade. Dva izmed članov komisije imenuje predsednik republike na priporočilo predsednika, pet pa na priporočilo parlamenta (od tega dva na

([138]) To vključuje splošno obveznost uradnega obveščanja (člen 32(7) zakona o uporabi in varstvu kreditnih informacij) in posebno obveznost glede preglednosti, če se informacije, iz katerih je razvidna kreditna sposobnost posameznika, zagotavljajo določenim subjektom, kot so bonitetne agencije in agencije za zbiranje kreditnih informacij (člen 35-3 zakona o uporabi in varstvu kreditnih informacij ter člen 30-3 uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij), ali kadar se razmerje, ki je podlaga za poslovne transakcije, zavrne ali odpove na podlagi osebnih kreditnih informacij, prejetih od tretje osebe (člen 36 zakona o uporabi in varstvu kreditnih informacij ter člen 31 uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij).

([139]) Člen 35 zakona o uporabi in varstvu kreditnih informacij. Za nekatere gospodarske organizacije, npr. zadruge in javna podjetja (člen 21(2) uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij), veljajo dodatne zahteve glede preglednosti, na primer da morajo nekatere informacije javno objaviti (člen 31 zakona o uporabi in varstvu kreditnih informacij) in da morajo posameznike obvestiti o morebitnih negativnih vplivih na njihovo bonitetno oceno, kadar sklepajo finančne transakcije, ki prinašajo kreditna tveganja (člen 35-2 zakona o uporabi in varstvu kreditnih informacij).

([140]) Glede pogojev in izjem od pravic do dostopa in popravka se uporabljajo pravila iz zakona o varstvu osebnih podatkov (opisana v uvodnih izjavah (76) in (77)). Poleg tega so podrobnejši pogoji določeni v členu 38(4) do (8) zakona o uporabi in varstvu kreditnih informacij ter členu 33 uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij. Zlasti velja, da mora gospodarski subjekt, ki je popravil ali izbrisal netočne kreditne informacije, o tem uradno obvestiti posameznika. Poleg tega je treba uradno obvestiti tretjo osebo, ki so ji bile take informacije razkrite v preteklih šestih mesecih, zadevni posameznik pa mora biti o tem obveščen. Če posameznik ni zadovoljen s tem, kako je bila obravnavana njegova zahteva za popravek, lahko vloži pritožbo pri komisiji za varstvo osebnih podatkov, ki preveri dejanja upravljavca in lahko naloži popravne ukrepe.

([141]) Člen 38-3 zakona o uporabi in varstvu kreditnih informacij.

priporočilo politične stranke, ki ji pripada predsednik, in tri na priporočilo drugih političnih strank (člen 7-2(2) zakona o varstvu osebnih podatkov), kar pomaga preprečevati pristranskost v postopku imenovanja) ([142]). Ta postopek je v skladu z zahtevami, ki se uporabljajo za imenovanje članov organov za varstvo podatkov v Uniji (člen 53(1) Uredbe (EU) 2016/679). Poleg tega se morajo vsi člani komisije vzdržati opravljanja dobičkonosnih poslovnih dejavnosti, političnega udejstvovanja in zasedbe funkcij v javni upravi ali parlamentu (člen 7-6 in člen 7-7(1), točka 3, zakona o varstvu osebnih podatkov) ([143]). Za vse člane komisije veljajo tudi posebna pravila, ki jim preprečujejo sodelovanje v razpravah v zadevi, v kateri je možnost navzkrižja interesov (člen 7-11 zakona o varstvu osebnih podatkov). Komisiji za varstvo osebnih podatkov pomaga sekretariat (člen 7-13), prav tako lahko komisija ustanovi pododbore (ki jih sestavljajo trije člani komisije), ki obravnavajo manjše kršitve in ponavljajoče se zadeve (člen 7-12 zakona o varstvu osebnih podatkov).

(114) Vsak član komisije za varstvo osebnih podatkov je imenovan za tri leta in je lahko enkrat ponovno imenovan (člen 7-4(1) zakona o varstvu osebnih podatkov). Člana komisije je mogoče odpoklicati le v posebnih okoliščinah, in sicer če ne zmore več opravljati svojih nalog zaradi dolgotrajne duševne ali telesne nezmožnosti, če krši zakon ali če je izpolnjen eden od pogojev za razrešitev s položaja ([144]) (člen 7-5 zakona o varstvu osebnih podatkov). To članom zagotavlja institucionalno zaščito pri izvajanju njihovih nalog.

(115) Splošneje, člen 7(1) zakona o varstvu osebnih podatkov izrecno zagotavlja neodvisnost komisije za varstvo osebnih podatkov, člen 7-5(2) navedenega zakona pa določa, da morajo člani komisije svoje naloge opravljati neodvisno, v skladu z zakonom in po svoji vesti ([145]). Opisani institucionalni in postopkovni zaščitni ukrepi, med drugim glede imenovanja in odpoklica članov komisije za varstvo osebnih podatkov, zagotavljajo, da lahko navedena komisija deluje povsem neodvisno, brez zunanjih vplivov ali navodil. Poleg tega komisija za varstvo osebnih podatkov kot osrednja upravna agencija vsako leto predlaga svoj proračun (ki ga ministrstvo za finance pregleda kot del splošnega nacionalnega proračuna, preden ga sprejme državni zbor) in je odgovorna za lastno kadrovsko vodenje. Trenutni proračun komisije za varstvo osebnih podatkov znaša približno 35 milijonov EUR, komisija pa ima 154 zaposlenih (vključno s 40 zaposlenimi, specializiranimi za informacijsko in komunikacijsko tehnologijo, 32 zaposlenimi, ki se osredotočajo na preiskave, in 40 pravnimi strokovnjaki).

(116) Naloge in pristojnosti komisije za varstvo osebnih podatkov so večinoma opredeljene v členih 7-8 in 7-9 ter členih 61-66 zakona o varstvu osebnih podatkov ([146]). Naloge komisije za varstvo osebnih podatkov vključujejo zlasti svetovanje o zakonodaji in predpisih v zvezi z varstvom podatkov, pripravo politik in smernic s področja varstva podatkov, preiskovanje kršitev pravic posameznikov, obravnavanje pritožb in mediacijo v sporih, zagotavljanje skladnosti z zakonom o varstvu osebnih podatkov, zagotavljanje izobraževanja in promocije na področju varstva podatkov ter izmenjavo in sodelovanje z organi za varstvo podatkov iz tretjih držav ([147]).

(117) Na podlagi člena 68 zakona o varstvu osebnih podatkov v povezavi s členom 62 uredbe o izvajanju zakona o varstvu osebnih podatkov so bile nekatere naloge komisije za varstvo osebnih podatkov prenesene na korejsko agencijo za splet in varnost, in sicer: (1) izobraževanje in odnosi z javnostmi, (2) usposabljanje strokovnjakov in razvoj meril za ocene učinka na zasebnost, (3) obravnavanje zahtev za imenovanje tako imenovane ustanove za izvajanje ocen učinka na zasebnost, (4) obravnavanje zahtev za posredni dostop do osebnih podatkov, ki jih hranijo javni organi (člen 35(2) zakona o varstvu osebnih podatkov), ter (5) izdajanje zahtev za gradivo in

([142]) Za člane komisije za varstvo osebnih podatkov so lahko imenovani le posamezniki, ki izpolnjujejo naslednja merila: višji državni uslužbenci, pristojni za zadeve v zvezi z osebnimi podatki; nekdanji sodniki, državni tožilci ali odvetniki z vsaj desetimi leti delovnih izkušenj; nekdanji vodstveni delavci z izkušnjami s področja varstva podatkov, ki so več kot tri leta delali v javnem organu ali organizaciji oziroma jih je priporočil tak organ ali organizacija; ter nekdanji izredni profesorji s strokovnim znanjem s področja varstva podatkov, ki so vsaj pet let delali v akademski ustanovi (člen 7-2 zakona o varstvu osebnih podatkov).

([143]) Glej tudi člen 4-2 uredbe o izvajanju zakona o varstvu osebnih podatkov.

([144]) Glej člen 7-7 zakona o varstvu osebnih podatkov, v skladu s katerim člani komisije za varstvo osebnih podatkov ne morejo postati posamezniki, ki niso državljani Koreje, in člani političnih strank. Enako velja za posameznike, ki jim je bila izrečena določena vrsta kazenske sankcije ali ki so bili v zadnjih petih letih razrešeni s funkcije zaradi disciplinske kršitve itd. (člen 7-7 zakona o varstvu osebnih podatkov v povezavi s členom 33 zakona o javnih uslužbencih).

([145]) Čeprav člen 7(2) zakona o varstvu osebnih podatkov določa splošno pristojnost predsednika vlade na podlagi člena 18 zakona o organizaciji vlade, da začasno zadrži ali prekliče – s soglasjem predsednika republike – katero koli nezakonito ali nepravično odločitev osrednjega upravnega organa, pa take pristojnosti nima glede preiskovalnih ali izvršilnih pooblastil komisije za varstvo osebnih podatkov (glej člen 7(2), točki 1 in 2, zakona o varstvu osebnih podatkov). Glede na pojasnila korejske vlade je namen člena 18 zakona o organizaciji vlade predsedniku vlade omogočiti ukrepanje v izrednih okoliščinah, kot je spor med več vladnimi agencijami. Vse od sprejetja te določbe leta 1963 še noben predsednik vlade ni uporabil te pristojnosti.

([146]) Kadar je treba izvesti naloge v skladu s členom 7-9(1) zakona o varstvu osebnih podatkov, lahko komisija za varstvo osebnih podatkov pridobi mnenja zadevnih javnih uslužbencev, strokovnjakov za varstvo podatkov, civilnih organizacij in zadevnih poslovnih subjektov. Poleg tega lahko komisija za varstvo osebnih podatkov zahteva ustrezno gradivo, izda priporočila za izboljšave in preverja, ali se ta priporočila izvajajo (člen 7-9(2)-(5) zakona o varstvu osebnih podatkov).

([147]) Glej tudi člen 9 zakona o varstvu osebnih podatkov (triletni krovni načrt za varstvo osebnih podatkov), člen 12 zakona o varstvu osebnih podatkov (standardne smernice za varstvo osebnih podatkov) in člen 13 zakona o varstvu osebnih podatkov (politike za spodbujanje in podpiranje samoregulacije).

izvajanje inšpekcijskih pregledov v zvezi s pritožbami, prejetimi prek tako imenovanega klicnega centra za vprašanja v zvezi z zasebnostjo. V okviru obravnavanja pritožb prek klicnega centra za vprašanja v zvezi z zasebnostjo korejska agencija za splet in varnost zadevo preda komisiji za varstvo osebnih podatkov ali tožilstvu, če ugotovi, da je bil kršen zakon. Možnost vložitve pritožbe prek klicnega centra za vprašanja v zvezi z zasebnostjo posameznikom ne preprečuje, da pritožbo vložijo neposredno pri komisiji za varstvo osebnih podatkov ali da se nanjo obrnejo, če menijo, da korejska agencija za splet in varnost njihove pritožbe ni zadovoljivo obravnavala.

2.4.2 *Izvrševanje, vključno s sankcijami*

(118) Da bi se zagotovila skladnost z zakonom o varstvu osebnih podatkov, je zakonodajalec komisiji za varstvo osebnih podatkov podelil preiskovalna in izvršilna pooblastila, ki segajo od izdajanja priporočil do izrekanja upravnih glob. Ta pooblastila dodatno dopolnjuje ureditev kazenskih sankcij.

(119) Glede preiskovalnih pooblastil velja, da lahko komisija za varstvo osebnih podatkov opravlja inšpekcijske preglede na kraju samem in od upravljavcev osebnih podatkov zahteva vse zadevno gradivo (kot so članki in dokumenti) (člen 63 zakona o varstvu osebnih podatkov v povezavi s členom 60 uredbe o izvajanju zakona o varstvu osebnih podatkov), če obstaja sum kršitve zakona o varstvu osebnih podatkov ali je bila taka kršitev prijavljena oziroma če je to potrebno za varstvo pravic posameznikov, na katere se nanašajo osebni podatki, pred kršitvami ([148]).

(120) Glede izvrševanja člen 61(2) zakona o varstvu osebnih podatkov določa, da lahko komisija za varstvo osebnih podatkov upravljavcem podatkov svetuje, kako izboljšati raven varstva osebnih podatkov pri posameznih dejavnostih obdelave. Upravljavci podatkov si morajo v dobri veri prizadevati za upoštevanje takih nasvetov in morajo komisijo za varstvo osebnih podatkov obveščati o rezultatih. Prav tako lahko komisija za varstvo osebnih podatkov, kadar obstajajo utemeljeni razlogi za sum, da je bil kršen zakon o varstvu osebnih podatkov, in bi neukrepanje verjetno povzročilo škodo, ki bi jo bilo težko odpraviti, naloži popravne ukrepe (člen 64(1) zakona o varstvu osebnih podatkov) ([149]). V oddelku 5 uradnega obvestila št. 2021-5 (Priloga I) je z zavezujočim učinkom pojasnjeno, da so ti pogoji izpolnjeni v zvezi s kršitvijo katere koli določbe zakona o varstvu osebnih podatkov, ki ščiti pravice do zasebnosti posameznikov v zvezi z osebnimi podatki ([150]). Ukrepi, ki jih lahko sprejme komisija za varstvo osebnih podatkov, vključujejo odreditev prenehanja ravnanja, ki povzroča kršitev, začasno prenehanje obdelave podatkov ali katere koli druge potrebne ukrepe. Za neizpolnitev popravnega ukrepa se lahko izreče globa v višini največ 50 milijonov KRW (člen 75(2), točka 13, zakona o varstvu osebnih podatkov).

(121) V zvezi z nekaterimi javnimi organi (kot so parlament, osrednji upravni organi, lokalni organi in sodišča) člen 64 (4) zakona o varstvu osebnih podatkov določa, da lahko komisija za varstvo osebnih podatkov „priporoči“ katerega koli od popravnih ukrepov, navedenih v uvodni izjavi (120), navedeni organi pa morajo tako priporočilo upoštevati, razen če gre za izredne okoliščine. V skladu z oddelkom 5 uradnega obvestila št. 2021-5 se to nanaša na izredne dejanske ali pravne okoliščine, za katere komisija za varstvo osebnih podatkov ob izdaji priporočila ni vedela. Zadevni javni organ se lahko na take izredne okoliščine sklicuje le, če jasno dokaže, da kršitve ni bilo, in komisija za varstvo osebnih podatkov ugotovi, da je res tako. V nasprotnem primeru mora javni organ upoštevati priporočilo komisije za varstvo osebnih podatkov in „sprejeti popravni ukrep, vključno s takojšnjim prenehanjem dejanja, v izjemnih primerih, ko je bilo nezakonito dejanje kljub temu storjeno, pa povrniti škodo“.

(122) Komisija za varstvo osebnih podatkov lahko od drugih upravnih agencij, ki imajo posebne pristojnosti v skladu s sektorsko zakonodajo (npr. zdravje, izobraževanje), zahteva, da same ali skupaj z njo izvedejo preiskavo (suma) kršitev zasebnosti s strani upravljavcev, ki delujejo v teh sektorjih pod njihovo pristojnostjo, in uvedejo korektivne ukrepe (člen 63(4)–(5) zakona o varstvu osebnih podatkov). V tem primeru komisija za varstvo osebnih podatkov opredeli razloge, predmet in obseg preiskave ([151]). Nato mora zadevni upravni organ komisiji za varstvo osebnih podatkov predložiti načrt preiskave in jo uradno obvestiti o rezultatih preiskave. Komisija za varstvo osebnih podatkov lahko priporoči sprejetje posebnega korektivnega ukrepa, ki ga mora zadevna agencija izvajati. V vsakem primeru lahko komisija za varstvo osebnih podatkov kljub taki zahtevi opravi lastno preiskavo ali izreče sankcije.

([148]) Komisija za varstvo osebnih podatkov lahko tudi vstopi v prostore upravljavca in preveri poslovno dejavnost, evidence, dokumente itd. (člen 63(2) zakona o varstvu osebnih podatkov). Glej tudi člen 45-3 zakona o uporabi in varstvu kreditnih informacij ter člen 36-4 uredbe o izvajanju zakona o uporabi in varstvu kreditnih informacij glede pristojnosti komisije za varstvo osebnih podatkov na podlagi navedenega zakona.

([149]) Glej tudi člen 45-4 zakona o uporabi in varstvu kreditnih informacij v zvezi s pristojnostmi komisije za varstvo osebnih podatkov na podlagi navedenega zakona.

([150]) Oddelek 5 uradnega obvestila določa, da se „upravičen razlog za domnevo, da je prišlo do kršitve varstva osebnih podatkov in da bi neukrepanje verjetno povzročilo škodo, ki bi jo bilo težko odpraviti, v smislu odstavkov 1 in 2 člena 64 zakona o varstvu osebnih podatkov, nanaša na kršitev katerega koli od načel, pravic in obveznosti iz zakona, katerih namen je varstvo pravic posameznikov glede osebnih podatkov“. Enako velja glede pristojnosti komisije za varstvo osebnih podatkov na podlagi člena 45-4 zakona o uporabi in varstvu kreditnih informacij.

([151]) Člen 60 uredbe o izvajanju zakona o varstvu osebnih podatkov.

(123) Poleg tega, da ima komisija za varstvo osebnih podatkov popravljalna pooblastila, lahko tudi izreka upravne globe v višini med 10 in 50 milijonov KRW za kršitve različnih zahtev zakona o varstvu osebnih podatkov (člen 75 navedenega zakona) ([152]). To med drugim vključuje neskladnost z zahtevami za zakonitost obdelave, nesprejetje potrebnih varnostnih ukrepov, neobveščanje posameznikov, na katere se nanašajo osebni podatki, o kršitvi varnosti podatkov, neskladnost z zahtevami za podobdelavo, nesprejetje in neobjavo politike zasebnosti, neimenovanje pooblaščene osebe za varstvo zasebnosti ali neukrepanje na podlagi zahteve posameznika, na katerega se nanašajo osebni podatki, kadar ta uresničuje svoje pravice, ter nekatere procesne kršitve (nesodelovanje med preiskavo). Če isti upravljavec krši več določb zakona o varstvu osebnih podatkov, se lahko za vsako kršitev naloži globa, pri določanju višine globe pa se upošteva število prizadetih posameznikov.

(124) Prav tako lahko komisija za varstvo osebnih podatkov, kadar obstaja utemeljen sum kršitve zakona o varstvu osebnih podatkov ali katerega koli drugega „predpisa, ki se nanaša na varstvo osebnih podatkov“, pri pristojnem preiskovalnem organu (npr. pri tožilcu) vloži ovadbo (glej člen 65(1) zakona o varstvu osebnih podatkov). Poleg tega lahko komisija za varstvo osebnih podatkov upravljavcu svetuje sprejetje disciplinskih ukrepov zoper odgovorno osebo (tudi zoper vodilne delavce, glej člen 65(2) zakona o varstvu osebnih podatkov). Upravljavec mora tak nasvet upoštevati ([153]) in komisijo za varstvo osebnih podatkov pisno obvestiti o rezultatih (glej člen 65 zakona o varstvu osebnih podatkov v povezavi s členom 58 uredbe o izvajanju zakona o varstvu osebnih podatkov).

(125) V zvezi z nasvetom na podlagi člena 61, popravnimi ukrepi na podlagi člena 64, obtožbo ali svetovanjem glede disciplinskih ukrepov na podlagi člena 65 in izrekom upravnih glob na podlagi člena 75 zakona o varstvu osebnih podatkov lahko komisija za varstvo osebnih podatkov dejstva javno objavi (tj. kršitev, subjekt, ki je kršil zakon, in izrečene ukrepe) na svojem spletnem mestu ali v splošnem dnevnem časopisu, ki izhaja na ozemlju celotne države (člen 66 zakona o varstvu osebnih podatkov v povezavi s členom 61(1) uredbe o izvajanju zakona o varstvu osebnih podatkov) ([154]).

(126) Nazadnje, skladnost z zahtevami o varstvu podatkov iz zakona o varstvu osebnih podatkov (in iz drugih „predpisov, ki se nanašajo na varstvo osebnih podatkov“) podpira tudi ureditev kazenskih sankcij. V tem smislu členi 70 do 73 zakona o varstvu osebnih podatkov vsebujejo kazenske določbe, na podlagi katerih se lahko izreče globa (med 20 in 100 milijoni KRW) ali zaporna kazen (najvišja je od dveh do deset let). Med zadevnimi kršitvami so uporaba osebnih podatkov ali njihovo zagotavljanje tretji osebi brez potrebne privolitve, obdelava občutljivih podatkov v nasprotju s prepovedjo iz člena 23(1) zakona o varstvu osebnih podatkov, neskladnost z veljavnimi zahtevami glede varnosti, če to povzroči izgubo, krajo, razkritje, ponarejanje ali spreminjanje osebnih podatkov ali poseganje vanje, nesprejetje potrebnih ukrepov za popravek, izbris ali prenehanje obdelave osebnih podatkov ali nezakonit prenos osebnih podatkov v tretjo državo ([155]). V skladu s členom 74 zakona o varstvu osebnih podatkov so v vsakem od navedenih primerov odgovorni zaposleni, zastopnik ali predstavnik upravljavca in sam upravljavec ([156]).

(127) Za zlorabo osebnih podatkov se lahko izrečejo kazenske sankcije, določene v zakonu o varstvu osebnih podatkov, lahko pa pomeni tudi kaznivo dejanje na podlagi kazenskega zakona. To velja zlasti v zvezi s kršitvijo zaupnosti pisanj, dokumentov ali elektronskih evidenc (člen 316), razkritjem informacij, za katere se šteje, da so poklicna skrivnost (člen 317), goljufijo z uporabo računalnika (člen 347-2) ter poneverbo in zlorabo zaupanja (člen 355).

(128) Korejski sistem torej združuje različne vrste sankcij, od popravnih ukrepov in upravnih glob do kazenskih sankcij, za katere je verjetno, da imajo še posebno močan odvračalni učinek na upravljavce in posameznike, ki ravnajo s podatki. Komisija za varstvo osebnih podatkov je takoj po ustanovitvi v letu 2020 začela uresničevati svoje pristojnosti. Iz letnega poročila komisije za varstvo osebnih podatkov za leto 2021 je razvidno, da je komisija

([152]) Prav tako lahko komisija za varstvo osebnih podatkov, če so bili postopki obdelave osebnih podatkov in varnostni sistemi upravljavca potrjeni kot skladni z zakonom o varstvu osebnih podatkov, vendar merila za izdajo takega potrdila na podlagi člena 34-2(1) uredbe o izvajanju zakona o varstvu osebnih podatkov dejansko niso bila izpolnjena, ali v primeru hude kršitve katerega koli „predpisa, ki se nanaša na varstvo osebnih podatkov“, potrdilo prekliče (člen 32-2(3) in (5) zakona o varstvu osebnih podatkov). Komisija o takem preklicu uradno obvesti upravljavca in preklic javno objavi oziroma ga objavi na svojem spletišču ali v uradnem listu (člen 34-4 uredbe o izvajanju zakona o varstvu osebnih podatkov). Upravne globe (člen 52 zakona o uporabi in varstvu kreditnih informacij) in kazenske sankcije (člen 50 zakona o uporabi in varstvu kreditnih informacij) se lahko izrečejo tudi za kršitve zakona o uporabi in varstvu kreditnih informacij.

([153]) V skladu s členom 58(2) uredbe o izvajanju zakona o varstvu osebnih podatkov mora upravljavec, če zaradi posebnih okoliščin nasveta „ni mogoče“ upoštevati, komisiji za varstvo osebnih podatkov to utemeljiti.

([154]) Pri odločanju o takem javnem razkritju komisija za varstvo osebnih podatkov upošteva vsebino in resnost kršitve, njeno trajanje in pogostost ter posledice (obseg škode). Zadevni subjekt je treba o tem vnaprej obvestiti in mu omogočiti obrambo. Glej člen 61 (2) in (3) uredbe o izvajanju zakona o varstvu osebnih podatkov.

([155]) Glej člen 71, točka 2, v povezavi s členom 18(1) zakona o varstvu osebnih podatkov (neupoštevanje pogojev iz člena 17(3) navedenega zakona, na katerega se sklicuje člen 18(1)). Glej tudi člen 75(2), točka 1, v povezavi s členom 17(2) zakona o varstvu osebnih podatkov (neobveščanje zadevnega posameznika na podlagi člena 17(2) navedenega zakona, na katerega se sklicuje člen 17(3)).

([156]) Poleg tega člen 74-2 zakona o varstvu osebnih podatkov omogoča zaseg denarja, blaga ali druge koristi, ki je bila pridobljena s kršitvijo, če zaseg ni mogoč, pa „odvzem“ nezakonito pridobljene koristi.

za varstvo osebnih podatkov že izdala številna priporočila in upravne globe ter odredila popravne ukrepe, tako za javni sektor (približno 34 javnih organov) kot za zasebne subjekte (približno 140 družb) ([157]). Med pomembnejšimi primeri je decembra 2020 neki družbi na primer izrekla globo v višini 6,7 milijarde KRW zaradi kršitve različnih določb zakona o varstvu osebnih podatkov (vključno z zahtevami glede varnosti, privolitve za zagotavljanje podatkov tretji osebi in preglednosti) ([158]), aprila 2021 pa je družbi s področja tehnologije umetne inteligence izrekla globo v višini 103,3 milijona KRW zaradi kršitve, med drugim, pravil o zakonitosti obdelave, zlasti privolitve, in obdelave psevdonimiziranih podatkov ([159]). Komisija za varstvo osebnih podatkov je avgusta 2021 dokončala še eno preiskavo dejavnosti treh družb, na podlagi katere so bili sprejeti korektivni ukrepi in naložene denarne kazni v višini do 6,47 milijarde (med drugim zaradi neobveščanja posameznikov o razkritju osebnih podatkov tretjim osebam, vključno s prenosi v tretje države) ([160]). Prav tako je Južna Koreja že pred nedavno reformo dosegala dobre rezultate pri izvrševanju, pri čemer so pristojni organi uporabljali najrazličnejše izvršilne ukrepe, vključno z upravnimi globami, popravnimi ukrepi in javnim razkrivanjem kršitev različnih upravljavcev, vključno s ponudniki komunikacijskih storitev (korejska komisija za komunikacije) ter gospodarskimi subjekti, finančnimi institucijami, javnimi organi, univerzami in bolnišnicami (ministrstvo za notranje zadeve in varnost) ([161]). Na podlagi navedenega Komisija ugotavlja, da korejski sistem zagotavlja učinkovito izvrševanje pravil o varstvu podatkov v praksi, s čimer zagotavlja raven varstva, ki je v osnovi enakovredna tisti iz Uredbe (EU) 2016/679.

2.5 **Pravno varstvo**

(129) Posameznik, na katerega se nanašajo osebni podatki, mora imeti na voljo učinkovito upravno in sodno varstvo, vključno z odškodnino za škodo, da se zagotovita ustrezno varstvo in zlasti uresničevanje pravic posameznika.

(130) Korejski sistem posameznikom zagotavlja različne mehanizme, s katerimi lahko učinkovito uresničujejo svoje pravice in dobijo (sodno) varstvo.

(131) V prvem koraku se lahko posamezniki, ki menijo, da so bile kršene njihove pravice oziroma interesi glede varstva podatkov, obrnejo na zadevnega upravljavca. V skladu s členom 30(1), točka 5, zakona o varstvu osebnih podatkov mora upravljavec v svojo politiko zasebnosti vključiti tudi informacije o pravicah posameznikov, na katere se nanašajo osebni podatki, in o tem, kako jih uresničevati. Poleg tega mora navesti kontaktne informacije (kot so ime in telefonska številka pooblaščene osebe za varstvo zasebnosti ali oddelka, ki je odgovoren za varstvo podatkov), da se lahko vložijo pritožbe. V organizacijski strukturi upravljavca je pooblaščena oseba za varstvo zasebnosti odgovorna za obravnavanje pritožb, sprejemanje popravnih ukrepov v primeru kršitve zasebnosti in priznavanje odškodnine (člen 31(2), točka 3, in člen 31(4) zakona o varstvu osebnih podatkov). Slednje je na primer pomembno v primeru kršitve varstva podatkov, saj mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, med drugim obvesti o kontaktnih točkah, pri katerih lahko prijavi morebitno škodo (člen 34(1), točka 5, zakona o varstvu osebnih podatkov).

(132) Poleg tega zakon o varstvu osebnih podatkov posameznikom zagotavlja več pravnih sredstev zoper upravljavce. Prvič, vsak posameznik, ki meni, da je upravljavec kršil njegove pravice ali interese glede varstva podatkov, lahko tako kršitev prijavi neposredno komisiji za varstvo osebnih podatkov in/ali enemu od specializiranih subjektov, ki jih je navedena komisija imenovala za sprejemanje in obravnavanje pritožb; to vključuje korejsko agencijo za splet in varnost, ki v ta namen vodi klicni center za vprašanja v zvezi z osebnimi podatki (tako imenovani klicni center za vprašanja v zvezi z zasebnostjo) (člen 62(1) in (2) zakona o varstvu osebnih podatkov v povezavi s členom 59 uredbe o izvajanju zakona o varstvu osebnih podatkov). Klicni center za vprašanja v zvezi z zasebnostjo preiskuje in ugotavlja kršitve, zagotavlja svetovanje v zvezi z obdelavo osebnih podatkov (člen 62(3) zakona o varstvu osebnih podatkov) ter lahko kršitve prijavi komisiji za varstvo osebnih podatkov (ne more

([157]) Glej letno poročilo komisije za varstvo osebnih podatkov 2021, str. 50 do 55 (na voljo le v korejščini), na naslovu https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK.

([158]) Glej na naslednji povezavi (na voljo le v korejščini): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) Glej na naslednji povezavi (na voljo le v korejščini): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) Glej na naslednji povezavi (na voljo le v korejščini): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Glej na primer letno poročilo za leto 2020 (na voljo le v korejščini) na povezavi https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 in primere, navedene v angleščini, na povezavi https://www.privacy.go.kr/eng/enforcement_02.do.

pa sam sprejeti izvršilnih ukrepov). Klicni center za vprašanja v zvezi z zasebnostjo prejme veliko število pritožb in zahtev (npr. 177 457 v letu 2020, 159 255 v letu 2019 in 164 497 v letu 2018) ([162]). Po informacijah, prejetih od komisije za varstvo osebnih podatkov, je komisija za varstvo osebnih podatkov med avgustom 2020 in avgustom 2021 sama prejel približno 1 000 pritožb. V odgovor na pritožbo lahko komisija za varstvo osebnih podatkov pristojnemu preiskovalnemu organu (vključno s tožilcem) poda nasvete za izboljšave, korektivne ukrepe, „obtožnico“ ali predlog za disciplinske ukrepe (glej člene 61, 64 in 65 zakona o varstvu osebnih podatkov). Odločitve komisije za varstvo osebnih podatkov (kot je zavrnitev obravnave pritožbe ali njena vsebinska zavrnitev) je mogoče izpodbijati na podlagi zakona o upravnem sporu ([163]).

(133) Drugič, členi 40 do 50 zakona o varstvu osebnih podatkov v povezavi s členi 48-14 do 57 uredbe o izvajanju zakona o varstvu osebnih podatkov določajo, da lahko posamezniki, na katere se nanašajo osebni podatki, vložijo zahtevke pri tako imenovanem odboru za mediacijo v sporih, v katerem so predstavniki, ki jih imenuje predsednik komisije za varstvo osebnih podatkov, in sicer izmed članov višje izvršilne službe navedene komisije, in posamezniki, ki so na podlagi svojih izkušenj na področju varstva podatkov imenovani iz določenih upravičenih skupin (glej člen 40(2), (3) in (7) zakona o varstvu osebnih podatkov ter člen 48-14 uredbe o izvajanju zakona o varstvu osebnih podatkov) ([164]). Možnost uporabe mediacije pred odborom za mediacijo v primeru sporov zagotavlja alternativno možnost za pridobitev odškodnine, vendar ne omejuje pravice posameznika, da se namesto tega obrne na komisijo za varstvo osebnih podatkov ali sodišče. V okviru obravnave zadeve lahko odbor od strank v sporu zahteva predložitev potrebnega gradiva in/ali k pričanju pozove zadevne priče (člen 45 zakona o varstvu osebnih podatkov). Ko je zadeva razjasnjena, odbor pripravi osnutek mediacijskega dogovora ([165]), s katerim se mora strinjati večina članov odbora. Osnutek lahko vključuje prenehanje kršitve, potrebne popravne ukrepe (vključno z vrnitvijo v prejšnje stanje ali odškodnino) in vse druge ukrepe, ki so morda potrebni, da se prepeči ponovitev take ali podobne kršitve (člen 47(1) zakona o varstvu osebnih podatkov). Če se z mediacijskim dogovorom strinjata obe stranki, ima enak učinek kot sodna poravnava (člen 47(5) zakona o varstvu osebnih podatkov). Stranki lahko med postopkom mediacije vložita tudi tožbo pri sodišču, v takem primeru pa se mediacija prekine (glej člen 48(2) zakona o varstvu osebnih podatkov) ([166]). Letni podatki, ki jih objavi komisija za varstvo osebnih podatkov, kažejo, da posamezniki redno uporabljajo postopek pred odborom za mediacijo v primeru sporov, ki pogosto privede do uspešnega izida. Odbor je na primer leta 2020 obravnaval 126 zadev, od katerih jih je bilo 89 rešenih pred odborom (77 primerov, v katerih sta stranki dosegli dogovor že pred koncem postopka mediacije, 12 zadev, v katerih so stranke sprejele predlog mediacije), kar pomeni 70,6-odstotno stopnjo mediacije ([167]). Podobno je odbor v letu 2019 obravnaval 139 primerov, od katerih jih je bilo 92 rešenih, kar pomeni 62,2-odstotno stopnjo mediacije.

(134) Nadalje, če vsaj 50 posameznikov utrpi škodo ali če so njihove pravice do varstva podatkov kršene na isti ali podoben način, pri čemer kršitev izhaja iz istega dogodka ali dogodka iste vrste ([168]), lahko posameznik, na katerega se nanašajo osebni podatki, ali organizacija za varstvo podatkov v imenu take skupine vloži vlogo za kolektivno mediacijo; postopku mediacije se lahko pridružijo še drugi posamezniki, na katere se nanašajo osebni podatki, saj odbor za mediacijo v sporih uvedbo takega postopka javno objavi (člen 49(1) do (3) zakona o varstvu osebnih podatkov v povezavi s členi 52 do 54 uredbe o izvajanju zakona o varstvu osebnih podatkov) ([169]). Odbor za mediacijo v sporih lahko vsaj eno osebo, ki najustrezneje zastopa skupne interese, izbere za predstavnika (člen 49(4) zakona o varstvu osebnih podatkov). Če upravljavec zavrne kolektivno mediacijo ali ne

([162]) Glej letno poročilo komisije za varstvo osebnih podatkov za leto 2021, str. 174. Leta 2020 so se take pritožbe nanašale na primer na zbiranje podatkov brez privolitve, neizpolnjevanje obveznosti glede preglednosti, kršitve zakona o varstvu osebnih podatkov s strani obdelovalcev, nezadostne varnostne ukrepe, neodzivnost na zahteve posameznikov, na katere se nanašajo osebni podatki, in splošne preiskave.

([163]) Posamezniki se lahko zlasti pritožijo nad izvajanjem javnih pooblastil upravnega organa ali zavrnitvijo njihovega izvajanja (člen 2 (1), točka 1, in člen 3, točka 1, zakona o upravnem sporu). Več informacij o procesnih vidikih, vključno z zahtevami glede dopustnosti, vsebuje uvodna izjava (181).

([164]) Vsi člani so imenovani za določen čas, razrešiti pa jih je mogoče le iz upravičenih razlogov (glej člen 40(5) in člen 41 zakona o varstvu osebnih podatkov). Poleg tega člen 42 zakona o varstvu osebnih podatkov vsebuje zaščitne ukrepe zoper navzkrižje interesov.

([165]) Glej člen 44 zakona o varstvu osebnih podatkov. Poleg tega lahko tudi predloži osnutek poravnave in priporoči poravnavo brez mediacije (glej člen 46 zakona o varstvu osebnih podatkov).

([166]) Poleg tega lahko odbor zavrne mediacijo, če meni, da ta ni primerna zaradi narave spora ali ker je bila vloga za mediacijo vložena z nepoštenimi nameni (člen 48 zakona o varstvu osebnih podatkov).

([167]) Glej letno poročilo komisije za varstvo osebnih podatkov za leto 2021, str.179 in 180. Ti primeri so se med drugim nanašali na kršitve zahteve po pridobitvi privolitve za zbiranje podatkov, načela omejitve namena in pravic posameznika, na katerega se nanašajo osebni podatki.

([168]) Glej člen 49(1) zakona o varstvu osebnih podatkov, ki določa, da morajo posamezniki, na katere se nanašajo osebni podatki, utrpeti škodo ali poseg v svoje pravice „na enak ali podoben način“, in člen 52, točka 2, uredbe o izvajanju zakona o varstvu osebnih podatkov, ki določa, da morajo imeti „pomembni vidiki dogodka podobno dejansko ali pravno stanje“.

([169]) Poleg tega imajo lahko koristi od dogovora, ki ga upravljavec sklene v okviru kolektivne mediacije, tudi subjekti, ki niso stranke v mediaciji, saj lahko odbor za mediacijo v sporih upravljavcu svetuje pripravo in predložitev odškodninskega načrta, ki vključuje (tudi) take subjekte (člen 49(5) zakona o varstvu osebnih podatkov).

sprejme mediacijskega dogovora, lahko nekatere organizacije ([170]) vložijo skupinsko tožbo zaradi kršitve (členi 51 do 57 zakona o varstvu osebnih podatkov).

(135) Tretjič, v primeru kršitve zasebnosti, zaradi katere posameznik utrpi „škodo“, ima posameznik, na katerega se nanašajo osebni podatki, pravico do ustreznega pravnega varstva v „hitrem in poštenem postopku“ (člen 4, točka 5, in člen 39 zakona o varstvu osebnih podatkov) ([171]). Upravljavec se lahko razbremeni odgovornosti, če dokaže, da mu ni mogoče očitati krivde (naklepa ali malomarnosti). Če posameznik, na katerega se nanašajo osebni podatki, utrpi škodo zaradi izgube, kraje, razkritja, ponarejanja, spreminjanja ali poškodovanja njegovih osebnih podatkov, mu lahko sodišče dodeli odškodnino do višine trikratnika vrednosti dejanske škode, pri čemer upošteva več dejavnikov (člen 39(3) in (4) zakona o varstvu osebnih podatkov). Posameznik, na katerega se nanašajo osebni podatki, pa lahko zahteva tudi „razumno“ odškodnino, ki ne presega 3 milijone KRW (člen 39-2 (1) in (2) zakona o varstvu osebnih podatkov). Poleg tega se lahko v skladu s civilnim zakonom odškodnina zahteva od katere koli osebe, „ki z nezakonitim dejanjem, naklepno ali iz malomarnosti, povzroči izgubo ali škodo drugi osebi“ ([172]), ali od osebe, „ki je škodila telesu, svobodi ali ugledu druge osebe ali je povzročila kakršne koli duševne bolečine drugi osebi“ ([173]). Tako civilno odgovornost zaradi kršitve pravil o varstvu podatkov je potrdilo tudi vrhovno sodišče ([174]). Če je bila škoda povzročena z nezakonitim dejanjem javnega organa, se lahko odškodninski zahtevek vloži tudi na podlagi zakona o državni odškodnini ([175]). Zahtevek na podlagi zakona o državni odškodnini se lahko vloži pri specializiranem „odškodninskem odboru“ ali neposredno pri korejskih sodiščih ([176]). Odgovornost države vključuje tudi nepremoženjsko škodo (npr. duševne bolečine) ([177]). Če je žrtev tuji državljan, se zakon o državni odškodnini uporablja, če država izvora take osebe enako zagotavlja državno odškodnino korejskim državljanom ([178]).

(136) Četrtič, vrhovno sodišče je posameznikom priznalo pravico, da zahtevajo sodno prepoved kršitev svojih ustavnih pravic, vključno s pravico do varstva osebnih podatkov ([179]). V tem okviru lahko sodišče upravljavcem na primer odredi prekinitev nezakonite dejavnosti ali njeno dokončno prenehanje. Poleg tega je mogoče pravice do varstva podatkov, vključno s tistimi, ki jih varuje zakon o varstvu osebnih podatkov, uresničevati prek civilnih tožb. To horizontalno uporabo ustavnega varstva zasebnosti v razmerjih med zasebniki je priznalo vrhovno sodišče ([180]).

([170]) To so skupine za varstvo potrošnikov ali nepridobitne nevladne organizacije z določenim številom članov, katerih prijavljena dejavnost je varstvo podatkov (čeprav v primeru slednjih velja dodatna zahteva, da vsaj 100 posameznikov, na katere se nanašajo osebni podatki in ki so utrpeli enako kršitev ali kršitev enake vrste, vloži zahtevo za vložitev kolektivne tožbe). Glej člen 51 zakona o varstvu osebnih podatkov.

([171]) Členi 43 do 43-3 zakona o uporabi in varstvu kreditnih informacij prav tako določajo odgovornost za povračilo škode, ki izhaja iz kršitev navedenega zakona.

([172]) Člen 750 civilnega zakona.

([173]) Člen 751(1) civilnega zakona.

([174]) Glej na primer odločbo vrhovnega sodišča št. 2015Da251539, 251546, 251553, 251560, 251577 z dne 30. maja 2018. Poleg tega je vrhovno sodišče potrdilo, da se lahko na podlagi civilnega zakona dodeli odškodnina zaradi kršitev varnosti podatkov, glej odločbo vrhovnega sodišča št. 2011Da59834, 59858, 59841 z dne 26. decembra 2012 (angleški povzetek je na voljo na naslovu: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). V tem primeru je vrhovno sodišče pojasnilo, da je treba pri oceni, ali je posameznik utrpel duševne bolečine, za katere je mogoče dodeliti odškodnino, upoštevati več dejavnikov, na primer vrsto in značilnosti razkritih informacij, možnost identifikacije posameznika zaradi kršitve, možnost dostopa tretjih oseb do podatkov, razširjenost osebnih podatkov po razkritju, vprašanje, ali je to povzročilo dodatne kršitve posameznikovih pravic, kako so bili osebni podatki upravljani in zaščiteni itd.

([175]) Na podlagi zakona o državni odškodnini lahko posamezniki zahtevajo odškodnino za škodo, ki jo javni uslužbenci povzročijo pri opravljanju svojih uradnih dolžnosti v nasprotju z zakonom (člen 2(1) navedenega zakona).

([176]) Člena 9 in 12 zakona o državni odškodnini. Z zakonom so ustanovljeni okrožni odbori (ki jim predseduje namestnik tožilca pristojnega tožilstva), osrednji odbor (ki mu predseduje namestnik ministra za pravosodje) in posebni odbor (ki obravnava odškodninske zahtevke v zvezi s škodo, ki jo povzroči vojaško osebje ali civilisti, zaposleni v vojski, predseduje pa mu namestnik ministra za narodno obrambo). Odškodninske zahtevke načeloma obravnavajo okrožni odbori, ki morajo v nekaterih okoliščinah take zadeve predati osrednjemu/posebnemu odboru, na primer če odškodnina presega določen znesek ali če posameznik zahteva ponovno odločanje. Člane vseh odborov imenuje minister za pravosodje (npr. izmed javnih uslužbencev ministrstva za pravosodje, pravosodnih uradnikov, odvetnikov in oseb, ki imajo strokovno znanje s področja državnih odškodnin), zanje pa veljajo posebna pravila glede navzkrižja interesov (glej člen 7 uredbe o izvajanju zakona o državni odškodnini).

([177]) Glej člen 8 zakona o državni odškodnini (ki se sklicuje na civilni zakon) in člen 751 civilnega zakona.

([178]) Člen 7 zakona o državni odškodnini.

([179]) Odločba vrhovnega sodišča št. 93Da40614 z dne 12. aprila 1996 in odločba št. 2008Da42430 z dne 2. septembra 2011 (angleški povzetek je na voljo na: https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Glej na primer odločbo vrhovnega sodišča št. 2008Da42430 z dne 2. septembra 2011 (angleški povzetek je na voljo na: https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) Nazadnje, posamezniki lahko na podlagi zakona o kazenskem postopku (člen 223) vložijo ovadbo pri državnem tožilcu ali pravosodnem policistu ([181]).

(138) Korejski sistem torej zagotavlja več načinov za uveljavljanje pravnega varstva, od lahko dostopnih in cenovno ugodnih možnosti (npr. prek klicnega centra za vprašanja v zvezi z zasebnostjo ali s (kolektivno) mediacijo) do upravnih (pred komisijo za varstvo osebnih podatkov) in sodnih pravnih sredstev, vključno z možnostjo pridobitve odškodnine.

3. DOSTOP DO OSEBNIH PODATKOV, KI JIH IZ EVROPSKE UNIJE PRENESEJO JAVNI ORGANI V REPUBLIKI KOREJI, IN UPORABA TEH PODATKOV

(139) Komisija je proučila tudi omejitve in zaščitne ukrepe, vključno z nadzorom in posameznimi mehanizmi pravnih sredstev, ki so na voljo v korejskem pravu glede zbiranja in naknadne uporabe osebnih podatkov s strani korejskih javnih organov, tj. podatkov, ki se v javnem interesu (zlasti za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter nacionalne varnosti („vladni dostop“)) prenašajo upravljavcem v Koreji. V zvezi s tem je korejska vlada Komisiji predložila uradne navedbe, zagotovila in zaveze, podpisane na najvišji ministrski in agencijski ravni, ki jih vsebuje Priloga II k temu sklepu.

(140) Komisija je pri oceni, ali pogoji, pod katerimi vlada dostopa do podatkov, prenesenih v Korejo, na podlagi tega sklepa izpolnjujejo preskus „osnovne enakovrednosti“ na podlagi člena 45(1) Uredbe (EU) 2016/679, kakor ga razlaga Sodišče Evropske unije glede na Listino o temeljnih pravicah, upoštevala zlasti naslednja merila.

(141) Prvič, vsaka omejitev pravice do varstva osebnih podatkov mora biti določena v zakonu, pravna podlaga, ki dovoljuje poseganje v tako pravico, pa mora že sama opredeljevati obseg omejitve izvrševanja zadevne pravice ([182]).

(142) Drugič, da se izpolni zahteva glede sorazmernosti, v skladu s katero se lahko odstopanja od varstva osebnih podatkov in omejitve tega varstva uporabljajo le, kolikor je to nujno potrebno v demokratični družbi, da se dosežejo specifični cilji splošnega interesa, ki so enakovredni interesom, priznanim v Uniji, morajo biti z zakonodajo zadevne tretje države, ki dovoljuje poseganje, določena jasna in natančna pravila, ki urejajo obseg in uporabo zadevnih ukrepov, ter minimalne zahteve, tako da imajo osebe, katerih podatki so bili preneseni, na voljo zadostna jamstva, ki omogočajo učinkovito varovanje njihovih osebnih podatkov pred tveganjem zlorab ([183]). V zakonodaji mora biti zlasti navedeno, v kakšnih okoliščinah in pod katerimi pogoji je mogoče sprejeti ukrep, ki določa obdelavo takih podatkov ([184]), izpolnjevanje teh zahtev pa mora biti podvrženo neodvisnemu nadzoru ([185]).

(143) Tretjič, navedena zakonodaja in njene zahteve morajo biti pravno zavezujoče po nacionalnem pravu. To zadeva zlasti organe zadevne tretje države, vendar morajo biti take pravne zahteve zoper navedene organe izvršljive tudi pred sodišči ([186]). Posamezniki, na katere se nanašajo osebni podatki, morajo zlasti imeti možnost uveljavljanja pravnih sredstev pred neodvisnim in nepristranskim sodiščem, da si tako zagotovijo dostop do osebnih podatkov, ki se nanje nanašajo, ali dosežejo popravek oziroma izbris takih podatkov ([187]).

3.1 Splošni pravni okvir

(144) Omejitve in zaščitni ukrepi, ki se uporabljajo glede zbiranja in naknadne uporabe osebnih podatkov s strani korejskih javnih organov, izhajajo iz krovnega ustavnega okvira, posebnih zakonov, ki urejajo njihovo dejavnost na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter nacionalne varnosti, pa tudi iz pravil, ki veljajo posebej za obdelavo osebnih podatkov.

([181]) Kot je pojasnjeno v uvodni izjavi (127), se lahko zloraba podatkov po kazenskem zakonu šteje za kaznivo dejanje.

([182]) Glej sodbo v zadevi Schrems II, točki 174 in 175 ter navedena sodna praksa. Glede dostopa javnih organov držav članic glej tudi sodbo z dne 6. oktobra 2020, Privacy International, C-623/17, EU:C:2020:790, točka 65, in sodbo z dne 6. oktobra 2020, La Quadrature du Net in drugi, združene zadeve C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točka 175.

([183]) Glej sodbo v zadevi Schrems II, točki 176 in 181 ter navedena sodna praksa. Glede dostopa javnih organov držav članic glej tudi sodbi v zadevi Privacy International, točka 68, in v zadevi La Quadrature du Net in drugi, točka 132.

([184]) Glej sodbo v zadevi Schrems II, točka 176. Glede dostopa javnih organov držav članic glej tudi sodbi v zadevi Privacy International, točka 68, in v zadevi La Quadrature du Net in drugi, točka 132.

([185]) Glej sodbo v zadevi Schrems II, točka 179.

([186]) Glej sodbo v zadevi Schrems II, točki 181 in 182.

([187]) Glej sodbo v zadevi Schrems I, točka 95, in sodbo v zadevi Schrems II, točka 194. V zvezi s tem je Sodišče Evropske unije poudarilo predvsem, da skladnost s členom 47 Listine o temeljnih pravicah, ki zagotavlja pravico do učinkovitega pravnega sredstva pred neodvisnim in nepristranskim sodiščem, „prispeva k ravni varstva, ki se zahteva v Uniji, in katere spoštovanje mora Komisija ugotoviti, preden sprejme sklep o ustreznosti na podlagi člena 45(1) Splošne uredbe o varstvu podatkov“ (sodba v zadevi Schrems II, točka 186).

(145) Prvič, dostop korejskih javnih organov do osebnih podatkov urejajo splošna načela zakonitosti, nujnosti in sorazmernosti, ki izhajajo iz korejske ustave ([188]). Zlasti temeljne pravice in svoboščine (vključno s pravico do zasebnosti in pravico do zasebnosti komunikacij) ([189]) se lahko omejijo le z zakonom in kadar je to potrebno zaradi nacionalne varnosti ali ohranjanja javnega reda in miru v javno dobro. Take omejitve ne smejo vplivati na bistvo zadevne pravice ali svoboščine. Zlasti glede preiskav in zasegov ustava določa, da se lahko izvajajo le v skladu z zakonom, na podlagi odredbe sodnika in v ustreznem pravnem postopku ([190]). Nazadnje, posamezniki lahko svoje pravice in svoboščine uresničujejo pred ustavnim sodiščem, če menijo, da so jim jih kršili javni organi pri izvrševanju svojih pristojnosti ([191]). Podobno velja, da lahko posamezniki zahtevajo pravično odškodnino, če so utrpeli škodo zaradi nezakonitega dejanja javnega uslužbenca, storjenega med opravljanjem uradnih dolžnosti ([192]).

(146) Drugič, kot je podrobneje opisano v oddelkih 3.2.1 in 3.3.1, se splošna načela, navedena v uvodni izjavi (145), odražajo tudi v specifičnih zakonih, ki urejajo pooblastila organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter organov za nacionalno varnost. V zvezi s preiskavami kaznivih dejanj na primer zakon o kazenskem postopku določa, da je mogoče obvezne ukrepe izreči le, če jih navedeni zakon izrecno določa, in v najmanjšem možnem obsegu, ki je potreben za dosego namena preiskave ([193]). Podobno člen 3 zakona o varstvu zasebnosti komunikacij prepoveduje dostop do zasebnih komunikacij, razen na podlagi zakona ter ob upoštevanju v zakonu navedenih omejitev in zaščitnih ukrepov. Na področju nacionalne varnosti zakon o nacionalni obveščevalni službi določa, da mora biti vsak dostop do podatkov o komunikaciji ali lokaciji skladen z zakonom, za zlorabo pooblastil in kršitve zakona pa so predvidene kazenske sankcije ([194]).

(147) Tretjič, za obdelavo osebnih podatkov s strani javnih organov, vključno z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter organi za nacionalno varnost, veljajo pravila o varstvu podatkov iz zakona o varstvu osebnih podatkov ([195]). Na splošno člen 5(1) zakona o varstvu osebnih podatkov določa, da morajo javni organi oblikovati politike za preprečevanje „zlorabe in nepravilne uporabe osebnih podatkov, nediskretnega nadzora in sledenja itd. ter krepitev dostojanstva ljudi in zasebnosti posameznikov“. Poleg tega mora vsak upravljavec osebne podatke obdelovati tako, da se čim bolj zmanjša možnost kršitve zasebnosti posameznika, na katerega se nanašajo osebni podatki (člen 3(6) zakona o varstvu osebnih podatkov).

(148) Vse zahteve iz zakona o varstvu osebnih podatkov, kot so podrobneje opisane v oddelku 2, se uporabljajo za obdelavo osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. To vključuje osnovna načela (kot so zakonitost in poštenost, omejitev namena, točnost, najmanjši obseg podatkov, omejitev hrambe, varnost in preglednost), obveznosti (npr. glede uradnega obveščanja o kršitvi varnosti podatkov in glede občutljivih podatkov) in pravice (do dostopa, popravka, izbrisa in prenehanja obdelave).

(149) Čeprav se za obdelavo osebnih podatkov za namene nacionalne varnosti uporablja bolj omejen sklop določb zakona o varstvu osebnih podatkov, pa se osnovna načela ter pravila glede nadzora, izvrševanja in pravnega varstva uporabljajo v celoti ([196]). Natančneje, člena 3 in 4 zakona o varstvu osebnih podatkov določata splošna načela varstva podatkov (zakonitost in poštenost, omejitev namena, točnost, najmanjši obseg podatkov, varnost in preglednost) in pravice posameznika (do obveščenosti, dostopa, popravka, izbrisa in prenehanja obdelave) ([197]). S členom 4(5) zakona o varstvu osebnih podatkov se posameznikom priznava pravica do ustreznega pravnega varstva za vsako škodo, ki izhaja iz obdelave njihovih osebnih podatkov, v hitrem in poštenem postopku. To je dopolnjeno z bolj specifičnimi obveznostmi, da se osebni podatki obdelujejo le v najmanjšem možnem obsegu, da se doseže želeni namen, in za najkrajše možno obdobje, da se vzpostavijo potrebni ukrepi za zagotavljanje

([188]) Glej Prilogo II, oddelek 1.1.
([189]) Člen 37(2) ustave.
([190]) Člen 16 in člen 12(3) ustave. V členu 12(3) ustave so nadalje opredeljene izjemne okoliščine, v katerih se lahko preiskava ali zaseg opravi brez odredbe (čeprav se še vedno zahteva naknadna odredba), na primer kadar je storilec zaloten pri storitvi kaznivega dejanja ali če gre za kaznivo dejanje, za katero je zagrožena zaporna kazen najmanj treh let, če obstaja tveganje za uničenje dokazov ali izginotje osumljenca.
([191]) Člen 68(1) zakona o ustavnem sodišču.
([192]) Člen 29(1) ustave.
([193]) Člen 199(1) zakona o kazenskem postopku. Splošneje velja, da morajo javni organi pri izvrševanju pooblastil na podlagi zakona o kazenskem postopku upoštevati temeljne pravice osumljencev za kazniva dejanja in vseh drugih zadevnih oseb (člen 198(2) zakona o kazenskem postopku).
([194]) Člen 14 zakona o nacionalni obveščevalni službi.
([195]) Glej Prilogo II, oddelek 1.2.
([196]) Člen 58(1), točka 2, zakona o varstvu osebnih podatkov. Glej tudi oddelek 6 uradnega obvestila št. 2021-5 (Priloga I). Izvzetje iz nekaterih določb zakona o varstvu osebnih podatkov se uporablja le, kadar se osebni podatki obdelujejo „za namene nacionalne varnosti“. Ko se nacionalne varnostne razmere, ki upravičujejo obdelavo podatkov, končajo, se ni več mogoče sklicevati na izvzetje in veljajo vse zahteve iz zakona o varstvu osebnih podatkov.
([197]) Take pravice se lahko omejijo le, če to določa zakon, in sicer v obsegu in trajanju, kot je potrebno in sorazmerno, da se zaščiti pomemben cilj v javnem interesu, ali kadar bi priznanje pravice lahko ogrozilo življenje ali telo tretje osebe oziroma bi pomenilo neupravičeno poseganje v premoženjske in druge interese tretje osebe. Glej oddelek 6 uradnega obvestila št. 2021-5.

varnega upravljanja podatkov in njihovo ustrezno obdelavo (npr. tehnični, upravljavski in fizični zaščitni ukrepi) ter da se vzpostavijo ukrepi za ustrezno obravnavo pritožb posameznikov ([198]). Nazadnje, splošna načela zakonitosti, nujnosti in sorazmernosti iz korejske ustave (glej uvodno izjavo (145)) se uporabljajo tudi za obdelavo osebnih podatkov za namene nacionalne varnosti.

(150) Posamezniki se lahko na te splošne omejitve in zaščitne ukrepe sklicujejo pred neodvisnimi nadzornimi organi (npr. pred komisijo za varstvo osebnih podatkov in/ali nacionalno komisijo za človekove pravice, glej uvodni izjavi (177) in (178)) in sodišči (glej uvodne izjave (179) do (183)) ter tako uveljavljajo pravno varstvo.

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

(151) Pravo Republike Koreje določa več omejitev glede dostopa do osebnih podatkov in njihove uporabe za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter zagotavlja nadzorne mehanizme in mehanizme pravnih sredstev, ki so v skladu z zahtevami iz uvodnih izjav (141) do (143) tega sklepa. Pogoji, pod katerimi je tak dostop mogoč, in zaščitni ukrepi glede uporabe teh pooblastil so podrobneje ocenjeni v naslednjih oddelkih.

3.2.1 *Pravna podlaga, omejitve in zaščitni ukrepi*

(152) Osebne podatke, ki jih bodo obdelovali korejski upravljavci in bodo preneseni iz Unije na podlagi tega sklepa ([199]), lahko korejski organi zbirajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj v okviru preiskav ali zasegov (na podlagi zakona o kazenskem postopku), in sicer z dostopom do podatkov o komunikaciji (na podlagi zakona o varstvu zasebnosti komunikacij) ali s pridobitvijo podatkov o naročnikih na podlagi zahteve za prostovoljno razkritje (na podlagi zakona o zagotavljanju telekomunikacijskih storitev) ([200]).

3.2.1.1 Preiskave in zasegi

(153) Zakon o kazenskem postopku določa, da se lahko preiskava ali zaseg opravi le, če je oseba osumljena kaznivega dejanja, če je to potrebno za preiskavo in če je dokazana povezava med preiskavo in osebo, ki se preiskuje, ali predmetom, ki ga je treba preiskati ali zaseči ([201]). Poleg tega se lahko preiskava ali zaseg (kot vsak obvezni ukrep) dovoli/opravi le v najmanjšem potrebnem obsegu ([202]). Če se preiskava nanaša na računalniški disk ali drug nosilec podatkov, se načeloma zasežejo le potrebni podatki (ki se kopirajo ali natisnejo), ne pa celoten nosilec podatkov ([203]). Nosilec podatkov se lahko zaseže le, kadar praktično ni mogoče ločeno natisniti ali kopirati potrebnih podatkov ali kadar namena preiskave praktično ni mogoče doseči drugače ([204]). Zakon o kazenskem postopku zato določa jasna in natančna pravila o obsegu in uporabi teh ukrepov, s čimer zagotavlja, da je poseganje v pravice posameznikov v primeru preiskave ali zasega omejeno na tisto, kar je v konkretni kazenski preiskavi potrebno in sorazmerno glede na namen.

([198]) Člen 58(4) zakona o varstvu osebnih podatkov.

([199]) Glej Prilogo II, oddelek 2.1. Uradna navedba korejske vlade (Priloga II, oddelek 2.1) se sklicuje tudi na možnost zbiranja informacij o finančnih transakcijah za namene preprečevanja pranja denarja in financiranja terorizma na podlagi zakona o sporočanju in uporabi specifičnih informacij o finančnih transakcijah. Vendar pa navedeni zakon določa obveznosti razkritja le za upravljavce, ki osebne kreditne informacije obdelujejo na podlagi zakon o uporabi in varstvu kreditnih informacij ter jih nadzoruje komisija za finančne storitve (glej uvodno izjavo (13)). Ker obdelava osebnih kreditnih informacij s strani takih upravljavcev ne spada na področje uporabe tega sklepa, zakon o sporočanju in uporabi specifičnih informacij o finančnih transakcijah ni relevanten za to oceno.

([200]) V členu 3 zakona o varstvu zasebnosti komunikacij je kot možna pravna podlaga za zbiranje podatkov o komunikaciji naveden tudi zakon o vojaškem sodišču. Vendar pa navedeni zakon ureja zbiranje informacij o vojaškem osebju, za civiliste pa se lahko uporablja le v omejenih primerih (npr. če bi vojaško osebje in civilisti skupaj storili kaznivo dejanje ali če posameznik stori kaznivo dejanje zoper vojsko, je mogoče postopke začeti pred vojaškim sodiščem, glej člen 2 zakona o vojaškem sodišču). Vsekakor vsebuje splošne določbe, ki urejajo preiskave in zasege ter so podobne tistim iz zakona o kazenskem postopku (glej npr. člene 146 do 149 in 153 do 156 zakona o vojaškem sodišču), pri čemer na primer določa, da se lahko poštne pošiljke zbirajo le, če je to potrebno za preiskavo in na podlagi odredbe vojaškega sodišča. Če bi se elektronske komunikacije zbirale na podlagi navedenega zakona, bi se uporabljale omejitve in zaščitni ukrepi iz zakona o varstvu zasebnosti komunikacij. Glej Prilogo II, oddelek 2.2.2, in opombo 50.

([201]) Člen 215(1) in (2) zakona o kazenskem postopku. Glej tudi člen 106(1) ter člena 107 in 109 zakona o kazenskem postopku, ki določajo, da sodišča lahko opravljajo preiskave in zasege, če so zadevni predmeti ali osebe povezani s konkretno zadevo. Glej Prilogo II, oddelek 2.2.1.2.

([202]) Člen 199(1) zakona o kazenskem postopku.

([203]) Člen 106(3) zakona o kazenskem postopku.

([204]) Člen 106(3) zakona o kazenskem postopku.

(154) Glede postopkovnih zaščitnih ukrepov zakon o kazenskem postopku določa, da je treba za izvedbo preiskave ali zasega pridobiti sodno odredbo ([205]). Preiskava ali zaseg brez odredbe sta dovoljena le izjemoma, in sicer v nujnih primerih ([206]), na licu mesta ob aretaciji ali odvzemu prostosti osumljencu kaznivega dejanja ([207]), ali kadar osumljenec ali tretja oseba zavrže predmet ali ga prostovoljno izroči (v primeru osebnih podatkov lahko to stori le zadevni posameznik sam) ([208]). Za nezakonite preiskave in zasege se lahko izrečejo kazenske sankcije ([209]), dokazi, pridobljeni v nasprotju z zakonom o kazenskem postopku, pa se ne upoštevajo ([210]). Nazadnje, zadevni posameznik mora biti vedno brez odlašanja uradno obveščen o preiskavi ali zasegu (vključno z zasegom njegovih podatkov) ([211]), kar mu olajša uresničevanje materialnih pravic in pravice do pravnega varstva (glej zlasti možnost izpodbijanja izvršitve odredbe o zasegu, glej uvodno izjavo (180)).

3.2.1.2 Dostop do podatkov o komunikaciji

(155) Na podlagi zakona o varstvu zasebnosti komunikacij lahko korejski organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj sprejmejo dve vrsti ukrepov ([212]): na eni strani zbiranje „podrobnih podatkov o opravljeni komunikaciji“ ([213]), kar vključuje podatke o datumu telekomunikacij ter času njihovega začetka in konca, številu odhodnih in dohodnih klicev, naročniški številki sogovornika ter pogostosti uporabe, dnevniške datoteke o uporabi telekomunikacijskih storitev in podatke o lokaciji (npr. iz baznih postaj, ki sprejemajo signal); na drugi pa „ukrepe za omejevanje komunikacij“, ki vključujejo zbiranje vsebine navadne pošte in neposredno prestrezanje vsebine telekomunikacij ([214]).

(156) Dostop do podrobnih podatkov o opravljeni komunikaciji je mogoč samo, če je to potrebno za izvedbo kazenske preiskave ali izvršitev kazni ([215]), in sicer na podlagi odredbe sodišča ([216]). Glede tega zakon o varstvu zasebnosti komunikacij določa, da morajo biti podrobne informacije navedene v vlogi za izdajo odredbe (npr. o razlogih za vlogo, povezavi s ciljno osebo/naročnikom in potrebnih podatkih) in v sami odredbi (npr. o cilju, namenu in obsegu ukrepa) ([217]). Zbiranje brez odredbe je dovoljeno le, če zaradi nujnosti okoliščin ni mogoče pridobiti

([205]) Člen 215(1) in (2) zakona o kazenskem postopku ter člen 113 navedenega zakona. Zadevni organ mora vlogi za izdajo odredbe priložiti dokazno gradivo, iz katerega so razvidni razlogi za sum, da je posameznik storil kaznivo dejanje, da je potrebna preiskava, pregled ali zaseg in da obstajajo zadevni predmeti, ki jih je treba zaseči (člen 108(1) uredbe o kazenskem postopku). Odredba mora med drugim vsebovati ime osumljenca in opredelitev kaznivega dejanja, navedbo kraja, osebe ali predmetov, ki jih je treba preiskati, ali predmete, ki jih je treba zaseči, datum izdaje in obdobje veljavnosti (člen 114(1) v povezavi s členom 219 zakona o kazenskem postopku). Glej Prilogo II, oddelek 2.2.1.2.

([206]) In sicer kadar odredbe zaradi nujnosti na kraju izvršitve kaznivega dejanja ni mogoče pridobiti (člen 216(3) zakona o kazenskem postopku), vendar je treba tudi v takem primeru odredbo brez odlašanja pridobiti naknadno (člen 216(3) zakona o kazenskem postopku).

([207]) Člen 216(1) in (2) zakona o kazenskem postopku.

([208]) Člen 218 zakona o kazenskem postopku. Kot je pojasnjeno v Prilogi II, oddelek 2.2.1.2, so poleg tega prostovoljno izročeni predmeti dopustni kot dokaz v sodnem postopku le, če ni razumnega dvoma o prostovoljnosti razkritja, kar mora dokazati tožilec.

([209]) Člen 321 kazenskega zakona.

([210]) Člen 308-2 zakona o kazenskem postopku. Poleg tega je lahko posameznik (in njegov zagovornik) prisoten pri izvrševanju odredbe o preiskavi ali zasegu in lahko takrat temu tudi ugovarja (člena 121 in 219 zakona o kazenskem postopku).

([211]) Člena 121 in 122 zakona o kazenskem postopku (v zvezi s preiskavami) ter člen 219 v povezavi s členom 106(4) zakona o kazenskem postopku (v zvezi z zasegi).

([212]) Glej tudi Prilogo II, oddelek 2.2.2.1. Taki ukrepi se lahko sprejmejo ob obveznem sodelovanju telekomunikacijskih operaterjev, ki se jim predloži pisno dovoljenje sodišča (člen 9(2) zakona o varstvu zasebnosti komunikacij), tako dovoljenje pa morajo operaterji hraniti (člen 15-2 zakona o varstvu zasebnosti komunikacij in člen 12 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij). Ponudniki telekomunikacij lahko zavrnejo sodelovanje, če podatki o ciljnem posamezniku, kot so navedeni na pisnem dovoljenju sodišča (npr. posameznikova telefonska številka) niso točni, prav tako v nobenem primeru ne smejo razkriti gesel, ki se uporabljajo za telekomunikacije (člen 9(4) zakona o varstvu zasebnosti komunikacij).

([213]) Člen 2(11) zakona o varstvu zasebnosti komunikacij.

([214]) Glej člen 2(6) zakona o varstvu zasebnosti komunikacij, ki se nanaša na „cenzuro“ (odpiranje pošte brez privolitve zadevne osebe ali seznanjanje z njeno vsebino, snemanje vsebine ali zadrževanje vsebine na druge načine), in člen 2(7) zakona o varstvu zasebnosti komunikacij, ki se nanaša na „prisluškovanje“ (seznanitev z vsebino telekomunikacij ali njeno snemanje s poslušanjem ali branjem zvokov, besed, simbolov ali podob iz komunikacije s pomočjo elektronskih in mehanskih naprav, brez privolitve zadevne osebe, ali poseganje v njihov prenos in sprejem).

([215]) Člen 13(1) zakona o varstvu zasebnosti komunikacij. Glej tudi Prilogo II, oddelek 2.2.2.3. Poleg tega je mogoče podatke o sledenju lokaciji v realnem času in podrobne podatke o opravljeni komunikaciji, ki se nanašajo na določeno bazno postajo, zbirati le za preiskavo hudih kaznivih dejanj, ali če bi bilo drugače težko preprečiti izvršitev kaznivega dejanja ali zbrati dokaze (člen 13(2) zakona o varstvu zasebnosti komunikacij). To torej pomeni, da je treba zagotoviti dodatne zaščitne ukrepe, kadar gre za ukrepe, ki močno posegajo v zasebnost, in sicer v skladu z načelom sorazmernosti.

([216]) Člena 13 in 6 zakona o varstvu zasebnosti komunikacij.

([217]) Glej člen 13(3) in (9) v povezavi s členom 6(4) in (6) zakona o varstvu zasebnosti komunikacij.

dovoljenja sodišča, v takem primeru pa je treba odredbo pridobiti in jo poslati ponudniku telekomunikacij takoj po vložitvi zahteve za predložitev podatkov ([218]). Če sodišče zavrne izdajo naknadnega dovoljenja, je treba zbrane podatke uničiti ([219]).

(157) Glede dodatnih zaščitnih ukrepov v zvezi z zbiranjem podrobnih podatkov o opravljeni komunikaciji zakon o varstvu zasebnosti komunikacij določa posebne zahteve glede vodenja evidenc in preglednosti ([220]). Natančneje, organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ([221]) in ponudniki telekomunikacij ([222]) morajo voditi evidence zahtev za razkritje in dejanskih razkritij. Poleg tega morajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj načeloma uradno obvestiti posameznike, da so bili zbrani njihovi podrobni podatki o opravljeni komunikaciji ([223]). Tako uradno obveščanje se lahko odloži le v izrednih okoliščinah, in sicer na podlagi dovoljenja direktorja pristojnega okrožnega državnega tožilstva ([224]). Tako dovoljenje se lahko izda le, če bi uradno obveščanje verjetno (1) ogrozilo nacionalno varnost, javno varnost in red, (2) povzročilo smrt ali telesno poškodbo, (3) oviralo pošten sodni postopek (npr. imelo za posledico uničenje dokazov ali grožnje pričam) ali (4) škodilo ugledu osumljenca, žrtev ali drugih oseb, povezanih z zadevo, oziroma posegalo v njihovo zasebnost. V navedenih primerih je treba uradno obvestilo poslati v 30 dneh po prenehanju razlogov za odlog ([225]). Po prejemu uradnega obvestila imajo posamezniki pravico pridobiti informacije o razlogih za zbiranje njihovih podatkov ([226]).

(158) Strožja pravila veljajo glede ukrepov za omejevanje komunikacij, ki se lahko uporabijo le, če obstajajo utemeljeni razlogi za sum, da se načrtujejo, izvajajo ali so bila storjena določena huda kazniva dejanja, izrecno navedena v zakonu o varstvu zasebnosti komunikacij ([227]). Poleg tega se lahko ukrepi za omejevanje komunikacij sprejmejo le v skrajnem primeru, če bi bilo sicer težko preprečiti storitev kaznivega dejanja, prijeti storilca ali zbrati dokaze ([228]). Z njimi je treba prenehati takoj, ko niso več potrebni, s čimer se zagotovi, da je kršitev zasebnosti komunikacij čim bolj omejena ([229]). Informacije, pridobljene nezakonito na podlagi ukrepov za omejevanje komunikacij, niso dopustne kot dokazi v sodnem ali disciplinskem postopku ([230]).

(159) Glede postopkovnih zaščitnih ukrepov zakon o varstvu zasebnosti komunikacij določa, da je treba za izvajanje ukrepov za omejevanje komunikacij pridobiti sodno odredbo ([231]). Prav tako morata v skladu z navedenim zakonom vloga za izdajo odredbe in sama odredba vsebovati podrobne informacije ([232]), vključno z obrazložitvijo zahteve in podatki o komunikaciji, ki jih je treba zbrati (ti se morajo nanašati na osumljenca, ki je predmet preiskave) ([233]). Taki ukrepi se lahko brez odredbe izvedejo le v primeru neposredne grožnje organiziranega kriminala ali storitve drugega hudega kaznivega dejanja, katerega neposredna posledica bi lahko bila smrt ali

([218]) Člen 13(2) zakona o varstvu zasebnosti komunikacij.
([219]) Člen 13(3) zakona o varstvu zasebnosti komunikacij.
([220]) Glej Prilogo II, oddelek 2.2.2.3.
([221]) Člen 13(5) in (6) zakona o varstvu zasebnosti komunikacij.
([222]) Člen 13(7) zakona o varstvu zasebnosti komunikacij. Poleg tega morajo ponudniki telekomunikacij dvakrat letno ministrstvu za znanost in IKT poročati o razkritjih podrobnih podatkov o opravljeni komunikaciji.
([223]) Glej člen 13-3(7) v povezavi s členom 9-2 zakona o varstvu zasebnosti komunikacij. Posamezniki morajo biti zlasti uradno obveščeni v 30 dneh po sprejetju odločitve o pregonu ali opustitvi pregona oziroma v 30 dneh po preteku enega leta od sprejetja odločitve o zadržanju vložitve obtožnice (vsekakor pa je treba posameznika uradno obvestiti v 30 dneh po preteku enega leta od zbiranja podatkov), glej člen 13-3(1) zakona o varstvu zasebnosti komunikacij.
([224]) Člen 13-3(2)-(3) zakona o varstvu zasebnosti komunikacij.
([225]) Člen 13-3(4) zakona o varstvu zasebnosti komunikacij.
([226]) Člen 13-3(5) zakona o varstvu zasebnosti komunikacij. Na zahtevo posameznika mora tožilec ali pravosodni policist v 30 dneh po prejetju zahteve pisno navesti razloge, razen če se uporablja ena od izjem za odlog uradnega obveščanja (člen 13-3(6) zakona o varstvu zasebnosti komunikacij).
([227]) Na primer vstaja, kazniva dejanja, povezana z drogami, kazniva dejanja, ki vključujejo uporabo eksploziva, ter kazniva dejanja, povezana z nacionalno varnostjo, diplomatskimi odnosi ali vojaškimi oporišči in objekti, glej člen 5(1) zakona o varstvu zasebnosti komunikacij. Glej tudi Prilogo II, oddelek 2.2.2.2.
([228]) Člen 3(2) in člen 5(1) zakona o varstvu zasebnosti komunikacij.
([229]) Člen 2 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([230]) Člen 4 zakona o varstvu zasebnosti komunikacij.
([231]) Člen 6(1), (2) in (5)-(6) zakona o varstvu zasebnosti komunikacij.
([232]) V vlogi za izdajo odredbe morajo biti opisani (1) utemeljeni razlogi za sum, iz katerih (že na prvi pogled) izhaja, da se načrtuje, izvaja ali je bilo storjeno eno od kaznivih dejanja s seznama, in vse dokazno gradivo; (2) ukrepi za omejevanje komunikacij ter njihovi cilji, področje uporabe, namen in dejansko obdobje uporabe; ter (3) kraj in način izvedbe ukrepov (člen 6(4) zakona o varstvu zasebnosti komunikacij in člen 4(1) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij). V sami odredbi morajo biti podrobno določeni ukrepi ter njihov cilj, področje uporabe, dejansko obdobje uporabe, kraj in način izvedbe (člen 6(6) zakona o varstvu zasebnosti komunikacij).
([233]) Cilj ukrepa za omejevanje komunikacij morajo biti določene poštne pošiljke oziroma telekomunikacije, ki jih pošlje ali prejme osumljenec, ali poštne pošiljke oziroma telekomunikacije, ki jih osumljenec pošlje ali prejme v določenem obdobju (člen 5(2) zakona o varstvu zasebnosti komunikacij).

huda poškodba, ukrepanje pa je tako nujno, da ni mogoče izvesti rednega postopka ([234]). Vendar pa je treba v takem primeru takoj po izvedbi ukrepa vložiti vlogo za izdajo odredbe ([235]). Ukrepi za omejevanje komunikacij se lahko izvajajo največ dva meseca ([236]) in podaljšajo le s soglasjem sodišča, če so pogoji za izvajanje ukrepa še vedno izpolnjeni ([237]). Podaljšanje skupno ne sme presegati enega leta ali treh let v primeru nekaterih posebno hudih kaznivih dejanj (kot so kazniva dejanja, povezana z vstajami, tujo agresijo ali nacionalno varnostjo) ([238]).

(160) Tako kot v zvezi s podrobnimi podatki o opravljeni komunikaciji zakon o varstvu zasebnosti komunikacij določa, da morajo ponudniki telekomunikacij ([239]) ter organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ([240]) voditi evidence izvedenih ukrepov za omejevanje komunikacij, določa pa tudi obveznost uradnega obveščanja zadevnega posameznika, ki se lahko izjemoma odloži, če je to potrebno iz pomembnih razlogov v javnem interesu ([241]).

(161) Nazadnje, zaradi neupoštevanja več omejitev in zaščitnih ukrepov iz zakona o varstvu zasebnosti komunikacij (med drugim na primer obveznosti pridobitve odredbe, vodenja evidenc in obveščanja posameznika) tako glede zbiranja podrobnih podatkov o opravljeni komunikaciji kot tudi glede uporabe ukrepov za omejevanje komunikacij se lahko izrečejo kazenske sankcije ([242]).

(162) Pooblastila organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj glede zbiranja podatkov o komunikaciji na podlagi zakona o varstvu zasebnosti komunikacij (vsebine komunikacij in podrobnih podatkov o opravljeni komunikaciji) so torej omejena z jasnimi in natančnimi pravili, zanje pa se uporablja tudi več zaščitnih ukrepov. Zlasti slednji zagotavljajo nadzor nad izvajanjem takih ukrepov, in sicer vnaprej (na podlagi predhodne odobritve sodišča) in za nazaj (na podlagi zahtev glede vodenja evidenc in poročanja), ter lajšajo dostop posameznikov do učinkovitih pravnih sredstev (z zagotavljanjem, da so posamezniki obveščeni o zbiranju njihovih podatkov).

3.2.1.3 Prošnje za prostovoljno razkritje podatkov o naročnikih

(163) Poleg obveznih ukrepov, opisanih v uvodnih izjavah (153) do (162), lahko korejski organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj zaprosijo ponudnike telekomunikacij za prostovoljno razkritje „podatkov o komunikaciji“ v podporo kazenskemu postopku, preiskavi ali izvršitvi sankcije (člen 83(3) zakona o zagotavljanju telekomunikacijskih storitev). Ta možnost je na voljo le v zvezi z omejenimi nabori podatkov, tj. imenom, registrsko številko prebivalca, naslovom in telefonsko številko uporabnika, datumi, ko so uporabniki sklenili ali prekinili naročnino, ter oznakami za identifikacijo uporabnikov (tj. oznakami, ki se uporabljajo za identifikacijo legitimnega uporabnika računalniških sistemov ali komunikacijskih omrežij) ([243]). Ker se za „uporabnike“ štejejo le posamezniki, ki neposredno sklenejo pogodbeno razmerje s korejskim ponudnikom telekomunikacijskih storitev ([244]), posamezniki iz EU, katerih podatki se prenašajo v Republiko Korejo, običajno ne spadajo v to kategorijo ([245]).

(164) Za tako prostovoljno razkritje veljajo različne omejitve, tako glede izvrševanja pooblastil organa za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj kot tudi glede odziva telekomunikacijskega operaterja. Na splošno velja, da morajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ravnati v skladu z ustavnima načeloma nujnosti in sorazmernosti (člen 12(1) in člen 37(2) ustave), tudi kadar zaprosijo za informacije na prostovoljni podlagi. Poleg tega morajo upoštevati zakon o varstvu osebnih podatkov, zlasti z zbiranjem podatkov le v najmanjšem možnem obsegu, kolikor je to potrebno za dosego zakonitega namena, da se čim

([234]) Člen 8(1) zakona o varstvu zasebnosti komunikacij. Vendar pa mora zbiranje informacij v nujnih primerih vedno potekati v skladu z „izjavo o cenzuri/prisluškovanju v nujnem primeru“, organ, ki izvaja zbiranje, pa mora voditi evidenco vseh nujnih ukrepov (člen 8(4) zakona o varstvu zasebnosti komunikacij).

([235]) Zbiranje je treba nemudoma prekiniti, če organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v 36 urah ne pridobi dovoljenja sodišča (člen 8(2) zakona o varstvu zasebnosti komunikacij), v takem primeru (kot je pojasnjeno v Prilogi II, oddelek 2.2.2.2) pa se zbrani podatki načeloma uničijo. Sodišče je treba uradno obvestiti tudi, če se ukrepi, izvedeni v nujnih primerih, zaključijo tako hitro, da dovoljenje ni več potrebno (npr. če je osumljenec prijet takoj po začetku prestrezanja, glej člen 8(5) zakona o varstvu zasebnosti komunikacij). V takem primeru je treba sodišče obvestiti o namenu, cilju, obsegu, obdobju, kraju izvedbe in načinu zbiranja ter razlogih za nevložitev zahteve za dovoljenje sodišča (člen 8(6)-(7) zakona o varstvu zasebnosti komunikacij).

([236]) Člen 6(7) zakona o varstvu zasebnosti komunikacij. Če je namen ukrepov dosežen pred koncem navedenega obdobja, jih je treba takoj prenehati izvajati.

([237]) Člen 6(7)-(8) zakona o varstvu zasebnosti komunikacij.

([238]) Člen 6(8) zakona o varstvu zasebnosti komunikacij.

([239]) Člen 9(3) zakona o varstvu zasebnosti komunikacij.

([240]) Člen 18(1) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.

([241]) Zlasti velja, da mora tožilec posameznika uradno obvestiti v 30 dneh od vložitve obtožnice ali odločitve o tem, da obtožnica ne bo vložena ali da se ne bo zahtevalo prijetje osumljenca (člen 9-2(1) zakona o varstvu zasebnosti komunikacij). Uradno obveščanje se lahko odloži s soglasjem vodje okrožnega državnega tožilstva, če je verjetno, da bi resno ogrozilo nacionalno varnost ali poseglo v javno varnost in red, ali če je verjetno, da bi povzročilo bistveno škodo za življenje in telo drugih oseb (člen 9-2(4)-(6) zakona o varstvu zasebnosti komunikacij).

([242]) Člena 16 in 17 zakona o varstvu zasebnosti komunikacij.

([243]) Člen 83(3) zakona o zagotavljanju telekomunikacijskih storitev. Glej tudi Prilogo II, oddelek 2.2.3.

([244]) Člen 2(9) zakona o zagotavljanju telekomunikacijskih storitev.

([245]) Glej tudi Prilogo II, oddelek 2.2.3.

bolj omeji poseganje v zasebnost posameznika (npr. člen 3(1) in (6) zakona o varstvu osebnih podatkov). Natančneje, prošnje za pridobitev podatkov o komunikaciji na podlagi zakona o zagotavljanju telekomunikacijskih storitev je treba predložiti pisno in navesti razloge zanje, povezavo z zadevnim uporabnikom in obseg zahtevanih podatkov ([246]).

(165) Ponudniki telekomunikacij niso zavezani ugoditi takim prošnjam, če to storijo, pa morajo upoštevati zakon o varstvu osebnih podatkov. To zlasti pomeni, da morajo pretehtati različne zadevne interese in podatkov ne smejo zagotoviti, če bi s tem najverjetneje nepošteno posegli v interese posameznika ali tretje osebe ([247]). Tako bi bilo na primer v primeru, ko je jasno, da je organ prosilec zlorabil svoja pooblastila ([248]). Telekomunikacijski operaterji morajo voditi evidence razkritij na podlagi zakona o zagotavljanju telekomunikacijskih storitev in o tem dvakrat letno poročati ministru za znanost in IKT ([249]).

(166) Poleg tega morajo ponudniki telekomunikacijskih storitev v skladu z oddelkom 3 uradnega obvestila št. 2021-5 (Priloga I) obvestiti zadevnega posameznika, kadar prostovoljno ugodijo taki prošnji ([250]). To pa posamezniku omogoča, da uresničuje svoje pravice in uveljavlja pravno varstvo, če so bili njegovi podatki razkriti nezakonito, in sicer zoper upravljavca (npr. zaradi razkritja podatkov v nasprotju z zakonom o varstvu osebnih podatkov ali zaradi ugoditve prošnji, ki je bila očitno nesorazmerna) ali zoper organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj (npr. ker je z ravnanjem presegel mejo nujnega in sorazmernega ali ker ni upošteval procesnih zahtev iz zakona o zagotavljanju telekomunikacijskih storitev).

3.2.2 *Nadaljnja uporaba zbranih informacij*

(167) Za obdelavo osebnih podatkov, ki jih zberejo korejski organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, se uporabljajo vse zahteve iz zakona o varstvu osebnih podatkov, med drugim glede omejitve namena (člen 3(1)-(2) zakona o varstvu osebnih podatkov), zakonitosti uporabe in zagotavljanja tretjim osebam (členi 15, 17 in 18 zakona o varstvu osebnih podatkov), mednarodnega prenosa (člena 17 in 18 zakona o varstvu osebnih podatkov v povezavi z oddelkom 2 uradnega obvestila št. 2021-5) ([251]) sorazmernosti oziroma najmanjšega obsega podatkov (člen 3(1) in (6) navedenega zakona) ter omejitve hrambe (člen 21 zakona o varstvu osebnih podatkov) ([252]).

(168) Kar zadeva vsebino komunikacij, pridobljeno na podlagi izvajanja ukrepov za omejevanje komunikacij, je z zakonom o varstvu zasebnosti komunikacij možnost njene uporabe izrecno omejena na preiskovanje, pregon ali preprečevanje hudih kaznivih dejanj ([253]), disciplinske postopke za ista kazniva dejanja, odškodninske zahtevke, ki jih vloži udeleženec komunikacije, ali kadar je to izrecno dovoljeno z drugimi zakoni ([254]). Poleg tega se lahko zbrana vsebina telekomunikacij, ki se prenaša prek spleta, hrani le s soglasjem sodišča, ki je dovolilo ukrepe za omejevanje komunikacije ([255]), da bi se uporabila za preiskovanje, pregon ali preprečevanje hudih kaznivih dejanj ([256]). Splošneje, zakon o varstvu zasebnosti komunikacij prepoveduje razkritje zaupnih podatkov, pridobljenih na podlagi ukrepov za omejevanje komunikacije, in uporabo takih podatkov za škodovanje ugledu tistih, zoper katere so se ukrepi izvajali ([257]).

3.2.3 *Nadzor*

(169) V Koreji dejavnosti organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj nadzorujejo različni organi ([258]).

([246]) Člen 83(4) zakona o zagotavljanju telekomunikacijskih storitev. Kadar zaradi nujnosti ni mogoče predložiti pisne prošnje, jo je treba predložiti takoj po prenehanju razloga za nujnost (člen 83(4) zakona o zagotavljanju telekomunikacijskih storitev).
([247]) Člen 18(2) zakona o varstvu osebnih podatkov.
([248]) Odločba vrhovnega sodišča št. 2012Da105482 z dne 10. marca 2016. Glej tudi Prilogo II, oddelek 2.2.3, o tej odločbi vrhovnega sodišča.
([249]) Člen 83(5)–(6) zakona o zagotavljanju telekomunikacijskih storitev.
([250]) Za to zahtevo veljajo omejene in kvalificirane izjeme, zlasti če in dokler bi uradno obveščanje ogrozilo tekočo kazensko preiskavo ali če bi verjetno povzročilo škodo življenju ali telesu druge osebe, kadar te pravice ali interesi očitno prevladajo nad pravicami posameznika, na katerega se nanašajo osebni podatki. Glej oddelek 3, (iii) (1) uradnega obvestila.
([251]) Zlasti morajo korejski javni organi s pravno zavezujočim instrumentom zagotoviti raven zaščite, ki je enakovredna zakonu o varstvu osebnih podatkov, glej tudi uvodno izjavo (90).
([252]) Glej tudi Prilogo II, oddelek 1.2.
([253]) Glej uvodno izjavo (158).
([254]) Člen 12 zakona o varstvu zasebnosti komunikacij. Glej Prilogo II, oddelek 2.2.2.2.
([255]) Tožilec ali policist, ki izvaja ukrepe za omejevanje komunikacij, mora v 14 dneh po zaključku ukrepov izbrati telekomunikacije, ki se bodo shranile, in zaprositi za soglasje sodišča (policist mora vlogo predložiti tožilcu, ta pa jo nato vloži pri sodišču), glej člen 12-2(1) in (2) zakona o varstvu zasebnosti komunikacij.
([256]) Vloga za tako soglasje mora vsebovati informacije o ukrepih za omejevanje komunikacij, povzetek rezultatov ukrepov, razloge za hrambo (skupaj z dokazili) in telekomunikacije, ki naj bi se shranile (člen 12-2(3) zakona o varstvu zasebnosti komunikacij). Če taka vloga ni vložena, je treba pridobljene podatke izbrisati v 14 dneh po prenehanju ukrepov za omejevanje komunikacij (člen 12-2(5) zakona o varstvu zasebnosti komunikacij), če je vloga zavrnjena, pa v sedmih dneh (člen 12-2(5) zakona o varstvu zasebnosti komunikacij). V obeh primerih je treba sodišču, ki je dovolilo zbiranje, v sedmih dneh predložiti poročilo o izbrisu.
([257]) Člen 11(2) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([258]) Glej Prilogo II, oddelek 2.3.

(170) Prvič, policija je podvržena notranjemu nadzoru generalnega inšpektorata ([259]), ki nadzoruje zakonitost, med drugim glede morebitnih kršitev človekovih pravic. Generalni inšpektorat je bil ustanovljen za izvajanje zakona o revizijah v javnem sektorju, s katerim se spodbuja vzpostavitev organov za notranjo revizijo ter ki določa posebne zahteve glede njihove sestave in nalog. Zakon zlasti določa, da mora biti vodja organa za notranjo revizijo imenovan od zunaj, torej ne izmed članov zadevnega organa (vodje so lahko na primer nekdanji sodniki ali profesorji), in sicer za obdobje dveh do petih let ([260]), da ga je mogoče razrešiti le iz upravičenih razlogov (npr. če ni zmožen opravljati svojih nalog iz zdravstvenih razlogov ali če je razrešitev posledica disciplinskega ukrepa) ([261]) in da mu je v največji možni meri zagotovljena neodvisnost ([262]). Za oviranje notranje revizije se lahko izrečejo upravne globe ([263]). Revizijska poročila (ki lahko vključujejo priporočila, zahteve za disciplinske ukrepe in zahteve za odškodnino ali popravek) se predložijo vodji zadevnega javnega organa, odboru za revizijo in inšpekcijski pregled ([264]) ter se običajno javno objavijo ([265]). Odbor za revizijo in inšpekcijski pregled je treba uradno obvestiti tudi o rezultatih izvajanja poročila ([266]) (glej uvodno izjavo (173) o nadzorni vlogi in pooblastilih navedenega odbora).

(171) Drugič, komisija za varstvo osebnih podatkov nadzoruje, ali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj pri obdelavi podatkov zagotavljajo skladnost z zakonom o varstvu osebnih podatkov in drugimi zakoni, ki varujejo zasebnost posameznikov, vključno z zakoni, ki urejajo zbiranje (elektronskih) dokazov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, kot je opisano v oddelku 3.2.1 ([267]). Zlasti ker lahko komisija za varstvo osebnih podatkov nadzoruje tudi zakonitost in poštenost zbiranja in obdelave podatkov (člen 3(1) zakona o varstvu osebnih podatkov), ta pa je kršena, če se do osebnih podatkov dostopa in se jih uporablja v nasprotju z navedenimi zakoni ([268]), lahko navedena komisija tudi preiskuje in zagotavlja skladnost z omejitvami in zaščitnimi ukrepi, opisanimi v oddelku 3.2.1 ([269]). Pri izvrševanju te nadzorne vloge lahko komisija za varstvo osebnih podatkov uporabi vsa svoja preiskovalna in popravna pooblastila, kot so podrobno opisana v oddelku 2.4.2. Komisija za varstvo osebnih podatkov je že pred nedavno reformo zakona o varstvu osebnih podatkov (tj. v svoji predhodni nadzorni vlogi v javnem sektorju) izvajala več nadzornih dejavnosti glede obdelave osebnih podatkov pri organih za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, na primer v okviru zaslišanja osumljencev (zadeva št. 2013-16 z dne 26. avgusta 2013), v zvezi z obveščanjem posameznikov o izreku upravnih glob (zadeva št. 2015-02-04 z dne 26. januarja 2015), glede izmenjave podatkov z drugimi organi (zadeva št. 2018-15-146 z dne 9. julija 2018, zadeva št. 2018-25-308 z dne 10. decembra 2018, zadeva št. 2019-02-015 z dne 29. januarja 2019), glede zbiranja prstnih odtisov ali fotografij (zadeva št. 2019-17-273 z dne 9. septembra 2019) in glede uporabe dronov (zadeva št. 2020-01-004 z dne 13. januarja 2020). V navedenih primerih je komisija za varstvo osebnih podatkov preiskovala skladnost z več določbami zakona o varstvu osebnih podatkov (npr. zakonitost obdelave, načeli omejitve namena in najmanjšega obsega podatkov), pa tudi z zadevnimi določbami drugih zakonov, kot so zakon o kazenskem postopku, in, kadar je bilo potrebno, izdala priporočila za uskladitev obdelave z zahtevami varstva podatkov.

(172) Tretjič, neodvisni nadzor zagotavlja nacionalna komisija za človekove pravice ([270]), ki lahko v okviru svojega splošnega mandata za varstvo temeljnih pravic iz členov 10 do 22 ustave preiskuje kršitve pravice do zasebnosti in pravice do zasebnosti komunikacij. Nacionalno komisijo za človekove pravice sestavlja 11 članov, ki morajo izpolnjevati posebne pogoje ([271]), imenuje pa jih predsednik republike, in sicer v skladu s postopki, določenimi v zakonu. Štiri člane v imenovanje predlaga parlament, štiri predsednik republike in tri predsednik vrhovnega sodišča ([272]). Predsednika komisije izmed članov komisije imenuje predsednik republike, potrditi pa ga mora parlament ([273]). Člani komisije (vključno s predsednikom) so imenovani za triletni mandat z možnostjo podaljšanja, razrešiti pa jih je mogoče le, če so obsojeni na kazen zapora ali ne zmorejo več opravljati svojih nalog zaradi

([259]) Glej Prilogo II, oddelek 2.3.1. Glej tudi https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) Podobno so revizorji imenovani na podlagi posebnih pogojev iz zakona, glej člen 16 in naslednje zakona o revizijah v javnem sektorju.
([261]) Členi 8 do 11 zakona o revizijah v javnem sektorju.
([262]) Člen 7 zakona o revizijah v javnem sektorju.
([263]) Člen 41 zakona o revizijah v javnem sektorju.
([264]) Člen 23(1) zakona o revizijah v javnem sektorju.
([265]) Člen 26 zakona o revizijah v javnem sektorju.
([266]) Člen 23(3) zakona o revizijah v javnem sektorju.
([267]) Glej člen 7-8(3) in (4) ter člen 7-9(5) zakona o varstvu osebnih podatkov.
([268]) Glej uradno obvestilo komisije za varstvo osebnih podatkov št. 2021-5, oddelek 6 (Priloga I).
([269]) Glej tudi Prilogo II, oddelek 2.3.4.
([270]) Člen 1 zakona o nacionalni komisiji za človekove pravice.
([271]) Za člana komisije je lahko imenovana oseba, ki (1) je bila najmanj deset let zaposlena na univerzi ali pooblaščenem raziskovalnem inštitutu, in sicer najmanj na položaju izrednega profesorja, (2) je najmanj deset let opravljala funkcijo sodnika, državnega tožilca ali odvetnika, (3) se je najmanj deset let ukvarjala z dejavnostmi na področju človekovih pravic (npr. za nepridobitno, nevladno organizacijo ali mednarodno organizacijo), ali (4) so jo priporočile skupine civilne družbe (člen 5(3) zakona o nacionalni komisiji za človekove pravice). Poleg tega člani nacionalne komisije za človekove pravice po imenovanju ne smejo hkrati zasedati funkcij v državnem zboru, lokalnih svetih ali katerem koli državnem ali lokalnem upravnem organu (kot javni uslužbenci), glej člen 10 zakona o nacionalni komisiji za človekove pravice.
([272]) Člen 5(1) in (2) zakona o nacionalni komisiji za človekove pravice.
([273]) Člen 5(5) zakona o nacionalni komisiji za človekove pravice.

dolgotrajne duševne ali telesne nezmožnosti (v tem primeru se morata z razrešitvijo strinjati dve tretjini članov komisije) ([274]). V okviru preiskave lahko nacionalna komisija za človekove pravice zahteva predložitev ustreznega dokaznega gradiva, opravi preglede in zasliši posameznike kot priče ([275]). V okviru svojih popravnih pooblastil lahko nacionalna komisija za človekove pravice izda (javna) priporočila za izboljšanje ali popravek posameznih politik in praks, javni organi pa morajo nato predlagati načrt izvajanja ([276]). Če zadevni organ ne upošteva priporočil, mora o tem obvestiti komisijo ([277]), ta pa lahko nato o takem neupoštevanju poroča parlamentu in/ali to javno objavi. Glede na uradne navedbe korejske vlade (Priloga II, oddelek 2.3.5) korejski organi na splošno upoštevajo priporočila nacionalne komisije za človekove pravice, k čemur jih močno spodbuja dejstvo, da se njihovo izvajanje ocenjuje v okviru splošnega in stalnega vrednotenja pod vodstvom urada predsednika vlade. Iz letnih podatkov o dejavnostih nacionalne komisije za človekove pravice izhaja, da ta aktivno nadzoruje dejavnosti organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, in sicer na podlagi posameznih vlog ali preiskav po uradni dolžnosti ([278]).

(173) Četrtič, splošni nadzor nad zakonitostjo dejavnosti javnih organov izvaja odbor za revizijo in inšpekcijski pregled, ki preverja prihodke in izdatke države, ob tem pa splošneje tudi preverja izpolnjevanje obveznosti javnih organov, s ciljem izboljšanja delovanja javne uprave ([279]). Odbor za revizijo in inšpekcijski pregled je uradno ustanovil predsednik Republike Koreje, pri opravljanju svojih nalog pa je neodvisen ([280]). Poleg tega je povsem neodvisen glede imenovanja, razrešitve in organizacije svojega osebja ter priprave proračuna ([281]). Odbor za revizijo in inšpekcijski pregled sestavljajo predsednik odbora (ki ga imenuje predsednik republike ob soglasju parlamenta) ([282]) in šest članov (ki jih imenuje predsednik republike na predlog predsednika odbora) ([283]), ki morajo izpolnjevati posebne pogoje, določene v zakonu ([284]), in so lahko razrešeni le v primeru ustavne obtožbe, obsodbe na zaporno kazen ali nezmožnosti opravljanja nalog zaradi dolgotrajne duševne ali fizične nezmožnosti ([285]). Odbor za revizijo in inšpekcijski pregled vsako leto izvede splošno revizijo, lahko pa izvaja tudi posebne revizije v zvezi z zadevami posebnega interesa. Pri izvajanju revizij ali pregledov lahko odbor zahteva predložitev dokumentov in navzočnost posameznikov ([286]). Odbor lahko izda priporočila, zahteva izrek disciplinskih ukrepov ali vloži ovadbo ([287]).

(174) Nazadnje, parlament opravlja parlamentarni nadzor nad javnimi organi v okviru preiskav in pregledov ([288]) njihovih dejavnosti ([289]). Zahteva lahko predložitev listin in navzočnost prič ([290]), priporoči popravne ukrepe

([274]) Člen 7(1) in člen 8 zakona o nacionalni komisiji za človekove pravice.
([275]) Člen 36 zakona o nacionalni komisiji za človekove pravice. Predložitev dokaznega gradiva ali predmetov se lahko v skladu s členom 6(7) zakona zavrne, če bi to posegalo v državne skrivnosti, tako da bi lahko bistveno vplivalo na državno varnost ali diplomatske odnose, ali če bi to resno oviralo kazensko preiskavo ali sojenje, ki še poteka. V takih primerih lahko komisija od vodje zadevnega organa zahteva dodatne informacije (vodja pa mora to zahtevo v dobri veri izpolniti), če jih potrebuje za preverjanje, ali je zavrnitev zagotovitve informacij upravičena.
([276]) Člen 25(1) in (3) zakona o nacionalni komisiji za človekove pravice.
([277]) Člen 25(4) zakona o nacionalni komisiji za človekove pravice.
([278]) Med letoma 2015 in 2019 je nacionalna komisija za človekove pravice na primer vsako leto prejela med 1 380 in 1 699 pritožb zoper organe za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, podobno veliko število pritožb pa je tudi obravnavala (npr. 1 546 pritožb zoper policijo leta 2018 in 1 249 pritožb leta 2019); prav tako je opravila več preiskav po uradni dolžnosti, kot je podrobneje opisano v letnem poročilu komisije za leto 2018 (na voljo na naslovu: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) in v letnem poročilu za leto 2019 (na voljo na: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([279]) Člena 20 in 24 zakona o odboru za revizijo in inšpekcijski pregled. Glej Prilogo II, oddelek 2.3.2.
([280]) Člen 2(1) zakona o odboru za revizijo in inšpekcijski pregled.
([281]) Člen 2(2) zakona o odboru za revizijo in inšpekcijski pregled.
([282]) Člen 4(1) zakona o odboru za revizijo in inšpekcijski pregled.
([283]) Člen 5(1) in člen 6 zakona o odboru za revizijo in inšpekcijski pregled.
([284]) Da so na primer najmanj deset let opravljali funkcijo sodnika, državnega tožilca ali odvetnika, da so bili najmanj osem let zaposleni kot javni uslužbenci ali profesorji ali na višjem položaju na univerzi ali da so bili najmanj deset let (od tega najmanj pet let kot direktorji) zaposleni v družbi, ki kotira na borzi, ali ustanovi, v katero vlaga država, glej člen 7 zakona o odboru za revizijo in inšpekcijski pregled. Poleg tega se člani komisije ne smejo politično udejstvovati in hkrati imeti funkcije v parlamentu, upravnih organih in organizacijah, v katerih odbor za revizijo in inšpekcijski pregled izvaja ti dejavnosti, ali na katerem koli drugem plačanem delovnem mestu ali položaju (člen 9 zakona o odbor za revizijo in inšpekcijski pregled).
([285]) Člen 8 zakona o odboru za revizijo in inšpekcijski pregled.
([286]) Glej na primer člen 27 zakona o odboru za revizijo in inšpekcijski pregled.
([287]) Členi 24 in 31 do 35 zakona o odboru za revizijo in inšpekcijski pregled.
([288]) Člen 128 zakona o parlamentu ter členi 2, 3 in 15 zakona o pregledih in preiskavah v državni upravi. To vključuje letne preglede vladnih zadev kot celote, pa tudi preiskave posebnih zadev.
([289]) Glej Prilogo, oddelek 2.2.3.
([290]) Člen 10(1) zakona o pregledih in preiskavah v državni upravi. Glej tudi člena 128 in 129 zakona o parlamentu.

(če ugotovi, da so bile izvedene nezakonite ali neprimerne dejavnosti) ([291]) ter javno objavi rezultate svojih ugotovitev ([292]). Kadar parlament zahteva izvedbo popravnih ukrepov (ki lahko na primer vključujejo dodelitev odškodnine, sprejetje disciplinskih ukrepov ali izboljšanje notranjih postopkov), mora zadevni javni organ brez odlašanja ukrepati in o rezultatu poročati parlamentu ([293]).

3.2.4 *Pravno varstvo*

(175) Korejski sistem ponuja različne (sodne) poti za uveljavljanje pravnega varstva, vključno z odškodnino za škodo.

(176) Prvič, zakon o varstvu osebnih podatkov posameznikom zagotavlja pravico do dostopa do osebnih podatkov, njihovega popravka in izbrisa ter prenehanja njihove obdelave za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ([294]).

(177) Drugič, posamezniki lahko uporabijo različne mehanizme pravnih sredstev, ki jih zagotavlja zakon o varstvu osebnih podatkov, če organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj obdeluje njihove podatke v nasprotju z zakonom o varstvu osebnih podatkov ali v nasprotju z omejitvami in zaščitnimi ukrepi glede zbiranja osebnih podatkov, kot so določeni v drugih zakonih (npr. v zakonu o kazenskem postopku ali zakonu o varstvu zasebnosti komunikacij, glej uvodno izjavo (171)). Posamezniki lahko zlasti vložijo pritožbo pri komisiji za varstvo osebnih podatkov (tudi prek klicnega centra za vprašanja v zvezi z zasebnostjo, ki ga upravlja korejska agencija za splet in varnost ([295])) ali prek odbora za mediacijo v primeru sporov v zvezi z osebnimi podatki ([296]). Za te možnosti pravnih sredstev ne veljajo dodatne zahteve glede dopustnosti. Na podlagi zakona o upravnem sporu se lahko posamezniki tudi pritožijo zoper odločitev komisije za varstvo osebnih podatkov ali jo izpodbijajo oziroma se pritožijo zoper neukrepanje navedene komisije (glej uvodno izjavo (132)).

(178) Tretjič, vsak posameznik ([297]) lahko pri nacionalni komisiji za človekove pravice vloži pritožbo zaradi kršitve pravice do zasebnosti in varstva podatkov s strani korejskega organa za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Nacionalna komisija za človekove pravice lahko predlaga popravek ali izboljšanje zadevnega predpisa, instituta, politike ali prakse ([298]) oziroma sprejetje ukrepov, kot je mediacija ([299]), prenehanje kršenja človekovih pravic, izplačilo odškodnine za škodo in ukrepe za preprečitev ponovitve enakih ali podobnih kršitev ([300]). Glede na uradne navedbe korejske vlade (Priloga II, oddelek 2.4.2) lahko to vključuje tudi izbris nezakonito zbranih osebnih podatkov. Čeprav nacionalna komisija za človekove pravice nima pristojnosti za izdajanje zavezujočih odločb, pa omogoča bolj neformalen, poceni in lahko dostopen način uveljavljanja pravnega varstva, zlasti ker za uvedbo preiskave ni treba dokazati, da je škoda dejansko nastala (kot je pojasnjeno v Prilogi II, oddelek 2.4.2) ([301]). To zagotavlja, da je mogoče pritožbe posameznikov v zvezi z zbiranjem njihovih podatkov preiskovati, tudi če posameznik ne more dokazati, da so bili njegovi podatki dejansko zbrani (npr. ker posameznik še ni bil obveščen). Iz letnih poročil o dejavnostih nacionalne komisije za človekove pravice izhaja, da posamezniki to možnost uporabljajo tudi za izpodbijanje ravnanj organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, med drugim glede ravnanja z osebnimi podatki ([302]). Če posameznik ni zadovoljen

([291]) Člen 16(2) zakona o pregledih in preiskavah v državni upravi.
([292]) Člen 12-2 zakona o pregledih in preiskavah v državni upravi.
([293]) Člen 16(3) zakona o pregledih in preiskavah v državni upravi.
([294]) Ta pravica se lahko uresničuje neposredno pri pristojnem organu ali posredno prek komisije za varstvo osebnih podatkov (člen 35 (2) zakona o varstvu osebnih podatkov). Kot je podrobneje opisano v uvodnih izjavah (76) do (78), se izjeme od teh pravic uporabljajo le, kadar je to potrebno za varstvo pomembnih (javnih) interesov.
([295]) Člen 62 zakona o varstvu osebnih podatkov.
([296]) Členi 40 do 50 zakona o varstvu osebnih podatkov in členi 48-2 do 57 uredbe o izvajanju zakona o varstvu osebnih podatkov. Glej tudi Prilogo II, oddelek 2.4.1.
([297]) Kot je pojasnjeno v Prilogi II, oddelek 2.4.2, velja, da čeprav se člen 4 zakona o nacionalni komisiji za človekove pravice sklicuje na državljane in tujce, ki prebivajo v Republiki Koreji, se izraz „prebivajo“ nanaša na pristojnost in ne na ozemlje. Če torej nacionalne institucije v Koreji kršijo temeljne pravice tujca zunaj Koreje, lahko ta posameznik vloži pritožbo pri nacionalni komisiji za človekove pravice. To bi veljalo, če bi korejski javni organi nezakonito dostopali do osebnih podatkov tujca, ki se prenesejo v Korejo. Glej zlasti pojasnila na: https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) Člen 44 zakona o nacionalni komisiji za človekove pravice.
([299]) Posameznik lahko tudi predlaga rešitev pritožbe v okviru mediacije, glej člen 42 in naslednje zakona o nacionalni komisiji za človekove pravice.
([300]) Člen 42(4) zakona o nacionalni komisiji za človekove pravice. Poleg tega lahko nacionalna komisija za človekove pravice sprejme nujne popravne ukrepe v primeru kršitve, ki še traja, če bi ob neukrepanju zaradi nje verjetno nastala škoda, ki bi jo bilo pozneje težko odpraviti, glej člen 48 zakona o nacionalni komisiji za človekove pravice.
([301]) Pritožbo je načeloma treba vložiti v enem letu po kršitvi, vendar se lahko nacionalna komisija za človekove pravice kljub temu odloči za proučitev pritožbe, vložene po tem roku, če zastaralni rok na podlagi kazenskega ali civilnega prava še ni potekel (člen 32(1), točka 4, zakona o nacionalni komisiji za človekove pravice).
([302]) Nacionalna komisija za človekove pravice je na primer v preteklosti že obravnavala pritožbe in izdala priporočila glede nezakonitih zasegov in kršitve zahteve po obveščanju posameznikov o zasegu (glej str. 80 in 91 letnega poročila nacionalne komisije za človekove pravice za leto 2018, ki je na voljo na naslovu: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), ter glede nezakonite obdelave osebnih podatkov s strani policije, tožilstva in sodišč (glej strani 157 in 158 letnega poročila nacionalne komisije za človekove pravice za leto 2019, ki je na voljo na naslovu: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, in stran 76 letnega poročila za leto 2019, ki je na voljo na naslovu: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

z rezultatom postopka pred nacionalno komisijo za človekove pravice, lahko njene odločitve (npr. o opustitvi preiskave pritožbe ([303])) ali priporočila izpodbija pred korejskimi sodišči na podlagi zakona o upravnem sporu (glej uvodno izjavo (181)) ([304]). Poleg tega lahko postopek pred nacionalno komisijo za človekove pravice nadalje olajša dostop do sodišča, saj lahko posameznik na podlagi ugotovitev navedene komisije uporabi nadaljnja pravna sredstva zoper javni organ, ki je nezakonito obdeloval njegove podatke, v skladu s postopki, opisanimi v uvodnih izjavah (181) do (183).

(179) Nazadnje, na voljo so različna sodna pravna sredstva, ki posameznikom omogočajo sklicevanje na omejitve in zaščitne ukrepe, opisane v oddelku 3.2.1, za uveljavljanje pravnega varstva ([305]).

(180) Glede zasegov (tudi zasegov podatkov) zakon o kazenskem postopku določa možnost ugovarjanja izvršitvi odredbe ali njenega izpodbijanja z vložitvijo t. i. kvazipritožbe pri pristojnem sodišču, s katero se zahteva preklic ali sprememba odločitve tožilca ali policista ([306]).

(181) Splošneje, posamezniki lahko izpodbijajo dejanja ([307]) ali opustitve ([308]) javnih organov (vključno z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj) na podlagi zakona o upravnem sporu ([309]). Upravno dejanje se šteje za „izpodbojno odločitev“, če neposredno vpliva na državljanske pravice in dolžnosti ([310]), kar po zagotovilih korejske vlade (glej Prilogo II oddelek 2.4.3) velja tudi za ukrepe zbiranja osebnih podatkov, in sicer neposredno (npr. s prestrezanjem komunikacij) ali v obliki zavezujočih zahtev za razkritje (npr. ponudniku storitev) oziroma zahtev za prostovoljno sodelovanje. Pritožba na podlagi zakona o upravnem sporu je dopustna, če ima posameznik pravni interes za njeno vložitev ([311]). „Pravni interes“ se v skladu s sodno prakso vrhovnega sodišča razlaga kot „pravno zaščiten interes“, tj. neposreden in poseben interes, zaščiten z zakoni in drugimi predpisi, na katerih temeljijo upravne odločitve (kar pomeni, da ne gre za splošne, posredne in abstraktne interese javnosti) ([312]). Posamezniki imajo tak pravni interes v primeru kršitev omejitev in zaščitnih ukrepov, ki se uporabljajo pri zbiranju njihovih osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (na podlagi posebnih predpisov ali zakona o varstvu osebnih podatkov). Na podlagi zakona o upravnem sporu lahko sodišče odpravi ali spremeni nezakonito odločitev, razglasi njeno ničnost (tj. ugotovi, da odločitev nima pravnega učinka ali da v pravnem redu ne obstaja) ali ugotovi, da je bila opustitev nezakonita ([313]). Pravnomočna sodba na podlagi zakona o upravnem sporu je za stranke v postopku zavezujoča ([314]).

([303]) Če nacionalna komisija za človekove pravice na primer izjemoma ne more pregledati določenega dokaznega gradiva ali objektov, ker zadevajo državne skrivnosti, ki bi lahko bistveno vplivale na državno varnost ali diplomatske odnose, oziroma če bi pregled resno oviral kazensko preiskavo ali sojenje, ki še poteka, in kadar navedena komisija zato ne more izvesti preiskave, potrebne za oceno utemeljenosti prejetega zahtevka, posameznika obvesti o razlogih za zavrnitev pritožbe, in sicer v skladu s členom 39 zakona o nacionalni komisiji za človekove pravice. Posameznik lahko v takem primeru izpodbija odločitev navedene komisije na podlagi zakona o upravnem sporu.

([304]) Glej npr. odločbo višjega sodišča v Seulu št. 2007Nu27259 z dne 18. aprila 2008, potrjeno z odločbo vrhovnega sodišča št. 2008Du7854 z dne 9. oktobra 2008; in odločbo višjega sodišča v Seulu št. 2017Nu69382 z dne 2. februarja 2018.

([305]) Glej Prilogo II, oddelek 2.4.3.

([306]) Člen 417 zakona o kazenskem postopku v povezavi s členom 414(2) navedenega zakona. Glej tudi odločbo vrhovnega sodišča št. 97Mo66 z dne 29. septembra 1997.

([307]) V zakonu o upravnem sporu se uporablja izraz „odločitev“, tj. izvršitev ali zavrnitev izvršitve javnega pooblastila v posamezni zadevi.

([308]) Na podlagi zakona o upravnem sporu se to nanaša na dolgotrajno odlašanje upravnega organa s sprejetjem odločitve, kar je v nasprotju s pravno obveznostjo organa, da odloči v zadevi.

([309]) Upravne odločitve se lahko najprej izpodbijajo pri komisijah za upravne pritožbe, ki so ustanovljene v okviru nekaterih javnih organov (npr. nacionalna obveščevalna služba, nacionalna komisija za človekove pravice), ali pri centralni komisiji za upravne pritožbe, ustanovljeni v okviru komisije za preprečevanje korupcije in državljanske pravice (člen 6 zakona o upravni pritožbi in člen 18(1) zakona o upravnem sporu), kar je bolj neformalno pravno sredstvo. Na podlagi zakona o upravnem sporu pa se lahko vloži tudi tožba neposredno pri korejskih sodiščih.

([310]) Odločba vrhovnega sodišča št. 98Du18435 z dne 22. oktobra 1999, odločba vrhovnega sodišča št. 99Du1113 z dne 8. septembra 2000 in odločba vrhovnega sodišča št. 2010Du3541 z dne 27. septembra 2012.

([311]) Členi 12, 35 in 36 zakona o upravnem sporu. Poleg tega je treba vlogo za razveljavitev/spremembo odločitve in vlogo za ugotovitev nezakonitosti opustitve vložiti v 90 dneh od datuma, ko posameznik izve za odločitev/opustitev, načeloma pa najpozneje eno leto od datuma sprejetja odločitve ali datuma opustitve, razen če obstajajo upravičeni razlogi (člen 20 in člen 38(2) zakona o upravnem sporu). Vrhovno sodišče pojem „upravičeni razlogi“ razlaga široko, tako da je treba presoditi, ali je glede na vse okoliščine zadeve družbeno sprejemljivo dopustiti vložitev zapoznele pritožbe (odločba vrhovnega sodišča št. 90Nu6521 z dne 28. junija 1991). Kot je korejska vlada potrdila v Prilogi II, oddelek 2.4.3, to (med drugim) vključuje razloge za zamudo, za katere zadevna stranka ne more biti odgovorna (tj. okoliščine, na katere pritožnik ne more vplivati, ker na primer ni bil uradno obveščen o zbiranju svojih osebnih podatkov), ali višjo silo (npr. naravno nesrečo, vojno).

([312]) Odločba vrhovnega sodišča št. 2006Du330 z dne 26. marca 2006.

([313]) Člena 2 in 4 zakona o upravnem sporu.

([314]) Člen 30(1) zakona o upravnem sporu.

(182) Poleg izpodbijanja vladnih ukrepov v upravnem sporu lahko posamezniki vložijo tudi ustavno pritožbo pri ustavnem sodišču glede kršitev njihovih temeljnih pravic zaradi izvrševanja ali neizvrševanja pooblastil državnih organov (razen sodnih odločb) ([315]). Najprej pa je treba izčrpati druga pravna sredstva, če so na voljo. Tuji državljani lahko v skladu s sodno prakso ustavnega sodišča vložijo ustavno pritožbo, če so njihove osnovne pravice priznane na podlagi korejske ustave (glej pojasnila v oddelku 1.1) ([316]). Ustavno sodišče lahko izvrševanje pristojnosti državnih organov, ki je povzročilo kršitev, razglasi za nično ali potrdi, da določena opustitev ukrepanja ni ustavna ([317]). V takem primeru mora zadevni organ sprejeti ukrepe za upoštevanje odločbe sodišča.

(183) Poleg tega lahko korejsko sodišče posameznikom prizna odškodnino za škodo. To vključuje predvsem možnost, da se zahteva odškodnina zaradi kršitev zakona o varstvu osebnih podatkov, ki jih storijo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, in sicer v skladu s členom 39 (glej tudi uvodno izjavo (135)). Splošneje velja, da lahko posamezniki zahtevajo odškodnino za škodo, ki jo javni organi povzročijo pri opravljanju svojih dolžnosti v nasprotju z zakonom, in sicer na podlagi zakona o državni odškodnini (glej tudi uvodno izjavo (135)) ([318]).

(184) Mehanizmi, opisani v uvodnih izjavah (176) do (183) posameznikom, na katere se nanašajo osebni podatki, zagotavljajo učinkovito upravno in sodno varstvo, zlasti jim omogočajo uresničevanje pravic, vključno s pravico do dostopa do njihovih osebnih podatkov ali do popravka oziroma izbrisa takih podatkov.

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

(185) Pravo Republike Koreje vsebuje več omejitev in zaščitnih ukrepov glede dostopa do osebnih podatkov in njihove uporabe za namene nacionalne varnosti ter zagotavlja nadzorne mehanizme in mehanizme pravnih sredstev, ki so v skladu z zahtevami iz uvodnih izjav (141) do (143) tega sklepa. Pogoji, pod katerimi je tak dostop mogoč, in zaščitni ukrepi glede uporabe teh pooblastil so podrobneje ocenjeni v naslednjih oddelkih.

3.3.1 *Pravna podlaga, omejitve in zaščitni ukrepi*

(186) V Republiki Koreji je dostop do osebnih podatkov za namene nacionalne varnosti dovoljen na podlagi zakona o varstvu zasebnosti komunikacij, zakona o zagotavljanju telekomunikacijskih storitev ter zakona o boju proti terorizmu za zaščito državljanov in javne varnosti (v nadaljnjem besedilu: zakon o boju proti terorizmu) ([319]). Glavni organ ([320]) s pristojnostmi na področju nacionalne varnosti je nacionalna obveščevalna služba ([321]). Ta mora pri zbiranju in uporabi osebnih podatkov upoštevati ustrezne pravne zahteve (vključno z zakonom

([315]) Člen 68(1) zakona o ustavnem sodišču. Ustavno pritožbo je treba vložiti v 90 dneh po tem, ko je posameznik izvedel za kršitev, in v enem letu po nastanku kršitve. Kot je pojasnjeno tudi v Prilogi II, oddelek 2.4.3, je glede na to, da se za pravdne postopke na podlagi zakona o ustavnem sodišču v skladu s členom 40 navedenega zakona uporablja postopek iz zakona o upravnem sporu, pritožba še vedno dopustna, če za to obstajajo „upravičeni razlogi“, kot se razlagajo v skladu s sodno prakso vrhovnega sodišča, opisano v opombi 312. Če je treba najprej izčrpati druga pravna sredstva, je treba ustavno pritožbo vložiti v 30 dneh po pravnomočni odločbi o takem sredstvu (člen 69 zakona o ustavnem sodišču).

([316]) Odločba ustavnega sodišča št. 99HeonMa194 z dne 29. novembra 2001.

([317]) Člen 75(3) zakona o ustavnem sodišču.

([318]) Člen 2(1) zakona o državni odškodnini.

([319]) Glej Prilogo II, oddelek 3.1.

([320]) Izjemoma lahko tudi policija in tožilstvo zbirata osebne podatke za namene nacionalne varnosti (glej opombo 327 in Prilogo II, oddelek 3.2.1.2). Poleg tega je na področju nacionalne varnosti pristojna tudi korejska vojaška obveščevalna agencija (poveljstvo za varnostno podporo obrambnih sil, ki je ustanovljeno v okviru ministrstva za obrambo). Vendar pa, kot je pojasnjeno v Prilogi II, oddelek 3.1, je navedeno poveljstvo pristojno le za vojaško obveščevalno dejavnost in nadzor nad civilisti izvaja le, kadar je to potrebno za izvajanje njegovih vojaških nalog. Preiskuje lahko na primer le vojaško osebje, civiliste, zaposlene v vojski, osebe na vojaškem usposabljanju, osebe v vojaški službi v rezervni sestavi ali v službi za novačenje in vojne ujetnike (člen 1 zakona o vojaškem sodišču). Poveljstvo za varnostno podporo obrambnih sil mora pri zbiranju podatkov o komunikaciji za namene nacionalne varnosti upoštevati omejitve in zaščitne ukrepe iz zakona o varstvu zasebnosti komunikacij in uredbe o izvajanju tega zakona.

([321]) Nacionalna obveščevalna služba je pristojna za zbiranje, združevanje in razširjanje informacij o tujih državah (tj. splošnih informacij o trendih in razvoju dogodkov v zvezi s tujimi državami ali v zvezi z dejavnostmi državnih akterjev), za obveščevalno dejavnost v zvezi s preprečevanjem vohunjenja (vključno z vojaškim in industrijskim vohunjenjem), terorizma in dejavnosti mednarodnih hudodelskih združb, obveščevalno dejavnost v zvezi z nekaterimi vrstami kaznivih dejanj zoper javno in nacionalno varnost (npr. vstaje v domači državi, tuja agresija) ter obveščevalno dejavnost, povezano z zagotavljanjem kibernetske varnosti, preprečevanjem kibernetskih napadov in groženj ter bojem proti njim (člen 4(2) zakona o nacionalni obveščevalni službi). Glej tudi Prilogo II, oddelek 3.1.

o varstvu osebnih podatkov in zakonom o varstvu zasebnosti komunikacij) ([322]) ter splošne smernice, ki jih pripravi predsednik republike in pregleda parlament ([323]). Nacionalna obveščevalna služba mora na splošno ohranjati politično nevtralnost ter varovati svoboščine in pravice posameznikov ([324]). Poleg tega osebje nacionalne obveščevalne službe ne sme zlorabljati svojih uradnih pooblastil tako, da bi kateri koli organ, organizacijo ali posameznika prisilili v nekaj, kar (po zakonu) niso dolžni storiti, ali posameznika ovirati pri uresničevanju njegovih pravic ([325]).

3.3.1.1 Dostop do podatkov o komunikaciji

(187) Na podlagi zakona o varstvu zasebnosti komunikacij lahko korejski javni organi ([326]) zbirajo podrobne podatke o opravljeni komunikaciji (tj. datum telekomunikacij, čas njihovega začetka in konca, število dohodnih in odhodnih klicev ter naročniška številka sogovornika, pogostost uporabe, dnevniške datoteke o uporabi telekomunikacijskih storitev in podatki o lokaciji, glej uvodno izjavo (155)) in vsebino komunikacij (z ukrepi za omejevanje komunikacij, glej uvodno izjavo (155)) za namene nacionalne varnosti (kot je opredeljena z mandatom nacionalne obveščevalne službe, glej opombo 322 zgoraj). Te pristojnosti se nanašajo na dve vrsti podatkov: (1) na komunikacije, pri katerih je vsaj en udeleženec korejski državljan ([327]); in (2) na komunikacije (a) držav, ki so sovražne Republiki Koreji, (b) tujih organov, skupin ali državljanov, pri katerih obstaja sum sodelovanja pri protikorejskih dejavnostih ([328]), ali (c) članov skupin, ki delujejo na korejskem polotoku, vendar dejansko niso pod pristojnostjo Republike Koreje, in njihovih krovnih skupin v tujih državah ([329]). Komunikacije posameznikov iz EU, ki se prenašajo iz Unije v Republiko Korejo na podlagi tega sklepa, se torej lahko zbirajo le na podlagi zakona o varstvu zasebnosti komunikacij za namene nacionalne varnosti (ob upoštevanju pogojev iz uvodnih izjav (188) do (192)), če potekajo med posameznikom iz EU in korejskim državljanom, ali – če se nanašajo na komunikacije med posamezniki, ki niso korejski državljani – spadajo v eno od treh zgoraj navedenih kategorij (2(a), (b) ali (c)).

(188) V obeh primerih je zbiranje podrobnih podatkov o opravljeni komunikaciji dovoljeno le za namene preprečevanja groženj nacionalni varnosti ([330]), ukrepi za omejevanje komunikacij pa se lahko izvedejo le, če obstaja resna nevarnost za nacionalno varnost in je zbiranje potrebno za preprečitev te nevarnosti ([331]). Poleg tega je dostop do vsebine komunikacij dovoljen le v skrajnem primeru, pri čemer si je treba prizadevati za čim manjšo kršitev zasebnosti komunikacij ([332]), s čimer se zagotovi, da je ukrep sorazmeren s ciljem nacionalne varnosti. Zbiranje podatkov o vsebini komunikacij in podrobnih podatkov o opravljeni komunikaciji lahko traja največ štiri mesece in mora takoj prenehati, če je zastavljeni cilj dosežen predčasno ([333]). Če so ustrezni pogoji še naprej izpolnjeni, se lahko to obdobje podaljša še za največ štiri mesece, in sicer s predhodnim dovoljenjem sodišča (za ukrepe, opisane v uvodni izjavi (189)) ali predsednika republike (za ukrepe, opisane v uvodni izjavi (190)) ([334]).

(189) Enaki postopkovni zaščitni ukrepi veljajo pri zbiranju podrobnih podatkov o opravljeni komunikaciji in pri zbiranju vsebine komunikacij ([335]). Natančneje, kadar je vsaj eden od udeležencev komunikacije korejski državljan, mora obveščevalna agencija vložiti pisno zahtevo pri višjem državnem tožilstvu, to pa mora nato pri predsedniku

([322]) Glej tudi člene 14, 22 in 23 zakona o nacionalni obveščevalni službi.
([323]) Člen 4(2) zakona o nacionalni obveščevalni službi.
([324]) Člen 3(1), člen 6(2) ter člena 11 in 21 zakona o nacionalni obveščevalni službi. Glej tudi pravila o navzkrižju interesov, zlasti člena 10 in 12 zakona o nacionalni obveščevalni službi.
([325]) Člen 13 zakona o nacionalni obveščevalni službi.
([326]) To vključuje obveščevalne agencije (tj. nacionalno obveščevalno službo in poveljstvo za varnostno podporo obrambnih sil) ter policijo/tožilstvo.
([327]) Člen 7(1)1 zakona o varstvu zasebnosti komunikacij.
([328]) Kot je korejska vlada pojasnila v opombi 244 Priloge II, se to nanaša na dejavnosti, ki ogrožajo obstoj in varnost države, demokratično ureditev ali preživetje in svobodo ljudi.
([329]) Člen 7(1)2 zakona o varstvu zasebnosti komunikacij.
([330]) Člen 13-4 zakona o varstvu zasebnosti komunikacij.
([331]) Člen 7(1) zakona o varstvu zasebnosti komunikacij.
([332]) Člen 3(2) zakona o varstvu zasebnosti komunikacij. Poleg tega morajo ukrepi za omejevanje komunikacij prenehati takoj, ko niso več potrebni, da se čim manj posega v zaupnost komunikacij posameznika (člen 2 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij).
([333]) Člen 7(2) zakona o varstvu zasebnosti komunikacij.
([334]) Vlogo za odobritev podaljšanja nadzornih ukrepov je treba vložiti pisno, pri tem pa navesti razloge za podaljšanje in predložiti dokazno gradivo (člen 7(2) zakona o varstvu zasebnosti komunikacij in člen 5 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij).
([335]) Glej člen 13-4(2) zakona o varstvu zasebnosti komunikacij in člen 37(4) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij, v skladu s katerima se postopki, ki se uporabljajo za zbiranje vsebine komunikacij, uporabljajo tudi za zbiranje podrobnih podatkov o opravljeni komunikaciji. Glej tudi Prilogo II, oddelek 3.2.1.1.1.

višjega sodišča vložiti vlogo za izdajo odredbe ([336]). Zakon o varstvu zasebnosti komunikacij vsebuje seznam informacij, ki jih je treba navesti v zahtevi tožilstvu, vlogi za izdajo odredbe in sami odredbi, in sicer zlasti obrazložitev zahteve in glavne razloge za sum, dokazno gradivo ter informacije o cilju, tarči (tj. ciljnem posamezniku), obsegu in trajanju predlaganega ukrepa ([337]). Zbiranje podatkov brez odredbe je dovoljeno le v primeru zarote, ki ogroža nacionalno varnost, ukrepanje pa je tako nujno, da ni mogoče izvesti zgoraj navedenih postopkov ([338]). Vendar pa je treba biti tudi v takem primeru vlogo za izdajo odredbe vložiti takoj po izvedbi ukrepa ([339]). Zakon o varstvu zasebnosti komunikacij torej jasno določa obseg in pogoje takega zbiranja ter v zvezi z njim vzpostavlja posebne (postopkovne) zaščitne ukrepe (vključno s predhodnim soglasjem sodišča), ki zagotavljajo, da je uporaba takih ukrepov omejena na tisto, kar je nujno in sorazmerno. Poleg tega zahteva, da se v vlogi za izdajo odredbe in v sami odredbi zagotovijo podrobne informacije, izključuje možnost neselektivnega dostopa.

(190) V primeru komunikacij med posamezniki, ki niso korejski državljani in spadajo v eno od treh kategorij, navedenih v uvodni izjavi (187), je treba vložiti vlogo pri direktorju nacionalne obveščevalne službe, ki mora po preverjanju ustreznosti predlaganih ukrepov predsednika Republike Koreje zaprositi za predhodno pisno soglasje ([340]). Vloga, ki jo pripravi obveščevalna agencija, mora vključevati enake podrobne informacije kot vloga za izdajo sodne odredbe (glej uvodno izjavo (189)), zlasti glede obrazložitve vloge in glavnih razlogov za sum, dokaznega gradiva ter informacij o ciljih, ciljnih posameznikih, obsegu in trajanju predlaganih ukrepov ([341]). V nujnih primerih ([342]) je treba pridobiti predhodno soglasje ministra, pod katerega ministrstvo spada zadevna obveščevalna agencija, kljub temu pa mora obveščevalna agencija vložiti vlogo za soglasje predsednika republike takoj po izvedbi nujnih ukrepov ([343]). Tudi v zvezi z zbiranjem komunikacij, ki potekajo izključno med posamezniki, ki niso korejski državljani, zakon o varstvu zasebnosti komunikacij torej omejuje uporabo takih ukrepov na tisto, kar je nujno in sorazmerno, pri čemer jasno določa omejene kategorije posameznikov, zoper katere se lahko uporabijo taki ukrepi, in podrobna merila, katerih izpolnjevanje morajo obveščevalne agencije dokazati, da upravičijo vlogo za zbiranje podatkov. Prav tako se s tem tudi izključi neselektiven dostop. Medtem ko za take ukrepe ni predhodnega neodvisnega soglasja, neodvisen nadzor naknadno zagotavljata zlasti komisija za varstvo osebnih podatkov in nacionalna komisija za človekove pravice (glej na primer uvodni izjavi (199) in (200)).

(191) Zakon o varstvu zasebnosti komunikacij nadalje določa še več dodatnih zaščitnih ukrepov, ki prispevajo k naknadnemu nadzoru in posameznikom lajšajo dostop do učinkovitih pravnih sredstev. Prvič, v zvezi s kakršnim koli zbiranjem za namene nacionalne varnosti zakon o varstvu zasebnosti komunikacij določa različne zahteve glede evidentiranja in poročanja. Zlasti kadar obveščevalne agencije zahtevajo sodelovanje zasebnih subjektov, morajo zagotoviti odredbo sodišča/soglasje predsednika republike ali izvod naslovnice izjave o cenzuri v nujnem primeru, ki jo mora, subjekt od katerega se zahteva sodelovanje, hraniti v svoji evidenci ([344]). Če so zasebni subjekti zavezani sodelovati, morata evidence o namenu in cilju ukrepov ter datumu njihove

([336]) Člen 6(5) in (8) ter člen 7(1)1 (3) in zakona o varstvu zasebnosti komunikacij, v povezavi s členom 7(3)-(4) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.

([337]) Glej člen 7(3) in člen 6(4) zakona o varstvu zasebnosti komunikacij (glede vloge, ki jo vloži obveščevalna agencija), člen 4 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij (glede vloge, ki jo vloži tožilstvo) ter člen 7(3) in člen 6(6) navedenega zakona (glede same odredbe).

([338]) Člen 8 zakona o varstvu zasebnosti komunikacij.

([339]) Člen 8(2) in (8) zakona o varstvu zasebnosti komunikacij. Zbiranje mora takoj prenehati, če dovoljenje sodišča ni pridobljeno v 36 urah od začetka izvajanja ukrepov. Če se nadzor zaključi tako hitro, da dovoljenje sodišča ni več potrebno, mora vodja pristojnega višjega državnega tožilstva vodji pristojnega sodišča poslati obvestilo o izvedenem nujnem ukrepu, ki ga pripravi obveščevalna agencija, vodja pristojnega sodišča pa lahko na tej podlagi prouči zakonitost zbiranja (člen 8(5) in (7) zakona o varstvu zasebnosti komunikacij). V tem obvestilu morajo biti navedeni namen, cilj, obseg, obdobje in kraj izvedbe ter način izvajanja nadzora, pa tudi razlogi, zakaj vloga ni bila vložena pred sprejetjem ukrepa (člen 8(6) zakona o varstvu zasebnosti komunikacij). Splošneje velja, da lahko obveščevalne agencije sprejemajo nujne ukrepe le v skladu z „izjavo o cenzuri/prisluškovanju v nujnem primeru“ in da morajo voditi evidence takih ukrepov (člen 8(4) zakona o varstvu zasebnosti komunikacij).

([340]) Člen 8(1) in (2) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.

([341]) Člen 8(3) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij v povezavi s členom 6(4) zakona o varstvu zasebnosti komunikacij.

([342]) To je v primerih, ko je ukrep usmerjen zoper dejanje zarote, ki ogroža nacionalno varnost, in za pridobitev soglasja predsednika republike ni dovolj časa, nesprejetje nujnih ukrepov pa bi lahko ogrozilo nacionalno varnost (člen 8(8) zakona o varstvu zasebnosti komunikacij).

([343]) Člen 8(9) zakona o varstvu zasebnosti komunikacij. Zbiranje mora takoj prenehati, če dovoljenje ni pridobljeno v 36 urah od vložitve vloge.

([344]) Člen 9(2) zakona o varstvu zasebnosti komunikacij in člen 12 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij. Glej člen 13 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij glede možnosti zahtevati sodelovanje poštnih uradov in ponudnikov telekomunikacijskih storitev. Zasebni subjekti, od katerih se zahteva razkritje informacij, lahko tako razkritje zavrnejo, če se odredba/soglasje ali izjava o cenzuri v nujnem primeru nanaša na napačen identifikator (npr. telefonsko številko, ki pripada drugemu posamezniku in ne tistemu, ki je opredeljen). Nikakor pa ne smejo razkriti gesel, ki se uporabljajo za komunikacijo (člen 9(4) zakona o varstvu zasebnosti komunikacij).

izvedbe voditi javni organ, ki zahteva tako sodelovanje, in zadevni subjekt ([345]). Poleg tega morajo obveščevalne agencije o zbranih informacijah in rezultatu dejavnosti nadzora poročati direktorju nacionalne obveščevalne službe ([346]).

(192) Drugič, posamezniki morajo biti uradno obveščeni o zbiranju njihovih podatkov za namene nacionalne varnosti (podrobnih podatkov o opravljeni komunikaciji ali vsebini komunikacij), če se nanašajo na komunikacijo, pri kateri je vsaj eden od udeležencev korejski državljan ([347]). Tako uradno obvestilo je treba poslati pisno v 30 dneh od dneva, ko se zbiranje konča (tudi če so bili podatki pridobljeni na podlagi nujnega postopka), pošiljanje pa se lahko odloži le, če in dokler bi ogrožalo nacionalno varnost ali škodilo življenju in telesni varnosti ljudi ([348]). Ne glede na tako uradno obveščanje lahko posamezniki na različne načine uveljavljajo pravno varstvo, kot je podrobneje pojasnjeno v oddelku 3.3.4.

3.3.1.2 Zbiranje podatkov o osumljencih terorizma

(193) Zakon o boju proti terorizmu določa, da lahko nacionalna obveščevalna služba zbira podatke o osumljencih terorizma ([349]) v skladu z omejitvami in zaščitnimi ukrepi, določenimi v drugih zakonih ([350]). Nacionalna obveščevalna služba lahko zlasti pridobi podatke o komunikaciji (na podlagi zakona o varstvu zasebnosti komunikacij) in druge osebne podatke (na podlagi zahteve za prostovoljno razkritje) ([351]). V zvezi z zbiranjem podatkov o komunikaciji (tj. vsebini komunikacij ali podrobnih podatkih o opravljeni komunikaciji) veljajo omejitve in zaščitni ukrepi, opisani v oddelku 3.3.1.1, vključno z zahtevo za pridobitev sodne odredbe. Glede prošenj za prostovoljno razkritje drugih kategorij osebnih podatkov o osumljencih terorizma mora nacionalna obveščevalna služba upoštevati zahteve iz ustave in zakona o varstvu osebnih podatkov v zvezi z nujnostjo in sorazmernostjo (glej uvodno izjavo (164)) ([352]). Upravljavci, ki prejmejo take prošnje, jih lahko prostovoljno izpolnijo ob upoštevanju pogojev iz zakona o varstvu osebnih podatkov (npr. v skladu z načelom najmanjšega obsega podatkov in z omejitvijo vpliva na zasebnost posameznika) ([353]). V tem primeru morajo upoštevati tudi zahtevo po uradnem obveščanju zadevnega posameznika v skladu z uradnim obvestilom št. 2021-5 (glej uvodno izjavo (166)).

([345]) V primeru ukrepov za omejevanje komunikacij je treba take evidence hraniti tri leta, glej člen 9(3) zakona o varstvu zasebnosti komunikacij in člen 17(2) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij. V zvezi s podrobnimi podatki o opravljeni komunikaciji morajo obveščevalne agencije hraniti evidence o tem, da je bila vložena zahteva za take podatke, ter o sami pisni zahtevi in instituciji, ki se je nanjo oprla (člen 13(5) in člen 13-4(3) zakona o varstvu zasebnosti komunikacij). Ponudniki telekomunikacijskih storitev morajo evidence hraniti sedem let ter dvakrat letno ministrstvu za znanost in IKT poročati o pogostosti takih razkritij (člen 9(3) zakona o varstvu zasebnosti komunikacij v povezavi s členom 13(7) navedenega zakona ter členom 37(4) in členom 39 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij).

([346]) Člen 18(3) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.

([347]) Člen 9-2(3) in člen 13-4 zakona o varstvu zasebnosti komunikacij. V uradnem obvestilu mora biti navedeno, (1) da so se podatki zbirali, (2) kateri organ jih je zbiral in (3) obdobje zbiranja.

([348]) Člen 9-2(4) zakona o varstvu zasebnosti komunikacij. V takem primeru je treba uradno obvestilo poslati v 30 dneh po prenehanju razlogov za odlog, glej člen 13-4(2) in člen 9-2(6) zakona o varstvu zasebnosti komunikacij.

([349]) Torej o članih terorističnih skupin (kot jih opredeljujejo Združeni narodi, glej člen 2(2) zakona o boju proti terorizmu), osebah, ki spodbujajo in razširjajo zamisli ali taktike teroristične skupine, zbirajo ali prispevajo sredstva za terorizem oziroma so vpletene v druge dejavnosti pripravljanja ali širjenja terorizma, sodelovanja pri njem ali napeljevanja k njemu, ali osebah, v zvezi s katerimi obstaja utemeljen sum, da so take dejavnosti izvajale (člen 2(3) zakona o boju proti terorizmu). „Terorizem“ je v členu 2(1) zakona o boju proti terorizmu opredeljen kot ravnanje, storjeno z namenom oviranja izvajanja pooblastil države, lokalne države ali tuje vlade (vključno z mednarodnimi organizacijami) ali z namenom, da se jih prisili k ukrepanju, kadar za to ni pravne obveznosti, ali za namene zastraševanja javnosti. Tako ravnanje lahko na primer vključuje povzročitev smrti, ugrabitev oseb ali zajemanje talcev, ugrabitev ali zaseg prevoznih sredstev, uničenje ali poškodovanje plovila ali zrakoplova, uporabo biokemičnega, eksplozivnega ali zažigalnega orožja z namenom povzročitve smrti, resne poškodbe ali škode in zlorabo jedrskih ali radioaktivnih materialov.

([350]) Člen 9(1) in (3) zakona o boju proti terorizmu.

([351]) Čeprav se zakon o boju proti terorizmu sklicuje tudi na možnost zbiranja podatkov o vstopu v Republiko Korejo in izstopu iz nje na podlagi zakona o priseljevanju in carinskega zakona, pa navedena zakona trenutno takega pooblastila ne vsebujeta (glej Prilogo II, oddelek 3.2.2.1). Vsekakor naj se navedena zakona načeloma ne bi uporabljala za podatke, prenesene na podlagi tega sklepa, saj se običajno nanašata na podatke, ki jih neposredno zberejo korejski organi (in ne na dostop do podatkov, ki so bili predhodno preneseni iz Unije korejskim upravljavcem). Poleg tega je v zakonu o boju proti terorizmu kot pravna podlaga za zbiranje podatkov o finančnih transakcijah naveden zakon o sporočanju in uporabi specifičnih informacij o finančnih transakcijah. Kot pa je pojasnjeno v opombi 200, kategorije podatkov, ki bi jih bilo mogoče pridobiti na podlagi tega zakona, ne spadajo na področje tega sklepa. Nazadnje, zakon o boju proti terorizmu tudi določa, da lahko nacionalna obveščevalna služba zbira podatke o lokaciji na podlagi nezavezujočih prošenj – v takem primeru lahko ponudniki podatkov o lokaciji prostovoljno razkrijejo take podatke ob upoštevanju pogojev iz zakona o varstvu osebnih podatkov (kot je opisano v uvodni izjavi (193)) in zakona o podatkih o lokaciji. Kot pa je pojasnjeno tudi v opombi 17, se podatki o lokaciji ne bodo prenašali iz Unije korejskim upravljavcem na podlagi tega sklepa, ampak se bodo ustvarjali znotraj Koreje.

([352]) Glej Prilogo II, oddelek 3.2.2.2.

([353]) Glej člen 58(4) zakona o varstvu osebnih podatkov, v skladu s katerim se morajo osebni podatki obdelovati v najmanjšem možnem obsegu, da se doseže želeni namen, in člen 3(6) navedenega zakona, ki določa, da je treba osebne podatke obdelovati tako, da se čim bolj zmanjša možnost poseganja v zasebnost posameznika. Glej tudi člen 59, točki 2 in 3, zakona o varstvu osebnih podatkov, v skladu s katerim upravljavci ne smejo razkriti osebnih podatkov tretjim osebam brez pooblastila.

3.3.1.3 Prošnje za prostovoljno razkritje podatkov o naročnikih

(194) Na podlagi zakona o zagotavljanju telekomunikacijskih storitev lahko ponudniki telekomunikacijskih storitev prostovoljno razkrijejo podatke o naročnikih (glej uvodno izjavo (163)) na prošnjo obveščevalne agencije, ki namerava take podatke zbrati za preprečitev grožnje nacionalni varnosti ([354]). V zvezi s takimi prošnjami nacionalne obveščevalne službe veljajo enake omejitve (na podlagi ustave, zakona o varstvu osebnih podatkov in zakona o zagotavljanju telekomunikacijskih storitev) kot na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, kot je navedeno v uvodni izjavi (164) ([355]). Ponudniki telekomunikacij niso zavezani ugoditi prošnji, če to storijo, pa morajo upoštevati pogoje iz zakona o varstvu osebnih podatkov (zlasti v skladu z načelom najmanjšega obsega podatkov in z omejitvijo vpliva na zasebnost posameznika, glej tudi uvodno izjavo (193)). Veljajo enake zahteve glede vodenja evidenc in uradnega obveščanja zadevnih posameznikov kot na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (glej uvodni izjavi (165) in (166)).

3.3.2 *Nadaljnja uporaba zbranih informacij*

(195) Pri obdelavi osebnih podatkov, ki jih korejski organi zberejo za namene nacionalne varnosti, se uporabljajo načela omejitve namena (člen 3(1)-(2) zakona o varstvu osebnih podatkov), zakonitosti in poštenosti obdelave (člen 3(1) zakona o varstvu osebnih podatkov), sorazmernosti/najmanjšega obsega podatkov (člen 3(1) in (6) ter člen 58 zakona o varstvu osebnih podatkov), točnosti (člen 3(3) zakona o varstvu osebnih podatkov), preglednosti (člen 3 (5) zakona o varstvu osebnih podatkov), varnosti (člen 58(4) zakona o varstvu osebnih podatkov) in omejitve hrambe (člen 58(4) zakona o varstvu osebnih podatkov) ([356]). Morebitno razkritje osebnih podatkov tretjim osebam (vključno s tretjimi državami) se lahko izvede le v skladu s temi načeli (zlasti omejitev namena in najmanjši obseg podatkov), potem ko se oceni skladnost z načeloma nujnosti in sorazmernosti (člen 37(2) ustave) in ob upoštevanju vpliva na pravice zadevnih posameznikov (člen 3(6) zakona o varstvu osebnih podatkov).

(196) Glede vsebine komunikacij in podrobnih podatkov o opravljeni komunikaciji zakon o varstvu zasebnosti komunikacij nadalje omejuje uporabo takih podatkov na sodne postopke, v katerih se udeleženec komunikacije nanje sklicuje v okviru odškodninskega zahtevka, oziroma na dovoljeno uporabo na podlagi drugih zakonov ([357]).

3.3.3 *Nadzor*

(197) Dejavnosti korejskih organov za nacionalno varnost nadzorujejo različni organi ([358]).

(198) Prvič, zakon o boju proti terorizmu določa posebne nadzorne mehanizme za dejavnosti boja proti terorizmu, vključno z zbiranjem podatkov o osumljencih terorizma. Natančneje, na izvršilni ravni dejavnosti boja proti terorizmu nadzoruje komisija za boj proti terorizmu ([359]), ki ji mora direktor nacionalne obveščevalne službe poročati o preiskavah in sledenju osumljencem terorizma za namene zbiranja informacij ali gradiv, potrebnih za izvajanje dejavnosti boja proti terorizmu ([360]). Poleg tega pooblaščena oseba za varstvo človekovih pravic posebej nadzoruje skladnost dejavnosti boja proti terorizmu s temeljnimi pravicami ([361]). Pooblaščeno osebo za varstvo človekovih pravic imenuje predsednik komisije za boj proti terorizmu izmed posameznikov, ki izpolnjujejo posebne pogoje, navedene v uredbi o izvajanju zakona o boju proti terorizmu ([362]), in sicer za obdobje dveh let, ki ga je mogoče podaljšati, razrešiti pa jo je mogoče le iz posebnih, omejenih in upravičenih razlogov ([363]). Pooblaščena oseba za varstvo človekovih pravic lahko pri izvajanju svoje nadzorne funkcije izdaja splošna

([354]) Člen 83(3) zakona o zagotavljanju telekomunikacijskih storitev.
([355]) Glej tudi Prilogo II, oddelek 3.2.3.
([356]) Glej Prilogo II, oddelek 1.2.
([357]) Člen 5(1)-(2), člen 12 in člen 13-5 zakona o varstvu zasebnosti komunikacij.
([358]) Glej Prilogo II, oddelek 3.3.
([359]) Člen 5(3) zakona o boju proti terorizmu. Komisiji predseduje predsednik vlade, sestavlja pa jo več ministrov in vodij vladnih agencij, kot so ministri za zunanje zadeve, pravosodje, obrambo ter notranje zadeve in varnost, direktor nacionalne obveščevalne službe in generalni komisar nacionalne policije (člen 3(1) uredbe o izvajanju zakona o boju proti terorizmu).
([360]) Člen 9(4) zakona o boju proti terorizmu.
([361]) Člen 7 zakona o boju proti terorizmu.
([362]) Torej vsakdo, ki je usposobljen kot odvetnik in ima vsaj deset let delovnih izkušenj, ki ima strokovno znanje na področju človekovih pravic in je ali je bil (vsaj) deset let zaposlen na položaju izrednega profesorja ali na položaju višjega javnega uslužbenca v državnih organih ali lokalnih upravnih organih ali ki ima najmanj deset let delovnih izkušenj na področju človekovih pravic, na primer v nevladni organizaciji (člen 7(1) uredbe o izvajanju zakona o boju proti terorizmu).
([363]) Če je na primer obsojena v kazenski zadevi v povezavi z opravljanjem svojih nalog, če razkrije zaupne informacije ali zaradi dolgotrajne duševne ali fizične nezmožnosti (člen 7(3) uredbe o izvajanju zakona o boju proti terorizmu).

priporočila za izboljšanje varstva človekovih pravic ([364]) ter posebna priporočila za popravne ukrepe, če se ugotovi kršitev človekovih pravic ([365]). Javni organi morajo pooblaščeno osebo za varstvo človekovih pravic obveščati o nadaljnjem ukrepanju na podlagi njenih priporočil ([366]).

(199) Drugič, komisija za varstvo osebnih podatkov nadzoruje zagotavljanje skladnosti organov za nacionalno varnost s pravili o varstvu podatkov, kar vključuje upoštevne določbe zakona o varstvu osebnih podatkov (glej uvodno izjavo (149)) ter omejitve in zaščitne ukrepe, ki se uporabljajo za zbiranje osebnih podatkov na podlagi drugih zakonov (zakona o varstvu zasebnosti komunikacij, zakona o boju proti terorizmu in zakona o zagotavljanju telekomunikacijskih storitev, glej tudi uvodno izjavo (171)) ([367]). Pri izvrševanju te nadzorne vloge lahko komisija za varstvo osebnih podatkov uporabi vsa svoja preiskovalna in popravna pooblastila, kot so podrobno opisana v oddelku 2.4.2.

(200) Tretjič, dejavnosti organov nacionalne varnosti neodvisno nadzoruje nacionalna komisija za človekove pravice, in sicer v skladu s postopki, opisanimi v uvodni izjavi (172) ([368]).

(201) Četrtič, nadzorna funkcija odbora za revizijo in inšpekcijski pregled se nanaša tudi na organe za nacionalno varnost, čeprav lahko nacionalna obveščevalna služba v izjemnih okoliščinah zavrne predložitev nekaterih informacij ali gradiva, tj. če gre za državne skrivnosti in bi njihovo javno razkritje pomembno vplivalo na nacionalno varnost ([369]).

(202) Nazadnje, parlamentarni nadzor nad dejavnostjo nacionalne obveščevalne službe opravlja parlament (prek posebnega odbora za obveščevalno dejavnost) ([370]). Zakon o varstvu zasebnosti komunikacij določa posebno nadzorno vlogo parlamenta v zvezi z uporabo ukrepov za omejevanje komunikacij za namene nacionalne varnosti ([371]). Parlament lahko opravlja zlasti preglede na terenu, in sicer preglede opreme za prisluškovanje, ter lahko od nacionalne obveščevalne službe in telekomunikacijskih operaterjev, ki so razkrili vsebino komunikacij, zahteva poročilo o takih razkritjih. Parlament lahko izvaja tudi splošni nadzor (v skladu s postopki, opisanimi v uvodni izjavi (174)). V skladu z zakonom o nacionalni obveščevalni službi se mora direktor navedene službe brez odlašanja odzvati, če odbor za obveščevalno dejavnost zahteva poročilo o posamezni zadevi ([372]), določa pa tudi posebna pravila glede nekaterih posebno občutljivih podatkov. Dejansko to pomeni, da lahko direktor nacionalne obveščevalne službe zavrne odgovor ali pričanje pred odborom le v izjemnih okoliščinah, tj. če se zahteva nanaša na državne skrivnosti v zvezi z vojaškimi ali diplomatskimi zadevami ali zadevami, povezanimi s Severno Korejo, katerih javno razkritje bi lahko resno vplivalo na „nacionalno usodo“ ([373]). V takem primeru lahko odbor za obveščevalno dejavnost od predsednika vlade zahteva pojasnilo in če to ni predloženo v sedmih dneh, odgovora ali pričanja ni mogoče zavrniti.

3.3.4 *Pravno varstvo*

(203) Korejski sistem tudi na področju nacionalne varnosti ponuja različne (sodne) poti za uveljavljanje pravnega varstva, vključno z odškodnino za škodo. Ti mehanizmi posameznikom, na katere se nanašajo osebni podatki, zagotavljajo učinkovito upravno in sodno varstvo, zlasti jim omogočajo uresničevanje pravic, vključno s pravico do dostopa do njihovih osebnih podatkov ali do popravka oziroma izbrisa takih podatkov.

(204) Prvič, v skladu s členom 3(5) ter členom 4(1), (3) in (4) zakona o varstvu osebnih podatkov lahko posamezniki pri organih za nacionalno varnost uresničujejo svoje pravice do dostopa, popravka, izbrisa in prenehanja. V oddelku 6 uradnega obvestila št. 2021-5 (Priloga I k temu sklepu) je nadalje pojasnjeno, kako se te pravice uporabljajo v okviru obdelave podatkov za namene nacionalne varnosti. Zlasti velja, da lahko organ za nacionalno varnost uresničevanje pravice omeji ali zavrne le, kolikor in dokler je to potrebno in sorazmerno za zaščito

([364]) Člen 8(1) uredbe o izvajanju zakona o boju proti terorizmu.
([365]) Člen 9(1) uredbe o izvajanju zakona o boju proti terorizmu. Pooblaščena oseba za varstvo človekovih pravic samostojno odloča o sprejetju priporočil, vendar mora o njih poročati predsedniku komisije za boj proti terorizmu.
([366]) Člen 9(2) uredbe o izvajanju zakona o boju proti terorizmu. Glede na uradne navedbe korejske vlade v primeru neupoštevanja priporočila pooblaščene osebe za varstvo človekovih pravic to vprašanje obravnava komisija za boj proti terorizmu, vključno s predsednikom vlade, čeprav se do zdaj še ni zgodilo, da priporočila pooblaščene osebe za varstvo človekovih pravic ne bi bila upoštevana (glej Prilogo II, oddelek 3.3.1).
([367]) Priloga II, oddelek 3.3.4.
([368]) Nacionalna komisija za človekove pravice je v preteklosti zlasti glede nacionalne obveščevalne službe izvedla preiskave po uradni dolžnosti in obravnavala več pritožb posameznikov. Glej na primer letno poročilo nacionalne komisije za človekove pravice za leto 2018, str. 128 (na voljo na naslovu: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) in njeno letno poročilo za leto 2019, str. 70 (na voljo na naslovu: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) Člen 13(1) zakona o nacionalni obveščevalni službi.
([370]) Člen 36 in člen 37(1)15 zakona o parlamentu.
([371]) Člen 15 zakona o varstvu zasebnosti komunikacij.
([372]) Člen 15(2) zakona o nacionalni obveščevalni službi.
([373]) Člen 17(2) zakona o nacionalni obveščevalni službi. „Državne skrivnosti“ so opredeljene kot (tajna) dejstva, dobrine ali znanje, ki se ne smejo razkriti nobeni drugi državi ali organizaciji, da se prepreči kakršno koli resno poslabšanje nacionalne varnosti, in do katerih je dovoljen le omejen dostop. Glej člen 13(4) zakona o nacionalni obveščevalni službi.

pomembnega cilja v javnem interesu (npr. kolikor in dokler bi priznanje pravice ogrozilo tekočo preiskavo ali nacionalno varnost) ali kadar bi lahko priznanje pravice povzročilo škodo življenju ali telesu tretje osebe. Pri uveljavljanju take omejitve je torej treba tehtati med pravicami in interesi posameznika ter pomembnimi javnimi interesi, pri čemer se nikakor ne sme posegati v bistvo pravice (člen 37(2) ustave). Če se zahteva zavrne ali njeno uresničevanje omeji, je treba posameznika nemudoma uradno obvestiti o razlogih.

(205) Drugič, posamezniki imajo pravico uveljavljati pravno varstvo na podlagi zakona o varstvu osebnih podatkov, če je organ za nacionalno varnost obdeloval njihove podatke v nasprotju z zakonom o varstvu osebnih podatkov ali v nasprotju z omejitvami in zaščitnimi ukrepi iz drugih zakonov, ki urejajo zbiranje osebnih podatkov (zlasti zakona o varstvu zasebnosti komunikacij, glej uvodno izjavo (171)) ([374]). To pravico je mogoče uresničevati z vložitvijo pritožbe pri komisiji za varstvo osebnih podatkov (tudi prek klicnega centra za vprašanja v zvezi z zasebnostjo, ki ga vodi korejska agencija za splet in varnost) ([375]). Poleg tega lahko posamezniki iz EU za lažji dostop do pravnega sredstva zoper korejske organe za nacionalno varnost vložijo pritožbo pri komisiji za varstvo osebnih podatkov prek svojega nacionalnega organa za varstvo podatkov ([376]). V tem primeru komisija za varstvo osebnih podatkov posameznika uradno obvesti prek nacionalnega organa za varstvo podatkov po zaključku preiskave (med drugim, če je ustrezno, o naloženih popravnih ukrepih). Na podlagi zakona o upravnem sporu se lahko posamezniki tudi pritožijo zoper odločitev komisije za varstvo osebnih podatkov ali jo izpodbijajo oziroma se pritožijo zoper neukrepanje navedene komisije (glej uvodno izjavo (132)).

(206) Tretjič, posamezniki lahko pri pooblaščeni osebi za varstvo človekovih pravic vložijo pritožbo zaradi kršitve pravice do zasebnosti/varstva podatkov v okviru dejavnosti boja proti terorizmu (tj. na podlagi zakona o boju proti terorizmu) ([377]), pooblaščena oseba pa lahko priporoči popravne ukrepe. Ker za pritožbo pri pooblaščeni osebi za varstvo človekovih pravic ne veljajo zahteve glede dopustnosti, se taka pritožba obravnava tudi, če zadevni posameznik ne more dokazati, da mu je dejansko nastala škoda (npr. zaradi domnevnega nezakonitega zbiranja njegovih podatkov s strani organa za nacionalno varnost) ([378]). Zadevni organ mora pooblaščeno osebo za varstvo človekovih pravic obvestiti o vseh ukrepih, ki jih je sprejel za izpolnitev njenih priporočil.

(207) Četrtič, posamezniki lahko vložijo pritožbo pri nacionalni komisiji za človekove pravice v zvezi z zbiranjem njihovih podatkov s strani organa za nacionalno varnost in uveljavljajo pravno varstvo v skladu s postopkom, opisanim v uvodni izjavi (178) ([379]).

(208) Nazadnje, na voljo so različna sodna pravna sredstva ([380]), ki posameznikom omogočajo sklicevanje na omejitve in zaščitne ukrepe, opisane v oddelku 3.3.1, za uveljavljanje pravnega varstva. Posamezniki lahko zlasti izpodbijajo zakonitost dejanj organov za nacionalno varnost na podlagi zakona o upravnem sporu (v skladu s postopkom, opisanim v uvodni izjavi (181)) ali zakona o ustavnem sodišču (glej uvodno izjavo (182)). Poleg tega lahko prejmejo odškodnino za škodo na podlagi zakona o državni odškodnini (kot je podrobneje opisano v uvodni izjavi (183)).

4. **SKLEPNA UGOTOVITEV**

(209) Komisija meni, da Republika Koreja – z zakonom o varstvu osebnih podatkov, posebnimi pravili, ki se uporabljajo v nekaterih sektorjih (kot je analizirano v oddelku 2), in dodatnimi zaščitnimi ukrepi iz uradnega obvestila št. 2021-5 (Priloga I) – zagotavlja raven varstva osebnih podatkov, prenesenih iz Evropske unije, ki je v osnovi enakovredna ravni, zagotovljeni z Uredbo (EU) 2016/679.

(210) Komisija prav tako meni, da kot celota nadzorni mehanizmi in pravna sredstva v korejskem pravu omogočajo ugotavljanje in obravnavanje kršitev pravil o varstvu podatkov s strani upravljavcev v Koreji ter posameznikom, na katere se nanašajo osebni podatki, zagotavljajo pravna sredstva, s katerimi lahko pridobijo dostop do svojih osebnih podatkov in po potrebi dosežejo popravek ali izbris takih podatkov.

([374]) Člen 58(4) in člen 4(5) zakona o varstvu osebnih podatkov. Glej Prilogo II, oddelek 3.4.2.
([375]) Člen 62 in člen 63(2) zakona o varstvu osebnih podatkov.
([376]) Uradno obvestilo št. 2021-5 (Priloga I, oddelek 6).
([377]) Člen 8(1), točka 2, uredbe o izvajanju zakona o boju proti terorizmu.
([378]) Glej Prilogo II, oddelek 3.4.1.
([379]) Nacionalna komisija za človekove pravice na primer redno prejema pritožbe zoper nacionalno obveščevalno službo, glej podatke v letnem poročilu navedene komisije za leto 2019 o številu prejetih pritožb med letoma 2015 in 2019, str. 70 (na voljo na naslovu: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Glej Prilogo II, oddelek 3.4.4.

(211) Nazadnje, Komisija na podlagi razpoložljivih informacij o korejskem pravnem redu, vključno z navedbami, zagotovili in zavezami korejske vlade iz Priloge II, meni, da bo kakršno koli poseganje v temeljne pravice posameznikov, katerih osebni podatki se prenašajo iz Evropske unije v Republiko Korejo, s strani korejskih javnih organov v javnem interesu, zlasti za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter namene nacionalne varnosti, omejeno na to, kar je nujno potrebno za dosego zadevnega zakonitega cilja, ter da obstaja učinkovita pravna zaščita pred takim poseganjem.

(212) Glede na ugotovitve iz tega sklepa je torej treba odločiti, da Republika Koreja zagotavlja ustrezno raven varstva v smislu člena 45 Uredbe (EU) 2016/679, kakor se razlaga glede na Listino Evropske unije o temeljnih pravicah, glede osebnih podatkov, ki se iz Evropske unije prenesejo upravljavcem osebnih podatkov v Republiki Koreji, za katere se uporablja zakon o varstvu osebnih podatkov, z izjemo verskih organizacij, če osebne podatke obdelujejo za namen misijonarske dejavnosti, političnih strank, če osebne podatke obdelujejo v okviru imenovanja kandidatov, in upravljavcev, ki jih nadzoruje komisija za finančne storitve, glede obdelave osebnih kreditnih informacij v skladu z zakonom o kreditnih informacijah, če obdelujejo take podatke.

5. **UČINKI TEGA SKLEPA IN UKREPI ORGANOV ZA VARSTVO PODATKOV**

(213) 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 izpodbojne tožbe ali razglašeni za neveljavne na podlagi predloga za sprejetje predhodne odločbe ali sklicevanja na nezakonitost.

(214) Zato je sklep 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. Natančneje, prenosi od upravljavca ali obdelovalca v Evropski uniji upravljavcem v Republiki Koreji lahko potekajo, ne da bi bilo treba pridobiti nadaljnje dovoljenje.

(215) V skladu s členom 58(5) Uredbe (EU) 2016/679 in glede na pojasnila Sodišča EU v sodbi v zadevi Schrems ([381]) je treba opozoriti, da če ima nacionalni organ za varstvo podatkov, med drugim po prejemu pritožbe, pomisleke o skladnosti sklepa Komisije o ustreznosti s temeljnimi pravicami posameznika do zasebnosti in varstva podatkov, mu mora nacionalno pravo zagotavljati pravno sredstvo za predložitev teh ugovorov nacionalnemu sodišču, ki bi morda moralo pri Sodišču Evropske unije vložiti predlog za sprejetje predhodne odločbe ([382]).

6. **SPREMLJANJE IN PREGLED TEGA SKLEPA**

(216) V skladu s sodno prakso Sodišča ([383]) in kot je navedeno v členu 45(4) Uredbe (EU) 2016/679, bi morala Komisija po sprejetju sklepa o ustreznosti redno spremljati razvoj dogodkov v tretji državi, da se presodi, ali tretja država še zagotavlja v osnovi enakovredno raven varstva. Tako preverjanje je vsekakor nujno, kadar Komisija prejme kakršne koli informacije, ki zbujajo upravičen dvom o tem.

(217) Komisija bi zato morala stalno spremljati razmere v Republiki Koreji, kar zadeva pravni okvir in dejansko prakso obdelave osebnih podatkov, kot sta ocenjena v tem sklepu, vključno z zagotavljanjem skladnosti korejskih organov z navedbami, zagotovili in zavezami iz Priloge II. Za olajšanje tega postopka Komisija korejske organe poziva, naj jo takoj obvestijo o razvoju dogodkov, bistvenih za ta sklep, in sicer glede obdelave osebnih podatkov s strani poslovnih subjektov in javnih organov ter glede omejitev in zaščitnih ukrepov, ki se uporabljajo v zvezi z dostopom javnih organov do osebnih podatkov.

([381]) Sodba v zadevi Schrems, točka 65.

([382]) 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.“

([383]) Sodba v zadevi Schrems, točka 76.

(218) Poleg tega bi morale države članice 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, v zvezi s prenosom osebnih podatkov iz Evropske unije upravljavcem podatkov v Republiki Koreji, da lahko Komisija učinkovito izvaja naloge spremljanja. Komisija bi morala biti obveščena tudi o kakršnih koli indicih, da ukrepi korejskih 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.

(219) Komisija bi morala po sprejetju tega sklepa na podlagi člena 45(3) Uredbe (EU) 2016/679 ([384]) in ob upoštevanju dejstva, da se lahko raven varstva, ki ga zagotavlja korejski pravni red, spremeni, redno preverjati, ali so ugotovitve, ki se nanašajo na ustreznost ravni varstva, ki jo zagotavlja Republika Koreja, še vedno dejansko in pravno upravičene.

(220) V ta namen bi bilo treba ta sklep prvič pregledati v treh letih po začetku njegove veljavnosti. Komisija po tem prvem pregledu in glede na rezultate pregleda v tesnem posvetovanju z odborom, ustanovljenim v skladu s členom 93(1) Uredbe (EU) 2016/679, odloči, ali je treba ohraniti triletni cikel. V vsakem primeru morajo nadaljnji pregledi potekati vsaj vsaka štiri leta ([385]). Pregled bi moral vključevati vse vidike delovanja tega sklepa, zlasti uporabo dodatnih zaščitnih ukrepov iz Priloge I k temu sklepu, pri čemer bi bilo treba posebno pozornost nameniti varstvu v primeru nadaljnjih prenosov; razvoj ustrezne sodne prakse; pravila o obdelavi psevdonimiziranih informacij za statistične namene, znanstvene raziskave in arhiviranje v javnem interesu ter uporabo izjem iz člena 28(7) zakona o varstvu osebnih podatkov; učinkovitost uresničevanja pravic posameznikov, med drugim pred nedavno prenovljeno komisijo za varstvo osebnih podatkov uporabo delnih izjem iz zakona o varstvu osebnih podatkov; ter omejitve in zaščitne ukrepe glede vladnega dostopa (kot je navedeno v Prilogi II k temu sklepu), vključno s sodelovanjem komisije za varstvo osebnih podatkov z organi EU za varstvo podatkov glede pritožb posameznikov. Vključevati bi moral tudi učinkovitost nadzora in izvrševanja na področju zakona o varstvu osebnih podatkov, preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter nacionalne varnosti (zlasti v okviru komisije za varstvo osebnih podatkov in nacionalne komisije za človekove pravice).

(221) Komisija bi se morala v okviru izvajanja pregleda srečati s komisijo za varstvo osebnih podatkov, ki bi jo po potrebi spremljali še drugi korejski organi, odgovorni za vladni dostop, vključno z zadevnimi nadzornimi organi. Možnost sodelovanja na takem srečanju bi morali imeti tudi predstavniki članov Evropskega odbora za varstvo podatkov. Komisija bi morala v okviru pregleda od komisije za varstvo osebnih podatkov zahtevati predložitev celovitih informacij o vseh vidikih, pomembnih za ugotavljanje ustreznosti, med drugim o omejitvah in zaščitnih ukrepih v zvezi z vladnim dostopom ([386]). Komisija bi morala tudi zahtevati pojasnila o vseh prejetih informacijah, pomembnih za ta sklep, vključno z javnimi poročili korejskih organov ali drugih deležnikov v Koreji, Evropskega odbora za varstvo podatkov, posameznih organov za varstvo podatkov, skupin civilne družbe, poročil medijev ali katerih koli drugih razpoložljivih virov informacij.

(222) Komisija bi morala na podlagi pregleda pripraviti javno poročilo, ki se predloži Evropskemu parlamentu in Svetu.

7. ZAČASNO ZADRŽANJE IZVAJANJA, RAZVELJAVITEV ALI SPREMEMBA TEGA SKLEPA

(223) Če se na podlagi razpoložljivih informacij, zlasti tistih, ki izhajajo iz spremljanja tega sklepa ali ki jih zagotovijo korejski organi ali organi držav članic, ugotovi, da raven varstva, ki ga zagotavlja Republika Koreja, morda ni več ustrezna, bi morala Komisija o tem takoj obvestiti pristojne korejske organe in zahtevati, naj se v določenem razumnem roku sprejmejo ustrezni ukrepi.

(224) Če pristojni korejski organi ob preteku tega določenega roka ne sprejmejo navedenih ukrepov ali drugače zadovoljivo dokažejo, da ta sklep še naprej temelji na ustrezni ravni varstva, bo Komisija začela postopek iz člena 93(2) Uredbe (EU) 2016/679 za začasno zadržanje izvajanja ali za razveljavitev dela ali celotnega tega sklepa.

(225) Druga možnost je, da bo Komisija začela navedeni postopek za spremembo tega sklepa, zlasti z uvedbo dodatnih pogojev za prenos podatkov ali z omejitvijo področja uporabe ugotovitve o ustreznosti samo na prenose podatkov, za katere je še naprej zagotovljena ustrezna raven varstva.

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

([385]) 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.

([386]) Glej Prilogo II k temu sklepu.

(226) Komisija bi morala zlasti začeti postopek za začasno zadržanje izvajanja ali razveljavitev v primeru indicev, da poslovni subjekti, ki prejemajo osebne podatke na podlagi tega sklepa, ne upoštevajo dodatnih zaščitnih ukrepov iz Priloge I in/ali da se ti ukrepi ne izvršujejo učinkovito oziroma da korejski organi ne upoštevajo navedb, zagotovil in zavez iz Priloge II k temu sklepu.

(227) Prav tako bi morala Komisija razmisliti o začetku postopka za spremembo, začasno zadržanje izvajanja ali razveljavitev tega sklepa, če v okviru pregleda ali kako drugače pristojni korejski organi ne zagotovijo informacij ali pojasnil, potrebnih za oceno ravni varstva, ki se zagotavlja glede osebnih podatkov, prenesenih iz Evropske unije v Republiko Korejo, ali skladnosti s tem sklepom. V tem smislu bi morala Komisija upoštevati, v kolikšni meri je mogoče zadevne informacije pridobiti iz drugih virov.

(228) Komisija bo v ustrezno utemeljenih nujnih primerih uporabila možnost, da v skladu s postopkom iz člena 93(3) Uredbe (EU) 2016/679 sprejme izvedbene akte, ki se začnejo uporabljati takoj in s katerimi se začasno zadrži izvajanje tega sklepa oziroma se sklep razveljavi ali spremeni.

8. **SKLEPNE UGOTOVITVE**

(229) Evropski odbor za varstvo podatkov je objavil svoje mnenje ([387]), ki je bilo upoštevano pri pripravi tega sklepa.

(230) Ukrepi iz tega sklepa so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 93(1) Uredbe (EU) 2016/679 –

SPREJELA NASLEDNJI SKLEP:

Člen 1

1. Za namen člena 45 Uredbe (EU) 2016/679 Republika Koreja zagotavlja ustrezno raven varstva osebnih podatkov, ki se iz Evropske unije prenašajo subjektom v Republiki Koreji, za katere se uporablja zakon o varstvu osebnih podatkov, kot je dopolnjen z dodatnimi zaščitnimi ukrepi iz Priloge I ter uradnimi navedbami, zagotovili in zavezami iz Priloge II.

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 tam navedenih namenov, in sicer:

(a) verskim organizacijam, če obdelujejo osebne podatke za svoje misijonarske dejavnosti;

(b) političnim strankam, če obdelujejo osebne podatke v okviru imenovanja kandidatov;

(c) subjektom, ki jih nadzoruje komisija za finančne storitve glede obdelave osebnih kreditnih informacij na podlagi zakona o kreditnih informacijah, če obdelujejo take podatke.

Člen 2

Kadar pristojni organi v državah članicah z namenom varstva posameznikov v zvezi z obdelavo njihovih osebnih podatkov izvajajo svoja pooblastila na podlagi člena 58 Uredbe (EU) 2016/679 v zvezi s prenosom podatkov, ki spadajo na področje uporabe iz člena 1 tega sklepa, 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 in uveljavljajo individualne pravice ter pod katerimi imajo javni organi Republike Koreje dostop do podatkov, prenesenih na podlagi tega sklepa, da bi ocenila, ali Republika Koreja še naprej zagotavlja ustrezno raven varstva v smislu člena 1.

([387]) Mnenje 32/2021 o osnutku izvedbenega sklepa Evropske komisije v skladu z Uredbo (EU) 2016/679 o ustreznem varstvu osebnih podatkov v Republiki Koreji, ki je na voljo na naslednji povezavi: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. Države članice in Komisija se medsebojno obveščajo o primerih, ko komisija za varstvo osebnih podatkov ali kateri koli drug korejski pristojni organ ne zagotavlja skladnosti s pravnim okvirom, na katerem temelji ta sklep.

3. Države članice in Komisija se medsebojno obveščajo o vseh indicih, da poseganje korejskih javnih organov v pravico posameznikov do varstva njihovih osebnih podatkov presega to, kar je nujno potrebno, ali da zoper tako poseganje ni učinkovitega pravnega varstva.

4. Komisija po treh 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 pregleda, ki se opravi z zadevnimi korejskimi organi.

5. Če Komisija prejme indic, da ustrezna raven varstva ni več zagotovljena, o tem obvesti pristojne korejske organe. Po potrebi se lahko odloči, da začasno zadrži izvajanje tega sklepa, ga spremeni ali razveljavi ali pa omeji njegovo področje uporabe, v skladu s členom 45(5) Uredbe (EU) 2016/679, zlasti kadar obstajajo indici, da:

(a) upravljavci v Koreji, ki prejmejo osebne podatke iz Evropske unije v skladu s tem sklepom, ne upoštevajo dodatnih zaščitnih ukrepov iz Priloge I, ali da nadzor in izvrševanje glede tega nista zadostna;

(b) korejski javni organi ne zagotavljajo skladnosti z navedbami, zagotovili in zavezami iz Priloge II, med drugim v zvezi s pogoji in omejitvami glede zbiranja osebnih podatkov, ki se prenašajo v skladu s tem sklepom, in dostopa do njih s strani korejskih javnih organov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali nacionalne varnosti.

Komisija lahko take ukrepe sprejme tudi, če zaradi nesodelovanja korejske vlade ne more ugotoviti, ali Republika Koreja še naprej zagotavlja ustrezno raven varstva.

Člen 4

Ta sklep je naslovljen na države članice.

V Bruslju, 17. decembra 2021

Za Komisijo
Didier REYNDERS
član Komisije

PRILOGA I

DODATNA PRAVILA ZA RAZLAGO IN UPORABO ZAKONA O VARSTVU OSEBNIH PODATKOV V ZVEZI Z OBDELAVO OSEBNIH PODATKOV, PRENESENIH V KOREJO

Vsebina

I. Pregled 54

II. Opredelitve pojmov 55

III. Dodatna pravila 55

1. Omejitev na uporabo, ki presega namen, in zagotavljanje osebnih podatkov (členi 3, 15 in 18 zakona) 55

2. Omejitev na nadaljnje prenose osebnih podatkov (člen 17(3) in (4) ter člen 18 zakona) 57

3. Uradno obvestilo za podatke, kadar osebni podatki niso bili pridobljeni od posameznika, na katerega se nanašajo osebni podatki (člen 20 zakona) 58

4. Področje uporabe posebne izjeme pri obdelavi psevdonimiziranih informacij (členi 28-2, 28-3, 28-4, 28-5, 28-6 in 28-7, člen 3, člen 58-2 zakona) 60

5. Popravni ukrepi itd. (člen 64(1), (2) in (4) zakona) 61

6. Uporaba zakona o varstvu osebnih podatkov pri obdelavi osebnih podatkov za namene nacionalne varnosti, vključno s preiskavo kršitev in pregonom v skladu z navedenim zakonom (člena 7-8 in 7-9 ter členi 58, 3, 4 in 62 zakona o varstvu osebnih podatkov) 62

I. **Pregled**

Koreja in Evropska unija (EU) sta sodelovali v razpravah o ustreznosti, na podlagi katerih je Evropska komisija ugotovila, da Koreja zagotavlja ustrezno raven varstva osebnih podatkov v skladu s členom 45 GDPR.

Komisija za varstvo osebnih podatkov je v tem okviru sprejela to uradno obvestilo na podlagi členov 5 (obveznosti države itd.) in 14 (mednarodno sodelovanje) ([1]) zakona o varstvu osebnih podatkov, da bi pojasnila razlago, uporabo in izvajanje nekaterih določb zakona, tudi glede obdelave osebnih podatkov, ki se v Korejo prenašajo na podlagi sklepa EU o ustreznosti.

Ker ima to uradno obvestilo status upravnega predpisa, ki ga pristojni upravni organ določi in objavi za pojasnitev standardov za razlago, uporabo in izvajanje zakona o varstvu osebnih podatkov v pravnem sistemu Koreje, ima pravno zavezujoč učinek na upravljavca osebnih podatkov v smislu, da se lahko kakršna koli kršitev tega uradnega obvestila šteje za kršitev ustreznih določb zakona o varstvu osebnih podatkov. Če se poleg tega zaradi kršitve tega uradnega obvestila posega v osebne pravice in interese, imajo zadevni posamezniki pravico uveljavljati pravna sredstva pred komisijo za varstvo osebnih podatkov ali pred sodiščem.

Če upravljavec osebnih podatkov, ki osebne podatke, prenesene v Korejo, obdeluje v skladu s sklepom EU o ustreznosti, ne sprejme ukrepov, ki so v skladu s tem uradnim obvestilom, se posledično šteje, da „se utemeljeno domneva, da je prišlo do kršitve v zvezi z osebnimi podatki, zaradi neukrepanja pa je najverjetneje nastala škoda, ki jo je težko popraviti," kot je določeno v členu 64(1) in (2) zakona. V takih primerih lahko komisija za varstvo osebnih podatkov ali povezani osrednji upravni organi zadevnemu upravljavcu osebnih podatkov odredijo, naj v skladu s pooblastilom, ki

([1]) Člen 14 zakona o varstvu osebnih podatkov določa, da organ korejske vlade uvede politike za izboljšanje ravni varstva osebnih podatkov v mednarodnem okolju in preprečitev kršenja pravic posameznikov, na katere se nanašajo osebni podatki, zaradi čezmejnih prenosov takih podatkov.

ga daje ta določba, sprejme popravne ukrepe itd., glede na konkretne kršitve zakona pa se lahko naloži tudi ustrezna kazen (kazni, globe itd.).

II. **Opredelitev pojmov**

Pojmi, ki se uporabljajo v tej določbi, so opredeljeni tako:

(i) „zakon“ pomeni zakon o varstvu osebnih podatkov (zakon št. 16930, kakor je bil spremenjen 4. februarja 2020 in se izvaja od 5. avgusta 2020);

(ii) „predsedniška uredba“ pomeni uredbo o izvajanju zakona o varstvu osebnih podatkov (predsedniška uredba št. 30509 z dne 3. marca 2020, ki spreminja druge akte);

(iii) „posameznik, na katerega se nanašajo osebni podatki“ pomeni posameznika, ki ga je mogoče na podlagi informacij, ki se obdelujejo, identificirati, s čimer postane subjekt teh informacij;

(iv) „upravljavec osebnih podatkov“ pomeni javno institucijo, pravno osebo, organizacijo, posameznika itd., ki neposredno ali posredno obdeluje osebne podatke kot del svojih dejavnosti;

(v) „EU“ pomeni EU (ki konec februarja 2020 obsega 27 držav članic ([2]), vključno z Belgijo, Nemčijo, Francijo, Italijo, Luksemburgom, Nizozemsko, Dansko, Irsko, Grčijo, Portugalsko, Španijo, Avstrijo, Finsko, Švedsko, Ciprom, Češko, Estonijo, Madžarsko, Latvijo, Litvo, Malto, Poljsko, Slovaško, Slovenijo, Romunijo, Bolgarijo in Hrvaško) in države, pridružene k EU s Sporazumom EGP (Islandija, Lihtenštajn in Norveška);

(vi) „GDPR“ pomeni splošno uredbo o varstvu podatkov, ki je splošni zakon EU o varstvu osebnih podatkov (Uredba EU 2016/679);

(vii) „sklep o ustreznosti“ pomeni odločitev Evropske komisije v skladu s členom 45(3) GDPR, da tretja država, ozemlje ali en ali več sektorjev v tretji državi ali mednarodna organizacija zagotavlja ustrezno raven varstva osebnih podatkov.

III. **Dodatna pravila**

1. **Omejitev na uporabo, ki presega namen, in zagotavljanje osebnih podatkov (členi 3, 15 in 18 zakona)**

<Zakon o varstvu osebnih podatkov

(zakon št. 16930, kakor je bil deloma spremenjen 4. februarja 2020)>

Člen 3 (Načela za varstvo osebnih podatkov) (1) Upravljavec osebnih podatkov izrecno določi namene, za katere se osebni podatki obdelujejo, ter take podatke zakonito in pošteno zbira v najmanjšem možnem obsegu, ki je potreben za take namene.

(2) Upravljavec osebnih podatkov obdeluje osebne podatke na način, ki je ustrezen in potreben za namene obdelave, in jih ne uporablja zunaj teh namenov.

Člen 15 (Zbiranje in uporaba osebnih podatkov) (1) Upravljavec osebnih podatkov lahko osebne podatke zbira v kateri koli od naslednjih okoliščin in jih uporablja v okviru namena zbiranja:

1. kadar se pridobi privolitev posameznika, na katerega se nanašajo osebni podatki;

2. kadar zakonodaja vsebuje posebne določbe ali je to neizogibno za izpolnjevanje pravnih obveznosti;

3. kadar je to neizogibno za opravljanje nalog javne institucije v njeni pristojnosti, kot je določeno v predpisih, itd.;

4. kadar je to neizogibno za sklenitev in izpolnitev pogodbe s posameznikom, na katerega se nanašajo osebni podatki;

([2]) Do konca prehodnega obdobja ta pojem zajema tudi Združeno kraljestvo, kot je določeno v členih 126, 127 in 132 Sporazuma o izstopu Združenega kraljestva Velika Britanija in Severna Irska iz Evropske unije in Evropske skupnosti za atomsko energijo (2019/C 384 I/01).

5. kadar je to očitno nujno za zaščito življenja, telesa ali premoženja posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe pred neposredno nevarnostjo, če posameznik, na katerega se nanašajo osebni podatki, ali njegov zakoniti zastopnik ne more izraziti svojega namena ali če predhodne privolitve ni mogoče pridobiti zaradi neznanega naslova itd.;

6. kadar je nujna uresničitev upravičenega interesa upravljavca osebnih podatkov, če ta očitno prevlada nad pravicami posameznika, na katerega se nanašajo osebni podatki. Obdelava je v takih primerih dovoljena le, če je pomembno povezana z zakonitim interesom upravljavca osebnih podatkov in ne presega tega, kar je razumno.

Člen 18 (Omejitev na uporabo, ki presega namen, in zagotavljanje osebnih podatkov) (1) Upravljavec osebnih podatkov takih podatkov ne uporablja v obsegu, ki presega tistega iz člena 15(1) in člena 39-3(1) in (2), oziroma jih ne zagotavlja tretji osebi v obsegu, ki presega tistega iz člena 17(1) in (3).

(2) Ne glede na odstavek 1 lahko upravljavec osebnih podatkov, kadar se uporablja kateri koli od naslednjih pododstavkov, osebne podatke uporablja ali jih zagotavlja tretji osebi za druge namene, razen če bi to verjetno nepošteno posegalo v interese posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe: če za ponudnike informacijskih in komunikacijskih storitev [kot so opredeljeni v členu 2(1), točka 3, zakona o spodbujanju uporabe informacijskih in komunikacijskih omrežij ter varstvu podatkov itd.; v nadaljnjem besedilu se uporablja enako], ki obdelujejo osebne podatke uporabnikov [kot so opredeljeni v členu 2(1), točka 4, zakona o spodbujanju uporabe informacijskih in komunikacijskih omrežij ter varstvu podatkov itd.; v nadaljnjem besedilu se uporablja enako], veljata le pododstavka 1 in 2, pododstavki 5 do 9 pa se uporabljajo le za javne institucije:

1. kadar se pridobi dodatna privolitev posameznika, na katerega se nanašajo osebni podatki;

2. kadar zakonodaja vsebuje druge posebne določbe;

3. kadar je to očitno nujno za zaščito življenja, telesa ali premoženja posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe pred neposredno nevarnostjo, če posameznik, na katerega se nanašajo osebni podatki, ali njegov zakoniti zastopnik ne more izraziti svojega namena ali če predhodne privolitve ni mogoče pridobiti zaradi neznanega naslova;

4. izbrisano; <z zakonom št. 16930 z dne 4. februarja 2020>

5. kadar ni mogoče opravljati nalog v njegovi pristojnosti, kot so določene v katerem koli zakonu, razen če upravljavec osebnih podatkov take podatke uporabi za druge namene od predvidenega ali jih zagotovi tretji osebi ter o tem razpravlja in odloči komisija;

6. kadar je treba osebne podatke zagotoviti tuji vladi ali mednarodni organizaciji zaradi izpolnitve pogodbe ali druge mednarodne konvencije;

7. kadar je to potrebno zaradi preiskovanja kaznivih dejanj, vložitve obtožnice in kazenskega pregona;

8. kadar mora sodišče opraviti naloge, povezane s sojenjem;

9. kadar je to potrebno zaradi izvrševanja kazni, pogojnih obsodb in odvzema prostosti.

Izpuščeno (3) do (4)

(5) Kadar upravljavec osebnih podatkov take podatke zagotovi tretji osebi za drug namen od predvidenega, kot je v vsakem primeru opredeljen v odstavku 2, od prejemnika osebnih podatkov zahteva, naj omeji namen in način uporabe ter druge potrebne zadeve ali naj pripravi potrebne zaščitne ukrepe za zagotovitev varnosti osebnih podatkov. V takih primerih oseba, ki prejme tako zahtevo, sprejme potrebne ukrepe za zagotovitev varnosti osebnih podatkov.

(i) Člen 3(1) in (2) zakona določa načelo, da mora upravljavec osebnih podatkov take podatke zbirati le v najmanjšem obsegu, ki je potreben za pravno zavezujočo in zakonito izvedbo namena obdelave osebnih podatkov, ter da jih ne sme uporabljati za namene, ki se razlikujejo od predvidenega. ([3])

(ii) V skladu s tem načelom člen 15(1) zakona določa, da se lahko osebni podatki, kadar jih zbira upravljavec osebnih podatkov, uporabljajo v okviru namena zbiranja, člen 18(1) pa določa, da se osebni podatki ne smejo uporabljati za namen, ki presega namen zbiranja, ali zagotoviti tretji osebi.

([3]) Ker te določbe določajo splošna načela, ki se uporabljajo za vsako obdelavo osebnih podatkov, tudi kadar tako obdelavo izrecno urejajo drugi zakoni, pojasnila v tem oddelku veljajo tudi, kadar se osebni podatki obdelujejo na podlagi drugih zakonov (glej npr. člen 15(1) zakona o kreditnih informacijah, ki se izrecno sklicuje na te določbe).

(iii) Poleg tega, čeprav se lahko osebni podatki v izjemnih primerih ([4]) iz pododstavkov člena 18(2) zakona uporabijo za namene, ki se razlikujejo od predvidenega, ali zagotovijo tretji osebi, je treba zahtevati, da se namen ali način uporabe omeji, tako da se lahko osebni podatki obdelujejo varno v skladu z odstavkom 5, ali da se sprejmejo ukrepi, potrebni za zagotavljanje varnosti osebnih podatkov.

(iv) Navedene določbe se enako uporabljajo za obdelavo vseh osebnih podatkov, ki se na območju sodne pristojnosti Koreje prejmejo iz tretjih držav, in to ne glede na državljanstvo posameznika, na katerega se nanašajo osebni podatki.

(v) Če na primer upravljavec osebnih podatkov v EU osebne podatke prenese korejskemu upravljavcu osebnih podatkov na podlagi sklepa Evropske komisije o ustreznosti, se namen prenosa osebnih podatkov upravljavca osebnih podatkov v EU šteje kot namen zbiranja osebnih podatkov korejskega upravljavca osebnih podatkov in v takih primerih lahko zadnjenavedeni uporabi ali tretji osebi zagotovi osebne podatke le v okviru namena zbiranja, razen v izjemnih primerih iz pododstavkov člena 18(2) zakona.

2. **Omejitev na nadaljnje prenose osebnih podatkov (člen 17(3) in (4) ter člen 18 zakona)**

<Zakon o varstvu osebnih podatkov

(zakon št. 16930, kakor je bil deloma spremenjen 4. februarja 2020)>

Člen 17 (Zagotavljanje osebnih podatkov) (1) opustitev

(2) Ko upravljavec osebnih podatkov pridobi privolitev v skladu z odstavkom 1, točka 1, obvesti posameznika, na katerega se nanašajo osebni podatki, o naslednjih zadevah. Enako velja, če se spremeni kaj od naslednjega:

1. prejemnik osebnih podatkov;
2. namen, za katerega prejemnik osebnih podatkov uporablja te podatke;
3. podrobnosti osebnih podatkov, ki naj bi se zagotovili;
4. obdobje, v katerem prejemnik hrani in uporablja osebne podatke;
5. dejstvo, da lahko posameznik, na katerega se nanašajo osebni podatki, privolitev odkloni, in morebitne težave, ki izhajajo iz odklonitve privolitve.

(3) Upravljavec osebnih podatkov posameznika, na katerega se nanašajo osebni podatki, obvesti o zadevah iz odstavka 2 in od njega pridobi privolitev za zagotavljanje osebnih podatkov tretji osebi v tujini ter ne sklepa pogodb o čezmejnih prenosih osebnih podatkov v nasprotju s tem zakonom.

(4) Upravljavec osebnih podatkov lahko zagotavlja osebne podatke brez privolitve posameznika, na katerega se nanašajo osebni podatki, v obsegu, ki je razumno povezan z namenom, za katerega so bili ti podatki prvotno zbrani, v skladu z zadevami iz predsedniške uredbe, pri čemer upošteva, ali to škoduje posamezniku, na katerega se nanašajo osebni podatki, ali so bili sprejeti potrebni ukrepi za zagotovitev varnosti, kot je šifriranje itd.

※ Za člen 18 glej strani 3, 4 in 5.

< **uredba o izvajanju zakona o varstvu osebnih podatkov**

([Začetek izvajanja 5. februar 2021.] [Predsedniška uredba št. 3089 z dne 4. avgusta 2020, ki spreminja druge zakone])>

Člen 14-2 (Standardi o dodatni uporabi/zagotavljanju osebnih podatkov itd.)

(1) Če upravljavec osebnih podatkov osebne podatke uporablja ali zagotavlja (v nadaljnjem besedilu: dodatna uporaba ali zagotavljanje osebnih podatkov) brez privolitve posameznika, na katerega se nanašajo osebni podatki, v skladu s členom 15(3) ali 17(4) zakona, upošteva naslednje:

1. ali je to razumno povezano z izvirnim namenom, za katerega so bili osebni podatki zbrani;
2. ali je glede na okoliščine, v katerih so se zbrali osebni podatki, in prakse obdelave predvidena dodatna uporaba ali zagotavljanje osebnih podatkov;
3. ali se z dodatno uporabo ali zagotavljanjem osebnih podatkov nepošteno ne posega v interese posameznika, na katerega se nanašajo osebni podatki, ter
4. ali so bili sprejeti potrebni ukrepi za zagotavljanje varnosti, kot sta psevdonimizacija ali šifriranje.

([4]) Za ponudnike storitev zagotavljanja informacij in komunikacij se uporablja le člen 18(2), pododstavka 1 in 2. Pododstavki 5 do 9 se uporabljajo le za javne institucije.

(2) Upravljavec osebnih podatkov v skladu s členom 30(1) zakona v izjavi o varstvu osebnih podatkov vnaprej razkrije merila za ocenjevanje zadev iz pododstavkov odstavka 1, pooblaščena oseba za varstvo zasebnosti pa v skladu s členom 31(1) zakona preveri, ali upravljavec osebnih podatkov uporablja ali zagotavlja dodatne osebne podatke v skladu z ustreznimi standardi.

(i) Če upravljavec osebnih podatkov osebne podatke zagotavlja tretji osebi v tujini, mora posameznike, na katere se nanašajo osebni podatki, vnaprej obvestiti o vseh zadevah iz člena 17(2) zakona in pridobiti njihovo privolitev, razen v primerih iz odstavka 1 ali 2. V zvezi s čezmejnim zagotavljanjem osebnih podatkov v nasprotju s tem zakonom ni treba skleniti pogodbe:

(1) če se osebni podatki zagotavljajo v obsegu, ki je razumno povezan s prvotnim namenom zbiranja v skladu s členom 17(4) zakona. Vendar se lahko ta določba uporablja le v primerih, ko so izpolnjeni standardi za dodatno uporabo in zagotavljanje osebnih podatkov iz člena 14-2 uredbe o izvajanju. Poleg tega mora upravljavec osebnih podatkov proučiti, ali bi lahko zagotavljanje osebnih podatkov škodovalo posameznikom, na katere se nanašajo osebni podatki, in ali je sprejel potrebne ukrepe za zagotavljanje varnosti, kot je šifriranje;

(2) če se lahko osebni podatki zagotavljajo tretji osebi v izjemnih primerih iz člena 18(2) zakona (glej strani 3 do 5). Tudi v takih primerih pa se osebni podatki ne smejo zagotoviti tretji osebi, če bi se z njihovim zagotavljanjem najverjetneje nepošteno poseglo v interese posameznikov, na katere se nanašajo osebni podatki, ali tretje osebe. Poleg tega mora oseba, ki zagotavlja osebne podatke, od prejemnika osebnih podatkov zahtevati, naj omeji namen ali način uporabe osebnih podatkov ali sprejme potrebne ukrepe za zagotavljanje njihove varnosti, da se lahko varno obdelujejo.

(ii) Če se osebni podatki zagotavljajo tretji osebi v tujini, zaradi razlik v sistemih varstva osebnih podatkov v različnih državah zanje morda ne velja enaka raven varstva, kot jo zagotavlja korejski zakon o varstvu osebnih podatkov. Zato se bodo taki primeri obravnavali kot „primeri, ko je lahko posamezniku, na katerega se nanašajo osebni podatki, povzročena škoda“, kot je navedeno v členu 17(4) zakona, ali „primeri, ko se nepošteno posega v interese posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe“, kot je navedeno v členu 18(2) zakona in členu 14-2 uredbe o izvajanju istega zakona. ([5]) Upravljavec osebnih podatkov in tretja oseba morata za izpolnitev zahtev iz teh določb zato izrecno zagotoviti raven varstva, enakovredno tisti na podlagi zakona, vključno z zagotovilom, da bo lahko posameznik, na katerega se nanašajo osebni podatki, tudi po prenosu osebnih podatkov v tujino uresničeval svoje pravice v pravno zavezujočih dokumentih, kot so pogodbe.

3. **Uradno obvestilo za podatke, kadar osebni podatki niso bili pridobljeni od posameznika, na katerega se nanašajo osebni podatki (člen 20 zakona)**

<Zakon o varstvu osebnih podatkov

(zakon št. 16930, kakor je bil deloma spremenjen 4. februarja 2020)>

Člen 20 (Uradno obvestilo o virih itd. osebnih podatkov, zbranih od tretjih oseb) (1) Kadar upravljavec osebnih podatkov obdeluje osebne podatke, zbrane od tretjih oseb, mora posameznika, na katerega se nanašajo osebni podatki, na njegovo zahtevo nemudoma uradno obvestiti o naslednjih zadevah:

1. viru zbranih osebnih podatkov;

2. namenu obdelave osebnih podatkov;

3. dejstvu, da lahko posameznik, na katerega se nanašajo osebni podatki, zahteva prekinitev obdelave osebnih podatkov, kot je določeno v členu 37.

(2) Ne glede na odstavek 1 mora upravljavec osebnih podatkov, ki izpolnjuje merila iz predsedniške uredbe, pri čemer se upoštevajo vrsta in količina obdelanih osebnih podatkov, število zaposlenih, obseg prodaje itd., pri zbiranju osebnih podatkov od tretjih oseb in njihovi obdelavi v skladu s členom 17(1), točka 1, posameznika, na katerega se nanašajo osebni podatki, uradno obvestiti o zadevah iz odstavka 1: pri čemer to ne velja, kadar podatki, ki jih zbere upravljavec osebnih podatkov, ne vsebujejo osebnih podatkov, kot so kontaktni podatki, na podlagi katerih bi bilo mogoče uradno obvestiti posameznika, na katerega se nanašajo osebni podatki.

([5]) V skladu s členom 18(2), točka 2, zakona o varstvu osebnih podatkov to velja tudi, kadar se osebni podatki tretjim osebam v tujini razkrijejo na podlagi določb iz drugih zakonov (kot je na primer zakon o kreditnih informacijah).

(3) Potrebne zadeve, povezane s časom, načinom in postopkom uradnega obveščanja posameznika, na katerega se nanašajo osebni podatki, v skladu z glavnim stavkom odstavka 2, so predpisane s predsedniško uredbo.

(4) Odstavek 1 in glavni stavek odstavka 2 se ne uporabljata v nobeni od naslednjih okoliščin: pri čemer to velja le, kadar to očitno prevlada nad pravicami posameznika, na katerega se nanašajo osebni podatki, na podlagi tega zakona:

1. kadar so osebni podatki, v zvezi s katerimi se zahteva uradno obveščanje, vključeni v datoteke z osebnimi podatki iz enega od pododstavkov člena 32(2);

2. kadar bi tako uradno obveščanje verjetno povzročilo škodo za življenje ali telo druge osebe ali neupravičeno škodovalo premoženju in drugim interesom druge osebe.

(i) Če upravljavec osebnih podatkov prejme osebne podatke, prenesene iz EU na podlagi sklepa o ustreznosti ([6]), mora posameznika, na katerega se nanašajo osebni podatki, brez nepotrebnega odlašanja in vsekakor najpozneje en mesec po prenosu uradno obvestiti o naslednjih informacijah iz točk 1 do 5:

(1) imenu in kontaktnih podatkih osebe, ki osebne podatke prenese, in osebe, ki jih prejme;

(2) postavkah ali kategorijah prenesenih osebnih podatkov;

(3) namenu zbiranja in uporabe osebnih podatkov (kot ga je opredelil izvoznik podatkov v skladu s točko 1 tega uradnega obvestila);

(4) obdobju hrambe osebnih podatkov;

(5) informacijah o pravicah posameznika, na katerega se nanašajo osebni podatki, v zvezi z obdelavo osebnih podatkov, načinom in postopkom uresničevanja pravic ter morebitno škodo, če njihovo uresničevanje povzroča škodo.

(ii) Tudi če upravljavec osebnih podatkov osebne podatke iz točke (i) zagotavlja tretji osebi v Republiki Koreji ali v tujini, mora posamezniku, na katerega se nanašajo osebni podatki, pred zagotovitvijo osebnih podatkov sporočiti informacije iz točk 1 do 5:

(1) ime in kontaktne podatke osebe, ki osebne podatke prenese, in osebe, ki jih prejme;

(2) postavke ali kategorije prenesenih osebnih podatkov;

(3) državo, v katero se zagotovijo osebni podatki, predvideni datum in način njihovega zagotavljanja (omejeno na primere, ko se osebni podatki zagotavljajo tretjim osebam v tujini);

(4) namen osebe, ki zagotavlja osebne podatke, in pravno podlago za njihovo zagotavljanje;

(5) informacije o pravicah posameznika, na katerega se nanašajo osebni podatki, v zvezi z obdelavo osebnih podatkov, načinom in postopkom uresničevanja pravic ter morebitno škodo, če njihovo uresničevanje povzroča škodo.

(iii) Upravljavcu osebnih podatkov ni treba uporabiti točke (i) ali (ii) v katerem koli od naslednjih primerov iz točk 1 do 4:

(1) Če so osebni podatki, ki jih je treba sporočiti, vključeni v katero od naslednjih datotek z osebnimi podatki iz člena 32(2) zakona, kolikor interesi, zaščiteni s to določbo, očitno prevladajo nad pravicami posameznika, na katerega se nanašajo osebni podatki, in le če bi uradno obveščanje ogrozilo uresničevanje zadevnih interesov, na primer ogrozilo tekoče kazenske preiskave ali nacionalno varnost.

(2) Če in kolikor bi uradno obveščanje verjetno povzročilo škodo za življenje ali telo druge osebe ali pomenilo neupravičeno poseganje v premoženjske interese druge osebe, kadar te pravice ali interesi očitno prevladajo na pravicami posameznika, na katerega se nanašajo osebni podatki.

(3) Če posameznik, na katerega se nanašajo osebni podatki, že ima informacije, ki jih mora upravljavec osebnih podatkov sporočiti v skladu s točko (i) ali (ii).

(4) Če upravljavec osebnih podatkov nima kontaktnih podatkov o posamezniku, na katerega se nanašajo osebni podatki, ali je za navezavo stika s takim posameznikom potreben čezmeren napor, tudi v okviru obdelave pod pogoji iz oddelka 3 zakona o varstvu osebnih podatkov. Pri ugotavljanju, ali je mogoče navezati stik s posameznikom, na katerega se nanašajo osebni podatki, ali ne oziroma ali je za to potreben čezmeren napor, je treba upoštevati možnost sodelovanja z izvoznikom podatkov v EU.

([6]) Obveznosti iz točk (i), (ii) in (iii) enako veljajo tudi, kadar upravljavec, ki prejme osebne podatke iz EU na podlagi sklepa o ustreznosti, obdeluje take podatke na podlagi drugih zakonov, na primer zakona o kreditnih informacijah.

4. **Področje uporabe posebne izjeme pri obdelavi psevdonimiziranih podatkov (členi 28-2, 28-3, 28-4, 28-5, 28-6 in 28-7, člen 3 in člen 58-2 zakona)**

<Zakon o varstvu osebnih podatkov

(zakon št. 16930, kakor je bil deloma spremenjen 4. februarja 2020)>

Poglavje III Obdelava osebnih podatkov

ODDELEK 3 Posebni primeri v zvezi s psevdonimiziranimi podatki

Člen 28-2 (Obdelava psevdonimiziranih podatkov) (1) Upravljavec osebnih podatkov lahko obdeluje psevdonimizirane podatke brez privolitve posameznika, na katerega se nanašajo osebni podatki, za statistične in znanstveno-raziskovalne namene ter namene arhiviranja v javnem interesu itd.

(2) Upravljavec osebnih podatkov pri zagotavljanju psevdonimiziranih podatkov tretji osebi v skladu z odstavkom 1 ne vključi podatkov, ki se lahko uporabijo za identifikacijo določenega posameznika.

Člen 28-3 (Omejitev glede združevanja psevdonimiziranih podatkov) (1) Ne glede na člen 28-2 združevanje psevdonimiziranih podatkov, ki jih različni upravljavci osebnih podatkov obdelujejo v statistične in znanstveno-raziskovalne namene ter namene hrambe evidenc v javnem interesu itd., opravi specializirana institucija, ki jo določi komisija za varstvo osebnih podatkov ali vodja povezanega osrednjega upravnega organa.

(2) Upravljavec osebnih podatkov, ki namerava združene podatke objaviti zunaj organizacije, ki je podatke združila, pridobi soglasje vodje specializirane institucije po obdelavi podatkov v psevdonimizirane podatke ali obliko iz člena 58-2.

(3) Potrebne zadeve, vključno s postopki in načini združevanja v skladu z odstavkom 1, standardi in postopki za določitev ali preklic določitve specializirane institucije za upravljanje in nazor ter standardi in postopki za izvoz in soglasje v skladu z odstavkom 2, so predpisane s predsedniško uredbo.

Člen 28-4 (Obveznost sprejemanja varnostnih ukrepov za psevdonimizirane podatke) (1) Upravljavec osebnih podatkov pri obdelavi psevdonimiziranih podatkov sprejme take tehnične, organizacijske in fizične ukrepe, kot so ločena hramba in upravljanje dodatnih informacij, potrebnih za obnovitev v prvotno stanje, kot so morda potrebni za zagotovitev varnosti, predpisane s predsedniško uredbo, tako da osebnih podatkov ni mogoče izgubiti, ukrasti, razkriti, ponarediti, spremeniti ali poškodovati.

(2) Upravljavec osebnih podatkov, ki namerava obdelovati psevdonimizirane podatke, pripravi in vodi evidence o zadevah, predpisanih s predsedniško uredbo, vključno z namenom obdelave psevdonimiziranih podatkov in prejemnikom, ki je tretja oseba, ko se taki podatki zagotovijo za upravljanje njihove obdelave.

Člen 28-5 (Prepovedana dejanja pri obdelavi psevdonimiziranih podatkov) (1) Nihče ne obdeluje psevdonimiziranih podatkov z namenom identifikacije določenega posameznika.

(2) Kadar se med obdelavo psevdonimiziranih podatkov ustvarijo informacije, ki omogočajo identifikacijo določenega posameznika, upravljavec osebnih podatkov preneha obdelovati informacije ter jih prikliče in takoj uniči.

Člen 28-6 (Izrek upravnih glob za obdelavo psevdonimiziranih podatkov) (1) Komisija lahko izreče globo v višini manj kot treh stotink celotnega obsega prodaje upravljavcu podatkov, ki je podatke obdeloval z namenom identifikacije določenega posameznika in s tem kršil člen 28-5(1): pri čemer se lahko upravljavcu podatkov, kadar nima prodaje ali kadar se težko izračunajo prihodki, izreče globa, ki ne presega 400 milijonov KRW ali treh stotink kapitalskega zneska, kar koli je večje.

(2) Člen 34-2(3) do (5) se smiselno uporablja za zadeve, potrebne za izrek in izterjavo upravnih glob.

Člen 28-7 (Področje uporabe) Za psevdonimizirane podatke se ne uporabljajo členi 20, 21 in 27, člen 34(1), členi 35 do 37, členi 39-3, 39-4 in 39-6 do 39-8.

Poglavje I Splošne določbe

Člen 3 (Načela za varstvo osebnih podatkov) (1) Upravljavec osebnih podatkov izrecno določi namene, za katere se osebni podatki obdelujejo, ter take podatke zakonito in pošteno zbira v najmanjšem možnem obsegu, ki je potreben za take namene.

(2) Upravljavec osebnih podatkov obdeluje osebne podatke na način, ki je ustrezen in potreben za namene obdelave, in jih ne uporablja zunaj teh namenov.

(3) Upravljavec osebnih podatkov zagotovi, da so osebni podatki točni, popolni in posodobljeni, kolikor je to potrebno glede na namene njihove obdelave.

(4) Upravljavec osebnih podatkov z osebnimi podatki ravna varno, v skladu z metodami obdelave ter vrstami itd. osebnih podatkov, pri čemer upošteva možnost poseganja v pravice posameznikov, na katere se nanašajo osebni podatki, in stopnjo ustreznih tveganj.

(5) Upravljavec osebnih podatkov javno objavi svojo politiko zasebnosti in druge zadeve, povezane z obdelavo osebnih podatkov, ter zagotavlja pravice posameznika, na katerega se nanašajo osebni podatki, kot je pravica do dostopa do osebnih podatkov.

(6) Upravljavec osebnih podatkov obdeluje osebne podatke tako, da je čim manj možnosti za poseganje v zasebnost posameznika, na katerega se nanašajo osebni podatki.

(7) Če je namene zbiranja osebnih podatkov še vedno mogoče izpolniti z obdelavo anonimiziranih ali psevdonimiziranih osebnih podatkov, si upravljavec osebnih podatkov prizadeva za obdelavo osebnih podatkov z anonimizacijo, kadar je ta mogoča, ali psevdoanonimizacijo, če namenov zbiranja osebnih podatkov ni mogoče izpolniti z anonimizacijo.

(8) Upravljavec osebnih podatkov si prizadeva pridobiti zaupanje posameznikov, na katere se nanašajo osebni podatki, z upoštevanjem in izvajanjem nalog in odgovornosti, kot so določene v tem zakonu in drugih povezanih predpisih.

Poglavje IX Dodatne določbe

Člen 58-2 (Izjema od uporabe) Ta zakon se ne uporablja za informacije, s katerimi ni več mogoče identificirati določenega posameznika, če se združijo z drugimi informacijami, pri čemer se razumno upoštevajo čas, stroški, tehnologija itd. <Ta člen je bil na novo vstavljen z zakonom št. 16930 z dne 4. februarja 2020>

(i) V poglavju III, oddelek 3, z naslovom Posebni primeri v zvezi s psevdonimiziranimi podatki (členi 28-2 do 28-7), je dovoljena obdelava psevdonimiziranih podatkov brez privolitve posameznika, na katerega se nanašajo osebni podatki, za namene zbiranja statističnih podatkov, znanstvenih raziskav, hrambe javnih evidenc itd. (člen 28-2), vendar so v takih primerih obvezni ustrezni zaščitni ukrepi in prepovedi, potrebni za varstvo pravic posameznikov, na katere se nanašajo osebni podatki, (člena 28-4 in 28-5), kršilcem se lahko izrečejo kazenske globe (člen 28-6), določeni zaščitni ukrepi, ki so sicer na voljo na podlagi zakona o varstvu osebnih podatkov, pa se ne uporabljajo (člen 28-7).

(ii) Te določbe se ne uporabljajo v primerih, ko se psevdonimizirani podatki obdelujejo za namene, ki niso zbiranje statističnih podatkov, znanstvene raziskave, hramba javnih evidenc itd. Če so osebni podatki posameznika iz EU, ki so bili v Korejo preneseni v skladu s sklepom Evropske komisije o ustreznosti, psevdonimizirani za namene, ki niso zbiranje statističnih podatkov, znanstvene raziskave, hramba javnih evidenc itd., se posebne določbe poglavja III, oddelek 3, ne uporabljajo ([7]).

(iii) Kadar upravljavec osebnih podatkov psevdonimizirane podatke obdeluje za namene zbiranja statističnih podatkov, znanstvenih raziskav, hrambe javnih evidenc itd. in če taki podatki po izpolnitvi posebnega namena obdelave niso bili uničeni v skladu s členom 37 ustave in členom 3 (Načela za varstvo osebnih podatkov) zakona, podatke anoninimiza za zagotovitev, da z njimi samimi ali v kombinaciji z drugimi podatki ni več mogoče identificirati določenega posameznika, pri čemer se razumno upoštevajo čas, stroški, tehnologija itd. v skladu s členom 58-2 zakona o varstvu osebnih podatkov.

5. **Popravni ukrepi itd. (člen 64(1), (2) in (4) zakona)**

<Zakon o varstvu osebnih podatkov

(zakon št. 16930, kakor je bil deloma spremenjen 4. februarja 2020)>

Člen 64 (Popravni ukrepi) (1) Če se po mnenju komisije za varstvo osebnih podatkov utemeljeno domneva, da je prišlo do kršitve v zvezi z osebnimi podatki, zaradi neukrepanja pa je najverjetneje nastala škoda, ki jo je težko popraviti, lahko kršitelju tega zakona (z izjemo osrednjih upravnih organov, lokalnih upravnih organov, parlamenta, sodišča, ustavnega sodišča in komisije za nacionalne volitve) odredi sprejetje katerega koli od naslednjih ukrepov:

1. prenehanje kršitve v zvezi z osebnimi podatki;

2. začasno prenehanje obdelave osebnih podatkov;

([7]) Podobno se izjema iz člena 40-3 zakona o kreditnih informacijah uporablja le za obdelavo psevdonimiziranih kreditnih informacij za namene zbiranja statističnih podatkov, znanstvenih raziskav in hrambe javnih evidenc.

3. izvedbo drugih ukrepov, ki so potrebni za varstvo osebnih podatkov in preprečitev kršenja osebnih podatkov.

(2) Kadar vodja povezanega osrednjega upravnega organa meni, da se utemeljeno domneva, da je prišlo do kršitve v zvezi z osebnimi podatki, zaradi neukrepanja pa bi najverjetneje nastala škoda, ki bi jo bilo težko popraviti, lahko odredi, da mora upravljavec osebnih podatkov sprejeti katerega od ukrepov iz odstavka 1 v skladu s predpisi, ki so v pristojnosti takega povezanega osrednjega upravnega organa.

(4) Kadar ta zakon krši osrednji upravni organ, lokalni upravni organ, parlament, sodišče, ustavno sodišče ali komisija za nacionalne volitve, lahko komisija za varstvo osebnih podatkov vodji zadevnega organa priporoči sprejetje katerega koli od ukrepov iz odstavka 1. Ko organ v takih primerih prejme priporočilo, ga upošteva, razen v izjemnih okoliščinah.

(i) V precedenčnih sodbah sodišča ([8]) ([9]) se „škoda, ki jo je težko popraviti“ razlaga kot primer, ki bi lahko škodoval osebnim pravicam ali zasebnosti posameznika.

(ii) Skladno s tem se „utemeljena domneva, da je prišlo do kršitve v zvezi z osebnimi podatki, zaradi neukrepanja pa je najverjetneje nastala škoda, ki jo je težko popraviti“, kot določa člen 64(1) in (2), nanaša na primere, v katerih se za kršitev zakonodaje domneva, da verjetno posega v pravice in svoboščine posameznika v zvezi z osebnimi podatki. To velja, kadar se kršijo načela, pravice in dolžnosti iz zakonodaje o varstvu osebnih podatkov. ([10])

(iii) V skladu s členom 64(4) zakona o varstvu osebnih podatkov gre za ukrep v zvezi s „kršitvijo tega zakona“, tj. ukrep zoper kršitev zakona o varstvu osebnih podatkov.

Osrednji upravni organ itd., ki je kot javni organ zavezan načelu pravne države, ne sme kršiti nobenega zakona in mora sprejeti popravni ukrep, vključno s takojšnjim prenehanjem dejanja, v izjemnih primerih, ko je bilo nezakonito dejanje kljub temu storjeno, pa povrniti škodo.

Posledično mora osrednji upravni organ itd., če izve za kršitev zakonodaje, tudi brez kakršnega koli posredovanja komisije za varstvo osebnih podatkov v skladu s členom 64(4) zakona o varstvu osebnih podatkov sprejeti popravni ukrep zoper kršitve.

Zlasti kadar komisija za varstvo osebnih podatkov priporoči popravni ukrep, je osrednjemu upravnemu organu itd. običajno objektivno jasno, da je kršil zakonodajo. Zato mora za utemeljitev, zakaj meni, da se ne bi smelo upoštevati priporočilo komisije za varstvo osebnih podatkov, predstaviti jasne razloge, s katerimi lahko dokaže, da ni kršil zakonodaje. Priporočilo je treba upoštevati, razen če komisija za varstvo osebnih podatkov odloči, da to dejansko ne velja.

Glede na to morajo biti „izjemne okoliščine“ iz člena 64(4) zakona o varstvu osebnih podatkov strogo omejene na izjemne okoliščine, v katerih lahko osrednji upravni organi itd. jasno dokažejo, da „ta zakon dejansko ni bil kršen“, kot so „primeri izjemnih (dejanskih ali pravnih) okoliščin,“ ki jih komisija za varstvo osebnih podatkov ob pripravi priporočila prvotno ni poznala, in ta komisija odloči, da kršitve dejansko ni bilo.

6. **Uporaba zakona o varstvu osebnih podatkov pri obdelavi osebnih podatkov za namene nacionalne varnosti, vključno s preiskavo kršitev in pregonom v skladu z navedenim zakonom (člena 7-8 in 7-9 ter členi 58, 3, 4 in 62 zakona o varstvu osebnih podatkov)**

<Zakon o varstvu osebnih podatkov

(zakon št. 16930, kakor je bil deloma spremenjen 4. februarja 2020)>

Člen 7-8 (Delo komisije za varstvo osebnih podatkov) (1) Komisija za varstvo osebnih podatkov opravlja naslednje delo: […]

3. zadeve v zvezi s preiskovanjem kršitve pravic posameznikov, na katere se nanašajo osebni podatki, in odločitve, ki iz tega izhajajo;

4. obravnavanje pritožb ali postopki popravnih ukrepov v zvezi z obdelavo osebnih podatkov in mediacija v sporih o osebnih podatkih;

[…]

([8]) (Sodba vrhovnega sodišča 97Da10215,10222 z dne 26. januarja 1999) Če se dejstva kaznivega dejanja obdolženca razkrijejo v medijih, bo to najverjetneje povzročilo nepopravljivo psihično ali fizično škodo ne le žrtvi, tj. tožniku, temveč tudi ljudem v njegovi bližini, vključno z družinami.

([9]) (Sodba višjega sodišča v Seulu št. 2006Na92006 z dne 16. januarja 2008) Objava obrekljivega članka bo najverjetneje povzročila resno nepopravljivo škodo udeleženim osebam.

([10]) Ista načela, kot so določena v točki (ii), se uporabljajo za člen 45-4 zakona o kreditnih informacijah.

Člen 7-9 (Zadeve, o katerih razpravlja in odloča komisija za varstvo osebnih podatkov) (1) Komisija za varstvo osebnih podatkov razpravlja in odloča o naslednjih zadevah: […]

5. zadevah v zvezi z razlago in izvajanjem zakonodaje, povezane z varstvom osebnih podatkov;

[…]

Člen 58 (Delna izključitev uporabe) (1) Poglavja III do VII se ne uporabljajo za katere koli od naslednjih osebnih podatkov:

1. osebne podatke, ki se v skladu z zakonom o statističnih podatkih zbirajo za obdelavo s strani javnih institucij;
2. osebne podatke, ki se zbirajo ali zahtevajo za analizo informacij, povezanih z nacionalno varnostjo;
3. osebne podatke, ki se obdelujejo začasno, kadar je to nujno potrebno zaradi javne varnosti in zaščite, javnega zdravja itd.;
4. osebne podatke, ki jih zbirajo ali obdelujejo mediji za lastne namene poročanja, verske organizacije za misijonarske dejavnosti oziroma politične stranke za imenovanje kandidatov.

[izpuščena odstavka 2 in 3]

(4) Upravljavec osebnih podatkov v primeru obdelave osebnih podatkov v skladu z odstavkom 1 obdeluje osebne podatke v najmanjšem možnem obsegu, potrebnem za dosego predvidenega namena, in za najkrajše možno obdobje; prav tako uredi vse potrebno, kot so tehnični, upravljavski in fizični zaščitni ukrepi, obravnavanje posameznih pritožb in drugi potrebni ukrepi za varno upravljanje in ustrezno obdelavo takih osebnih podatkov.

Člen 3 (Načela za varstvo osebnih podatkov) (1) Upravljavec osebnih podatkov izrecno določi namene, za katere se osebni podatki obdelujejo, ter take podatke zakonito in pošteno zbira v najmanjšem možnem obsegu, ki je potreben za take namene.

(2) Upravljavec osebnih podatkov obdeluje osebne podatke na način, ki je ustrezen in potreben za namene obdelave, in jih ne uporablja zunaj teh namenov.

(3) Upravljavec osebnih podatkov zagotovi, da so osebni podatki točni, popolni in posodobljeni, kolikor je to potrebno glede na namene njihove obdelave.

(4) Upravljavec osebnih podatkov z osebnimi podatki ravna varno, v skladu z metodami obdelave ter vrstami itd. osebnih podatkov, pri čemer upošteva možnost poseganja v pravice posameznikov, na katere se nanašajo osebni podatki, in stopnjo ustreznih tveganj.

(5) Upravljavec osebnih podatkov javno objavi svojo politiko zasebnosti in druge zadeve, povezane z obdelavo osebnih podatkov, ter zagotavlja pravice posameznika, na katerega se nanašajo osebni podatki, kot je pravica do dostopa do osebnih podatkov.

(6) Upravljavec osebnih podatkov obdeluje osebne podatke tako, da je čim manj možnosti za poseganje v zasebnost posameznika, na katerega se nanašajo osebni podatki.

(7) Če je namene zbiranja osebnih podatkov še vedno mogoče izpolniti z obdelavo anonimiziranih ali psevdonimiziranih osebnih podatkov, si upravljavec osebnih podatkov prizadeva, da osebne podatke obdela z anonimizacijo, kadar je ta mogoča, ali psevdoanonimizacijo, če namenov zbiranja osebnih podatkov ni mogoče izpolniti z anonimizacijo.

(8) Upravljavec osebnih podatkov si prizadeva pridobiti zaupanje posameznikov, na katere se nanašajo osebni podatki, z upoštevanjem in izvajanjem nalog in odgovornosti, kot so določene v tem zakonu in drugih povezanih predpisih.

Člen 4 (Pravice posameznikov, na katere se nanašajo osebni podatki) Posameznik, na katerega se nanašajo osebni podatki, ima v zvezi z obdelavo svojih osebnih podatkov naslednje pravice:

1. pravico do obveščenosti o obdelavi takih osebnih podatkov;
2. pravico do odločitve o privolitvi ali neprivolitvi v obdelavo in obsegu privolitve v zvezi z obdelavo osebnih podatkov;
3. pravico do potrditve, ali se osebni podatki obdelujejo ali ne, in do zahtevanja dostopa (vključno s predložitvijo kopij; v nadaljnjem besedilu velja enako) do takih osebnih podatkov;
4. pravico do prenehanja obdelave takih osebnih podatkov ter zahtevanja njihovega popravka, izbrisa in uničenja;
5. pravico do ustreznega pravnega sredstva za škodo, ki izhaja iz obdelave takih osebnih podatkov, v hitrem in poštenem postopku.

Člen 62 (Poročanje o kršitvah) (1) Vsakdo, ki so mu med obdelavo osebnih podatkov s strani upravljavca osebnih podatkov kršene pravice ali interesi v zvezi z osebnimi podatki, lahko o takih kršitvah poroča komisiji za varstvo osebnih podatkov.

(2) Komisija za varstvo osebnih podatkov lahko določi specializirano institucijo, ki učinkovito prejema in obravnava poročila o pritožbah v skladu z odstavkom 1, kot je določeno v predsedniški uredbi. Specializirana institucija v takih primerih vzpostavi in upravlja klicni center za kršitve osebnih podatkov (v nadaljnjem besedilu: klicni center za vprašanja v zvezi z zasebnostjo).

(3) Klicni center za vprašanja v zvezi z zasebnostjo opravlja naslednje naloge:

1. prejema poročila o pritožbah in svetuje glede obdelave osebnih podatkov;

2. preiskuje in potrjuje incidente ter prisluhne mnenjem povezanih strani;

3. opravlja naloge, povezane s pododstavkoma 1 in 2.

(4) Komisija za varstvo osebnih podatkov lahko v specializirano institucijo, določeno na podlagi odstavka 2, v skladu s členom 32-4 zakona o državnih javnih uradnikih po potrebi napoti svojega javnega uradnika, da učinkovito preišče in potrdi incidente na podlagi odstavka 3, točka 2.

(i) Zbiranje osebnih podatkov za namene nacionalne varnosti urejajo posebni predpisi, ki pristojne organe (npr. nacionalne obveščevalne službe) pooblaščajo, da pod določenimi pogoji in v okviru zaščitnih ukrepov prestrezajo komunikacije ali zahtevajo razkritje (v nadaljnjem besedilu: predpisi s področja nacionalne varnosti). Ti predpisi s področja nacionalne varnosti vključujejo na primer zakon o varstvu zasebnosti komunikacij, zakon o boju proti terorizmu za zaščito državljanov in javne varnosti ali zakon o zagotavljanju telekomunikacijskih storitev. Poleg tega je treba pri zbiranju in nadaljnji obdelavi osebnih podatkov upoštevati zahteve zakona o varstvu osebnih podatkov. V zvezi s tem člen 58(1), točka 2, zakona o varstvu osebnih podatkov določa, da se poglavja III do VII ne uporabljajo za osebne podatke, zbrane ali zahtevane za analizo informacij, povezanih z nacionalno varnostjo. Ta delna izjema se torej uporablja za obdelavo osebnih podatkov za namene nacionalne varnosti.

Hkrati se za obdelavo takih podatkov uporabljajo poglavje I (Splošne določbe), poglavje II (Oblikovanje politik za varstvo osebnih podatkov itd.), poglavje VIII (Kolektivna tožba zoper kršitev varstva podatkov), poglavje IX (Dodatne določbe) in poglavje X (Kazenske določbe) zakona o varstvu osebnih podatkov. To vključuje splošna načela o varstvu podatkov iz člena 3 (Načela varstva osebnih podatkov) in pravice posameznikov, zagotovljene s členom 4 zakona o varstvu osebnih podatkov (Pravice posameznikov, na katere se nanašajo osebni podatki).

Poleg tega člen 58(4) zakona o varstvu podatkov določa, da je treba take podatke obdelati v najmanjšem možnem obsegu, potrebnem za dosego predvidenega namena, in za najkrajše možno obdobje; poleg tega mora upravljavec osebnih podatkov sprejeti potrebne ukrepe za zagotovitev varnega upravljanja in ustrezne obdelave podatkov, kot so tehnični, upravljavski in fizični zaščitni ukrepi ter ukrepi za ustrezno obravnavanje posameznih pritožb.

Nazadnje, uporabljajo se določbe, ki urejajo naloge in pristojnosti komisije za varstvo osebnih podatkov (vključno s členi 60 do 65 zakona o varstvu osebnih podatkov, ki se nanašajo na obravnavanje pritožb ter sprejetje priporočil in popravnih ukrepov), ter določbe o upravnih in kazenskih sankcijah (člen 70 in naslednji zakona o varstvu osebnih podatkov). Ta preiskovalna in popravna pooblastila, tudi ko se izvršujejo v okviru obravnave pritožb, v skladu s členom 7-8(1), točki 3 in 4, ter členom 7-9(1), točka 5, zakona o varstvu osebnih podatkov zajemajo tudi morebitne kršitve pravil iz posebnih predpisov, ki določajo omejitve in zaščitne ukrepe v zvezi z zbiranjem osebnih podatkov, kot so predpisi s področja nacionalne varnosti. Vsaka taka kršitev glede na zahteve iz člena 3(1) zakona o varstvu osebnih podatkov, ki se uporabljajo za zakonito in pošteno zbiranje osebnih podatkov, pomeni kršitev „tega zakona“ v smislu členov 63 in 64, kar komisiji za varstvo osebnih podatkov omogoča, da izvede preiskavo in sprejme popravne ukrepe. ([11]) Izvajanje teh pooblastil s strani komisije za varstvo osebnih podatkov dopolnjuje pooblastila, ki jih ima nacionalna komisija za človekove pravice na podlagi zakona o komisiji za človekove pravice, hkrati pa teh pooblastil ne nadomešča.

Uporaba temeljnih načel, pravic in obveznosti iz zakona o varstvu osebnih podatkov pri obdelavi osebnih podatkov za namene nacionalne varnosti odraža zagotovila, zapisana v ustavi, za varstvo pravice posameznika do nadzora nad svojimi osebnimi podatki. Kot je priznalo ustavno sodišče, to vključuje pravico posameznika ([12]), „da se sam odloči, kdaj, komu ali prek koga in v kakšnem obsegu se bodo njegovi osebni podatki razkrili oziroma kdaj, pri kom ali prek koga in v kakšnem obsegu se bodo uporabili. S to temeljno pravico ([13]), […], se osebna svoboda odločanja zaščiti pred tveganjem, ki ga povzroča širitev državnih funkcij in informacijsko-komunikacijske tehnologije.“ Pri vsaki omejitvi te pravice, na primer ko je to potrebno zaradi zaščite nacionalne varnosti, je treba tehtati med pravicami in interesi posameznika ter ustreznimi javnimi interesi, pri tem pa se ne sme posegati v bistvo pravice (člen 37(2) ustave).

([11]) Glede popravnih ukrepov v skladu s členom 64 glej tudi oddelek 5 zgoraj.
([12]) Sodba ustavnega sodišča št. 99HunMa513, 2004HunMa190 z dne 26. maja 2005.
([13]) Sodba ustavnega sodišča št. 2003HunMa282 z dne 21. julija 2005.

Upravljavec (npr. nacionalna obveščevalna služba) pri obdelavi osebnih podatkov za namene nacionalne varnosti zato med drugim:

(1) izrecno določi namene, za katere se osebni podatki zakonito in pošteno obdelujejo in zbirajo v najmanjšem možnem obsegu, potrebnem za take namene (člen 3(1) zakona o varstvu osebnih podatkov); zlasti zbira in nadalje obdeluje osebne podatke le za namene opravljanja nalog na podlagi ustreznih predpisov, kot je zakon o nacionalni obveščevalni službi;

(2) obdeluje osebne podatke v najmanjšem možnem obsegu, potrebnem za dosego predvidenega namena, in za najkrajše možno obdobje (člen 58(4) zakona o varstvu osebnih podatkov); ko je namen obdelave dosežen, upravljavec trajno uniči osebne podatke, razen če je nadaljnja hramba izrecno odrejena s predpisom, v tem primeru se zadevni osebni podatki hranijo in upravljajo ločeno od drugih osebnih podatkov, uporabljajo samo za namen, opredeljen v predpisu, in ob koncu obdobja hrambe uničijo;

(3) obdeluje osebne podatke, kot je ustrezno in potrebno za namene njihove obdelave, in jih ne uporablja tako, da uporaba presega take namene (člen 3(2) zakona o varstvu osebnih podatkov);

(4) zagotovi, da so osebni podatki točni, popolni in posodobljeni, kolikor je to potrebno glede na namene njihove obdelave (člen 3(3) zakona o varstvu osebnih podatkov);

(5) z osebnimi podatki ravna varno, v skladu z metodami obdelave in vrstami itd. osebnih podatkov, pri tem pa upošteva možnost poseganja v pravice posameznikov, na katere se nanašajo osebni podatki, in stopnjo zadevnih tveganj (člen 3(4) zakona o varstvu osebnih podatkov);

(6) javno objavi svojo politiko zasebnosti in druge zadeve, povezane z obdelavo osebnih podatkov (člen 3(5) zakona o varstvu osebnih podatkov);

(7) osebne podatke obdeluje tako, da se čim bolj zmanjša možnost poseganja v zasebnost posameznika, na katerega se nanašajo osebni podatki (člen 3(6) zakona o varstvu osebnih podatkov).

(ii) V skladu s členom 58(4) zakona o varstvu osebnih podatkov upravljavec (npr. organi, pristojni za nacionalno varnost, kot je nacionalna obveščevalna služba) uredi vse potrebno, kot je sprejetje tehničnih, upravljavskih in fizičnih zaščitnih ukrepov, za zagotovitev skladnosti s temi načeli in ustrezne obravnave osebnih podatkov. To lahko na primer vključuje posebne ukrepe za zagotovitev varnosti osebnih podatkov, kot so omejitve dostopa do osebnih podatkov, nadzor nad dostopom, dnevniki, zagotavljanje namenskega usposabljanja zaposlenih o ravnanju z osebnimi podatki itd.

Posamezniki, na katere se nanašajo osebni podatki, imajo poleg tega v skladu s členom 3(5) in členom 4 zakona o varstvu osebnih podatkov med drugim naslednje pravice v zvezi z osebnimi podatki, ki se obdelujejo za namene nacionalne varnosti:

(1) pravico do pridobitve potrditve, ali se njihovi osebni podatki obdelujejo ali ne, in informacij o obdelavi ter pravico do dostopa do navedenih podatkov, vključno z zagotovitvijo kopij (člen 4(1) in (3) zakona o varstvu osebnih podatkov);

(2) pravico do prenehanja obdelave ter zahtevanja popravka, izbrisa in uničenja osebnih podatkov (člen 4(4) zakona o varstvu osebnih podatkov).

(iii) Posameznik, na katerega se nanašajo osebni podatki, lahko v okviru uresničevanja teh pravic vloži zahtevo neposredno pri upravljavcu ali posredno pri komisiji za varstvo osebnih podatkov, za to pa lahko pooblasti tudi svojega zastopnika. Kadar posameznik, na katerega se nanašajo osebni podatki, vloži zahtevo, mu upravljavec pravico nemudoma prizna; pod pogojem, da lahko pravico preloži, omeji ali zavrne, če je to izrecno določeno ali neizogibno za izpolnitev drugih predpisov, kolikor in dokler je to potrebno in sorazmerno za zaščito pomembnega cilja javnega interesa (npr. kolikor in dokler bi priznanje pravice ogrozilo tekočo preiskavo ali nacionalno varnost) ali kadar lahko priznanje pravice povzroči škodo za življenje ali telo tretje osebe ali pomeni neupravičeno poseganje v premoženje ali druge interese tretje osebe. Kadar se zahteva zavrne ali omeji, je posameznik, na katerega se nanašajo osebni podatki, nemudoma uradno obveščen o razlogih. Upravljavec pripravi način in postopek, ki posameznikom, na katere se nanašajo osebni podatki, omogočata vložitev zahtev, ter ju javno objavi, da se lahko ti posamezniki z njima seznanijo.

Poleg tega imajo posamezniki, na katere se nanašajo osebni podatki, v skladu s členom 58(4) zakona o varstvu osebnih podatkov (zahteva po zagotovitvi ustreznega obravnavanja posameznih pritožb) in členom 4(5) navedenega zakona (pravica do ustreznega pravnega sredstva za škodo, ki izhaja iz obdelave osebnih podatkov, v hitrem in poštenem postopku) pravico do uveljavljanja pravnih sredstev. To vključuje pravico do poročanja o domnevni kršitvi centru za poročanje o kršitvah varstva osebnih podatkov (v skladu s členom 62(3) zakona o varstvu osebnih podatkov), vložitve pritožbe pri komisiji za varstvo osebnih podatkov v skladu s členom 62 zakona o varstvu osebnih podatkov zaradi poseganja v pravice ali interese, povezane z osebnimi podatki posameznika, in do uveljavljanja pravnega sredstva zoper odločitve ali neukrepanje te komisije na podlagi zakona o upravnem sporu. Poleg tega lahko posamezniki, na katere se nanašajo osebni podatki, v primeru poseganja v njihove pravice ali interese zaradi odločitve ali opustitve dejanja upravljavca (npr. nezakonitega zbiranja osebnih podatkov) uveljavljajo pravna sredstva na podlagi zakona o upravnem sporu ali pridobijo odškodnino za škodo na podlagi zakona o državni odškodnini. Ta pravna sredstva so na voljo tako v primeru morebitnih kršitev pravil iz posebnih predpisov, ki določajo omejitve in zaščitne ukrepe v zvezi z zbiranjem osebnih podatkov, kot so predpisi s področja nacionalne varnosti, kot tudi v primeru kršitev zakona o varstvu osebnih podatkov.

Posameznik iz EU lahko vloži pritožbo pri komisiji za varstvo osebnih podatkov prek svojega nacionalnega organa za varstvo podatkov, komisija za varstvo osebnih podatkov pa bo posameznika po končani preiskavi ali izvedbi popravnih ukrepov (kadar je to ustrezno) o tem uradno obvestila prek nacionalnega organa za varstvo podatkov.

PRILOGA II

18. maj 2021

Spoštovani gospod Didier Reynders, komisar za pravosodje Evropske komisije

Spoštovani komisar,

pozdravljam konstruktivne razprave med Korejo in Evropsko komisijo za oblikovanje okvira za vzajemni prenos osebnih podatkov med Korejo in EU.

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

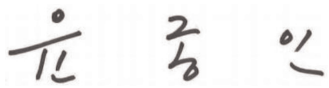
Ta dokument se nanaša na številna ministrstva in organe vlade Koreje, pri čemer so glede na vsebino dokumenta zadevna ministrstva in organi (komisija za varstvo osebnih podatkov, ministrstvo za pravosodje, nacionalna obveščevalna služba, korejska nacionalna komisija za človekove pravice, center za boj proti terorizmu in korejska finančno-obveščevalna enota) odgovorni za posamezne dele tega dokumenta, ki spadajo v njihovo pristojnost. V nadaljevanju so navedena zadevna ministrstva in organi, vključno z njihovimi podpisi.

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

Upam, da bo ta dokument Evropski komisiji v pomoč pri odločanju.

Cenim vaš dosedanji prispevek k tej zadevi.

S spoštovanjem,

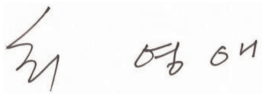


Yoon Jong In
predsednik komisije za varstvo osebnih podatkov

Ta dokument so pripravili komisija za varstvo osebnih podatkov ter naslednji zadevni ministrstva in organi:

Park Jie Won
direktor nacionalne obveščevalne službe

Lee Jung Soo
generalni direktor ministrstva za pravosodje



Choi Young Ae
predsednica korejske nacionalne komisije za človekove pravice

Kim Hyucksoo
direktor nacionalnega centra za boj proti terorizmu

Kim Jeong-kag
komisar korejske finančnoobveščevalne enote

Pravni okvir za zbiranje in uporabo osebnih podatkov s strani korejskih javnih organov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter nacionalne varnosti

Naslednji dokument vsebuje pregled pravnega okvira za zbiranje in uporabo osebnih podatkov s strani korejskih javnih organov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter nacionalne varnosti (v nadaljnjem besedilu: vladni dostop), zlasti kar zadeva razpoložljivo pravno podlago, pogoje (omejitve) in zaščitne ukrepe, ki se uporabljajo, ter neodvisni nadzor in individualne možnosti pravnega varstva.

1. SPLOŠNA PRAVNA NAČELA, POMEMBNA ZA VLADNI DOSTOP

1.1. Ustavni okvir

Ustava Republike Koreje določa pravico do zasebnosti na splošno (člen 17) in zlasti pravico do komunikacijske zasebnosti (člen 18). Dolžnost države je, da zagotavlja ti temeljni pravici ([1]). Ustava nadalje določa, da se lahko pravice in svoboščine državljanov omejijo le z zakonodajo, če je to potrebno zaradi nacionalne varnosti ali ohranjanja javnega reda in miru v javno dobro ([2]). Tudi če so take omejitve uvedene, pa ne smejo posegati v bistvo svoboščine ali pravice ([3]). Korejska sodišča so te določbe uporabljala v zadevah, ki so se nanašale na poseganje vlade v zasebnost. Vrhovno sodišče je na primer ugotovilo, da se z nadzorovanjem državljanov krši temeljna pravica do zasebnosti, pri čemer je poudarilo, da imajo državljani „pravico do samoodločanja glede osebnih podatkov“ ([4]). V drugi zadevi je ustavno sodišče odločilo, da je zasebnost temeljna pravica, ki državljanom zagotavlja zaščito pred poseganjem države v njihovo zasebno življenje in opazovanjem njihovega zasebnega življenja ([5]).

Korejska ustava nadalje zagotavlja, da se nikomur ne sme odvzeti prostost, ga pridržati, preiskati, zaslišati ali mu zaseči predmete, razen če tako določa zakon. ([6]) Poleg tega se lahko preiskave in zasegi opravijo le na podlagi odredbe, ki jo izda sodnik, na zahtevo tožilca in ob upoštevanju ustreznega postopka. ([7]) Preiskovalni organi lahko v izjemnih okoliščinah, tj. kadar je osumljenec kaznivega dejanja prijet med storitvijo kaznivega dejanja (*in flagrante delicto*) ali če obstaja tveganje, da bi lahko osumljenec storitve kaznivega dejanja, za katero se sme izreči kazen zapora treh let ali več, pobegnil ali uničil dokaze, opravijo preiskavo ali zaseg brez odredbe, vendar morajo v tem primeru njeno izdajo zahtevati naknadno. ([8]) Ta splošna načela so nadalje izoblikovana v posebnih zakonih, ki obravnavajo kazenski postopek in zaščito komunikacij (glej v nadaljevanju za podroben pregled).

Ustava glede tujih državljanov določa, da je njihov status zagotovljen v skladu z mednarodnim pravom in mednarodnimi pogodbami. ([9]) Pravice do zasebnosti zagotavlja več mednarodnih sporazumov, katerih podpisnica je Koreja, na primer Mednarodni pakt o državljanskih in političnih pravicah (člen 17), Konvencija o pravicah invalidov (člen 22) in Konvencija o otrokovih pravicah (člen 16). Čeprav se ustava načeloma sklicuje na pravice „državljanov“, je ustavno sodišče odločilo, da imajo temeljne pravice tudi tuji državljani. ([10]) Zlasti je navedlo, da ima vsak človek, ne le vsak

([1]) Člen 10 ustave Republike Koreje, razglašene 17. julija 1948 (v nadaljnjem besedilu: ustava).
([2]) Člen 37(2) ustave.
([3]) Člen 37(2) ustave.
([4]) Odločba vrhovnega sodišča Koreje št. 96DA42789 z dne 24. julija 1998.
([5]) Odločba ustavnega sodišča št. 2002 Hun-Ma51 z dne 30. oktobra 2003. Ustavno sodišče je podobno v odločbah št. 99Hun-Ma513 in št. 2004Hun-Ma190 (konsolidirana) z dne 26. maja 2005 pojasnilo, da „je pravica do nadzora nad lastnimi osebnimi podatki pravica posameznika, na katerega se nanašajo osebni podatki, da se sam odloči, kdaj, komu ali prek koga in v kakšnem obsegu se bodo njegovi osebni podatki razkrili oziroma kdaj, pri kom ali prek koga in v kakšnem obsegu se bodo uporabili. S to temeljno pravico, ki sicer ni opredeljena v ustavi, se osebna svoboda odločanja ščiti pred tveganjem, ki ga povzroča širitev državnih funkcij in informacijsko-komunikacijske tehnologije.“
([6]) Člen 12(1), prvi stavek, ustave.
([7]) Člen 16 in člen 12(3) ustave.
([8]) Člen 12(3) ustave.
([9]) Člen 6(2) ustave.
([10]) Odločba ustavnega sodišča št. 93 Hun-MA120 z dne 29. decembra 1994. Glej na primer tudi odločbo ustavnega sodišča št. 2014Hun-Ma346 (z dne 31. maja 2018), v kateri je sodišče ugotovilo, da je bila sudanskemu državljanu, pridržanemu na letališču, kršena ustavna pravica do prejema pomoči pravnega svetovalca. V drugem primeru je ustavno sodišče ugotovilo, da je svobodna izbira zakonitega delovnega mesta tesno povezana s pravico do prizadevanja za srečo ter človekovim dostojanstvom in vrednostjo, zato ni omejena le na državljane, temveč je lahko zagotovljena tudi tujcem, zakonito zaposlenim v Republiki Koreji (odločba ustavnega sodišča št. 2007Hun-Ma1083 z dne 29. septembra 2011).

državljan, pravico do varstva svojega dostojanstva in vrednosti ter pravico, da si prizadeva za srečo. ([11]) Pojasnilo je tudi, da je pravica do nadzora nad lastnimi podatki temeljna pravica, ki izhaja iz pravice do dostojanstva in prizadevanja za srečo ter pravice do zasebnega življenja. ([12]) Čeprav se v sodni praksi pravica do zasebnosti posameznikov, ki niso državljani Koreje, do zdaj ni posebej obravnavala, je torej med strokovnjaki splošno sprejeto, da so v členih 12 do 22 ustave (ki vključujejo pravico do zasebnosti in osebno svobodo) določene „pravice ljudi“.

Nazadnje, ustava določa tudi pravico, da se od javnih organov zahteva pravična odškodnina. ([13]) Poleg tega lahko na podlagi zakona o ustavnem sodišču vsakdo, katerega temeljne pravice, ki jih zagotavlja ustava, so kršene z izvajanjem pooblastil državnih organov (razen z odločbami sodišč), vloži ustavno pritožbo pri ustavnem sodišču. ([14])

1.2. **Splošna pravila o varstvu podatkov**

Splošni zakon o varstvu podatkov v Republiki Koreji je zakon o varstvu osebnih podatkov, ki se uporablja za zasebni in javni sektor. V zvezi z javnimi organi se navedeni zakon sklicuje zlasti na obveznost oblikovati politike za preprečevanje „škodljivih posledic zlorabe in nepravilne uporabe osebnih podatkov, nediskretnega nadzora in sledenja itd. ter krepitev dostojanstva ljudi in njihove zasebnosti“ ([15]).

Pri obdelavi osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj veljajo vse zahteve iz zakona o varstvu osebnih podatkov. To na primer pomeni, da morajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj izpolnjevati zahteve glede zakonite obdelave, tj. sklicevati se morajo na eno od pravnih podlag za zbiranje, uporabo ali zagotavljanje osebnih podatkov iz zakona o varstvu osebnih podatkov (členi 15 do 18 zakona o varstvu osebnih podatkov), ter načela omejitve namena (člen 3(1) in (2) zakona o varstvu osebnih podatkov), sorazmernosti/najmanjšega obsega podatkov (člen 3(1) in (6) zakona o varstvu osebnih podatkov), omejene hrambe podatkov (člen 21 zakona o varstvu osebnih podatkov), varnosti podatkov, vključno z uradnim obveščanjem o kršitvi varnosti podatkov (člen 3(4) ter člena 29 in 34 zakona o varstvu osebnih podatkov), in preglednosti (člen 3(1) in (5) ter členi 20, 30 in 32 zakona o varstvu osebnih podatkov). V zvezi z občutljivimi podatki se uporabljajo posebni zaščitni ukrepi (člen 23 zakona o varstvu osebnih podatkov). Poleg tega lahko posamezniki zoper organe za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v skladu s členom 3(5), členom 4 in členi 35 do 39-2 zakona o varstvu osebnih podatkov uresničujejo svoje pravice do dostopa, popravka, izbrisa in prenehanja obdelave.

Čeprav se zakon o varstvu osebnih podatkov torej v celoti uporablja za obdelavo osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, vsebuje izjemo, kadar se osebni podatki obdelujejo za namene nacionalne varnosti. V skladu s členom 58(1), točka 2, zakona o varstvu osebnih podatkov se členi 15 do 50 navedenega zakona ne uporabljajo za osebne podatke, zbrane ali zahtevane za analizo informacij, povezanih z nacionalno varnostjo. ([16]) Nasprotno pa se še naprej uporabljajo poglavje I (Splošne določbe), poglavje II (Oblikovanje politik za varstvo osebnih podatkov itd.), poglavje VIII (Kolektivna tožba zoper kršitev podatkov), poglavje IX (Dodatne določbe) in poglavje X (Kazenske določbe) zakona o varstvu osebnih podatkov. To vključuje splošna načela o varstvu podatkov iz člena 3 (Načela varstva osebnih podatkov) in pravice posameznikov, zagotovljene s členom 4 zakona o varstvu osebnih podatkov (Pravice posameznikov, na katere se nanašajo osebni podatki). To pomeni, da se tudi na tem področju zagotavljajo glavna načela in pravice. Poleg tega člen 58(4) zakona o varstvu podatkov določa, da je treba take podatke obdelati v najmanjšem možnem obsegu, potrebnem za dosego predvidenega namena, in za najkrajše možno obdobje; prav tako se z njim zahteva, da upravljavec osebnih podatkov sprejme potrebne ukrepe, da se zagotovita varno upravljanje in ustrezna obdelava podatkov, kot so tehnični, upravljavski in fizični zaščitni ukrepi ter ukrepi za ustrezno obravnavanje posameznih pritožb.

Komisija za varstvo osebnih podatkov je v uradnem obvestilu št. 2021-1 o dodatnih pravilih za razlago in uporabo zakona o varstvu osebnih podatkov dodatno pojasnila, kako se navedeni zakon glede na to delno izjemo uporablja pri obdelavi osebnih podatkov za namene nacionalne varnosti. ([17]) To vključuje zlasti pravice posameznikov (do dostopa, popravka, prenehanja obdelave in izbrisa) ter razloge in omejitve za morebitno omejevanje teh pravic. Glede na uradno

([11]) Odločba ustavnega sodišča št. 99HeonMa494 z dne 29. novembra 2001.
([12]) Glej na primer odločbo ustavnega sodišča št. 99HunMa513.
([13]) Člen 29(1) ustave.
([14]) Člen 68(1) zakona o ustavnem sodišču.
([15]) Člen 5(1) zakona o varstvu osebnih podatkov.
([16]) Člen 58(1), točka 2, zakona o varstvu osebnih podatkov.
([17]) Uradno obvestilo komisije za varstvo osebnih podatkov št. 2021-1 o dodatnih pravilih za razlago in uporabo zakona o varstvu osebnih podatkov, oddelek III, točka 6.

obvestilo uporaba temeljnih načel, pravic in obveznosti iz zakona o varstvu osebnih podatkov pri obdelavi osebnih podatkov za namene nacionalne varnosti odraža jamstva, določena z ustavo, za varstvo pravice posameznika do nadzora nad svojimi osebnimi podatki. Pri vsaki omejitvi te pravice, na primer ko je to potrebno zaradi zaščite nacionalne varnosti, je treba tehtati med pravicami in interesi posameznika ter ustreznimi javnimi interesi, pri tem pa se ne sme posegati v bistvo pravice (člen 37(2) ustave).

2. VLADNI DOSTOP ZA NAMENE PREPREČEVANJA, ODKRIVANJA IN PREISKOVANJA KAZNIVIH DEJANJ

2.1. Pristojni javni organi na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

Na podlagi zakona o kazenskem postopku, zakona o varstvu zasebnosti komunikacij in zakona o zagotavljanju telekomunikacijskih storitev lahko policija, tožilci in sodišča zbirajo osebne podatke za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. V obsegu, v katerem zakon o nacionalni obveščevalni službi podeljuje tako pooblastilo nacionalni obveščevalni službi, mora ta upoštevati navedene zakone. ([18]) Nazadnje, zakon o sporočanju in uporabi specifičnih informacij o finančnih transakcijah finančnim institucijam zagotavlja pravno podlago za razkritje informacij finančnoobveščevalni enoti Koreje za namen preprečevanja pranja denarja in financiranja terorizma. Ta specializirana agencija pa lahko take informacije nato zagotovi organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Vendar te obveznosti razkritja veljajo le za upravljavce podatkov, ki obdelujejo osebne kreditne informacije v skladu z zakonom o kreditnih informacijah in ki so pod nadzorom komisije za finančne storitve. Ker je obdelava osebnih kreditnih informacij s strani takih upravljavcev izključena iz področja uporabe sklepa o ustreznosti, omejitve in zaščitni ukrepi, ki se uporabljajo na podlagi zakona o sporočanju in uporabi specifičnih informacij o finančnih transakcijah v tem dokumentu niso podrobneje opisani.

2.2. Pravna podlaga in omejitve

Zakon o kazenskem postopku (glej oddelek 2.2.1), zakon o varstvu zasebnosti komunikacij (glej oddelek 2.2.2) ter zakon o zagotavljanju telekomunikacijskih storitev (glej oddelek 2.2.3) zagotavljajo pravno podlago za zbiranje osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter določajo omejitve in zaščitne ukrepe, ki se uporabljajo.

2.2.1. *Preiskave in zasegi*

2.2.1.1. Pravna podlaga

Tožilci in višji pravosodni policisti lahko pregledajo predmete, preiščejo osebe ali zasežejo predmete le, če (1) je oseba osumljena storitve kaznivega dejanja (v nadaljnjem besedilu: osumljenec kaznivega dejanja), (2) je to nujno za preiskavo ter (3) se šteje, da so predmeti, ki naj bi se pregledali, osebe, ki naj bi se preiskale, in morebitni zaseženi predmeti povezani z zadevo. ([19]) Enako lahko sodišča opravijo preiskave ali zasežejo predmete, ki naj bi se uporabili kot dokaz ali bi se lahko odvzeli, če se šteje, da so taki predmeti ali osebe povezani s konkretno zadevo. ([20])

2.2.1.2. Omejitve in zaščitni ukrepi

Tožilci in pravosodni policisti morajo kot splošno obveznost spoštovati človekove pravice osumljenca kaznivega dejanja in vseh drugih zadevnih oseb. ([21]) Poleg tega se lahko obvezni ukrepi za dosego namena preiskave sprejmejo le, kadar je to izrecno določeno v zakonu o kazenskem postopku, in v najmanjšem potrebnem obsegu. ([22])

Preiskave, pregledi ali zasegi, ki jih policisti ali tožilci izvedejo v okviru kazenskih preiskav, lahko potekajo le na podlagi pridobljene odredbe sodišča. ([23]) Organ, ki vloži vlogo za izdajo odredbe, mora predložiti dokazno gradivo, iz katerega so razvidni razlogi za sum, da je posameznik storil kaznivo dejanje, da je potrebna preiskava, pregled ali zaseg in da obstajajo ustrezni predmeti, ki jih je treba zaseči. ([24]) V odredbi morajo biti med drugim navedeni imena osumljenca kaznivega dejanja in kaznivo dejanje, kraj, oseba ali predmeti, ki jih je treba preiskati, ali predmeti, ki jih je treba zaseči, datum izdaje in dejansko obdobje uporabe. ([25]) Podobno je treba, ko se v okviru tekočega sodnega postopka zunaj glavne obravnave izvajajo preiskave in zasegi, predhodno pridobiti odredbo sodišča. ([26]) Zadevni posameznik in njegov zagovornik sta vnaprej uradno obveščena o preiskavi ali zasegu in sta lahko prisotna ob izvršitvi odredbe sodišča. ([27])

([18]) Glej člen 3 zakona o nacionalni obveščevalni službi (zakon št. 12948), ki se nanaša na kazenske preiskave določenih kaznivih dejanj, kot so vstaja, upor in kazniva dejanja, povezana z nacionalno varnostjo (npr. vohunjenje). V tem okviru bi se v zvezi s preiskavami in zasegi uporabljali postopki iz zakona o kazenskem postopku, medtem ko bi zakon o varstvu zasebnosti komunikacij urejal zbiranje komunikacijskih podatkov (glej del 3 o določbah, ki se nanašajo na dostop do komunikacij za namene nacionalne varnosti).
([19]) Člen 215(1) in (2) zakona o kazenskem postopku.
([20]) Člen 106(1) ter člena 107 in 109 zakona o kazenskem postopku.
([21]) Člen 198(2) zakona o kazenskem postopku.
([22]) Člen 199(1) zakona o kazenskem postopku.
([23]) Člen 215(1) in (2) zakona o kazenskem postopku.
([24]) Člen 108(1) uredbe o kazenskem postopku.
([25]) Člen 114(1) zakona o kazenskem postopku v povezavi s členom 219 navedenega zakona.
([26]) Člen 113 zakona o kazenskem postopku.
([27]) Člena 121 in 122 zakona o kazenskem postopku.

Kadar se izvajajo preiskave ali zasegi in je predmet, ki ga je treba preiskati, računalniški disk ali drug nosilec podatkov, se načeloma zasežejo le sami (kopirani ali natisnjeni) podatki in ne celoten nosilec podatkov. ([28]) Sam nosilec podatkov se lahko zaseže le, kadar je praktično nemogoče ločeno natisniti ali kopirati potrebne podatke ali kadar namena preiskave praktično ni mogoče doseči drugače. ([29]) Zadevnega posameznika je treba nemudoma uradno obvestiti o zasegu. ([30]) V zakonu o kazenskem postopku ni izjem v zvezi s tem uradnim obvestilom.

Preiskave, pregledi in zasegi brez odredbe lahko potekajo le v omejenih primerih. Prvič, tako je v primeru, ko odredbe zaradi nujnosti na kraju izvršitve kaznivega dejanja ni mogoče pridobiti. ([31]) Kljub temu je treba odredbo nemudoma pridobiti naknadno. ([32]) Drugič, preiskave in pregledi brez odredbe lahko potekajo na kraju samem, ko je osumljencu kaznivega dejanja odvzeta prostost ali je pridržan. ([33]) Nazadnje, tožilec ali višji pravosodni policist lahko brez odredbe zaseže predmet, ki ga je osumljenec kaznivega dejanja ali tretja oseba zavrgla ali je bil prostovoljno izročen. ([34])

Dokazi, pridobljeni v nasprotju z zakonom o kaznivih dejanjih, niso dopustni. ([35]) Poleg tega kazenski zakonik določa, da se nezakonite preiskave oseb ali prebivališča osebe, zastražene stavbe, gradnje, avtomobila, ladje, zrakoplova ali bivalnega prostora kaznujejo s kaznijo zapora do treh let. ([36]) Ta določba se zato uporablja tudi, kadar se med nezakonitim zasegom zasežejo predmeti, kot so naprave za shranjevanje podatkov.

2.2.2. *Zbiranje podatkov o komunikaciji*

2.2.2.1. Pravna podlaga

Zbiranje podatkov o komunikaciji ureja poseben zakon, tj. zakon o varstvu zasebnosti komunikacij. Navedeni zakon zlasti določa, da nihče ne sme cenzurirati pošte, prisluškovati pogovorom prek telekomunikacij, pošiljati podrobnih podatkov o opravljeni komunikaciji oziroma snemati ali poslušati pogovorov med drugimi, ki niso javni, razen na podlagi zakona o kazenskem postopku, zakona o varstvu zasebnosti komunikacij ali zakona o vojaškem sodišču. ([37]) Pojem „komunikacija“ v smislu zakona o varstvu zasebnosti komunikacij zajema običajno pošto in telekomunikacije. ([38]) V zvezi s tem se v zakonu razlikuje med „ukrepi za omejevanje komunikacij“ ([39]) in zbiranjem „podrobnih podatkov o opravljeni komunikaciji“.

Pojem ukrepi za omejevanje komunikacij zajema „cenzuro“, tj. zbiranje vsebine navadne pošte, in „prisluškovanje pogovorom“, tj. neposredno prestrezanje (pridobivanje ali snemanje) vsebine telekomunikacij. ([40]) Pojem podrobni podatki o opravljeni komunikaciji zajema „podatke o evidencah opravljenih telekomunikacij“, kar vključuje podatke o datumu telekomunikacij ter času njihovega začetka in konca, številu dohodnih in odhodnih klicev, naročniški številki sogovornika ter pogostosti uporabe, dnevniške datoteke o uporabi telekomunikacijskih storitev in podatke o lokaciji (npr. iz baznih postaj, ki sprejemajo signal). ([41])

([28]) Člen 106(3) zakona o kazenskem postopku.
([29]) Člen 106(3) zakona o kazenskem postopku.
([30]) Člen 219 zakona o kazenskem postopku v povezavi s členom 106(4) zakona o kazenskem postopku.
([31]) Člen 216(3) zakona o kazenskem postopku.
([32]) Člen 216(3) zakona o kazenskem postopku.
([33]) Člen 216(1) in (2) zakona o kazenskem postopku.
([34]) Člen 218 zakona o kazenskem postopku. V zvezi z osebnimi podatki to zajema le podatke, ki jih prostovoljno zagotovi zadevni posameznik sam, ne pa tudi upravljavec osebnih podatkov, ki ima take podatke (za kar bi bila na podlagi zakona o varstvu osebnih podatkov potrebna posebna pravna podlaga). Predmeti, izročeni prostovoljno, so dopustni kot dokazi v sodnem postopku le, če ni razumnega dvoma o prostovoljni naravi razkritja, kar mora dokazati tožilec. Glej odločbo vrhovnega sodišča št. 2013Do11233 z dne 10. marca 2016.
([35]) Člen 308-2 zakona o kazenskem postopku.
([36]) Člen 321 kazenskega zakona.
([37]) Člen 3 zakona o varstvu zasebnosti komunikacij. Zakon o vojaškem sodišču načeloma ureja zbiranje informacij o vojaškem osebju, za civiliste pa se lahko uporablja le v omejenih primerih (npr. če bi vojaško osebje in civilisti skupaj storili kaznivo dejanje ali če posameznik stori kaznivo dejanje zoper vojsko, se lahko postopek začne pred vojaškim sodiščem, glej člen 2 zakona o vojaškem sodišču). Splošne določbe, ki urejajo preiskave in zasege, so podobne zakonu o kazenskem postopku, glej na primer člene 146 do 149 in 153 do 156 zakona o vojaškem sodišču. Navadna pošta se lahko na primer zbira le, kadar je to potrebno za preiskavo in na podlagi odredbe vojaškega sodišča. Če bi se zbirale elektronske komunikacije, se uporabljajo omejitve in zaščitni ukrepi iz zakona o varstvu zasebnosti komunikacij.
([38]) V členu 2(1) zakona o varstvu zasebnosti komunikacij je navedeno: „prenos ali sprejem vseh vrst zvokov, besed, simbolov ali podob po žici, brezžično, po optičnem kablu ali drugih elektromagnetnih sistemih, vključno s telefonom, e-pošto, storitvijo podatkov o članstvu, telefaksom in radijskim osebnim klicem“.
([39]) Člen 2(7) in člen 3(2) zakona o varstvu zasebnosti komunikacij.
([40]) „Cenzura“ je opredeljena kot „odpiranje pošte brez privolitve zadevne osebe ali seznanitev z vsebino, njeno snemanje ali zadržanje z drugimi sredstvi“ (člen 2(6) zakona o varstvu zasebnosti komunikacij). „Prisluškovanje pogovorom“ pomeni „pridobivanje ali snemanje vsebine telekomunikacij s prisluškovanjem ali skupnim branjem zvokov, besed, simbolov ali podob v okviru komunikacij z elektronskimi in mehanskimi napravami brez privolitve zadevne osebe ali poseganje v njihov prenos in sprejem“ (člen 2(7) zakona o varstvu zasebnosti komunikacij).
([41]) Člen 2(11) zakona o varstvu zasebnosti komunikacij.

Zakon o varstvu zasebnosti komunikacij določa omejitve in zaščitne ukrepe za zbiranje obeh vrst podatkov, za neupoštevanje več teh zahtev pa se izrečejo kazenske sankcije. ([42])

2.2.2.2. Omejitve in zaščitni ukrepi, ki se uporabljajo za zbiranje vsebine komunikacij (ukrepi za omejevanje komunikacij)

Zbiranje vsebine komunikacij lahko poteka le kot dodatni način za lajšanje kazenske preiskave (tj. kot skrajni ukrep), pri čemer si je treba prizadevati za čim manjše poseganje v zaupnost komunikacij med ljudmi. ([43]) Ukrepi za omejevanje komunikacij se lahko v skladu s tem splošnim načelom uporabijo le, če bi se sicer težko preprečila storitev kaznivega dejanja, prijel storilec kaznivega dejanja ali zbrali dokazi. ([44]) Organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ki zbirajo vsebino komunikacij, morajo s tem takoj prenehati, ko nadaljnji dostop ni več potreben, s čimer zagotovijo, da je poseganje v zasebnost komunikacij čim manjše. ([45])

Poleg tega se lahko ukrepi za omejevanje komunikacij uporabijo le, če obstajajo utemeljeni razlogi za sum, da se načrtujejo, izvajajo ali so bila storjena določena huda kazniva dejanja, izrecno navedena v zakonu o varstvu zasebnosti komunikacij. To vključuje kazniva dejanja, kot so vstaja, kriminal, povezan z drogami, ali kazniva dejanja, ki vključujejo uporabo eksploziva, in kazniva dejanja, povezana z nacionalno varnostjo, diplomatskimi odnosi ali vojaškimi oporišči in objekti. ([46]) Cilj ukrepa za omejevanje komunikacij morajo biti določene poštne pošiljke oziroma telekomunikacije, ki jih pošlje ali prejme osumljenec, ali poštne pošiljke oziroma telekomunikacije, ki jih osumljenec pošlje ali prejme v določenem obdobju. ([47])

Tudi kadar so izpolnjeni vsi ti pogoji, lahko zbiranje podatkov o vsebini poteka le na podlagi odredbe sodišča. Zlasti lahko tožilec zahteva, da sodišče dovoli zbiranje podatkov o vsebini v zvezi z osumljencem ali preiskovancem. ([48]) Podobno lahko pravosodni policist za dovoljenje zaprosi tožilca, ta pa lahko nato zahteva odredbo sodišča. ([49]) Zahteva za izdajo odredbe mora biti pisna in mora vsebovati točno določene elemente. Zlasti morajo biti v njej navedeni (1) utemeljeni razlogi za sum, da se načrtuje, izvaja ali je bilo storjeno eno od kaznivih dejanja s seznama, ter vse dokazno gradivo, ki že na prvi pogled potrjuje sum, (2) ukrepi za omejevanje komunikacij, njihovi cilji, obseg, namen in dejansko obdobje izvajanja ter (3) kraj in način izvedbe ukrepov. ([50])

Če so izpolnjene pravne zahteve, lahko sodišče izda pisno dovoljenje za izvedbo ukrepov za omejevanje komunikacij v zvezi z osumljencem ali preiskovancem. ([51]) V njem so določene vrste ukrepov ter njihov cilj, obseg, dejansko obdobje izvajanja, kraj in način izvedbe. ([52])

Ukrepi za omejevanje komunikacij se lahko izvajajo le dva meseca. ([53]) Če je njihov namen dosežen še pred koncem tega obdobja, se morajo takoj prenehati izvajati. Če pa so zahtevani pogoji še vedno izpolnjeni, se lahko v dvomesečnem roku vloži zahteva za podaljšanje dejanskega obdobja uporabe teh ukrepov. Taka zahteva mora vključevati dokazno gradivo, ki že na prvi pogled utemeljuje podaljšanje ukrepov. ([54]) Podaljšano obdobje skupno ne sme presegati enega leta ali treh let za določena posebno huda kazniva dejanja (npr. kazniva dejanja, povezana z vstajo, vojaškim napadom tujih sil, nacionalno varnostjo itd.). ([55])

Organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj lahko zahtevajo pomoč komunikacijskih operaterjev, in sicer z zagotovitvijo pisnega dovoljenja sodišča. ([56]) Komunikacijski operaterji morajo sodelovati in prejeto dovoljenje hraniti v svojih evidencah. ([57]) Sodelovanje lahko zavrnejo, če so podatki o ciljnem posamezniku, kot so navedeni na pisnem dovoljenju sodišča (npr. njegova telefonska številka), nepravilni. Poleg tega ne smejo v nobenem primeru razkriti gesel, ki se uporabljajo za telekomunikacije. ([58])

([42]) Člena 16 in 17 zakona o varstvu zasebnosti komunikacij. To se nanaša na primere, ko zbiranje poteka brez odredbe sodišča, ko se ne vodijo evidence, ko zbiranje ne preneha ob koncu nujnega primera ali ko zadevni posameznik ni obveščen.
([43]) Člen 3(2) zakona o varstvu zasebnosti komunikacij.
([44]) Člen 5(1) zakona o varstvu zasebnosti komunikacij.
([45]) Člen 2 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([46]) Člen 5(1) zakona o varstvu zasebnosti komunikacij.
([47]) Člen 5(2) zakona o varstvu zasebnosti komunikacij.
([48]) Člen 6(1) zakona o varstvu zasebnosti komunikacij.
([49]) Člen 6(2) zakona o varstvu zasebnosti komunikacij.
([50]) Člen 6(4) zakona o varstvu zasebnosti komunikacij in člen 4(1) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([51]) Člen 6(5) in (8) zakona o varstvu zasebnosti komunikacij.
([52]) Člen 6(6) zakona o varstvu zasebnosti komunikacij.
([53]) Člen 6(7) zakona o varstvu zasebnosti komunikacij.
([54]) Člen 6(7) zakona o varstvu zasebnosti komunikacij.
([55]) Člen 6(8) zakona o varstvu zasebnosti komunikacij.
([56]) Člen 9(2) zakona o varstvu zasebnosti komunikacij.
([57]) Člen 15-2 zakona o varstvu zasebnosti komunikacij in člen 12 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([58]) Člen 9(4) zakona o varstvu zasebnosti komunikacij.

Vsakdo, ki izvaja ukrepe za omejevanje komunikacij ali od katerega se zahteva sodelovanje, mora voditi evidenco, v kateri navede namen ukrepov, njihovo izvedbo, datum zagotovitve sodelovanja in cilj. ([59]) Organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ki izvajajo ukrepe za omejevanje komunikacij, morajo prav tako voditi evidenco, v kateri navedejo podrobnosti in dosežene rezultate. ([60]) Pravosodni policisti morajo te informacije zagotoviti v poročilu tožilcu ob zaključku preiskave. ([61])

Ko tožilec v zvezi z zadevo, v kateri so se uporabili ukrepi za omejevanje komunikacij, vloži obtožni akt ali izda odločitev o tem, da obtožnica ne bo vložena oziroma da se ne bo zahtevalo prijetje zadevnega posameznika (tj. ne le sklep o začasni prekinitvi postopka), mora posameznika, zoper katerega se uporabljajo ukrepi za omejevanje komunikacij, uradno obvestiti o izvedbi takih ukrepov, organu, ki jih je izvedel, in obdobju njihovega izvajanja. Tako uradno obvestilo je treba poslati v 30 dneh po odločitvi. ([62]) Pošiljanje uradnega obvestila se lahko odloži, če je verjetno, da bi to resno ogrozilo nacionalno varnost ali poseglo v javno varnost in red, ali če je verjetno, da bi to povzročilo bistveno škodo za življenje in telo drugih oseb. ([63]) Če namerava tožilec ali pravosodni policist pošiljanje uradnega obvestila odložiti, mora pridobiti soglasje direktorja okrožnega državnega tožilstva. ([64]) Ko razlogi za odlog prenehajo, je treba uradno obvestilo poslati v 30 dneh po prenehanju. ([65])

Zakon o varstvu zasebnosti komunikacij določa tudi poseben postopek za zbiranje vsebine komunikacij v nujnih primerih. Organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj lahko vsebino komunikacij zbirajo zlasti v primeru skorajšnjega načrtovanja ali storitve kaznivega dejanja organiziranega kriminala ali drugega hudega kaznivega dejanja, katerega neposredna posledica bi lahko bila smrt ali huda poškodba, ukrepanje pa je tako nujno, da ni mogoče izvesti rednega postopka (kot je opredeljen zgoraj). ([66]) Policist ali tožilec lahko v takem nujnem primeru sprejme ukrepe za omejevanje komunikacij brez predhodnega dovoljenja sodišča, vendar mora zanj zaprositi takoj po izvedbi ukrepa. Če organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ne pridobi dovoljenja sodišča v 36 urah od trenutka, ko so bili izvedeni nujni ukrepi, mora zbiranje takoj prenehati, čemur običajno sledi uničenje zbranih informacij. ([67]) Policisti, ki izvajajo nadzor v nujnih primerih, to počnejo pod nadzorom tožilca, če pa navodil tožilca zaradi nujnosti hitrega ukrepanja ni mogoče zagotoviti vnaprej, mora policija pridobiti soglasje tožilca takoj po začetku izvajanja. ([68]) Pravila o uradnem obveščanju posameznika, kot so opisana zgoraj, se uporabljajo tudi za zbiranje vsebine komunikacij v nujnih primerih.

Zbiranje informacij v nujnih primerih mora vedno potekati v skladu z „izjavo o cenzuri/prisluškovanju v nujnem primeru“, organ, ki izvaja zbiranje, pa mora voditi evidenco vseh nujnih ukrepov. ([69]) Zahtevi sodišču za izdajo dovoljenja za nujne ukrepe je treba priložiti pisni dokument, v katerem so navedeni potrebni ukrepi za omejevanje komunikacij, cilj, obseg, obdobje izvajanja, kraj izvedbe, način in pojasnilo, kako zadevni ukrepi za omejevanje komunikacij izpolnjujejo člen 5(1) zakona o varstvu zasebnosti komunikacij ([70]), skupaj z dokazili.

V primerih, ko se nujni ukrepi zaključijo hitro, tako da dovoljenje sodišča ni več potrebno (npr. če je osumljenec prijet takoj po začetku prestrezanja, ki s tem preneha), direktor pristojnega državnega tožilstva o nujnem ukrepu obvesti pristojno sodišče. ([71]) V obvestilu morajo biti navedeni namen, cilj, obseg, obdobje izvajanja, kraj izvedbe in način zbiranja ter razlogi za nevložitev zahteve za dovoljenje sodišča. ([72]) To obvestilo, na podlagi katerega lahko sodišče, ki ga prejme, prouči zakonitost zbiranja, je treba vključitvi v evidenco obvestil o nujnih ukrepih.

([59]) Člen 9(3) zakona o varstvu zasebnosti komunikacij.
([60]) Člen 18(1) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([61]) Člen 18(2) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([62]) Člen 9-2(1) zakona o varstvu zasebnosti komunikacij.
([63]) Člen 9-2(4) zakona o varstvu zasebnosti komunikacij.
([64]) Člen 9-2(5) zakona o varstvu zasebnosti komunikacij.
([65]) Člen 9-2(6) zakona o varstvu zasebnosti komunikacij.
([66]) Člen 8(1) zakona o varstvu zasebnosti komunikacij.
([67]) Člen 8(2) zakona o varstvu zasebnosti komunikacij.
([68]) Člen 8(3) zakona o varstvu zasebnosti komunikacij in člen 16(3) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([69]) Člen 8(4) zakona o varstvu zasebnosti komunikacij.
([70]) In sicer, da obstaja utemeljen razlog za sum, da se načrtujejo, izvajajo ali so bila storjena določena huda kazniva dejanja, ter da drugače ni mogoče preprečiti storitve kaznivega dejanja, prijeti osumljenca ali zbrati dokazov.
([71]) Člen 8(5) zakona o varstvu zasebnosti komunikacij.
([72]) Člen 86(7) zakona o varstvu zasebnosti komunikacij.

Na splošno se zahteva, da se lahko vsebina komunikacij, pridobljenih z izvajanjem ukrepov za omejevanje komunikacij na podlagi zakona o varstvu zasebnosti komunikacij, uporabi le za preiskovanje, kazenski pregon ali preprečevanje zgoraj navedenih specifičnih kaznivih dejanj, v disciplinskem postopku za ista kazniva dejanja, v okviru odškodninske tožbe, ki jo vloži stranka v komunikaciji, ali kadar to dovoljujejo drugi predpisi. ([73])

V primeru zbiranja telekomunikacij, ki se prenašajo prek interneta, se uporabljajo posebni zaščitni ukrepi. ([74]) Take informacije se lahko uporabijo le za preiskovanje hudih kaznivih dejanj iz člena 5(1) zakona o varstvu zasebnosti komunikacij. Za hrambo informacij je treba pridobiti soglasje sodišča, ki je dovolilo ukrepe za omejevanje komunikacij. ([75]) V zahtevi za hrambo je treba navesti podatke o ukrepih za omejevanje komunikacij, povzetek rezultatov ukrepov, razloge za hrambo (skupaj z dokazili) in telekomunikacije, ki naj bi se hranile. ([76]) Če taka zahteva ni vložena, je treba pridobljene telekomunikacije izbrisati v 14 dneh po zaključku ukrepov za omejevanje komunikacij. ([77]) Če je zahteva zavrnjena, je treba telekomunikacije uničiti v sedmih dneh. ([78]) V primeru izbrisa telekomunikacij je treba sodišču, ki je dovolilo ukrepe za omejevanje komunikacij, v sedmih dneh poslati poročilo, v katerem so navedeni razlogi za izbris ter podrobnosti in čas izbrisa.

Če so bile informacije z ukrepi za omejevanje komunikacij pridobljene nezakonito, na splošno niso dopustne kot dokaz v sodnem ali disciplinskem postopku. ([79]) Zakon o varstvu zasebnosti komunikacij prav tako prepoveduje, da bi osebe, ki sodelujejo pri ukrepih za omejevanje komunikacij, razkrile zaupne informacije, pridobljene med izvajanjem takih ukrepov, in da bi take informacije uporabile za škodovanje ugledu oseb, na katere se ti ukrepi nanašajo. ([80])

2.2.2.3. Omejitve in zaščitni ukrepi, ki se uporabljajo za zbiranje podrobnih podatkov o opravljeni komunikaciji

Organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj lahko na podlagi zakona o varstvu zasebnosti komunikacij od telekomunikacijskih operaterjev zahtevajo predložitev podrobnih podatkov o opravljeni komunikaciji, kadar je to potrebno za izvedbo preiskave ali izvršitev kazni. ([81]) Možnost zbiranja podrobnih podatkov o opravljeni komunikaciji za razliko od zbiranja vsebine podatkov ni omejena na specifična kazniva dejanja. Tudi pri zbiranju tovrstnih podatkov pa je kot za podatke o vsebini potrebno predhodno pisno dovoljenje sodišča, za kar veljajo enaki pogoji, kot so opisani zgoraj. ([82]) Kadar iz nujnih razlogov dovoljenja sodišča ni mogoče pridobiti, se lahko podrobni podatki o opravljeni komunikaciji zbirajo brez odredbe, vendar je treba v tem primeru dovoljenje pridobiti takoj po tem, ko se podatki zahtevajo, in ga predložiti ponudniku telekomunikacijskih storitev. ([83]) Če se naknadno dovoljenje ne pridobi, je treba zbrane podatke uničiti. ([84])

Tožilci, pravosodni policisti in sodišča morajo voditi evidence zahtev za podrobne podatke o opravljeni komunikaciji. ([85]) Ponudniki telekomunikacijskih storitev morajo poleg tega o razkritju teh podatkov dvakrat letno poročati ministru za znanost in informacijsko tehnologijo, evidenco o njih pa morajo hraniti sedem let od datuma razkritja podatkov. ([86])

Posamezniki morajo biti načeloma uradno obveščeni o dejstvu, da se zbirajo podrobni podatki o opravljeni komunikaciji. ([87]) Roki za tako uradno obveščanje so odvisni od okoliščin preiskave. ([88]) Po sprejetju odločitve o pregonu (ali opustitvi pregona) je treba uradno obvestilo poslati v 30 dneh. Če pa je vložitev obtožnega akta odložena, je treba uradno obvestilo poslati v 30 dneh po preteku enega leta od datuma sprejetja take odločitve. Vsekakor je treba uradno obvestilo poslati v 30 dneh po preteku enega leta od datuma zbiranja podatkov.

Uradno obveščanje se lahko odloži, če je verjetno, da bi (1) ogrozilo nacionalno varnost, javno varnost in red, (2) povzročilo smrt ali telesno poškodbo, (3) oviralo pošten sodni postopek (npr. imelo za posledico uničenje dokazov

([73]) Člen 12 zakona o varstvu zasebnosti komunikacij.
([74]) Člen 12-2 zakona o varstvu zasebnosti komunikacij.
([75]) Tožilec ali policist, ki izvaja ukrepe za omejevanje komunikacij, mora v 14 dneh po zaključku ukrepov izbrati telekomunikacije, ki se bodo shranile, in zaprositi za soglasje sodišča (policist mora vlogo predložiti tožilcu, ta pa jo nato vloži pri sodišču), glej člen 12-2(1) in (2) zakona o varstvu zasebnosti komunikacij.
([76]) Člen 12-2(3) zakona o varstvu zasebnosti komunikacij.
([77]) Člen 12-2(5) zakona o varstvu zasebnosti komunikacij.
([78]) Člen 12-2(5) zakona o varstvu zasebnosti komunikacij.
([79]) Člen 4 zakona o varstvu zasebnosti komunikacij.
([80]) Člen 11(2) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([81]) Člen 13(1) zakona o varstvu zasebnosti komunikacij.
([82]) Člena 13 in 6 zakona o varstvu zasebnosti komunikacij.
([83]) Člen 13(2) zakona o varstvu zasebnosti komunikacij. Tudi v tem primeru je treba tako kot pri nujnih ukrepih za omejevanje komunikacij sestaviti dokument s podrobnostmi o zadevi (osumljenec, ukrepi, ki naj bi se sprejeli, domnevno kaznivo dejanje in nujnost). Glej člen 37(5) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([84]) Člen 13(3) zakona o varstvu zasebnosti komunikacij.
([85]) Člen 13(5) in (6) zakona o varstvu zasebnosti komunikacij.
([86]) Člen 13(7) zakona o varstvu zasebnosti komunikacij.
([87]) Glej člen 13-3(7) v povezavi s členom 9-2 zakona o varstvu zasebnosti komunikacij.
([88]) Člen 13-3(1) zakona o varstvu zasebnosti komunikacij.

ali grožnje pričam) ali (4) škodilo ugledu osumljenca, žrtev ali drugih oseb, povezanih s kaznivim dejanjem, ali poseglo v njihovo zasebnost. ([89]) Za uradno obvestilo, ki temelji na enem od navedenih razlogov, je potrebno dovoljenje direktorja pristojnega okrožnega državnega tožilstva. ([90]) Ko razlogi za odlog prenehajo, je treba uradno obvestilo poslati v 30 dneh po prenehanju. ([91])

Uradno obveščeni posamezniki lahko tožilcu ali pravosodnemu policistu predložijo pisno zahtevo v zvezi z razlogi za zbiranje podrobnih podatkov o opravljeni komunikaciji. ([92]) Tožilec ali pravosodni policist mora v tem primeru v 30 dneh po prejemu zahteve pisno navesti razloge, razen če velja ena od navedenih podlag (izjeme za odlog uradnega obveščanja). ([93])

2.2.3. *Prostovoljno razkritje s strani telekomunikacijskih operaterjev*

Člen 83(3) zakona o zagotavljanju telekomunikacijskih storitev dovoljuje, da telekomunikacijski operaterji prostovoljno izpolnijo zahtevo (v podporo sojenju v kazenski zadevi, preiskavi ali izvršitvi kazni) sodišča, tožilca ali vodje preiskovalnega organa za razkritje „podatkov o komunikacijah". „Podatki o komunikacijah" v okviru zakona o zagotavljanju telekomunikacijskih storitev zajemajo ime, registrsko številko prebivalca, naslov in telefonsko številko uporabnikov, datume, ko uporabniki sklenejo ali prekinejo naročnino, ter oznake za identifikacijo uporabnikov (npr. oznake, ki se uporabljajo za identifikacijo zakonitega uporabnika računalniških sistemov ali komunikacijskih omrežij). ([94]) Kot uporabniki se za namen zakona o zagotavljanju telekomunikacijskih storitev štejejo le posamezniki, ki imajo neposredno sklenjene pogodbe za storitve korejskih ponudnikov telekomunikacijskih storitev. ([95]) Zato bodo primeri, v katerih bi se posamezniki iz EU, katerih podatki so se prenesli v Republiko Korejo, šteli za uporabnike na podlagi zakona o zagotavljanju telekomunikacijskih storitev, verjetno zelo omejeni, saj ti posamezniki običajno ne bi sklenili neposredne pogodbe s korejskim ponudnikom telekomunikacijskih storitev.

Zahteve za pridobitev podatkov o komunikacijah na podlagi zakona o zagotavljanju telekomunikacijskih storitev je treba predložiti pisno, v njih pa je treba navesti razloge za zahtevo, povezavo z zadevnim uporabnikom in obseg zahtevanih podatkov. ([96]) Kadar zaradi nujnosti ni mogoče predložiti pisne zahteve, je treba tako zahtevo predložiti takoj po prenehanju razloga za nujnost. ([97]) Telekomunikacijski operaterji, ki ugodijo zahtevam za razkritje podatkov o komunikacijah, morajo hraniti evidence z zapisi o zagotovitvi telekomunikacijskih podatkov in s tem povezanim dokaznim gradivom, kot so pisne zahteve. ([98]) Poleg tega morajo o zagotavljanju podatkov o komunikacijah dvakrat letno poročati ministru za znanost in informacijsko tehnologijo. ([99])

Za telekomunikacijske operaterje ne velja obveznost, da morajo ugoditi zahtevam za razkritje podatkov o komunikacijah, na podlagi zakona o zagotavljanju telekomunikacijskih storitev. Zato mora operater vsako zahtevo proučiti glede na zahteve o varstvu podatkov, ki veljajo na podlagi zakona o varstvu osebnih podatkov. Zlasti mora upoštevati interese posameznika, na katerega se nanašajo osebni podatki, in informacij ne sme razkriti, če bi s tem verjetno nepošteno posegel v interese posameznika ali tretje osebe. ([100]) Poleg tega mora biti zadevni posameznik v skladu z uradnim obvestilom št. 2021-1 o dodatnih pravilih za razlago in uporabo zakona o varstvu osebnih podatkov uradno obveščen o razkritju. Tako uradno obveščanje se lahko v izjemnih primerih odloži, zlasti če in dokler bi ogrozilo tekočo kazensko preiskavo ali bi verjetno povzročilo škodo za življenje ali telo druge osebe, kadar te pravice ali interesi očitno prevladajo nad pravicami posameznika, na katerega se nanašajo osebni podatki. ([101])

Vrhovno sodišče je leta 2016 potrdilo, da prostovoljno zagotavljanje podatkov o komunikacijah s strani telekomunikacijskih operaterjev brez odredbe na podlagi zakona o zagotavljanju telekomunikacijskih storitev kot tako ne krši pravice do samoodločanja glede informacij uporabnika telekomunikacijske storitve. Hkrati je pojasnilo, da bi taka kršitev nastala, če je očitno, da je organ, ki podatke zahteva, zlorabil pooblastilo za zahtevanje razkritja podatkov o komunikacijah in s tem posegel v interese zadevnega posameznika ali tretje osebe. ([102]) Vsaka zahteva za prostovoljno razkrije, ki jo vloži organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, mora v skladu s korejsko ustavo (člen 12(1) in člen 37(2)) na splošno izpolnjevati načela zakonitosti, nujnosti in sorazmernosti.

([89]) Člen 13-3(2) zakona o varstvu zasebnosti komunikacij.
([90]) Člen 13-3(3) zakona o varstvu zasebnosti komunikacij.
([91]) Člen 13-3(4) zakona o varstvu zasebnosti komunikacij.
([92]) Člen 13-3(5) zakona o varstvu zasebnosti komunikacij.
([93]) Člen 13-3(6) zakona o varstvu zasebnosti komunikacij.
([94]) Člen 83(3) zakona o zagotavljanju telekomunikacijskih storitev.
([95]) Člen 2(9) zakona o zagotavljanju telekomunikacijskih storitev.
([96]) Člen 83(4) zakona o zagotavljanju telekomunikacijskih storitev.
([97]) Člen 83(4) zakona o zagotavljanju telekomunikacijskih storitev.
([98]) Člen 83(5) zakona o zagotavljanju telekomunikacijskih storitev.
([99]) Člen 83(6) zakona o zagotavljanju telekomunikacijskih storitev.
([100]) Člen 18(2) zakona o varstvu osebnih podatkov.
([101]) Uradno obvestilo komisije za varstvo osebnih podatkov št. 2021-1 o dodatnih pravilih za razlago in uporabo zakona o varstvu osebnih podatkov, oddelek III, točka 2(iii).
([102]) Odločba vrhovnega sodišča št. 2012Da105482 z dne 10. marca 2016.

2.3. **Nadzor**

Nadzor nad organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj se izvaja z različnimi mehanizmi, tako notranje kot s strani zunanjih organov.

2.3.1. *Notranja revizija*

Javni organi so v skladu z zakonom o revizijah v javnem sektorju spodbujeni, da ustanovijo notranji organ za notranjo revizijo, ki bi imel med drugim nalogo nadzora nad zakonitostjo. ([103]) Vodjem takih revizijskih organov mora biti zagotovljena čim večja neodvisnost. ([104]) Natančneje, imenujejo se izmed oseb zunaj zadevnega organa (npr. nekdanji sodniki, profesorji) za obdobje dveh do petih let, razrešiti pa jih je mogoče le iz utemeljenih razlogov (npr. ko niso zmožni opravljati nalog zaradi duševne ali fizične motnje ali ko so zoper njih uvedeni disciplinski ukrepi). ([105]) Podobno so revizorji imenovani na podlagi posebnih pogojev iz zakona. ([106]) Poročila o revizijah lahko vključujejo priporočila ali zahteve za nadomestila ali popravke ter graje in priporočila ali zahteve za disciplinske ukrepe. ([107]) V 60 dneh po zaključku revizije se priglasijo vodji javnega organa, ki je predmet revizije, ter odboru za revizijo in inšpekcijski pregled (glej oddelek 2.3.2). ([108]) Zadevni organ mora izvesti potrebne ukrepe ter o rezultatih poročati odboru za revizijo in inšpekcijski pregled. ([109]) Rezultati revizije so poleg tega običajno dajo na voljo javnosti. ([110]) Za zavrnitev ali oviranje notranje revizije se izrečejo upravne globe. ([111]) Za upoštevanje navedene zakonodaje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj nacionalna policija upravlja sistem generalnega inšpektorata za obravnavanje notranjih revizij, tudi glede morebitnih kršitev človekovih pravic. ([112])

2.3.2. *Odbor za revizijo in inšpekcijski pregled*

Odbor za revizijo in inšpekcijski pregled lahko pregleduje dejavnosti javnih organov in na podlagi teh pregledov izda priporočila, zahteva disciplinske ukrepe ali vloži ovadbo. ([113]) Ustanovil ga je predsednik Republike Koreje, glede svojih nalog pa je neodvisen. ([114]) Poleg tega je treba v skladu z zakonom o ustanovitvi odbora za revizijo in inšpekcijski pregled temu odboru zagotoviti čim večjo neodvisnost pri imenovanju, razrešitvi in organizacijski strukturi osebja ter pripravi proračuna. ([115]) Predsednika odbora za revizijo in inšpekcijski pregled na podlagi soglasja parlamenta imenuje predsednik republike. ([116]) Ta na predlog predsednika odbora imenuje tudi šest preostalih članov, in sicer za obdobje štirih let. ([117]) Člani odbora (vključno s predsednikom) morajo izpolnjevati posebne pogoje, določene z zakonom ([118]), razrešiti pa jih je mogoče le v primeru ustavne obtožbe, obsodbe na kazen zapora ali nezmožnosti za opravljanje nalog zaradi dolgotrajne duševne ali fizične nezmožnosti. ([119]) Člani odbora se prav tako ne smejo politično udejstvovati in hkrati zasedati funkcij v parlamentu, upravnih agencijah, organizacijah, v katerih odbor za revizijo in inšpekcijski pregled izvaja ti dejavnosti, ali na katerem koli drugem plačanem delovnem mestu ali položaju. ([120])

Odbor za revizijo in inšpekcijski pregled vsako leto izvede splošno revizijo, lahko pa izvaja tudi posebne revizije v zvezi z zadevami posebnega interesa. Med izvajanjem inšpekcijskega pregleda lahko zahteva predložitev dokumentov in navzočnost posameznikov. ([121]) V okviru revizije prouči prihodke in odhodke države, pa tudi nadzoruje splošno

([103]) Člena 3 in 5 zakona o revizijah v javnem sektorju.
([104]) Člen 7 zakona o revizijah v javnem sektorju.
([105]) Členi 8 do 11 zakona o revizijah v javnem sektorju.
([106]) Člen 16 in naslednji zakona o revizijah v javnem sektorju.
([107]) Člen 23(2) zakona o revizijah v javnem sektorju.
([108]) Člen 23(1) zakona o revizijah v javnem sektorju.
([109]) Člen 23(3) zakona o revizijah v javnem sektorju.
([110]) Člen 26 zakona o revizijah v javnem sektorju.
([111]) Člen 41 zakona o revizijah v javnem sektorju.
([112]) Glej zlasti oddelke v okviru generalnega direktorata za revizijo in inšpekcijski pregled: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Členi 24 in 31 do 35 zakona o odboru za revizijo in inšpekcijski pregled.
([114]) Člen 2(1) zakona o odboru za revizijo in inšpekcijski pregled.
([115]) Člen 2(2) zakona o odboru za revizijo in inšpekcijski pregled.
([116]) Člen 4(1) zakona o odboru za revizijo in inšpekcijski pregled.
([117]) Člen 5(1) in člen 6 zakona o odboru za revizijo in inšpekcijski pregled.
([118]) Da so na primer najmanj deset let opravljali funkcijo sodnika, državnega tožilca ali odvetnika, da so bili najmanj osem let zaposleni kot javni uslužbenci ali profesorji ali na višjem položaju na univerzi oziroma da so bili najmanj deset let (od tega najmanj pet let kot direktorji) zaposleni v družbi, ki kotira na borzi, ali ustanovi, v katero vlaga država, glej člen 7 zakona o odboru za revizijo in inšpekcijski pregled.
([119]) Člen 8 zakona o odboru za revizijo in inšpekcijski pregled.
([120]) Člen 9 zakona o odboru za revizijo in inšpekcijski pregled.
([121]) Glej na primer člen 27 zakona o odboru za revizijo in inšpekcijski pregled.

skladnost z nalogami javnih organov in javnih uslužbencev, da bi se izboljšalo delovanje javne uprave. ([122]) Njegov nadzor torej presega proračunske vidike in vključuje tudi preverjanje zakonitosti.

2.3.3. *Parlament*

Parlament lahko preiskuje in pregleduje delovanje javnih organov. ([123]) Med preiskavo ali pregledom lahko zahteva razkritje dokumentov in navzočnost prič. ([124]) Zoper vsakogar, ki med preiskavo parlamenta stori kaznivo dejanje krive izpovedbe, se lahko izrečejo kazenske sankcije (kazen zapora do deset let). ([125]) Postopek in rezultati pregledov se lahko javno objavijo. ([126]) Če parlament odkrije nezakonito ali neprimerno dejavnost, lahko od zadevnega javnega organa zahteva sprejetje popravnih ukrepov, vključno z dodelitvijo odškodnine, sprejetjem disciplinskega ukrepa in izboljšanjem notranjih postopkov. ([127]) Po taki zahtevi mora organ takoj ukrepati in o rezultatu poročati parlamentu. ([128])

2.3.4. *Komisija za varstvo osebnih podatkov*

Komisija za varstvo osebnih podatkov izvaja nadzor nad tem, ali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj obdelujejo osebne podatke v skladu z zakonom o varstvu osebnih podatkov. Poleg tega nadzor, ki ga izvaja ta komisija, v skladu s členom 7-8(3) in (4) ter členom 7-9(5) zakona o varstvu osebnih podatkov zajema tudi morebitne kršitve pravil, ki določajo omejitve in zaščitne ukrepe v zvezi z zbiranjem osebnih podatkov, vključno z omejitvami in ukrepi iz posebnih predpisov, ki urejajo zbiranje (elektronskih) dokazov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (glej oddelek 2.2). Vsaka taka kršitev glede na zahteve iz člena 3(1) zakona o varstvu osebnih podatkov, ki se uporabljajo za zakonito in pošteno zbiranje osebnih podatkov, pomeni tudi kršitev tega zakona, kar komisiji za varstvo osebnih podatkov omogoča, da izvede preiskavo in sprejme popravne ukrepe. ([129])

Komisija za varstvo osebnih podatkov ima v okviru izvajanja svoje nadzorne funkcije dostop do vseh ustreznih informacij. ([130]) Lahko svetuje organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, da izboljšajo raven varstva osebnih podatkov pri dejavnostih obdelave, naloži popravne ukrepe (npr. prenehanje obdelave podatkov ali sprejetje potrebnih ukrepov za varstvo osebnih podatkov) ali organu svetuje sprejetje disciplinskega ukrepa. ([131]) Nazadnje, za določene kršitve zakona o varstvu osebnih podatkov, kot so nezakonita uporaba ali razkritje osebnih podatkov tretjim osebam ali nezakonita obdelava občutljivih informacij, so predvidene kazenske sankcije. ([132]) Komisija za varstvo osebnih podatkov lahko v zvezi s tem zadevo predloži pristojnemu preiskovalnemu organu (vključno s tožilcem). ([133])

2.3.5. *Nacionalna komisija za človekove pravice*

Nacionalna komisija za človekove pravice, ki je neodvisen organ, katerega naloga je varovati in spodbujati temeljne pravice ([134]), ima pooblastila za preiskavo in odpravo kršitev členov 10 do 22 ustave, ki vključujejo pravici do zasebnosti in komunikacijske zasebnosti. Sestavlja jo 11 članov komisije, imenovanih na predlog parlamenta (štirje), predsednika republike (štirje) in predsednika vrhovnega sodišča (trije). ([135]) Za člana komisije je lahko imenovana oseba, ki (1) je bila najmanj deset let zaposlena na univerzi ali pooblaščenem raziskovalnem inštitutu, in sicer najmanj na položaju izrednega profesorja, (2) je najmanj deset let opravljala funkcijo sodnika, državnega tožilca ali odvetnika, (3) se je najmanj deset let ukvarjala z dejavnostmi na področju človekovih pravic (npr. za neprofitno, nevladno organizacijo ali mednarodno organizacijo) ali (4) so jo priporočile skupine civilne družbe. ([136]) Predsednika komisije izmed članov

([122]) Člena 20 in 24 zakona o odboru za revizijo in inšpekcijski pregled.
([123]) Člen 128 zakona o parlamentu ter členi 2, 3 in 15 zakona o pregledih in preiskavah v državni upravi. To vključuje letne preglede vladnih zadev kot celote in preiskave posameznih zadev.
([124]) Člen 10(1) zakona o pregledih in preiskavah v državni upravi. Glej tudi člena 128 in 129 zakona o parlamentu.
([125]) Člen 14 zakona o zaslišanju, oceni itd. pred parlamentom.
([126]) Člen 12-2 zakona o pregledih in preiskavah v državni upravi.
([127]) Člen 16(2) zakona o pregledih in preiskavah v državni upravi.
([128]) Člen 16(3) zakona o pregledih in preiskavah v državni upravi.
([129]) Glej uradno obvestilo komisije za varstvo osebnih podatkov št. 2021-1 o dodatnih pravilih za razlago in uporabo zakona o varstvu osebnih podatkov.
([130]) Člen 63 zakona o varstvu osebnih podatkov.
([131]) Člen 61(2), člen 65(1) in (2) ter člen 64(4) zakona o varstvu osebnih podatkov.
([132]) Členi 70 do 74 zakona o varstvu osebnih podatkov.
([133]) Člen 65(1) zakona o varstvu osebnih podatkov.
([134]) Člen 1 zakona o nacionalni komisiji za človekove pravice.
([135]) Člen 5(1) in (2) zakona o nacionalni komisiji za človekove pravice.
([136]) Člen 5(3) zakona o nacionalni komisiji za človekove pravice.

komisije imenuje predsednik republike, potrditi pa ga mora parlament. ([137]) Člani komisije (vključno s predsednikom) so imenovani za triletni mandat z možnostjo podaljšanja, razrešiti pa jih je mogoče le, če so obsojeni na kazen zapora ali ne zmorejo več opravljati svojih nalog zaradi dolgotrajne duševne ali telesne nezmožnosti (v tem primeru se morata z razrešitvijo strinjati dve tretjini članov komisije). ([138]) Člani nacionalne komisije za človekove pravice ne smejo hkrati zasedati funkcij v parlamentu, lokalnih svetih ali katerem koli državnem ali lokalnem upravnem organu (kot javni uslužbenci). ([139])

Nacionalna komisija za človekove pravice lahko preiskavo začne na lastno pobudo ali na zahtevo posameznika. V okviru preiskave lahko zahteva predložitev ustreznega dokaznega gradiva, opravi preglede in zasliši posameznike kot priče. ([140]) Po preiskavi lahko izda priporočila za izboljšanje ali popravek posameznih politik in praks, ki jih lahko tudi javno objavi. ([141]) Javni organi morajo nacionalni komisiji za človekove pravice priglasiti načrt izvedbe teh priporočil v 90 dneh po njihovem prejemu. ([142]) Poleg tega mora zadevni organ v primeru neizvajanja priporočil o tem obvestiti komisijo. ([143]) Ta pa lahko to neizvajanje nato razkrije parlamentu in/ali ga javno objavi. Javni organi običajno upoštevajo priporočila nacionalne komisije za človekove pravice, k čemur jih močno spodbuja dejstvo, da se njihovo izvajanje ocenjuje v okviru splošnega vrednotenja, ki ga izvaja urad za usklajevanje vladnih politik pod vodstvom urada predsednika vlade.

2.4. **Pravna sredstva posameznikov**

2.4.1. *Mehanizmi pravnih sredstev, ki so na voljo na podlagi zakona o varstvu osebnih podatkov*

Posamezniki lahko v zvezi z osebnimi podatki, ki jih obdelujejo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, uresničujejo svoje pravice do dostopa, popravka, izbrisa in prenehanja obdelave na podlagi zakona o varstvu osebnih podatkov. Dostop se lahko zahteva neposredno pri zadevnem organu ali posredno prek nacionalne komisije za človekove pravice ([144]). Pristojni organ lahko dostop omeji ali zavrne le, če tako določa zakon, če bi to verjetno povzročilo škodo za življenje ali telo tretje osebe ali če bi verjetno pomenilo neupravičen poseg v premoženjske in druge interese druge osebe (tj. kadar interesi druge osebe prevladajo nad interesi posameznika, ki zahteva dostop) ([145]). Če je dostop zavrnjen, je treba posameznika obvestiti o razlogih za zavrnitev in možnostih pritožbe. ([146]) Podobno se lahko zavrne zahteva za popravek ali izbris, če tako določajo drugi predpisi, tudi v tem primeru pa je treba posameznika obvestiti o razlogih za zavrnitev in možnosti pritožbe. ([147])

Kar zadeva pravna sredstva, lahko posamezniki vložijo pritožbo pri komisiji za varstvo osebnih podatkov, med drugim prek klicnega centra za vprašanja v zvezi z zasebnostjo, ki ga upravlja korejska agencija za splet in varnost. ([148]) Poleg tega je mediacija za posameznike mogoča v okviru odbora za mediacijo v primeru sporov v zvezi z osebnimi podatki. ([149]) Ta pravna sredstva so na voljo v primeru morebitnih kršitev pravil iz posebnih predpisov, ki določajo omejitve in zaščitne ukrepe v zvezi z zbiranjem osebnih podatkov (glej oddelek 2.2), in iz zakona o varstvu osebnih podatkov. Poleg tega lahko posamezniki izpodbijajo odločitve ali neukrepanje komisije za varstvo osebnih podatkov na podlagi zakona o upravnem sporu (glej oddelek 2.4.3).

([137]) Člen 5(5) zakona o nacionalni komisiji za človekove pravice.
([138]) Člen 7(1) in člen 8 zakona o nacionalni komisiji za človekove pravice.
([139]) Člen 10 zakona o nacionalni komisiji za človekove pravice.
([140]) Člen 36 zakona o nacionalni komisiji za človekove pravice. Predložitev dokaznega gradiva ali predmetov se lahko v skladu s členom 36(7) zakona zavrne, če bi to posegalo v državne skrivnosti, tako da bi lahko bistveno vplivalo na državno varnost ali diplomatske odnose, ali če bi to resno oviralo kazensko preiskavo ali sojenje, ki še poteka. V takih primerih lahko komisija od vodje zadevnega organa zahteva dodatne informacije (vodja pa mora to zahtevo v dobri veri izpolniti), če je to potrebno za preverjanje, ali je zavrnitev zagotovitve informacij upravičena.
([141]) Člen 25(1) zakona o nacionalni komisiji za človekove pravice.
([142]) Člen 25(3) zakona o nacionalni komisiji za človekove pravice.
([143]) Člen 25(4) zakona o nacionalni komisiji za človekove pravice.
([144]) Člen 35(2) zakona o varstvu osebnih podatkov.
([145]) Člen 35(4) zakona o varstvu osebnih podatkov.
([146]) Člen 42(2) uredbe o izvajanju zakona o varstvu osebnih podatkov.
([147]) Člen 36(1)-(2) zakona o varstvu osebnih podatkov in člen 43(3) uredbe o izvajanju zakona o varstvu osebnih podatkov.
([148]) Člen 62 zakona o varstvu osebnih podatkov.
([149]) Členi 40 do 50 zakona o varstvu osebnih podatkov in členi 48-2 do 57 uredbe o izvajanju zakona o varstvu osebnih podatkov.

2.4.2. *Pravna sredstva pred nacionalno komisijo za človekove pravice*

Nacionalna komisija za človekove pravice obravnava pritožbe posameznikov (korejskih in tujih državljanov) v zvezi s kršitvami človekovih pravic, ki jih storijo javni organi. ([150]) Da lahko posameznik vloži pritožbo pri nacionalni komisiji za človekove pravice, ni potrebno procesno upravičenje. ([151]) Zato bo ta komisija pritožbo obravnavala, čeprav zadevni posameznik v fazi dopustnosti dejansko ne more dokazati škode. Da bi bila pritožba pred to komisijo dopustna, posamezniku v okviru zbiranja osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj zato ne bi bilo treba dokazati, da so korejski javni organi dejansko dostopali do njegovih osebnih podatkov. Posameznik lahko tudi zahteva, da se pritožba reši z mediacijo. ([152])

Nacionalna komisija za človekove pravice lahko za proučitev pritožbe uporabi preiskovalna pooblastila, med drugim lahko zahteva predložitev ustreznega dokaznega gradiva, izvede preglede in zasliši posameznike kot priče. ([153]) Če preiskava razkrije, da so bili kršeni ustrezni zakoni, lahko nacionalna komisija za človekove pravice predlaga izvedbo popravnih ukrepov oziroma popravek ali izboljšavo zadevnega predpisa, ureditve, politike ali prakse. ([154]) Predlagani popravni ukrepi lahko vključujejo mediacijo, prenehanje kršitve človekovih pravic, odškodnino za škodo in ukrepe za preprečitev ponovitve enake ali podobne kršitve. ([155]) V primeru nezakonitega zbiranja osebnih podatkov na podlagi pravil, ki se uporabljajo, lahko popravni ukrepi vključujejo izbris zbranih osebnih podatkov. Če je zelo verjetno, da kršitev še traja, in je verjetno, da bi ob neukrepanju zaradi nje nastala škoda, ki bi jo bilo težko popraviti, lahko nacionalna komisija za človekove pravice sprejme nujne ukrepe pomoči. ([156])

Čeprav nacionalna komisija za človekove pravice nima pristojnosti, da kar koli zahteva, se lahko njeni sklepi (npr. sklep o prenehanju nadaljnje obravnave pritožbe) ([157]) in priporočila izpodbijajo pred korejskimi sodišči na podlagi zakona o upravnem sporu (glej oddelek 2.4.3 v nadaljevanju). ([158]) Če poleg tega ugotovitve te komisije razkrijejo, da je javni organ nezakonito zbiral javne podatke, bi lahko posameznik pred korejskimi sodišči zoper ta javni organ uveljavljal dodatna pravna sredstva, na primer z izpodbijanjem zbiranja na podlagi zakona o upravnem sporu, vložitvijo ustavne pritožbe na podlagi zakona o ustavnem sodišču ali vložitvijo odškodninskega zahtevka za škodo na podlagi zakona o državni odškodnini (glej oddelek 2.4.3 v nadaljevanju).

2.4.3. *Sodno varstvo*

Posamezniki se lahko sklicujejo na omejitve in zaščitne ukrepe, opisane v prejšnjih oddelkih, ter tako z različnimi pravnimi sredstvi uveljavljajo sodno varstvo pred korejskimi sodišči.

Prvič, zadevni posameznik in njegov zagovornik sta lahko v skladu zakonom o kazenskem postopku prisotna pri izvrševanju odredbe o preiskavi ali zasegu in lahko takrat temu tudi ugovarjata. ([159]) Poleg tega je v zakonu o kazenskem postopku določen mehanizem t. i. kvazipritožbe, ki posameznikom omogoča, da pri pristojnem sodišču vložijo vlogo za razveljavitev ali spremembo odločitve tožilca ali policista o zasegu. ([160]) To posameznikom omogoča, da izpodbijajo ukrepe, sprejete za izvršitev odredbe o zasegu.

([150]) Čeprav se člen 4 zakona o nacionalni komisiji za človekove pravice sklicuje na državljane in tujce, ki prebivajo v Republiki Koreji, se izraz „prebivajo“ nanaša na pristojnost in ne na ozemlje. Če torej nacionalne institucije v Koreji kršijo temeljne pravice tujca zunaj Koreje, lahko ta posameznik vloži pritožbo pri nacionalni komisiji za človekove pravice. Glej na primer ustrezno vprašanje na strani s pogosto zastavljenimi vprašanji nacionalne komisije za človekove pravice, ki je na voljo na povezavi https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. To bi veljalo, če bi korejski javni organi nezakonito dostopali do osebnih podatkov tujca, prenesenih v Korejo.

([151]) Pritožbo je načeloma treba vložiti v enem letu po kršitvi, vendar se lahko nacionalna komisija za človekove pravice kljub temu odloči za proučitev pritožbe, vložene po tem roku, če zastaralni rok na podlagi kazenskega ali civilnega prava še ni potekel (člen 32(1), točka 4, zakona o nacionalni komisiji za človekove pravice).

([152]) Člen 42 in naslednji zakona o nacionalni komisiji za človekove pravice.

([153]) Člena 36 in 37 zakona o nacionalni komisiji za človekove pravice.

([154]) Člen 44 zakona o nacionalni komisiji za človekove pravice.

([155]) Člen 42(4) zakona o nacionalni komisiji za človekove pravice.

([156]) Člen 48 zakona o nacionalni komisiji za človekove pravice.

([157]) Če nacionalna komisija za človekove pravice na primer izjemoma ne more pregledati določenega dokaznega gradiva ali objektov, ker zadevajo državne skrivnosti, ki bi lahko bistveno vplivale na državno varnost ali diplomatske odnose, oziroma če bi pregled resno oviral kazensko preiskavo ali sojenje, ki še poteka (glej opombo 163), in kadar navedena komisija zato ne more izvesti preiskave, potrebne za oceno utemeljenosti prejetega zahtevka, posameznika obvesti o razlogih za zavrnitev pritožbe, in sicer v skladu s členom 39 zakona o nacionalni komisiji za človekove pravice. Posameznik lahko v takem primeru izpodbija odločitev navedene komisije na podlagi zakona o upravnem sporu.

([158]) Glej npr. odločbo višjega sodišča v Seulu št. 2007Nu27259 z dne 18. aprila 2008, potrjeno z odločbo vrhovnega sodišča št. 2008Du7854 z dne 9. oktobra 2008; odločbo višjega sodišča v Seulu št. 2017Nu69382 z dne 2. februarja 2018.

([159]) Člena 121 in 219 zakona o kazenskem postopku.

([160]) Člen 417 zakona o kazenskem postopku v povezavi s členom 414(2) zakona o kazenskem postopku. Glej tudi odločbo vrhovnega sodišča št. 97Mo66 z dne 29. septembra 1997.

Poleg tega lahko posamezniki pred korejskimi sodišči pridobijo odškodnino za škodo. Posamezniki lahko na podlagi zakona o državni odškodnini zahtevajo odškodnino za škodo, ki jo javni uslužbenci povzročijo pri opravljanju svojih uradnih dolžnosti v nasprotju z zakonom. ([161]) Zahtevek na podlagi zakona o državni odškodnini se lahko vloži pri specializiranem „odškodninskem odboru“ ali neposredno pri korejskih sodiščih. ([162]) Če je žrtev tuji državljan, se zakon o državni odškodnini uporablja, če država izvora take osebe prav tako zagotavlja državno odškodnino korejskim državljanom. ([163]) Ta pogoj je v skladu s sodno prakso izpolnjen, če za vložitev odškodninskih zahtevkov v drugi državi „ne veljajo znatno drugačni pogoji v prid Koreje ali druge države“ in „na splošno niso strožji od tistih, ki jih določa Koreja, tj. nimajo bistvenih in vsebinskih razlik“ ([164]). Odgovornost države za odškodnino ureja civilni zakon, zato odgovornost države vključuje tudi nematerialno škodo (npr. duševne bolečine). ([165])

Za kršitve pravil o varstvu podatkov je na podlagi zakona o varstvu osebnih podatkov zagotovljeno dodatno pravno sredstvo. Vsakomur, ki mu je bila zaradi kršitve zakona o varstvu osebnih podatkov ali zaradi izgube, kraje, razkritja, ponarejanja, spreminjanja ali poškodovanja njegovih osebnih podatkov povzročena škoda, se lahko v skladu s členom 39 zakona o varstvu osebnih podatkov na sodišču dodeli odškodnina za škodo. Pri tem ne velja podobna zahteva glede vzajemnosti kot na podlagi zakona o državni odškodnini.

Poleg odškodnine za škodo je mogoče pridobiti upravno varstvo zoper dejanja ali opustitve upravnih organov na podlagi zakona o upravnem sporu. Vsakdo lahko izpodbija odločitev (npr. izvršitev ali zavrnitev izvršitve javnih pooblastil v konkretnem primeru) ali opustitev (javni organ v nasprotju z zakonsko obveznostjo dolgo ne sprejme določene odločitve), kar lahko povzroči razveljavitev/spremembo nezakonite odločitve, ugotovitev ničnosti (tj. ugotovitev, da odločitev ni pravno veljavna ali da ne obstaja v pravnem redu) ali ugotovitev, da je opustitev nezakonita. ([166]) Upravno odločitev je mogoče izpodbijati le, če neposredno vpliva na državljanske pravice in dolžnosti. ([167]) To vključuje ukrepe za zbiranje osebnih podatkov, bodisi neposredno (npr. s prestrezanjem komunikacij) bodisi z zahtevo po razkritju (npr. ponudniku storitev).

Navedeni zahtevki se lahko najprej vložijo pri komisijah za upravne pritožbe, ustanovljenih v okviru določenih javnih organov (npr. nacionalne obveščevalne službe, nacionalne komisije za človekove pravice), ali pri centralni komisiji za upravne pritožbe, ustanovljeni v okviru komisije za preprečevanje korupcije in državljanske pravice. ([168]) Taka upravna pritožba zagotavlja alternativno, bolj neformalno sredstvo za izpodbijanje odločitve ali opustitve javnega organa. Na podlagi zakona o upravnem sporu pa se lahko vloži tudi tožba neposredno pri korejskih sodiščih.

Vlogo za razveljavitev/spremembo odločitve na podlagi zakona o upravnem sporu lahko vloži vsaka oseba, ki ima pravni interes, da zahteva razveljavitev/spremembo ali da se ji z razveljavitvijo/spremembo povrnejo pravice, če odločitev ne učinkuje več. ([169]) Podobno lahko pravdni postopek za potrditev ničnosti začne oseba, ki ima pravni interes za tako potrditev, pravdni postopek za potrditev nezakonitosti ali opustitve pa vsaka oseba, ki je vložila vlogo za odločitev in ima pravni interes, da zahteva potrditev nezakonitosti opustitve. ([170]) „Pravni interes“ se v skladu s sodno prakso vrhovnega sodišča razlaga kot „pravno zaščiten interes“, tj. neposreden in poseben interes, zaščiten z zakoni in drugimi predpisi, na katerih temeljijo upravne odločitve (kar pomeni, da ne gre za splošne, posredne in abstraktne interese javnosti). ([171]) Posamezniki imajo zato pravni interes v primeru kršitev omejitev in zaščitnih ukrepov, povezanih z zbiranjem njihovih osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (na podlagi posebnih predpisov ali zakona o varstvu osebnih podatkov). Pravnomočna sodba na podlagi zakona o upravnem sporu je za stranke v postopku zavezujoča. ([172])

Vlogo za razveljavitev/spremembo odločitve in vlogo za potrditev nezakonitosti opustitve je treba vložiti v 90 dneh od datuma, ko je posameznik seznanjen z odločitvijo/opustitvijo, in načeloma najpozneje eno leto po datumu, ko je bila

([161]) Člen 2(1) zakona o državni odškodnini.

([162]) Člena 9 in 12 zakona o državni odškodnini. Z zakonom so ustanovljeni okrožni odbori (ki jim predseduje namestnik tožilca pristojnega tožilstva), osrednji odbor (ki mu predseduje namestnik ministra za pravosodje) in posebni odbor (ki mu predseduje namestnik ministra za narodno obrambo, obravnava pa odškodninske zahtevke za škodo, ki jo povzroči vojaško osebje ali civilisti, zaposleni v vojski). Odškodninske zahtevke načeloma obravnavajo okrožni odbori, ki morajo v nekaterih okoliščinah take zadeve predati osrednjemu/posebnemu odboru, na primer če odškodnina presega določen znesek ali če posameznik zahteva ponovno odločanje. Člane vseh odborov imenuje minister za pravosodje (npr. izmed javnih uslužbencev ministrstva za pravosodje, pravosodnih uradnikov, odvetnikov in oseb, ki imajo strokovno znanje s področja državnih odškodnin), zanje pa veljajo posebna pravila glede navzkrižja interesov (glej člen 7 uredbe o izvajanju zakona o državni odškodnini).

([163]) Člen 7 zakona o državni odškodnini.

([164]) Odločba vrhovnega sodišča št. 2013Da208388 z dne 11. junija 2015.

([165]) Glej člen 8 zakona o državni odškodnini in člen 751 civilnega zakona.

([166]) Člena 2 in 4 zakona o upravnem sporu.

([167]) Odločba vrhovnega sodišča št. 98Du18435 z dne 22. oktobra 1999, odločba vrhovnega sodišča št. 99Du1113 z dne 8. septembra 2000 in odločba vrhovnega sodišča št. 2010Du3541 z dne 27. septembra 2012.

([168]) Člen 6 zakona o upravni pritožbi in člen 18(1) zakona o upravnem sporu.

([169]) Člen 12 zakona o upravnem sporu.

([170]) Člena 35 in 36 zakona o upravnem sporu.

([171]) Odločba vrhovnega sodišča št. 2006Du330 z dne 26. marca 2006.

([172]) Člen 30(1) zakona o upravnem sporu.

odločitev sprejeta/je prišlo do opustitve, razen v primeru upravičenih razlogov. ([173]) Pojem „upravičeni razlogi“ je treba v skladu s sodno prakso vrhovnega sodišča razlagati široko, tako da je treba presoditi, ali je glede na vse okoliščine zadeve družbeno sprejemljivo dopustiti pritožbo, vloženo po roku. ([174]) To na primer (med drugim) vključuje razloge za zamudo, za katere zadevna stranka ne more biti odgovorna (tj. okoliščine, na katere pritožnik ne more vplivati, ker na primer ni bil uradno obveščen o zbiranju svojih osebnih podatkov), ali višjo silo (npr. naravno nesrečo, vojno).

Nazadnje, posamezniki lahko vložijo tudi ustavo pritožbo pri ustavnem sodišču. ([175]) Vse osebe, katerih temeljne pravice, ki jih zagotavlja ustava, so kršene zaradi izvrševanja ali neizvrševanja pristojnosti državnih organov (razen sodnih odločb), lahko na podlagi zakona o ustavnem sodišču zahtevajo odločanje o ustavni pritožbi. Najprej je treba izčrpati druga pravna sredstva, če so na voljo. Tuji državljani lahko v skladu s sodno prakso ustavnega sodišča vložijo ustavno pritožbo, če so njihove osnovne pravice priznane na podlagi korejske ustave (glej pojasnila v oddelku 1.1). ([176]) Ustavne pritožbe je treba vložiti v 90 dneh po tem, ko se je posameznik seznanil s kršitvijo, in v enem letu od nastanka kršitve. Glede na to, da se za pravdne postopke na podlagi zakona o ustavnem sodišču uporablja postopek iz zakona o upravnem sporu ([177]), bo pritožba v primeru „upravičenih razlogov“, kot se razlagajo v skladu z zgoraj opisano sodno prakso vrhovnega sodišča, še vedno dopustna.

Če je treba najprej izčrpati druga pravna sredstva, je treba ustavno pritožbo vložiti v 30 dneh po dokončni odločitvi o takem pravnem sredstvu. ([178]) Ustavno sodišče lahko izvrševanje pristojnosti državnih organov, ki je povzročilo kršitev, razglasi za nično ali potrdi, da določena opustitev ukrepanja ni ustavna. ([179]) V takem primeru mora zadevni organ sprejeti ukrepe za izpolnitev odločbe sodišča.

3. VLADNI DOSTOP ZA NAMENE NACIONALNE VARNOSTI

3.1. Pristojni javni organi na področju nacionalne varnosti

Republika Koreja ima dve posebni obveščevalni agenciji: nacionalno obveščevalno službo in poveljstvo za varnostno podporo obrambnih sil. Poleg njiju pa lahko osebne podatke za namene nacionalne varnosti zbirata tudi policija in tožilstvo.

Nacionalna obveščevalna služba je bila ustanovljena z zakonom o nacionalni obveščevalni službi, deluje pa neposredno pod pristojnostjo in nadzorom predsednika republike. ([180]) Ta služba zlasti zbira, združuje in razširja informacije o tujih državah (in Severni Koreji) ([181]), obveščevalne podatke, povezane z nalogo preprečevanja vohunjenja (vključno z vojaškim in gospodarskim vohunjenjem), terorizma in dejavnosti mednarodnih kriminalnih združb, obveščevalne podatke o določenih vrstah kaznivih dejanj, usmerjenih proti javnosti in nacionalni varnosti (npr. nacionalna vstaja, vojaški napad tujih sil), ter obveščevalne podatke, povezane z nalogo zagotavljanja kibernetske varnosti in preprečevanja kibernetskih napadov in groženj ali boja proti njim. ([182]) Zakon o nacionalni obveščevalni službi, ki določa ustanovitev te službe in opredeljuje njene naloge, določa tudi splošna načela, ki urejajo vse njene dejavnosti. Nacionalna obveščevalna služba mora na splošno ohranjati politično nevtralnost ter varovati svoboščine in pravice posameznikov. ([183]) Njen direktor mora oblikovati splošne smernice, ki določajo načela, področje uporabe in postopke za izpolnjevanje njenih nalog v zvezi z zbiranjem in uporabo informacij, ter mora o njih poročati parlamentu. ([184]) Ta pa lahko (prek svojega obveščevalnega odbora) zahteva, da se smernice popravijo ali dopolnijo, če meni, da so nezakonite ali nepravične. Splošneje velja, da direktor in uslužbenci nacionalne obveščevalne službe ne smejo zlorabljati svojih pooblastil tako, da bi kateri koli organ, organizacijo ali posameznika prisilili v nekaj, česar po zakonu ni dolžan storiti, ali posameznika ovirali pri uresničevanju pravic. ([185]) Poleg tega mora nacionalna obveščevalna služba pri kakršni koli cenzuri pošte,

([173]) Člen 20 zakona o upravnem sporu. Ta rok velja tudi za vloge za potrditev nezakonitosti opustitve, glej člen 38(2) zakona o upravnem sporu.
([174]) Odločba vrhovnega sodišča št. 90Nu6521 z dne 28. junija 1991.
([175]) Člen 68(1) zakona o ustavnem sodišču.
([176]) Odločba ustavnega sodišča št. 99HeonMa194 z dne 29. novembra 2001.
([177]) Člen 40 zakona o ustavnem sodišču.
([178]) Člen 69 zakona o ustavnem sodišču.
([179]) Člen 75(3) zakona o ustavnem sodišču.
([180]) Člen 2 in člen 4(2) zakona o nacionalni obveščevalni službi.
([181]) Ta pojem ne zajema informacij o posameznikih, temveč informacije o splošnih informacijah o tujih državah (trendi, razvoj dogodkov) ter o dejavnostih državnih akterjev iz tretjih držav.
([182]) Člen 3(1) zakona o nacionalni obveščevalni službi.
([183]) Člen 3(1) in člen 6(2) ter člena 11 in 21. Glej tudi pravila o navzkrižju interesov, zlasti člena 10 in 12.
([184]) Člen 4(2) zakona o nacionalni obveščevalni službi.
([185]) Člen 13 zakona o nacionalni obveščevalni službi.

prestrezanju telekomunikacij, zbiranju podatkov o lokaciji ali podrobnih podatkov o opravljeni komunikaciji ali snemanju zasebnih pogovorov ali prisluškovanju tem pogovorom upoštevati zakon o varstvu zasebnosti komunikacij, zakon o podatkih o lokaciji ali zakon o kazenskem postopku. ([186]) Za vsako zlorabo pooblastil ali zbiranje informacij v nasprotju s temi zakoni se izrečejo kazenske sankcije. ([187])

Poveljstvo za varnostno podporo obrambnih sil je vojaška obveščevalna agencija, ustanovljena v okviru ministrstva za obrambo. Pristojno je za varnostne zadeve v vojski, vojaške kazenske preiskave (za katere se uporablja zakon o vojaškem sodišču) in vojaške obveščevalne podatke. Na splošno ne izvaja nadzora nad civilisti, razen če je to nujno za opravljanje njegovih vojaških nalog. Osebe, ki jih je mogoče preiskovati, so vojaško osebje, civilisti, zaposleni v vojski, osebe na vojaškem usposabljanju, osebe v vojaški službi v rezervni sestavi ali v službi za novačenje in vojni ujetniki. ([188]) Poveljstvo za varnostno podporo obrambnih sil mora pri zbiranju podatkov o komunikaciji za namene nacionalne varnosti upoštevati omejitve in zaščitne ukrepe iz zakona o varstvu zasebnosti komunikacij in uredbe o izvajanju tega zakona.

3.2. **Pravna podlaga in omejitve**

Zakon o varstvu zasebnosti komunikacij, zakon o boju proti terorizmu za zaščito državljanov in javne varnosti ter zakon o zagotavljanju telekomunikacijskih storitev zagotavljajo pravno podlago za zbiranje osebnih podatkov za namene nacionalne varnosti ter določajo veljavne omejitve in zaščitne ukrepe ([189]). S temi omejitvami in zaščitnimi ukrepi, kot so opisani v naslednjih oddelkih, se zagotavlja, da sta zbiranje in obdelava podatkov omejena na to, kar je nujno potrebno za dosego zakonitega cilja. To izključuje kakršno koli množično in neselektivno zbiranje osebnih podatkov za namene nacionalne varnosti.

3.2.1. *Zbiranje podatkov o komunikaciji*

3.2.1.1. Zbiranje podatkov o komunikaciji s strani obveščevalnih agencij

3.2.1.1.1. Pravna podlaga

Zakon o varstvu zasebnosti komunikacij obveščevalne agencije pooblašča za zbiranje podatkov o komunikaciji, od ponudnikov komunikacijskih storitev pa zahteva, da ugodijo zahtevam teh agencij. ([190]) Kot je opisano v oddelku 2.2.2.1, se v tem zakonu razlikuje med zbiranjem vsebine komunikacij (tj. „ukrepi za omejevanje komunikacij“, kot so ukrepi „prisluškovanja“ ali „cenzure“ ([191])) in zbiranjem „podrobnih podatkov o opravljeni komunikaciji“. ([192])

Prag za zbiranje teh dveh vrst informacij se razlikuje, postopki, ki se uporabljajo, in zaščitni ukrepi pa so v veliki meri enaki. ([193]) Podrobni podatki o opravljeni komunikaciji (ali metapodatki) se lahko zbirajo za namen preprečevanja groženj mednarodni varnosti. ([194]) Za izvajanje ukrepov za omejevanje komunikacij (tj. zbiranje vsebine komunikacij) se uporablja višji prag, saj se ti ukrepi lahko sprejmejo le, če naj bi bila resno ogrožena nacionalna varnost in je zbiranje obveščevalnih podatkov nujno, da se prepreči taka ogroženost (tj. če obstaja resno tveganje za nacionalno varnost in je zbiranje nujno, da se to tveganje prepreči). ([195]) Poleg tega se lahko dostop do vsebine komunikacij izvaja le kot skrajni ukrep za zagotovitev nacionalne varnosti, pri čemer si je treba prizadevati za čim manjšo kršitev zasebnosti komunikacij. ([196]) Tudi če je pridobljeno ustrezno soglasje/dovoljenje, se morajo taki ukrepi, takoj prenehati izvajati, ko niso več potrebni, da se čim manj posega v zaupnost komunikacij posameznika. ([197])

3.2.1.1.2. Omejitve in zaščitni ukrepi za zbiranje podatkov o komunikaciji, ki vključuje vsaj enega korejskega državljana

Zbiranje podatkov o komunikaciji (vsebine in metapodatkov), kadar je najmanj en udeleženec komunikacije korejski

([186]) Člen 14 zakona o nacionalni obveščevalni službi.
([187]) Člena 22 in 23 zakona o nacionalni obveščevalni službi.
([188]) Člen 1 zakona o vojaškem sodišču.
([189]) Policija in nacionalna obveščevalna služba pri preiskovanju kaznivih dejanj, povezanih z nacionalno varnostjo, delujeta na podlagi zakona o kazenskem postopku, poveljstvo za varnostno podporo obrambnih sil pa mora upoštevati zakon o vojaškem sodišču.
([190]) Člen 15-2 zakona o varstvu zasebnosti komunikacij.
([191]) Člen 2(6) in (7) zakona o varstvu zasebnosti komunikacij.
([192]) Člen 2(11) zakona o varstvu zasebnosti komunikacij.
([193]) Glej tudi člen 13-4(2) zakona o varstvu zasebnosti komunikacij in člen 37(4) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij, ki določata, da se postopki, ki se uporabljajo za zbiranje vsebine komunikacij, smiselno uporabljajo tudi za zbiranje podrobnih podatkov o opravljeni komunikaciji.
([194]) Člen 13-4 zakona o varstvu zasebnosti komunikacij.
([195]) Člen 7(1) zakona o varstvu zasebnosti komunikacij.
([196]) Člen 3(2) zakona o varstvu zasebnosti komunikacij.
([197]) Člen 2 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.

državljan, lahko poteka le z dovoljenjem višjega predsednika višjega sodišča. ([198]) Obveščevalna agencija mora pisno zahtevo vložiti pri tožilcu ali višjem tožilstvu. ([199]) Navesti mora razloge za zbiranje (tj. da naj bi bila nacionalna varnost resno ogrožena ali da je zbiranje potrebno, da se preprečijo grožnje za nacionalno varnost) in priložiti dokazno gradivo, ki podpira te razloge in na prvi pogled izkazuje utemeljenost, ter podrobnosti o zahtevi (tj. nameni, ciljni posamezniki, obseg, dejansko obdobje zbiranja ter način in kraj zbiranja). ([200]) Tožilec/višje tožilstvo pa nato zahteva dovoljenje višjega predsednika višjega sodišča. ([201]) Ta lahko pisno dovoljenje izda le, če meni, da je vloga utemeljena, v nasprotnem primeru zahtevo zavrne. ([202]) V odredbi so podrobno določeni vrsta, namen, cilj, obseg, dejansko obdobje zbiranja ter dovoljen kraj in način zbiranja. ([203])

Če je cilj ukrepa preiskava kaznivega dejanja zarote, ki ogroža nacionalno varnost, ukrepanje pa je tako nujno, da ni mogoče izvesti navedenih postopkov, se uporabljajo posebna pravila. ([204]) Če so izpolnjeni ti pogoji, lahko obveščevalne agencije nadzorne ukrepe izvedejo brez predhodnega soglasja sodišča. ([205]) Vendar mora obveščevalna agencija takoj po izvedbi nujnih ukrepov zaprositi za dovoljenje sodišča. Če se dovoljenje ne pridobi v 36 urah od sprejetja ukrepov, se morajo ukrepi takoj prenehati izvajati. ([206]) Zbiranje informacij v nujnih primerih mora vedno potekati v skladu z „izjavo o cenzuri/prisluškovanju v nujnem primeru“, obveščevalna agencija, ki izvaja zbiranje, pa mora voditi evidenco vseh nujnih ukrepov. ([207])

V primerih, ko se nadzor hitro zaključi, tako da dovoljenje sodišča ni več potrebno, mora vodja pristojnega višjega državnega tožilstva vodji pristojnega sodišča, ki vodi evidenco nujnih ukrepov, poslati obvestilo o nujnem ukrepu, ki ga pripravi obveščevalna agencija. ([208]) To sodišču omogoči, da prouči zakonitost zbiranja.

3.2.1.1.3. Omejitve in zaščitni ukrepi za zbiranje podatkov o komunikaciji, ki vključuje le posameznike, ki niso državljani Koreje

Da lahko obveščevalne agencije zbirajo podatke o komunikaciji izključno med posamezniki, ki niso državljani Koreje, morajo pridobiti predhodno pisno soglasje predsednika republike. ([209]) Take komunikacije se bodo zbirale le za namene nacionalne varnosti, če spadajo v eno od več navedenih kategorij, in sicer komunikacije med državnimi uradniki ali drugimi posamezniki iz držav, ki so sovražne do Republike Koreje, tujimi agencijami, skupinami ali državljani, osumljenimi vpletenosti v dejavnosti proti Koreji ([210]), ali člani skupin na Korejskem polotoku, ki dejansko ne spadajo pod suverenost Republike Koreje, in njihovimi krovnimi skupinami s sedežem v tujih državah. ([211]) Če pa je ena stranka komunikacije korejski državljan in druga posameznik, ki ni državljan Koreje, je v skladu s postopkom, opisanim v oddelku 3.2.1.1.2, potrebno soglasje sodišča.

Vodja obveščevalne agencije mora direktorju nacionalne obveščevalne službe predložiti načrt ukrepov, ki bi jih bilo treba sprejeti. ([212]) Ta preveri, ali je načrt ustrezen, in ga v primeru ustreznosti pošlje predsedniku republike v odobritev. ([213]) V načrt je treba vključiti enake informacije, kot se zahtevajo v vlogi za pridobitev dovoljenja sodišča za zbiranje informacij o korejskih državljanih (kot je opisano zgoraj). ([214]) Zlasti je treba navesti razloge za zbiranje (tj. da naj bi bila nacionalna varnost resno ogrožena ali da je zbiranje potrebno, da se preprečijo grožnje za nacionalno varnost) in

([198]) Člen 7(1)1 zakona o varstvu zasebnosti komunikacij. Pristojno sodišče je višje sodišče, ki je pristojno v kraju stalnega prebivališča ali sedeža ene ali obeh strank, ki sta predmet nadzora.
([199]) Člen 7(3) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([200]) Člen 7(3) in člen 6(4) zakona o varstvu zasebnosti komunikacij.
([201]) Člen 7(4) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij. V zahtevi, ki jo tožilec vloži pri sodišču, morajo biti navedeni glavni razlogi za sum, če se zahteva več dovoljenj hkrati, pa tudi njihova utemeljitev (glej člen 4 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij).
([202]) Člen 7(3) ter člen 6(5) in (9) zakona o varstvu zasebnosti komunikacij.
([203]) Člen 7(3) in člen 6(6) zakona o varstvu zasebnosti komunikacij.
([204]) Člen 8 zakona o varstvu zasebnosti komunikacij.
([205]) Člen 8(1) zakona o varstvu zasebnosti komunikacij.
([206]) Člen 8(2) zakona o varstvu zasebnosti komunikacij.
([207]) Člen 8(4) zakona o varstvu zasebnosti komunikacij. Za nujne ukrepe v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj glej oddelek 2.2.2.2.
([208]) Člen 8(5) in (7) zakona o varstvu zasebnosti komunikacij. V tem obvestilu morajo biti navedeni namen, cilj, področje in obdobje uporabe, kraj izvedbe in način nadzora ter razlogi, zakaj vloga ni bila vložena pred sprejetjem ukrepa (člen 8(6) zakona o varstvu zasebnosti komunikacij).
([209]) Člen 7(1)2 zakona o varstvu zasebnosti komunikacij.
([210]) To se nanaša na dejavnosti, ki ogrožajo obstoj in varnost naroda, demokratični red ali preživetje in svobodo ljudi.
([211]) Poleg tega, če je ena stranka oseba, opisana v členu 7(1), točka 2, zakona o varstvu zasebnosti komunikacij, druga pa ni znana ali je ni mogoče opredeliti, se bo uporabljal postopek iz člena 7(1), točka 2, navedenega zakona.
([212]) Člen 8(1) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij. Direktorja nacionalne obveščevalne službe imenuje predsednik republike po potrditvi v parlamentu (člen 7 zakona o nacionalni obveščevalni službi).
([213]) Člen 8(2) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([214]) Člen 8(3) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij v povezavi s členom 6(4) zakona o varstvu zasebnosti komunikacij.

glavne razloge za sum ter priložiti dokazno gradivo, ki podpira te razloge in na prvi pogled izkazuje utemeljenost, in podrobnosti o zahtevi (tj. nameni, ciljni posamezniki, obseg, dejansko obdobje zbiranja ter način in kraj zbiranja). Če se zahteva več dovoljenj hkrati, je treba navesti njihov namen in razloge zanje. ([215])

V nujnih primerih ([216]) je treba pridobiti predhodno soglasje ministra, pod katerega ministrstvo spada zadevna obveščevalna agencija. Vendar mora v tem primeru obveščevalna agencija soglasje predsednika republike zahtevati takoj po sprejetju nujnih ukrepov. Če obveščevalna agencija soglasja ne pridobi v 36 urah od vložitve vloge, mora zbiranje podatkov takoj prenehati. ([217]) V takih primerih se zbrane informacije vedno uničijo.

3.2.1.1.4. Splošne omejitve in zaščitni ukrepi

Ko obveščevalne agencije zahtevajo sodelovanje zasebnih subjektov, jim morajo zagotoviti odredbo sodišča/dovoljenje predsednika ali izvod naslovnice izjave o cenzuri v nujnem primeru, ki jo mora subjekt, od katerega se zahteva sodelovanje, hraniti v svoji evidenci. ([218]) Subjekti, od katerih se zahteva, da obveščevalnim agencijam razkrijejo informacije na podlagi zakona o varstvu zasebnosti komunikacij, lahko to razkritje zavrnejo, če se dovoljenje ali izjava o cenzuri v nujnem primeru nanaša na napačen identifikator (npr. telefonsko številko, ki pripada drugemu posamezniku in ne tistemu, ki je opredeljen). Poleg tega se v nobenem primeru ne smejo razkriti gesla, ki se uporabljajo za komunikacije. ([219])

Obveščevalne agencije lahko izvajanje ukrepov za omejevanje komunikacij ali zbiranje podrobnih podatkov o opravljeni komunikaciji poverijo poštnemu uradu ali ponudniku telekomunikacijskih storitev (kot je opredeljen v zakonu o zagotavljanju telekomunikacijskih storitev). ([220]) Zadevna obveščevalna agencija in ponudnik, ki prejme zahtevo za sodelovanje, morata še tri leta hraniti evidenco, v kateri so navedeni namen, za katerega se zahtevajo ukrepi, datum izvedbe ali sodelovanja in predmet ukrepov (npr. pošta, telefon, e-pošta). ([221]) Ponudniki telekomunikacijskih storitev, ki zagotavljajo podrobne podatke o opravljeni komunikaciji, morajo v svojih evidencah še sedem let hraniti informacije o pogostosti zbiranja ter o tem dvakrat letno poročati ministru za znanost in informacijsko tehnologijo. ([222])

Obveščevalne agencije morajo o informacijah, ki so jih zbrale, in rezultatu dejavnosti nadzora poročati direktorju nacionalne obveščevalne službe. ([223]) V zvezi z zbiranjem podrobnih podatkov o opravljeni komunikaciji je treba hraniti evidence o tem, da je bila vložena zahteva za take podatke, ter same pisne zahteve in institucijo, ki se je nanjo oprla. ([224])

Zbiranje podatkov o vsebini komunikacij in podrobnih podatkov o opravljeni komunikaciji lahko traja največ štiri mesece in se mora takoj prenehati, če je zastavljeni cilj medtem že dosežen. ([225]) Če pogoji za dovoljenje še naprej veljajo, se lahko obdobje z dovoljenjem sodišča ali soglasjem predsednika republike podaljša za največ štiri mesece. Vlogo za pridobitev soglasja za podaljšanje nadzornih ukrepov je treba vložiti pisno, pri tem pa navesti razloge za podaljšanje in predložiti dokazno gradivo. ([226])

Posamezniki so običajno uradno obveščeni o zbiranju njihovih komunikacij, odvisno od pravne podlage za zbiranje. Zlasti mora vodja obveščevalne agencije ne glede na to, ali se zbrane informacije nanašajo na vsebino komunikacij ali na podrobne podatke o opravljeni komunikaciji, in ne glede na to, ali so bile informacije pridobljene v običajnem postopku ali v nujnem primeru, zadevnega posameznika o nadzornem ukrepu uradno pisno obvestiti v 30 dneh od datuma, na katerega se je nadzor končal ([227]). Uradno obvestilo mora vključevati (1) dejstvo, da so se zbirale informacije,

([215]) Člen 8(3) in člen 4 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([216]) To je v primerih, ko je ukrep usmerjen zoper dejanje zarote, ki ogroža nacionalno varnost, in za pridobitev soglasja predsednika republike ni dovolj časa, nesprejetje nujnih ukrepov pa bi lahko ogrozilo nacionalno varnost (člen 8(8) zakona o varstvu zasebnosti komunikacij).
([217]) Člen 8(9) zakona o varstvu zasebnosti komunikacij.
([218]) Člen 9(2) zakona o varstvu zasebnosti komunikacij in člen 12 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([219]) Člen 9(4) zakona o varstvu zasebnosti komunikacij.
([220]) Člen 13 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([221]) Člen 9(3) zakona o varstvu zasebnosti komunikacij in člen 17(2) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij. To obdobje ne velja za podrobne podatke o opravljeni komunikaciji (glej člen 39 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij).
([222]) Člen 13(7) zakona o varstvu zasebnosti komunikacij in člen 39 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([223]) Člen 18(3) uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([224]) Člen 13(5) in člen 13-4(3) zakona o varstvu zasebnosti komunikacij.
([225]) Člen 7(2) zakona o varstvu zasebnosti komunikacij.
([226]) Člen 7(2) zakona o varstvu zasebnosti komunikacij in člen 5 uredbe o izvajanju zakona o varstvu zasebnosti komunikacij.
([227]) Člen 9-2(3) zakona o varstvu zasebnosti komunikacij. To se v skladu s členom 13-4 zakona o varstvu zasebnosti komunikacij uporablja za zbiranje vsebine komunikacij in za podrobne podatke o opravljeni komunikaciji.

(2) izvedbeni organ in (3) obdobje izvajanja. Če pa bi uradno obvestilo verjetno ogrozilo nacionalno varnost ali življenje in fizično varnost ljudi, se lahko odloži ([228]). Uradno obvestilo je treba poslati v 30 dneh po prenehanju razlogov za odlog ([229]).

Vendar se ta zahteva po uradnem obveščanju nanaša le na zbiranje informacij, kadar je vsaj ena od strank korejski državljan. Zato bodo posamezniki, ki niso državljani Koreje, uradno obveščeni le, če se bodo zbirale njihove komunikacije s korejskimi državljani. Če se zbirajo komunikacije izključno med posamezniki, ki niso državljani Koreje, obveznost uradnega obveščanja torej ne velja.

Vsebina komunikacij in podrobni podatki o opravljeni komunikaciji, pridobljeni z nadzorom na podlagi zakona o varstvu zasebnosti komunikacij, se lahko uporabijo le (1) za preiskovanje, kazenski pregon ali preprečevanje določenih kaznivih dejanj, (2) za disciplinske postopke, (3) za sodne postopke, v katerih se ena od strank komunikacije sklicuje nanje v odškodninskem zahtevku, ali (4) na podlagi drugih predpisov. ([230])

3.2.1.2. Zbiranje podatkov o komunikaciji, ki ga za namene nacionalne varnosti izvaja policija/tožilci

Policija/tožilec lahko podatke o komunikaciji (vsebino komunikacij in podrobne podatke o opravljeni komunikaciji) za namene nacionalne varnosti zbira pod enakimi pogoji, kot so opisani v oddelku 3.2.1.1. Postopek, ki se uporablja za ukrepanje v nujnih primerih ([231]), je postopek, ki je bil opisan zgoraj v zvezi z zbiranjem vsebine komunikacij za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj v nujnih primerih (tj. člen 8 zakona o varstvu zasebnosti komunikacij).

3.2.2. *Zbiranje podatkov o osumljencih terorizma*

3.2.2.1. Pravna podlaga

Z zakonom o boju proti terorizmu je direktor nacionalne obveščevalne službe pooblaščen za zbiranje informacij o osumljencih terorizma. ([232]) „Osumljenec terorizma“ je opredeljen kot član teroristične skupine ([233]), oseba, ki spodbuja dejavnosti teroristične skupine (s spodbujanjem in razširjanjem zamisli ali taktik teroristične skupine), zbira ali prispeva sredstva za terorizem ([234]) ali je vpletena v druge dejavnosti pripravljanja ali širjenja terorizma, sodelovanja pri njem ali napeljevanja k njemu, ali oseba, za katero se utemeljeno sumi, da je take dejavnosti izvajala. ([235]) Vsak javni uslužbenec, ki izvaja zakon o boju proti terorizmu, mora praviloma spoštovati temeljne pravice iz korejske ustave. ([236])

Zakon o boju proti terorizmu sam po sebi ne določa posebnih pristojnosti, omejitev in zaščitnih ukrepov za zbiranje informacij o osumljencih terorizma, temveč se sklicuje na postopke v drugih predpisih. Prvič, direktor nacionalne obveščevalne službe lahko na podlagi zakona o boju proti terorizmu zbira (1) informacije o vstopu v Republiko Korejo in izstopu iz nje, (2) informacije o finančnih transakcijah in (3) podatke o komunikaciji. Ustrezne postopkovne zahteve so glede na iskano vrsto informacij določene v zakonu o priseljevanju, zakonu o carini, zakonu o sporočanju in uporabi specifičnih informacij o finančnih transakcijah oziroma zakonu o varstvu zasebnosti komunikacij. ([237]) V zvezi z zbiranjem informacij o vstopu v Korejo in izstopu iz nje se zakon o boju proti terorizmu sklicuje na postopke iz

([228]) Člen 9-2(4) zakona o varstvu zasebnosti komunikacij.
([229]) Člen 13-4(2) in člen 9-2(6) zakona o varstvu zasebnosti komunikacij.
([230]) Člen 5(1)-(2), člen 12 in člen 13-5 zakona o varstvu zasebnosti komunikacij.
([231]) In sicer, kadar ukrep usmerjen zoper kaznivo dejanje zarote, ki ogroža nacionalno varnost, ukrepanje pa je tako nujno, da ni mogoče izvesti običajnega postopka soglasja (člen 8(1) zakona o varstvu zasebnosti komunikacij).
([232]) Člen 9 zakona o boju proti terorizmu.
([233]) „Teroristična skupina“ je opredeljena kot skupina teroristov, ki jo je kot tako označila Organizacija združenih narodov (člen 2(2) zakona o boju proti terorizmu).
([234]) „Terorizem“ je v členu 2(1) zakona o boju proti terorizmu opredeljen kot ravnanje, storjeno z namenom oviranja izvajanja pooblastil države, lokalne uprave ali tuje vlade (vključno z lokalnimi upravnimi organi in mednarodnimi organizacijami) ali z namenom, da se ta pooblastila izvajajo za namene, ki za njihovo izvajanje niso obvezni, ali za namene zastraševanja javnosti. To vključuje (a) povzročitev smrti osebe ali ogrožanje njenega življenja s povzročitvijo telesne poškodbe ali njenim zadrževanjem, zapiranjem, ugrabitvijo ali zajetjem osebe za talca; (b) določene vrste ravnanja, usmerjene v zrakoplov (npr. povzročitev trčenja, ugrabitev ali poškodovanje zrakoplova med letom); (c) določene vrste ravnanja, povezane z ladjo (npr. zajetje ali uničenje ladje ali morske konstrukcije med obratovanjem ali poškodovanje ladje ali morske konstrukcije med obratovanjem do te mere, da je ogrožena njena varnost, vključno s poškodovanjem tovora, naloženega na ladjo ali morsko konstrukcijo med obratovanjem); (d) namestitev, sprožitev ali drugačen način uporabe biokemičnega, eksplozivnega ali zažigalnega orožja ali naprave z namenom povzročitve smrti, hude poškodbe ali hude materialne škode ali s takim učinkom na določeni vrsti vozil ali objektov (npr. vlakih, tramvajih, motornih vozilih, javnih parkih in postajah, energetski infrastrukturi za prenos in distribucijo električne energije in zemeljskega plina ter telekomunikacijski infrastrukturi); (e) določene vrste ravnanja, povezanega z jedrskimi ali radioaktivnimi materiali ali jedrskimi objekti (npr. ogrožanje človeških življenj, teles ali premoženja ali drugačno motenje javne varnosti z uničenjem jedrskega reaktorja ali nepravilnim ravnanjem z radioaktivnimi materiali itd.).
([235]) Člen 2(3) zakona o boju proti terorizmu.
([236]) Člen 3(3) zakona o boju proti terorizmu.
([237]) Člen 9(1) zakona o boju proti terorizmu.

zakona o priseljevanju in zakona o carini. Vendar v teh zakonih taka pooblastila za zdaj niso določena. V zvezi z zbiranjem podatkov o komunikaciji in informacij o finančnih transakcijah se zakon o boju proti terorizmu sklicuje na omejitve in zaščitne ukrepe iz zakona o varstvu zasebnosti komunikacij (ki so podrobneje opisani v nadaljevanju) in zakona o sporočanju in uporabi specifičnih informacij o finančnih transakcijah (ki, kot je obrazloženo v oddelku 2.1, ni upošteven za namene ocene za sklep o ustreznosti).

Poleg tega člen 9(3) zakona o boju proti terorizmu podrobno določa, da lahko direktor nacionalne obveščevalne službe od upravljavca osebnih podatkov ([238]) ali ponudnika podatkov o lokaciji ([239]) zahteva osebne podatke ali podatke o lokaciji osumljenca terorizma. Ta možnost je omejena na zahteve za prostovoljno razkritje, na katere se upravljavcem osebnih podatkov in ponudnikom podatkov o lokaciji ni treba odzvati, vsekakor pa to lahko storijo le v skladu z zakonom o varstvu osebnih podatkov in zakonom o podatkih o lokaciji (glej oddelek 3.2.2.2 v nadaljevanju).

3.2.2.2. Omejitve in zaščitni ukrepi, ki se uporabljajo za prostovoljno razkritje na podlagi zakona o varstvu osebnih podatkov in zakona o podatkih o lokaciji

Zahteve za prostovoljno sodelovanje na podlagi zakona o boju proti terorizmu morajo biti omejene na informacije o osumljencih terorizma (glej oddelek 3.2.2.1). Pri vsaki taki zahtevi nacionalne obveščevalne službe je treba upoštevati načela zakonitosti, potrebnosti in sorazmernosti, ki izhajajo iz korejske ustave (člen 12(1) in člen 37(2)) ([240]), ter zahteve za zbiranje osebnih podatkov iz zakona o varstvu osebnih podatkov (člen 3(1) navedenega zakona, glej oddelek 1.2). Zakon o nacionalni obveščevalni službi poleg tega podrobno določa, da nacionalna obveščevalna služba ne sme zlorabljati svojih pooblastil tako, da bi kateri koli organ, organizacijo ali posameznika prisilila v nekaj, česar po zakonu ni dolžan storiti, ali posameznika ovirala pri uresničevanju pravic. ([241]) Za kršitev te prepovedi se lahko izrečejo kazenske sankcije. ([242])

Upravljavci osebnih podatkov in ponudniki podatkov o lokaciji niso zavezani ugoditi zahtevam, ki jih na podlagi zakona o boju proti terorizmu prejmejo od nacionalne obveščevalne službe. Ugodijo jim lahko na prostovoljni podlagi, vendar morajo upoštevati zakon o varstvu osebnih podatkov in zakonom o podatkih o lokaciji. Kar zadeva skladnost z zakonom o varstvu osebnih podatkov, mora upravljavec zlasti upoštevati interese posameznika, na katerega se nanašajo osebni podatki, in informacij ne sme razkriti, če bi s tem verjetno nepošteno posegel v interese posameznika ali tretje osebe. ([243]) Poleg tega mora biti zadevni posameznik v skladu z uradnim obvestilom št. 2021-1 o dodatnih pravilih za razlago in uporabo zakona o varstvu osebnih podatkov uradno obveščen o razkritju. Tako uradno obveščanje se lahko v izjemnih primerih odloži, zlasti če in dokler bi ogrozilo tekočo kazensko preiskavo ali bi verjetno povzročilo škodo za življenje ali telo druge osebe, kadar te pravice ali interesi očitno prevladajo nad pravicami posameznika, na katerega se nanašajo osebni podatki. ([244])

3.2.2.3. Omejitve in zaščitni ukrepi na podlagi zakona o varstvu zasebnosti komunikacij

Na podlagi zakona o boju proti terorizmu lahko obveščevalne agencije zbirajo podatke o komunikaciji (vsebino komunikacij in podrobne podatke o opravljeni komunikaciji) le, kadar je to potrebno za protiteroristične dejavnosti, tj. dejavnosti, povezane s preprečevanjem in protiukrepi proti terorizmu. Za zbiranje osebnih podatkov za namene boja proti terorizmu se uporabljajo postopki iz zakona o varstvu zasebnosti komunikacij, opisani v oddelku 3.2.1.

3.2.3. *Prostovoljno razkritje s strani telekomunikacijskih operaterjev*

Telekomunikacijski operaterji lahko na podlagi zakona o zagotavljanju telekomunikacijskih storitev ugodijo zahtevi za razkritje „podatkov o komunikaciji“, ki jo poda obveščevalna agencija, ki namerava informacije zbirati za preprečitev grožnje državni varnosti. ([245]) Pri vsaki taki zahtevi je treba upoštevati načela zakonitosti, potrebnosti in sorazmernosti, ki izhajajo iz korejske ustave (člena 12(1) in 37(2)) ([246]), ter zahteve za zbiranje osebnih podatkov iz zakona o varstvu osebnih podatkov (člen 3(1) navedenega zakona, glej oddelek 1.2). Poleg tega se uporabljajo enake omejitve in zaščitni ukrepi kot v zvezi s prostovoljnimi razkritji za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (glej oddelek 2.2.4). ([247])

([238]) Kot je opredeljen v členu 2 zakona o varstvu osebnih podatkov, tj. javna institucija, pravna oseba, organizacija, posameznik itd., ki neposredno ali posredno obdeluje osebne podatke zaradi upravljanja datotek z osebnimi podatki za uradne ali poslovne namene.
([239]) Kot je opredeljen v členu 5 zakona o varstvu, uporabi itd. podatkov o lokaciji (v nadaljnjem besedilu: zakon o podatkih o lokaciji), tj. vsakdo, ki je dobil dovoljenje korejske komisije za komunikacije za opravljanje dejavnosti zagotavljanja podatkov o lokaciji.
([240]) Glej tudi člen 3(2) in (3) zakona o boju proti terorizmu.
([241]) Člen 11(1) zakona o nacionalni obveščevalni službi.
([242]) Člen 19 zakona o nacionalni obveščevalni službi.
([243]) Člen 18(2) zakona o varstvu osebnih podatkov.
([244]) Uradno obvestilo komisije za varstvo osebnih podatkov št. 2021-1 o dodatnih pravilih za razlago in uporabo zakona o varstvu osebnih podatkov, oddelek III, točka 2(iii).
([245]) Člen 83(3) zakona o zagotavljanju telekomunikacijskih storitev.
([246]) Glej tudi člen 3(2) in (3) zakona o boju proti terorizmu.
([247]) Zahtevo je treba zlasti predložiti pisno ter navesti razloge zanjo, povezavo z zadevnim uporabnikom in obseg zahtevanih informacij, ponudnik telekomunikacijskih storitev pa mora voditi evidenco in dvakrat letno poročati ministru za znanost in informacijsko tehnologijo.

Ponudniki telekomunikacijskih storitev niso zavezani ugoditi zahtevam, lahko pa to storijo na prostovoljni podlagi in le v skladu z zakonom o varstvu osebnih podatkov. V zvezi s tem veljajo za ponudnike telekomunikacijskih storitev iste obveznosti, tudi glede obveščanja posameznika, kot kadar prejmejo zahtevo organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, kakor je podrobneje razloženo v oddelku 2.2.3.

3.3. **Nadzor**

Dejavnosti korejskih obveščevalnih agencij nadzorujejo različni organi. Poveljstvo za varnostno podporo obrambnih sil je v skladu z direktivo ministra o izvajanju notranje revizije pod nadzorom ministrstva za narodno obrambo. Nacionalna obveščevalna služba je pod nadzorom izvršilne veje oblasti, parlamenta in drugih neodvisnih organov, kot je podrobneje pojasnjeno v nadaljevanju.

3.3.1. *Pooblaščena oseba za varstvo človekovih pravic*

Zakon o boju proti terorizmu določa, da so obveščevalne agencije pri zbiranju informacij o osumljencih terorizma pod nadzorom komisije za boj proti terorizmu in pooblaščene osebe za varstvo človekovih pravic. ([248])

Komisija za boj proti terorizmu med drugim oblikuje politike v zvezi z dejavnostmi boja proti terorizmu ter nadzoruje izvajanje ukrepov za boj proti terorizmu in dejavnosti različnih pristojnih organov na področju boja proti terorizmu. ([249]) Predseduje ji predsednik vlade, sestavlja pa jo več ministrov in vodij vladnih agencij, vključno z ministrom za zunanje zadeve, ministrom za pravosodje, ministrom za narodno obrambo, ministrom za notranje zadeve in varnost, direktorjem nacionalne obveščevalne službe, generalnim komisarjem korejske nacionalne policije in predsednikom komisije za finančne storitve. ([250]) Direktor nacionalne obveščevalne službe mora pri izvajanju preiskav v okviru boja proti terorizmu in pri sledenju osumljencem terorizma za zbiranje informacij ali dokaznega gradiva, potrebnega za dejavnosti boja proti terorizmu, poročati predsedniku komisije za boj proti terorizmu (tj. predsedniku vlade). ([251])

Z zakonom o boju proti terorizmu je poleg tega vzpostavljena pooblaščena oseba za varstvo človekovih pravic, da bi se temeljne pravice posameznikov varovale pred kršitvami, povzročenimi z dejavnostmi boja proti terorizmu. ([252]) Pooblaščeno osebo za varstvo človekovih pravic imenuje predsednik komisije za boj proti terorizmu izmed posameznikov, ki izpolnjujejo pogoje iz uredbe o izvajanju zakona o boju proti terorizmu (tj. vsakdo, ki je usposobljen kot odvetnik in ima najmanj deset let delovnih izkušenj ali strokovno znanje na področju človekovih pravic in je ali je bil najmanj deset let zaposlen na položaju (najmanj) izrednega profesorja ali zaposlen kot višji javni uslužbenec v državnih organih ali lokalnih upravnih organih oziroma ima najmanj deset let delovnih izkušenj na področju človekovih pravic, na primer v nevladni organizaciji). ([253]) Pooblaščena oseba za varstvo človekovih pravic je imenovana za dve leti (z možnostjo podaljšanja mandata), razrešiti pa jo je mogoče le iz posebnih, omejenih in upravičenih razlogov, npr. v primeru obtožbe v kazenski zadevi, povezani z njenimi nalogami, v primeru razkritja zaupnih informacij ali zaradi dolgotrajne duševne ali fizične nezmožnosti. ([254])

Pooblaščena oseba za varstvo človekovih pravic je pooblaščena za izdajanje priporočil za izboljšanje varstva človekovih pravic s strani organov, udeleženih v dejavnostih boja proti terorizmu, in obdelavo zahtevkov državljanov (glej oddelek 3.4.3). ([255]) Kadar je mogoče razumno ugotoviti, da so bile pri opravljanju uradnih dolžnosti kršene človekove pravice, lahko pooblaščena oseba za varstvo človekovih pravic vodji odgovornega organa priporoči odpravo take kršitve. ([256]) Odgovorni organ pa ji mora nato priglasiti ukrep, sprejet za izvedbo takega priporočila. ([257]) Če organ priporočila pooblaščene osebe za varstvo človekovih pravic ne bi izvedel, bi se zadeva predala komisiji za boj proti terorizmu, vključno z njenim predsednikom, tj. predsednikom vlade. Do zdaj še ni bilo primerov, ko se njena priporočila ne bi izvedla.

3.3.2. *Parlament*

Parlament lahko, kot je opisano v oddelku 2.3.2, preiskuje in pregleduje delovanje javnih organov ter v tem okviru zahteva razkritje dokumentov in navzočnost prič. Ta parlamentarni nadzor v zvezi z zadevami, ki spadajo v pristojnost nacionalne obveščevalne službe, izvaja obveščevalni odbor parlamenta. ([258]) Direktor nacionalne obveščevalne službe, ki

([248]) Člen 7 zakona o boju proti terorizmu.
([249]) Člen 5(3) zakona o boju proti terorizmu.
([250]) Člen 3(1) uredbe o izvajanju zakona o boju proti terorizmu.
([251]) Člen 9(4) zakona o boju proti terorizmu.
([252]) Člen 7 zakona o boju proti terorizmu.
([253]) Člen 7(1) uredbe o izvajanju zakona o boju proti terorizmu.
([254]) Člen 7(3) uredbe o izvajanju zakona o boju proti terorizmu.
([255]) Člen 8(1) uredbe o izvajanju zakona o boju proti terorizmu.
([256]) Člen 9(1) uredbe o izvajanju zakona o boju proti terorizmu. Pooblaščena oseba za varstvo človekovih pravic se samostojno odloča o sprejetju priporočil, o katerih pa mora poročati predsedniku komisije za boj proti terorizmu.
([257]) Člen 9(2) uredbe o izvajanju zakona o boju proti terorizmu.
([258]) Člen 36 in člen 37(1), točka 16, zakona o parlamentu.

nadzoruje, kako agencija izvaja svoje naloge, poroča obveščevalnemu odboru (in predsedniku republike). ([259]) Obveščevalni odbor sam lahko zahteva tudi poročilo o konkretni zadevi, na kar se mora direktor nacionalne obveščevalne službe nemudoma odzvati. ([260]) Odgovor obveščevalnemu odboru ali pričanje pred njim lahko zavrne le v zvezi z državnimi skrivnostmi o vojaških ali diplomatskih zadevah ali zadevah, povezanih s Severno Korejo, katerih javno razkritje bi lahko resno vplivalo na nacionalno usodo. ([261]) V tem primeru lahko obveščevalni odbor zahteva pojasnilo predsednika vlade. Če se tako pojasnilo ne zagotovi v sedmih dneh od vložitve zahteve, odgovora ali pričanja ni več mogoče zavrniti.

Če parlament odkrije, da se je izvajala nezakonita ali neprimerna dejavnost, lahko od zadevnega javnega organa zahteva sprejetje popravnih ukrepov, vključno z dodelitvijo odškodnine, sprejetjem disciplinskih ukrepov in izboljšanjem notranjih postopkov. ([262]) Po taki zahtevi mora organ takoj ukrepati in o rezultatu poročati parlamentu. V zvezi s parlamentarnim nadzorom obstajajo na podlagi zakona o varstvu zasebnosti komunikacij posebna pravila glede uporabe ukrepov za omejevanje komunikacij (tj. zbiranje vsebine komunikacij). ([263]) Parlament lahko vodje obveščevalnih agencij zaprosi za poročilo o posameznih ukrepih za omejevanje komunikacij. Poleg tega lahko na kraju samem izvede preglede opreme za prisluškovanje. Nazadnje, obveščevalne agencije, ki so zbrale informacije o vsebini za namene nacionalne varnosti, in operaterji, ki so te informacije razkrili, morajo o takem razkritju poročati na zahtevo parlamenta.

3.3.3. *Odbor za revizijo in inšpekcijski pregled*

Odbor za revizijo in inšpekcijski pregled izvaja enake nadzorne funkcije v zvezi z obveščevalnimi agencijami kot na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (glej oddelek 2.3.2). ([264])

3.3.4. *Komisija za varstvo osebnih podatkov*

Komisija za varstvo osebnih podatkov zagotavlja dodatni nadzor pri obdelavi podatkov za namene nacionalne varnosti, tudi v fazi zbiranja. Kot je podrobneje pojasnjeno v oddelku 1.2, to vključuje splošna načela in obveznosti iz člena 3 in člena 58(4) zakona o varstvu osebnih podatkov ter uresničevanje pravic posameznikov, zagotovljenih s členom 4 zakona o varstvu osebnih podatkov. Poleg tega nadzor komisije za varstvo podatkov v skladu s členom 7-8(3) in (4) ter členom 7-9(5) zakona o varstvu osebnih podatkov zajema tudi morebitne kršitve pravil iz posebnih predpisov, ki določajo omejitve in zaščitne ukrepe v zvezi z zbiranjem osebnih podatkov, kot so zakon o varstvu zasebnosti komunikacij, zakon o boju proti terorizmu in zakon o zagotavljanju telekomunikacijskih storitev. Vsaka kršitev navedenih zakonov glede na zahteve iz člena 3(1) zakona o varstvu osebnih podatkov, ki veljajo za zakonito in pošteno zbiranje osebnih podatkov, pomeni tudi kršitev navedenega zakona. Komisija za varstvo osebnih podatkov je tako pooblaščena, da preišče ([265]) kršitve zakonov, ki urejajo dostop do podatkov za namene nacionalne varnosti, in pravil za obdelavo iz zakona o varstvu osebnih podatkov, izda nasvete za izboljšanje, naloži popravne ukrepe, priporoči disciplinske ukrepe in predloži morebitna kazniva dejanja ustreznim preiskovalnim organom. ([266])

3.3.5. *Nacionalna komisija za človekove pravice*

Nadzor, ki ga izvaja nacionalna komisija za človekove pravice, velja enako za obveščevalne agencije in druge vladne organe (glej oddelek 2.3.2).

3.4. **Pravna sredstva posameznikov**

3.4.1. *Pravna sredstva pred pooblaščeno osebo za varstvo človekovih pravic*

Pooblaščena oseba za varstvo človekovih pravic, vzpostavljena v okviru komisije za boj proti terorizmu, zagotavlja posebno pravno sredstvo v zvezi z zbiranjem osebnih podatkov v okviru dejavnosti boja proti terorizmu. Obravnava zahtevke državljanov v zvezi s kršitvami človekovih pravic kot posledice dejavnosti boja proti terorizmu. ([267]) Priporoči lahko popravne ukrepe, zadevni organ pa ji mora poročati o vseh ukrepih, sprejetih za izvajanje takih priporočil. Da lahko posameznik vloži pritožbo pri pooblaščeni osebi za varstvo človekovih pravic, ni potrebno procesno upravičenje. Posledično bo ta pritožbo obravnavala, čeprav zadevni posameznik v fazi dopustnosti dejansko ne more dokazati škode.

([259]) Člen 18 zakona o nacionalni obveščevalni službi.
([260]) Člen 15(2) zakona o nacionalni obveščevalni službi.
([261]) Člen 17(2) zakona o nacionalni obveščevalni službi. „Državne skrivnosti“ so opredeljene kot „dejstva, dobrine ali znanje, ki se štejejo za državne skrivnosti, dostop do katerih je dovoljen omejenemu obsegu oseb in ki se ne razkrijejo nobeni drugi državi ali organizaciji, da se prepreči resno poslabšanje nacionalne varnosti,“ glej člen 13(4) zakona o nacionalni obveščevalni službi.
([262]) Člen 16(2) zakona o pregledih in preiskavah v državni upravi.
([263]) Člen 15 zakona o varstvu zasebnosti komunikacij.
([264]) Kot to velja za obveščevalni odbor parlamenta, lahko tudi direktor nacionalne obveščevalne službe odgovor odboru za revizijo in inšpekcijski pregled zavrne le, če gre za zadeve, ki so državna skrivnost, in bi njihovo javno razkritje resno vplivalo na nacionalno usodo (člen 13(1) zakona o nacionalni obveščevalni službi).
([265]) Člen 63 zakona o varstvu osebnih podatkov.
([266]) Člen 61(2), člen 65(1) in (2) ter člen 64(4) zakona o varstvu osebnih podatkov.
([267]) Člen 8(1), točka 2, uredbe o izvajanju zakona o boju proti terorizmu.

3.4.2. *Mehanizmi pravnih sredstev, ki so na voljo na podlagi zakona o varstvu osebnih podatkov*

Posamezniki lahko v zvezi z osebnimi podatki, ki se obdelujejo za namene nacionalne varnosti, uresničujejo svoje pravice do dostopa, popravka, izbrisa in prenehanja obdelave na podlagi zakona o varstvu osebnih podatkov. ([268]) Zahteve za uresničevanje teh pravic se lahko vložijo neposredno pri obveščevalni agenciji ali posredno prek komisije za varstvo osebnih podatkov. Obveščevalna agencija lahko uresničevanje pravice odloži, omeji ali zavrne, kolikor in dokler je to potrebno in sorazmerno za zaščito pomembnega cilja javnega interesa (npr. kolikor in dokler bi priznanje pravice ogrozilo tekočo preiskavo ali nacionalno varnost) ali kadar bi priznanje pravice lahko povzročilo škodo za življenje ali telo tretje osebe. Kadar se zahteva zavrne ali omeji, je treba posameznika nemudoma uradno obvestiti o razlogih.

Poleg tega imajo posamezniki v skladu s členom 58(4) zakona o varstvu osebnih podatkov (zahteva po zagotovitvi ustrezne obravnave posameznih pritožb) in členom 4(5) navedenega zakona (pravica do ustreznega pravnega sredstva za škodo, ki izhaja iz obdelave osebnih podatkov, v hitrem in poštenem postopku) pravico do uveljavljanja pravnih sredstev. To vključuje pravico do poročanja o domnevni kršitvi klicnemu centru za vprašanja v zvezi z zasebnostjo, ki ga upravlja korejska agencija za splet in varnost, in vložitev pritožbe pri komisiji za varstvo osebnih podatkov. ([269]) Ta pravna sredstva so na voljo v primeru morebitnih kršitev pravil iz posebnih predpisov, ki določajo omejitve in zaščitne ukrepe v zvezi z zbiranjem osebnih podatkov za namene nacionalne varnosti, in morebitnih kršitev zakona o varstvu osebnih podatkov. Kot je pojasnjeno v uradnem obvestilu št. 2021-1, lahko posameznik iz EU vloži pritožbo pri komisiji za varstvo osebnih podatkov prek svojega nacionalnega organa za varstvo podatkov. V tem primeru komisija za varstvo osebnih podatkov posameznika uradno obvesti prek nacionalnega organa za varstvo podatkov po zaključku preiskave (med drugim, če je ustrezno, o naloženih popravnih ukrepih). Zoper odločitve ali neukrepanje te komisije pa se je mogoče nadalje pritožiti pri korejskih sodiščih, in sicer na podlagi zakona o upravnem sporu.

3.4.3. *Pravna sredstva pred nacionalno komisijo za človekove pravice*

Možnost uveljavljanja individualnih pravnih sredstev pri nacionalni komisiji za človekove pravice velja enako za obveščevalne agencije in druge vladne organe (glej oddelek 2.4.2).

3.4.4. *Sodno varstvo*

Kot to velja v zvezi z dejavnostmi organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, lahko posamezniki uveljavljajo različna pravna sredstva zoper obveščevalne agencije v zvezi s kršitvami zgoraj navedenih omejitev in zaščitnih ukrepov.

Prvič, posamezniki lahko prejmejo odškodnino za škodo na podlagi zakona o državni odškodnini. V enem primeru je bila odškodnina na primer dodeljena v zvezi z nezakonitim nadzorom, ki ga je izvajalo poveljstvo za podporo obrambnih sil (predhodnik poveljstva za varnostno podporo obrambnih sil). ([270])

Drugič, posamezniki lahko na podlagi zakona o upravnem sporu izpodbijajo odločitve in opustitve s strani upravnih agencij, med drugim obveščevalnih agencij. ([271])

Nazadnje, posamezniki lahko zoper ukrepe, ki so jih sprejele obveščevalne agencije, vložijo ustavno pritožbo pri ustavnem sodišču na podlagi zakona o ustavnem sodišču.

([268]) Člen 3(5) ter člen 4(1), (3) in (4) zakona o varstvu osebnih podatkov.
([269]) Člen 62 in člen 63(2) zakona o varstvu osebnih podatkov.
([270]) Odločba vrhovnega sodišča št. 96Da42789 z dne 24. julija 1998.
([271]) Člena 3 in 4 zakona o upravnem sporu.