



REPUBLIKA SLOVENIJA
VLADA REPUBLIKE SLOVENIJE

Gregorčičeva ulica 20–25, 1000 Ljubljana

T: +386 1 478 1000

F: +386 1 478 1607

E: gp.gs@gov.si

<http://www.vlada.si/>

**NUJNI POSTOPEK
EVA 2025-1524-0001
PREDLOG**

ZAKON O SPREMEMBAH IN DOPOLNITVAH ZAKONA O SLOVENSKI OBVEŠČEVALNO- VARNOSTNI AGENCIJI

I. UVOD

1. OCENA STANJA IN RAZLOGI ZA SPREJEM PREDLOGA ZAKONA

Slovenska obveščevalno-varnostna agencija (v nadaljevanju: agencija) je vladna služba, ki predstavlja enega od ključnih stebrov nacionalne varnosti v Republiki Sloveniji. V demokratičnih družbah je obveščevalnim službam zakonsko podeljeno pooblastilo, da lahko v okviru svojih pooblastil in z uporabo posebnih oblik pridobivanja podatkov posegajo v sicer ustavno zagotovljene človekove pravice s širšim ciljem zagotavljanja nacionalne varnosti in ustavne ureditve. Področje delovanja agencije na obveščevalnem in varnostnem področju opredeljuje 2. člen Zakona o Slovenski obveščevalno-varnostni agenciji, ki določa, da agencija pridobiva in vrednoti podatke ter posreduje informacije iz tujine, pomembne za zagotavljanje varnostnih, političnih in gospodarskih interesov države ter o organizacijah, skupinah in osebah, ki s svojo dejavnostjo iz tujine ali v povezavi z njo ogrožajo ali bi lahko ogrozile nacionalno varnost države in njeno ustavno ureditev. Nadalje 2. člen določa, da agencija sodeluje s pristojnimi državnimi organi in službami pri varnostnem preverjanju ter posreduje podatke, pomembne za varnost določenih oseb, delovnih mest, organov, objektov in okolišev in opravlja naloge na podlagi zakona v skladu s prednostnimi nalogami, ki jih določi vlada na podlagi nacionalnovarnostnega programa (Resolucije o strategiji nacionalne varnosti Republike Slovenije, Uradni list RS, št. 59/19), ki ga sprejme Državni zbor Republike Slovenije.

Na vsebino dela agencije vplivajo vsakokratne varnostne razmere v državi, njeni bližnji in daljni okolici. Sodobno mednarodno varnostno okolje se sooča s spremembami, ki so posledica globalizacije in odzivov nanje. To okolje je postalo bolj povezano, kompleksno in negotovo, kar prinaša nove oblike kompleksnih varnostnih izzivov, ki jih dodatno omogočajo hiter tehnološki napredek in globalizacijski učinki. Terorizem in nasilni ekstremizem ostajata med najpomembnejšimi varnostnimi tveganji in grožnjami v Evropi, pri čemer se povezuje z drugimi varnostnimi grožnjami, kot so organizirani kriminal, nedovoljene dejavnosti na področju proizvodnje orožja za množično uničevanje in jedrske tehnologije, nezakonite migracije ter trgovina z ljudmi, orožjem in s prepovedanimi drogami. Čez ozemlje Slovenije potekajo tihotapske dejavnosti, ki lahko vključujejo tihotapljenje orožja in eksploziva, ter nezakonite migracije, ki lahko omogočajo prikrit prehod teroristov. Kriminalne metode se uporabljajo za logistično podporo in pridobivanje finančnih sredstev za teroristično delovanje, pri čemer se pojavne oblike nenehno spreminjajo, zaznamujejo pa jih dinamika, kompleksnost in individualizacija, pri čemer imajo ključno vlogo novi načini komunikacije in svetovni splet. Za izpolnjevanje nalog zagotavljanja nacionalne varnosti in odzivanja na kompleksne varnostne izzive je sprememba in dopolnitev obstoječega zakona zato nujen potreben korak.

Zakon o Slovenski obveščevalno-varnostni agenciji (v nadaljevanju: ZSOVA) je bil sprejet leta 1999 ter se je nato z novelama ZSOVA-A iz leta 2003 in ZSOVA-B iz leta 2006 noveliral. Na njegovo vsebino so vplivali tudi Zakon o javnih uslužbencih, Zakon o parlamentarnem nadzoru obveščevalnih

in varnostnih služb in Zakon o dohodnini. Zaradi vseh sprememb je bilo v Uradnem listu RS, št. 81/06 z dne 31. 7. 2006 objavljeno uradno prečiščeno besedilo zakona, in sicer ZSOVA-UPB2.

Od leta 2006, ko je bil ZSOVA zadnjič spremenjen, je bila prenovljena in sprejeta področna zakonodaja, ki ima neposreden in posreden vpliv na določbe ZSOVA ter s tem na izvajanje nalog in pooblastil agencije. Pomembne spremembe so se zgodile tudi na področju tehnologije, digitalizacije komuniciranja in poslovanja. Priča smo izjemnemu tehnološkemu napredku, ki je prinesel množično uporabo mobilnih naprav, aplikacij za komuniciranje ter umetno inteligenco, s čimer se je popolnoma spremenil način komuniciranja. Če želimo biti kot obveščevalno-varnostna agencija učinkoviti ter pripravljeni na prihodnje izzive, je treba zakonodajni okvir uskladiti z realnostjo digitalne dobe. Spremembe in kompleksnost mednarodnega varnostnega okolja so povzročile, da področje nacionalne varnosti deluje v še bolj nepredvidljivem okolju kot kadar koli prej, kar je ponovno nov razlog in utemeljitev za pripravo novele ZSOVA. Trenutno veljavni ZSOVA vsebinsko ne ustreza vsem sodobnim izzivom delovanja agencije, njenemu tehnološkemu razvoju, načinu delovanja globaliziranega sveta ter geostrateškemu položaju Republike Slovenije.

Novi Zakon o varstvu osebnih podatkov (v nadaljevanju: ZVOP-2) omogoča za področje varnosti države uporabo nekaterih izjem pri obravnavi in posredovanju osebnih podatkov, uporabo le-teh pa pogojuje z ustrezno ureditvijo v matičnih zakonih, ki urejajo delovanje posameznih organov. Predlog novele tako vključuje tudi spremembo več smiselno povezanih členov, ki uvajajo možnost obdelave biometričnih osebnih podatkov v agenciji. To bo omogočilo uporabo naprednih tehnologij za obdelavo podatkov, s čimer se bo zagotovila hitrejša in hkrati natančnejša obdelava osebnih podatkov, še vedno pa se bodo zagotavljale vse predpostavke zakonite obdelave osebnih podatkov.

S tem predlogom zakona se jasneje določajo pogoji predaje arhivskega gradiva agencije in njegove dostopnosti. V skladu s priporočili Računskega sodišča Republike Slovenije se med posebne delovne razmere dodaja možnost odreditve pripravljenosti na domu, v skladu s spremembo zakona, ki ureja položaj javnih uslužbencev, pa se smiselno dopolnjuje tudi določba, ki ureja postopek zaposlitve v agenciji.

2. CILJI, NAČELA IN POGLAVITNE REŠITVE PREDLOGA ZAKONA

1.1. Cilji

Cilj sprememb in dopolnitev zakona je prilagoditev pooblastil in pravnih podlag agencije sodobnemu mednarodnemu varnostnemu okolju, ki bodo zagotavljale ustrezen odziv na kompleksne varnostne izzive sodobnega časa. Uporaba modernih tehnologij in sredstev, ki so na voljo na trgu, in ki jih uporabljajo tako primerljive tuje službe kot tudi kriminalne organizacije, pomenijo ključni dejavnik pri zagotavljanju učinkovitega, varnega in zakonitega izvajanja nalog agencije, saj omogočajo hitrejšo, natančnejšo in bolj usmerjeno delovanje. Njihova uporaba bo pomembno prispevala k še uspešnejšemu izvajanju nalog agencije in s tem ustreznemu zagotavljanju tako nacionalne kot varnosti v širši mednarodni skupnosti. Uvedba novih oblik pridobivanja podatkov je zasnovana tako, da vključuje vgrajene omejitve in kavtele tudi po vzoru mednarodne prakse, ki onemogočajo potencialne zlorabe in arbitrarno delovanje agencije. Odpravljajo se s prakso ugotovljene praktične pomanjkljivosti, ki so nastale kot posledica zadnje novelacije zakona v letu 2006, vključujejo pa ureditev področja varstva osebnih podatkov, dokumentarnega gradiva agencije in delovnopravnega statusa uslužbencev. Z navedenimi spremembami bo agencija sledila tehnološkemu razvoju na več področjih svojega delovanja, navedeno pa bo pozitivno pripomoglo k opravljanju njenega temeljnega poslanstva.

1.2. Načela

Osnovna načela, ki jim sledi besedilo sprememb in dopolnitev zakona, so zaščita ustavne demokracije in nacionalnih interesov države, načelo varovanja človekovih pravic in temeljnih svoboščin ter načelo pravne države, s poudarkom na načelu zakonitosti in strokovnosti delovanja obveščevalno-varnostnih služb, ob upoštevanju načela sorazmernosti ter usklajenosti z drugo področno zakonodajo.

1.3. Poglavitne rešitve

1. Dejavnost agencije

Predlagana sprememba prvega odstavka 2. člena ZSOVA bo področje obveščevalne dejavnosti razširila z obstoječega zakonskega pogoja obdelave podatkov iz tujine na zakonski pogoj obdelave podatkov iz tujine ali v povezavi z njo. S tem bo smiselno izenačen pogoj za pridobivanje podatkov tako na obveščevalnem kot na protiobveščevalnem področju.

Obveščevalno dejavnost opredeljujemo kot aktivnost, pri kateri zaradi zaščite nacionalnih in mednarodnih interesov pooblaščen državní organi zbirajo, vrednotijo, analizirajo in posredujejo podatke oziroma informacije, ki imajo zunanjepolitični, varnostni, obrambni ali gospodarski pomen tako za državo kot tudi mednarodno skupnost. V sklop obveščevalnih dejavnosti sodijo tudi tajne dejavnosti, ki jih načrtujejo, pripravljajo in izvajajo predvsem obveščevalne službe, z namenom pridobivanja ključnih informacij o posameznikih ali dogodkih, izvajanje pa običajno pomeni uresničevanje zunanje politike države. Protiobveščevalna dejavnost pa zajema aktivnosti, ki so usmerjene v odkrivanje in preprečevanje dela tujih obveščevalnih služb, ki delujejo na ozemlju države protiobveščevalne službe.

Dejavnost agencije je v skladu z zakonsko opredelitvijo neločljivo povezana z elementom tujine. Aktualne družbene spremembe z modernizacijo in množično uporabo tehnoloških sredstev zabrisujejo državne meje, klasični element tujine pa postaja vse težje določljiv v transnacionalnosti, kar nujno terja dopolnitev opredelitve področja dela agencije.

Trenutna zakonska določba pridobivanja podatkov na obveščevalnem področju torej ne zajema vseh relevantnih situacij, saj je vezana na zakonski pogoj pridobivanja in vrednotenja podatkov ter posedovanja informacij zgolj iz tujine, ki so pomembne za zagotavljanje varnostnih, političnih in gospodarskih interesov države. V skladu z navedenim morajo relevantni podatki nujno izhajati iz tujine, sicer jih agencija ne more pridobivati, vrednotiti in nadalje posredovati. Dopolnitev področja delovanja agencije na pridobivanje in vrednotenje podatkov tudi v povezavi s tujino pa bo omogočila tudi obdelavo več relevantnih podatkov na obveščevalnem področju, kar se bo pozitivno odražalo tako na kvaliteti kot tudi kvantiteti obveščevalnih informacij, ki jih posreduje vodstvu države in drugim relevantnim deležnikom, s tem pa se bo nadalje pomembno prispevalo k zagotavljanju varnostnih, političnih in gospodarskih interesov Republike Slovenije ter tudi širšega mednarodnega okolja.

S predlagano dopolnitvijo bo torej agenciji omogočeno zakonito zbiranje podatkov tako iz tujine kot tudi v povezavi z njo na obveščevalnem in protiobveščevalnem področju.

2. Varovanje osebnih podatkov

Predlog spremembe več povezanih členov v 4. poglavju ZSOVA se nanaša na dopolnitev obdelave podatkov, ki jih agencija pridobiva sama ali z mednarodnim sodelovanjem, upošteva pa tudi spremembe predpisov s področja varovanja osebnih podatkov. V obdobju od zadnje spremembe ZSOVA se je področje varovanja osebnih podatkov pomembno spremenilo, saj je leta 2018 začela veljati Uredba (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 (UL L 119, 4. 5. 2016, str. 1–88; v nadaljevanju: Splošna uredba), sprejet pa je bil tudi novi Zakon o varstvu osebnih podatkov (Uradni list RS, št. 163/22 in 40/25 – ZInfV-1). Ta je podrobno uredil obravnavo osebnih podatkov na področju varnosti države, ki je sicer izvzeto iz področja urejanja prava EU in s tem ureditve tako v Splošni uredbi kot tudi v prenovljeni Konvenciji 108 Sveta Evrope.¹ Na mednarodni in nacionalni ravni je bila sprejeta obširna praksa, ki vpliva na

¹ Konvencija o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov (Uradni list RS – Mednarodne pogodbe, št. 3/94 in Uradni list RS, št. 86/04 – ZVOP-1), Konvencija št. 108, spremenjena s Protokolom CETS št. 223).

oblikovanje sprejetih standardov obdelave osebnih podatkov, predvsem s strani (represivnih) državnih organov, kar vsaj posredno vpliva tudi na delo agencije. Mehanizmi varovanja osebnih podatkov in družbeno zavedanje pomembnosti varstva osebnih podatkov so postali med najbolj izpostavljenimi ustavnimi pravicami, zaradi digitalizacije in možnosti masovnega avtomatskega obdelovanja osebnih podatkov pa so pogoji poseganja državnih organov v osebne podatke postali strožji.

V celoti je prenovljen 12. člen ZSOVA. Osrednjo spremembo prvega odstavka predstavlja napotilna določba na dodano novo vrsto osebnih podatkov, ki jih bo agencija obdelovala za uresničevanje nalog iz 2. člena ZSOVA. Gre za posebne vrste osebnih podatkov (biometrični podatki), ki so podrobneje urejene v spremembi 14. člena ZSOVA. Ker je bila obstoječa določba 12. člena zastarela, je bila v celoti prenovljena s terminologijo s področja varstva osebnih podatkov, pri čemer pa je dosedanja vsebina oziroma področje urejanja ostalo nespremenjeno.

Dodan je bil tretji odstavek, s katerim se v zakon uvaja t. i. pravilo tretjega, ki je mednarodno priznan pogoj za izmenjavo podatkov s tujimi službami, pogosto pa je vsebovan tudi v zakonodajah, ki urejajo tajne podatke. V mednarodnih okvirih se namreč posredovanje varnostno posebej občutljivih podatkov lahko pogojuje s prepovedjo posredovanja podatkov drugim organom ali z uporabo za druge namene. Neupoštevanje teh omejitev bi lahko privedlo do izključitve agencije iz mednarodne skupnosti obveščevalnih in varnostnih služb ter drugih sodelujočih organov oziroma organizacij, kar bi pomenilo omejitev dostopa do pomembnega vira informacij, ki ga agencija uporablja za varovanje interesov Republike Slovenije.

Naslednja sprememba v sklopu varovanja osebnih podatkov je dopolnitev drugega odstavka 14. člena ZSOVA. Določba se smiselno navezuje na že omenjen prvi odstavek 12. člena. Dopolnjuje se nabor vrst osebnih podatkov o osebah, ki jih agencija v zbirki podatkov sistematično operativno obravnava, in sicer gre za uvedbo biometričnih osebnih podatkov. V skladu s predlagano spremembo zakona bo tako agencija lahko obdelovala tudi podobo obraza, govora oziroma glasu posameznika. Z uvedbo nove vrste osebnih podatkov, v obsegu, kot je določen v omenjenem odstavku, bo omogočena uvedba modernejših pristopov pri obdelavi osebnih podatkov, kar bo pripomoglo k natančnejši in hitrejši obravnavi oseb, ki so predmet sistematične operativne obravnave agencije.

V neposredni povezavi z opredeljenimi biometričnimi podatki se dodaja tudi nov, četrti, odstavek, na podlagi katerega se bo določil namen obdelave podatkov. Agencija bo tako lahko obdelovala navedene biometrične podatke skupaj z že zbranimi podatki za primerjanje oziroma identifikacijo posameznikov, ko bo to glede na okoliščine konkretne zadeve nujno in potrebno ali ko to izrecno izhaja iz odredbe za posebne oblike pridobivanja podatkov.

Agencija bo z ustreznimi internimi postopki še naprej zagotavljala varno in zakonito obdelavo osebnih podatkov, saj je to neposredno izhaja tudi iz določb in standardov nacionalne² in mednarodne³ zakonodaje s področja tajnih podatkov standardov, ki so splošno sprejeti na področju obravnave tajnih podatkov. Osebnih podatki se bodo obdelovali do zaključitve zadeve v razvidu, potem bodo izbrisani oziroma blokirani, kot izhaja iz nespremenjenega tretjega odstavka 14. člena ZSOVA.

Tretja sprememba v sklopu varovanja osebnih podatkov pa je prenova 16. člena ZSOVA, kjer se prvi in drugi odstavek obstoječega člena združita v enoten odstavek. V skladu z dosedanjim zakonom je brezplačno posredovanje osebnih podatkov agenciji določeno zgolj za upravljavce, ki so državni organi in organizacije z javnimi pooblastili. Glede na to da upravljavci osebnih podatkov niso le državni

² Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11, 8/20 in 18/23 – ZDU-10), Uredba o varovanju tajnih podatkov (Uradni list RS, št. 50/22 in 103/24).

³ Zakon o ratifikaciji Sporazuma med pogodbenicami Severnoatlantske pogodbe o varnosti podatkov (Uradni list RS – Mednarodne pogodbe, št. 22/04), Zakon o ratifikaciji Sporazuma med državami članicami Evropske unije, ki so se sestale v okviru Sveta, o varovanju tajnih podatkov, ki se izmenjujejo v interesu Evropske unije (Uradni list RS – Mednarodne pogodbe, št. 14/11), Sklep Sveta z dne 23. septembra 2013 o varnostnih predpisih za varovanja tajnih podatkov (2013/488/EU) (UL L 274, 15. 10. 2013, p.I.), Sklep Komisije (EU, Euratom) 2015/444 z dne 13. marca 2015 o varnostnih predpisih za varovanje tajnih podatkov EU (UL L 72/53, 17. 3. 2015).

organi in organizacije z javnimi pooblastili, se s spremembo zakona krog upravljavcev širi na vse upravljavce in obdelovalce zbirk podatkov. Pridobitev podatkov, ki jih agencija potrebuje za opravljanje svojih delovnih nalog, ne sme biti pogojevana s plačilom prispevka ali kritjem stroškov, ki jih imajo upravljavci ali obdelovalci osebnih podatkov v zasebnem sektorju. Opravljanje dejavnosti agencije ne pomeni konkurenčnega posega v dejavnost zasebnega upravljavca ali obdelovalca podatkov, temveč je njeno delovanje v javnem interesu, ki je tesno prepleten z zagotavljanjem nacionalne varnosti ter varovanjem ustavne demokracije in pravne države. S tem se bo pripomoglo k zagotavljanju vseh prvin varnosti, ki imajo na koncu tudi povraten in posreden vpliv tudi na zagotavljanje varnega poslovnega okolja za omenjene zasebne upravljavce ali obdelovalce.

V istem členu sta opredeljena tudi dva načina posredovanja zaprošenih podatkov, in sicer da upravljavci ali obdelovalci podatkov posredujejo podatke agenciji oziroma ji omogočijo vpogled na predhodno dogovorjen način. Pri slednjem gre za vzpostavitev neposredne zakonske podlage, ki bo agenciji omogočila sklepanje dogovorov s posameznimi upravljavci in obdelovalci podatkov za vzpostavitev sistema elektronske izmenjave podatkov. Gre za pomemben korak k modernizaciji in digitalizaciji poslovanja, saj se vse bolj opušča klasično, tj. pisemsko oziroma fizično posredovanje zahtevkov, ki se nadomešča z elektronskim poslovanjem. Tako bi pomembno prispevali k hitrosti pridobivanja podatkov, ki so v posameznih operativnih primerih lahko ključnega pomena za nadaljevanje aktivnosti agencije. Pridobivanje podatkov bo še naprej temeljilo na obrazloženih zahtevah agencije, le poslovanje bo potekalo elektronsko, prav tako pa bodo pri tem še naprej spoštovane zahteve drugih področnih zakonov glede zagotavljanja varne in zakonite obdelave osebnih in tajnih podatkov.

3. Dokumentarno gradivo agencije

Zdajšnji zakon vsebuje posebno ureditev predaje gradiva Arhivu Republike Slovenije, ki je bila primerna zgolj za specifično obdobje po letu 1991 in nima primerjave v Sloveniji, niti v primerljivih tujih državah. Navedena ureditev je bila tako zastavljena kot izjema od siceršnjih pravil in načel arhivske stroke, saj se je zasledovala cilj učinkovitega prenosa gradiv nekdanje Službe državne varnosti v Arhiv Republike Slovenije zaradi spremembe državne ureditve oziroma prehoda v demokratični politični sistem. Z izvršitvijo zastavljenih ciljev so aktualne določbe postale zastarele, neuporabne oziroma celo škodljive za trenutno ureditev in nacionalno varnost države, hkrati pa je opazna praznina ob odsotnosti določb, ki bi jih morala vsebovati sodobna arhivska zakonodaja.

Dokumentarno gradivo iz obveščevalnega in varnostnega področja ima nedvomno veliko vrednost za zgodovinsko stroko, vendar pa je treba upoštevati, da je v javnem interesu ter v interesu posameznikov, ki so lahko ogroženi, tudi, da se nekateri podatki ohranijo kot tajni dlje časa. Evidenca agencije, kot je opredeljena v 13. členu ZSOVA, je organizirana tako, da so podatki zbrani kot vsebinsko zaokrožene celote – zadeve. Vendar pa zadeve vsebujejo tajne podatke, ki se pogosto ne nanašajo zgolj na eno zadevo, ampak se smiselno povezujejo v okviru posameznih področij dela. Ob ukinitvi posamezne zadeve je tako treba presojski škodljive posledice razkritja vsakega podatka oziroma dokumenta posebej, saj so lahko s predajo gradiva arhivu ogrožene ali razkrite tudi druge, še vedno aktivne zadeve. Predlagatelj zakona tako ocenjuje, da je določitev splošnega roka 50 let minimalna doba, ki še zagotavlja, da se ta nevarnost minimalizira, po tem roku pa se gradivo preda arhivu in postane javno dostopno.

S spremembo zakona se jasno razdeli arhivsko gradivo agencije na tisto, ki se nanaša na poslovanje agencije in je primerljivo z drugimi državnimi organi, ter na tisto, ki je specifično zaradi značilnosti obveščevalnega dela in sodelovanja s tujimi obveščevalnimi službami.

Prva kategorija gradiva oziroma t. i. splošno gradivo agencije se obravnava po splošnih pravilih, kot jih določata Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (v nadaljevanju: ZVDAGA) in Zakon o tajnih podatkih (v nadaljevanju: ZTP), če ta zakon tega ne ureja drugače. Za dokumente iz zbirke dokumentarnega gradiva agencije na področju splošnega poslovanja agencije torej veljajo splošni predpisi, po katerih je gradivo, ki je v pisnem strokovnem navodilu določeno kot

arhivsko v skladu s 40. členom ZVDAGA, treba izročiti pristojnemu arhivu najpozneje 30 let po nastanku, četudi vsebuje osebne ali tajne podatke. Ob predaji mora javnopravna oseba, ki gradivo izroča, v zapisniku navesti morebitne omejitve dostopnosti in razloge v skladu s 65. členom ZVDAGA – gradivo postane dostopno praviloma 40 let po nastanku (arhivsko gradivo, ki vsebuje tajne podatke) oziroma 75 let po nastanku oziroma 10 let po smrti posameznika (če vsebuje v drugem odstavku našete osebne podatke).

Za drugo kategorijo dokumentarnega gradiva, ki neposredno izhaja iz obveščevalne in protiobveščevalne dejavnosti oziroma mednarodnega sodelovanja, tj. dokumentarno gradivo iz razvida, pa je s spremembo zakona določena posebna ureditev, in sicer se določa, da le-to postane arhivsko gradivo in se preda Arhivu Republike Slovenije 50 let po zaključku posamezne zadeve. Izjemi od te določbe sta urejeni v tretjem in četrtem odstavku istega člena.

Prva izjema se nanaša na identifikacijske podatke uradnih oseb agencije in oseb, ki z agencijo sodelujejo, ter podatke o nazivu, ki ga v skladu s 45. členom ZSOVA agencija uporablja za finančno in materialno poslovanje do tretjih oseb. Ti podatki postanejo arhivsko gradivo in se predajo Arhivu Republike Slovenije po 75 letih od pridobitve oziroma nastanka tega gradiva. Predlagano podaljšanje roka za predajo tovrstnega gradiva bo zagotavljalo, da se tovrstni podatki zaščitijo pred morebitnimi zlorabami, ki bi lahko nastale, če bi se gradivo predalo pristojnemu arhivu po sedaj veljavnih rokih. Oboji podatki so namreč dodatno občutljivejši za javno razkrivanje, saj lahko neposredno negativno vplivajo na zadevne posameznike oziroma njihove družinske člane. Razkrivanje podatkov o nazivu, ki se uporablja za finančno in materialno poslovanje, pa bi lahko zaradi svoje povezanosti iz drugimi (finančnimi) podatki posredno razkrilo tudi druge tajne podatke, ki so s tem nazivom povezani ali iz njega izhajajo.

Druga izjema pa se nanaša na dokumentarno gradivo, ki vsebuje podatke, za katere je tuja obveščevalno varnostna služba ali mednarodna organizacija določila omejitve nadaljnjega posredovanja, ter podatke, ki omogočajo identifikacijo tajnih sodelavcev agencije ali pripadnikov tujih obveščevalno-varnostnih služb ali mednarodnih organizacij. Gre za specifično, še bolj občutljivo vrsto dokumentarnega gradiva z obveščevalnega in protiobveščevalnega področja, ki terja posebno ureditev tudi po izpolnitvi pogojev, navedenih v predhodnih odstavkih. Iz razloga spoštovanja t. i. *pravila tretjega* in smiselno povezane potrebe po nadaljevanju varovanja tajnosti identifikacijskih podatkov tajnih sodelavcev agencije oziroma pripadnikov tujih obveščevalno-varnostnih služb ali mednarodnih organizacij so predmetni podatki trajno hranjeni v arhivu agencije in ne bodo odstopljeni Arhivu Republike Slovenije. Dostopnost do podatkov oziroma sprememba statusa v arhivsko gradivo se bo določala v skladu z omejitvami tuje službe oziroma mednarodne organizacije ter z določili druge področne zakonodaje.

4. Pridobivanje podatkov

Uvodoma je pomembno poudariti razliko med organi pregona in agencijo. Agencija nima t. i. klasičnih policijskih pooblastil in njeno delo ni usmerjeno v kazenski pregon posameznika, temveč v varovanje interesov države in nacionalne varnosti. Dokazi, zbrani z obveščevalnim delom, tudi niso in ne morejo biti del kazenskega postopka zoper posameznika. V skladu z drugim odstavkom 8. člena ZSOVA mora agencija, kadar pri izvajanju svojih nalog ugotovi, da obstajajo utemeljeni razlogi za sum, da je določena oseba izvršila, izvršuje oziroma pripravlja ali organizira izvršitev kaznivega dejanja, za katerega se storilec preganja po uradni dolžnosti, o tem obvestiti generalnega direktorja policije in pristojnega državnega tožilca. Uporaba že obstoječih oblik tajnega pridobivanja podatkov, ki so podobne drugim primerljivim obveščevalnim službam po svetu, vključno z novima oblikama pridobivanja podatkov, že po naravi stvari predvideva drugačne razloge in pogoje za njihovo odobritev, zaradi česar ni ustrezno vzpostavljati neposredne povezave s primerljivim področjem dela v policijski zakonodaji.

Spremembe mednarodnega okolja, ki prinašajo nove oblike kompleksnih varnostnih izzivov, terjajo spremembo pooblastil agencije na področju tajnega pridobivanja podatkov oziroma posameznih posebnih oblik pridobivanja podatkov. Soočamo se z izjemnim tehnološkim napredkom, ki je prinesel množično uporabo telekomunikacijskih sredstev ter popolnoma spremenil način komuniciranja. Običajne načine komuniciranja je zamenjala izmenjava podatkov prek aplikacij, zaradi česar trenutne oblike zakonitega prestrezanja podatkov ne zadoščajo več svojemu namenu.

S spremembo zakona se uvajata novi posebni obliki pridobivanja podatkov – gre za uvedbo tehničnega sredstva za nadzor signala mobilne telefonije ter za uvedbo neposrednega dostopa do podatkov telekomunikacijskega sredstva za namen beleženja komunikacijskega prometa na sredstvu. Upošteva se raven posega v ustavno zagotovljene človekove pravice, sta spremembi smiselno umeščeni v del zakona, ki vsebuje pooblastilo agencije za kontrolo pisem in drugih pošilk oziroma nadzorovanje in snemanje telekomunikacij. Obstoječi 23. člen se spreminja tako, da pomeni napotilno določbo za vsa tri pooblastila agencije, tj. obe novi in obstoječe pooblastilo, pri katerih predsednik Vrhovnega sodišča Republike Slovenije lahko ukrep odobri ali zavrne.

Dejstvo, da je odločitev o odobritvi ali zavrnitvi ukrepa sprejme predsednik Vrhovnega sodišča Republike Slovenije, pomeni odobritev s strani najvišje sodne avtoritete, ki hkrati zagotavlja tudi najvišjo stopnjo strokovnosti in izkušenosti. S stalnim oziroma kontinuiranim obravnavanjem takšnih odredb pridobivata predsednik oziroma v njegovi odsotnosti njegov namestnik pomembne praktične izkušnje in jasne meje za presojo, v katerih primerih so zadostno utemeljeni posamezni zakonski pogoji in obrazloženi dokazni standardi. Navedeno omogoča predsedniku in oziroma njegovemu namestniku tudi neko obliko notranje sodne kontrole, s katero se vzpostavlja možnost graditve dobre prakse in učenja na predhodnih primerih. Nenazadnje takšna praksa omogoča tudi boljše poznavanje in razumevanje področja obveščevalne dejavnosti in s tem tudi dela agencije.

Zakonska opredelitev novih pooblastil je zaradi zagotavljanja kontinuitete in jasnosti v zakonu oblikovana po vzoru že veljavnih pooblastil. Z opredelitvijo kar največ elementov in podrobnosti v zakonu se izkazuje ustrezna stopnja transparentnosti in strokovnosti izvajanja novih dveh pooblastil.

Pri vseh treh oblikah pooblastil agencije obstaja enotni standard, v skladu s katerim mora biti podana velika verjetnost, da obstaja nevarnost za varnost države, ki pa se nadalje izkazuje v treh različnih aktivnostih, upošteva se intenziteto posega posameznega pooblastila agencije v ustavno zagotovljene človekove pravice in temeljne svoboščine. Vrstni red predmetnih pooblastil agencije oziroma ukrepov je oblikovan od najblažjega do najbolj invazivnega. Najblažji ukrep v zasebnost je uporaba tehničnega sredstva za nadzor signala mobilne telefonije, sledi že obstoječa kontrola pisem in drugih pošilk z nadzorovanjem in s snemanjem telekomunikacij, medtem ko pomeni najbolj invaziven ukrep v zasebnost neposredni dostop do podatkov telekomunikacijskega sredstva in beleženje komunikacijskega prometa na sredstvu. V skladu z navedenim so stopnjevani tudi pogoji in omejitve, ki ustrezno sledijo navedenemu stopnjevanju posameznih pooblastil.

Vsebinska opredelitev nove posebne oblike pridobivanja podatkov, tj. uporaba tehničnega sredstva za nadzor signala mobilne telefonije, je samostojno urejena v novem 23.a členu zakona. Predlagatelj zakona uvodoma pojasnjuje, da se bo v okviru tega pooblastila uporabljalo zgolj tehnično sredstvo, ki omogoča identifikacijo mobilnih komunikacijskih signalov, ne pa tudi vpogled v vsebino komunikacij ali metapodatke. Rezultat bo presek mobilnih signalov, in sicer le tistih, ki se bodo pojavljali na več varnostno relevantnih lokacijah oziroma v več varnostno relevantnih situacijah, medtem ko se podatki o drugih signalih ne bodo obdelovali niti hranili. Dodatno omejitev pomeni kratko obdobje uporabe tehničnega sredstva za nadzor signala mobilne telefonije, in sicer je tehnično sredstvo dovoljeno uporabljati le 15 dni, brez možnosti podaljšanja. Gre za minimalno obdobje, ki še omogoča analitično obdelavo podatkov na relevantnem vzorcu ter s tem avtomatsko izločanje nerelevantnih signalov, s čimer se tudi dodatno varuje komunikacijska zasebnost tretjih oseb. Prav tako ni dovoljena uporaba

tehničnega sredstva, ki omogočajo ali bi lahko omogočala prisluškovanje in snemanje elektronskih komunikacij, ter ugotavljanje lokacije komunikacijskih sredstev tretjih oseb.

Uporaba tehničnega sredstva za nadzor signala mobilne telefonije je opredeljena kot nova oblika pridobivanja podatkov, pri čemer se poudarja uporaba tehničnega sredstva kot delovnega pripomočka. Njegova uporaba bo namreč neke vrste prehodna faza, ki bo agenciji pomagala pri identifikaciji oziroma določanju potencialnih novih relevantnih posameznikov, ki bi na podlagi pridobljenih podatkov postali predmet sistematične operativne obravnave v skladu s 14. členom ZSOVA. Smiselno podobno je bila v policiji uvedena uporaba poligrafa, ki je zgolj pomagalo pri izločanju kroga osumljencev.

Agencija bo morala kot predlagateljica ukrepa v predlogu odredbe izkazati za vsak primer posebej obstoj velike verjetnosti, da obstaja nevarnost za varnost države, ki se kaže v alternativno naštetih aktivnostih. Aktivnosti izhajajo iz obstoječega 24. člena zakona, pri čemer je bil smiselno upoštevan blažji poseg v človekove pravice posameznikov, zato so aktivnosti v posameznih primerih splošneje opredeljene, da lahko zajamejo več potencialno relevantnih situacij.

Nadalje bo treba v predlogu odredbe izkazati, da je utemeljeno pričakovati, da bo na določenem območju in v določenem časovnem obdobju tako možno identificirati osebe, ki izvajajo navedene aktivnosti, oziroma ugotoviti komunikacijska ali druga tehnična sredstva, ki se uporabljajo za te aktivnosti. Kot že pojasnjeno, se tehnično sredstvo uporabi za identifikacijo mobilnih naprav, ki se uporabljajo na določenem mestu v določenem času, če je znana lokacija osebe, zoper katero je ukrep odrejen, niso pa znane podrobnosti glede mobilne naprave, ki jo uporablja. Zlasti je to relevantno v primeru predplačniških mobilnih naprav. Pri tem bo morala agencija tudi utemeljiti, da teh podatkov ni možno pridobiti na milejši način oziroma da bi bilo to povezano z nesorazmernimi težavami.

V okviru predmetnega ukrepa ne bo omogočeno prisluškovanje in snemanje elektronskih komunikacij, čemur bo agencija sledila tudi pri opredelitvi tehničnih karakteristik sredstva pri nakupu, saj bo izbrala takšnega, ki te funkcije ne omogoča. Posebej je tudi določeno, da ni dovoljeno ugotavljanje lokacije komunikacijskih sredstev tretjih oseb, s čimer se dodano potrjuje prvotni namen uporabe tehničnega sredstva.

Z opredelitvijo vsebine predloga in odredbe se nadaljuje obstoječ način odobravanja ukrepov pri predsedniku Vrhovnega sodišča Republike Slovenije, saj se sledi strukturi in že poznanemu postopku za odobritev ukrepa kontrole pisem in drugih pošilk ter nadzorovanja in snemanja telekomunikacij. Določena je tudi časovna opredelitev trajanja ukrepa, in sicer gre za rok 15 dni, brez možnosti podaljšanja. Tako omejeno časovno obdobje uporabe sredstva, z dodatno omejitvijo, da ni možno njegovo podaljšanje, pomeni pomembno varovalko ustavno zagotovljenih človekovih pravic, saj bo agencija morala temeljito pretehtati okoliščine, kdaj in kako bo lahko uporabila to sredstvo. Kratek čas uporabe zagotavlja bolj osredotočeno in usmerjeno uporabo, ki bo posledično pomenila tudi manjši poseg za tretje osebe. Tehnično sredstvo se preneha uporabljati takoj, ko prenehajo razlogi, zaradi katerih je bila odrejena njegova uporaba oziroma po preteku časovnega obdobja, določenega v odredbi. O prenehanju mora direktor agencije pisno obvestiti predsednika Vrhovnega sodišča Republike Slovenije.

Agencija bo lahko obdelovala osebne podatke oseb, za katere ugotavlja, da ne sodelujejo pri izvajanju aktivnosti iz prvega odstavka, zgolj v obsegu, ki je iz tehničnih razlogov neizogibno potreben za doseg namena iz prvega odstavka tega člena, in na način, ki najmanj posega v njihove pravice. Agencija sme začasno uporabiti podatke tretjih oseb izključno za ugotavljanje identitete oseb, zoper katere so usmerjene aktivnosti iz prvega odstavka, in jih po zaključku aktivnosti nemudoma izbrisati.

Po vsakem zaključku uporabe tehničnega sredstva mora agencija pripraviti poročilo o izvedeni aktivnosti in ga skupaj z zbranimi podatki posredovati v seznanitev predsedniku Vrhovnega sodišča

Republike Slovenije. S to določbo se omogoča t. i. zapisniška sledljivost izvedbe ukrepa in pridobljenih podatkov. Predsednik Vrhovnega sodišča Republike Slovenije odredi brisanje podatkov, za katere oceni, da niso potrebni za dosego namena iz prvega odstavka tega člena.

Dodana je tudi posebna določba, na podlagi katere je pod določenimi pogoji o izvedbi ukrepa obveščen tudi nadzorovani posameznik, s čimer mu je dana možnost, da zahteva naknadno sodno varstvo. Po zaključitvi zadeve v razvidu direktor agencije obvesti posameznika, na katerega se je ukrep nanašal, da ima pravico, seznaniti se s pridobljenim gradivom, v primerih večjega obsega tega gradiva pa s poročilom, ki obsega povzetek zbranega gradiva. Dodana je omejitev te pravice, in sicer se lahko v primerih, kadar je mogoče utemeljeno sklepati, da bo zaradi seznanitve z gradivom nastala nevarnost za življenje ali zdravje ljudi ali za nacionalno varnost, direktor agencije odloči, da posameznika z vsebino pridobljenega gradiva ne bo seznanil. Takšno gradivo bo v skladu z določbami tega zakona, ki ureja dokumentarno gradivo agencije iz razvida, po poteku določenega roka postalo arhivsko gradivo.

Poleg naštetih varovalk je dodana tudi obveznost agencije, da najmanj enkrat na leto pripravi poročilo o nadzoru nad uporabo tehničnega sredstva za nadzor signala mobilne telefonije in z njim seznanil predsednika Vrhovnega sodišča Republike Slovenije. Gre za t. i. periodično poročilo, ki pomeni preplet internega in sodnega nadzora nad izvajanjem tega pooblastila agencije. Postopek uporabe tehničnega sredstva bo agencija opredelila v internem aktu, h kateremu bo podala soglasje Vlada Republike Slovenije.

Upošteva je tehnične omejitve tehničnega sredstva ter vzpostavljenega notranjega in zunanjega nadzora, z obveznostjo periodičnega poročanja o njegovi uporabi, predlagateljica zakona meni, da je vzpostavljen primeren sistem uporabe tehničnega sredstva, ki je ustrezen in zadosten za zagotavljanje varstva človekovih pravic in svoboščin na eni strani ter zagotavljanja nacionalne varnosti na drugi. Razvoj tehnologije in prepletenost vsakdanjega življenja s telekomunikacijskimi napravami zahtevajo ustrezen odziv državnih organov, da se tovrstna sredstva, ki so sicer dostopna na trgu, uporabljajo zakonito. S tem se pomembno prispeva k obvladovanju virov ogrožanja varnosti in varnostnih tveganj za Republiko Slovenijo in širšo mednarodno skupnost.

Druga sprememba oziroma nova posebna oblika pridobivanja podatkov je predstavljena v novem a24.c členu predloga zakona. Gre za odobritev neposrednega dostopa do podatkov telekomunikacijskega sredstva za namen beleženja komunikacijskega prometa na sredstvu v Republiki Sloveniji.

Tak ukrep je v veljavi npr. na Norveškem, kjer ima zunanja obveščevalna služba NIS zakonsko pooblastilo za zbiranje (elektronskih) podatkov, ki niso javno dostopni v računalniških in podobnih sistemih.⁴ Podobno spremembo uvaja tudi Republika Avstrija, ki v predlagani spremembi Zakona o varnostni in obveščevalni službi⁵ za svojo varnostno in obveščevalno službo DSN⁶ uvaja možnost prestrezanja sporočil in informacij, ki se pošiljajo, posredujejo ali sprejemajo v šifrirani obliki, s programom, ki se z uporabo tehničnih sredstev naloži na računalniški sistem posameznika. V skladu s predlagano spremembo bo ukrep mogoče odobriti, kadar izvedba naloge z uporabo drugih preiskovalnih ukrepov sicer ne bi bila učinkovita, odobri pa se lahko pri zveznem upravnem sodišču, s predhodnim posvetovanjem pri pooblaščenca za pravno varstvo ter z obvestitvijo zveznega ministra za notranje zadeve. Ukrep se lahko odobri za obdobje treh mesecev, z možnostjo podaljšanja. Sprememba zakona predvideva tudi opredelitev tehničnega vidika izvedbe ukrepa, z obveznostjo

⁴ Act of 19 June 2020 no. 77 relating to the Norwegian Intelligence Service (the Intelligence Service Act), Chapter 6 – Methods of information collection that could entail interference against persons, Section 6-10 – End point collection).

⁵ Das Staatsschutz- und Nachrichtendienst-Gesetz (SNG).

⁶ Directorate State Protection and Intelligence Service (DSN), Federal Ministry, Republic of Austria, Interior.

odstranitve oziroma onesposobitve nameščenega programa po zaključku preiskovalnega ukrepa. Po izteku obdobja, za katerega je bila izdana odredba, je treba posameznika, ki je bil predmet odredbe, seznaniti z uvedenim ukrepom; prav tako je treba seznaniti z uvedenim ukrepom tudi tiste osebe, ki so poslane, posredovale ali prejele sporočilo, ki je bilo nadalje obravnavano v ukrepu, kadar je njihova identiteta znana ali jo je možno ugotoviti brez večjega truda.

Predlagateljica zakona se zaveda, da uporaba tehničnega sredstva za neposredni dostop do podatkov telekomunikacijskega sredstva za namen beleženja komunikacijskega prometa na sredstvu pomeni invaziven poseg v ustavno zagotovljene človekove pravice, zaradi česar si je pri pripravi besedila določb spremembe zakona prizadevala za čim jasnejšo in določno opredelitev pogojev in zahtev za uporabo. Upošteva konkretno opredeljene situacije oziroma aktivnosti tujih ali domačih akterjev, ki pomenijo nevarnost za varnost države in ki opravičujejo uporabo tehničnega sredstva, po mnenju predlagateljice ustrezno zamejujejo (potencialni širši) obseg njegove uporabe. Določnost pogojev oziroma zahtev v zakonu pa hkrati pomeni tudi lažji pregled nad njihovim izpolnjevanjem, kar je dobrodošlo predvsem pri postopku odobritve predlogov uporabe in tudi kasnejšega nadzora.

Predviden je večstopenjski sodni nadzor (pred odobritvijo in med njo, po neposrednem zaključku uporabe sredstva v posameznem primeru in naknadni periodični nadzor), interni nadzor in tudi nadzor posebnega Pooblaščenca za nadzor, ki pomeni novo obliko nadzora nad izvajanjem ukrepa. Vse navedene oblike nadzora se v prepletajo in si vzajemno zagotavljajo izmenjavo relevantnih informacij. Nad izvajanjem dejavnosti agencije bo še naprej bdela tudi Komisija za nadzor obveščevalnih in varnostnih služb v skladu s svojimi zakonskimi pooblastili.

V Sloveniji bo predmetni ukrep na predlog direktorja agencije odobril oziroma zavrnil za vsak primer posebej predsednik Vrhovnega sodišča Republike Slovenije. Pogoji za pridobitev odobritve odredbe za ta ukrep so sicer v osnovi enaki kot za odobritev kontrole pisem in drugih pošilk ter nadzorovanje in snemanje telekomunikacij iz obstoječega 24. člena ZSOVA, pri čemer bo za odobritev neposrednega dostopa za namen beleženja telekomunikacijskega prometa na sredstvu treba izkazati okoliščine, ki bodo zahtevale takojšnje ukrepanje in nujno sprejetje ustreznih ukrepov za zaščito nacionalne varnosti, pri čemer tega namena ni mogoče doseči z drugimi (obstoječimi) ukrepi iz tega zakona.

Agencija bo lahko predlagala uvedbo te posebne oblike pridobivanja podatkov le v primeru taksativno naštetih situacij, ko bo podana velika verjetnost, da obstaja nevarnost za varnost države, ki se bo izkazovala v opredeljenih neposrednih sedanjih ali predvidljivih aktivnostih, povezanih z ogrožanjem nacionalne varnosti. Opredelitev aktivnosti, ki bodo morale izpolnjevati pogoj resničnosti in sedanjosti ali predvidljivosti, je tako smiselno povzet po primerljivi praksi Sodišča Evropske unije.⁷ Gre za najhujše oblike ogrožanja nacionalne varnosti, ki bodo zaradi svoje resnosti, neposrednosti in sedanjosti oziroma predvidljivosti v prihodnosti s konkretizacijo v obrazložitvi upravičile poseg v ustavno zagotovljene človekove pravice.

Dokazni standard, kot je oblikovan in pripoznan pri delovanju obveščevalnih služb, je torej v primeru odobritve uporabe predmetne posebne oblike najstrožji, s čimer se pomembno oddalji od aktivnosti, za katere se uporabljajo druge, zlasti t. i. klasične metode pridobivanja podatkov na obveščevalnem področju. Ukrep in njegova odobritev sta neposredno povezana s primeri izjemnih varnostnih situacij, s čimer se omejuje uporaba predmetnega tehničnega sredstva, hkrati pa agenciji omogoča, da se v

⁷ Zadeva C-511/18 – La Quadrature du Net in drugi (ECLI:EU:C:2020:791), cit. 177: *"posebej resen poseg, ki ga pomeni splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji, ..., ter posebej resen poseg, ki ga pomeni avtomatizirana analiza teh podatkov, izpolnita zahtevo po sorazmernosti zgolj v položajih, ko se država članica spopada z resno grožnjo nacionalni varnosti, ki se izkaže za resnično in sedanjo ali predvidljivo..."*.

situacijah, ko nacionalni varnosti grozi neposredna sedanja oziroma predvidljiva prihodnja nevarnost, ustrezno odzove.

Agencija bo morala v predlogu odredbe jasno izkazati obstoj enega ali več od navedenih aktivnosti, hkrati pa utemeljiti prepričanje, da se v zvezi s to aktivnostjo uporablja določeno telekomunikacijsko sredstvo ali bo to sredstvo uporabljeno. Dodaten pogoj pomeni obrazložitev agencije, da je mogoče utemeljeno sklepati, da teh podatkov ni možno pridobiti drugače oziroma bi njihovo pridobivanje na drug način oziroma z drugo obliko lahko ogrozilo življenje ali zdravje ljudi oziroma bi pomenilo resno grožnjo nacionalni varnosti. Upošteva se najvišjo stopnjo invazivnosti ukrepa se torej tudi pri zadostitvi načela oziroma pogoja subsidiarnosti upošteva stopnja nevarnosti za javno varnost oziroma resna grožnja nacionalni varnosti.

Posebej sta navedeni tudi dve izrecni omejitvi agencije, in sicer se bo moralo tehnično sredstvo za izvajanje neposrednega dostopa do podatkov telekomunikacijskega sredstva za namen beleženja komunikacijskega prometa na sredstvu uporabljati tako, da bo omogočena namestitvev in s tem izvedba ukrepa brez vstopa v tuje stanovanje oziroma v druge prostore. Prav tako v okviru te oblike ne bo dovoljeno poseganje v vsebino komunikacije na njeno spreminjanje, dopolnjevanje ali kakšno koli drugo predrugačenje. S tem se postavljajo jasne meje delovanja agencije in s tem pomembna zamejitev pri poseganju v ustavno zagotovljene človekove pravice in temeljne svoboščine.

Jasno je določena vsebina predloga in odredbe, vključno z natančno opredelitvijo nujno potrebne spremembe na telekomunikacijskem sredstvu, ki je potrebna za dostop do podatkov in spremljanje oziroma beleženje komunikacijskega prometa.

Tehnično sredstvo se uporablja najkrajši možni čas za doseg zakonsko opredeljenega namena, vendar ne dlje kot en mesec od prejema odredbe predsednika Vrhovnega sodišča Republike Slovenije. Možno je podaljšanje ukrepa, vendar skupno ne več kot tri mesece. Njegova uporaba se odpravi takoj, ko prenehajo razlogi, zaradi katerih je bila odrejena oziroma po preteku časovnega obdobja, določenega v odredbi. Pri tem mora agencija tehnično zagotoviti, da se nameščeni program odstrani oziroma onesposobi. O prenehanju direktor agencije pisno obvesti predsednika Vrhovnega sodišča Republike Slovenije. Agencija lahko obdeluje osebne podatke tretjih oseb zgolj v obsegu, ki je iz tehničnih razlogov neizogibno potreben za doseg namena iz prvega odstavka tega člena in na način, ki najmanj posega v njihove pravice.

Po zaključku uporabe tehničnega sredstva agencija pripravi poročilo o izvedeni aktivnosti ter ga skupaj z zbranimi podatki posreduje v seznanitev predsedniku Vrhovnega sodišča Republike Slovenije. Ta odredi brisanje podatkov, za katere oceni, da niso potrebni za doseg namena iz prvega odstavka tega člena. Z navedenim se zadosti pogoju zapisniške sledljivosti. O izvedbi ukrepa je pod določenimi pogoji obveščen tudi nadzorovani posameznik, s čimer mu je dana možnost, da zahteva naknadno sodno varstvo.

Izvajanje nadzora nad omenjeno obliko bo večstopenjsko. Poleg sodnega nadzora je uveden tudi t. i. periodični nadzor nad zakonitostjo uporabe tehničnega sredstva, ki pomeni preplet internega in sodnega nadzora. Dodatno obliko nadzora pomeni nov *sui generis* institut, tj. pooblaščenec za nadzor, ki bo izvajal strokovni nadzor tako, da bo med izvajanjem posebne oblike pridobivanja podatkov oziroma po zaključku izvajanja le-tega presojal, ali se ukrep izvaja v skladu s predvidenimi postopki in tehnično ustrezno. Z ugotovitvami bo seznanjal neposredno agencijo in predsednika Vrhovnega sodišča Republike Slovenije, s čimer se bo smiselno zaokrožil nadzorni cikel. Tako agencija kot predsednik Vrhovnega sodišča bosta prejela dodatno informacijo o morebitnih nepravilnostih in se v skladu s tem ustrezno odzvala, o morebitnih nepravilnostih pa bo obveščena tudi Komisija za nadzor obveščevalnih in varnostnih služb. Namen izvajanja predmetne nadzorne funkcije je poleg zagotavljanja strokovnosti in zakonitosti dela prispevek k oblikovanju dobre prakse odobravanja odredbe ter posledično tudi krepitev transparentnosti delovanja agencije.

Podrobnejši način uporabe tehničnega sredstva bo agencija opredelila v svojem internem aktu, h kateremu bo soglasje podala Vlada Republike Slovenije.

Gre za novo in samostojno posebno obliko pridobivanja podatkov, ki jo bo v celoti izvajala agencija. Iz zapisanega izhaja, da bo morala agencija izpolniti vse predpisane zakonske pogoje, prav tako bo morala med uporabo sredstva spoštovati načeli sorazmernosti in nujnosti. Agencija bo morala pridobljene podatke obravnavati tudi v skladu s področno zakonodajo s področja varstva osebnih podatkov in tajnih podatkov, kar rezultira še v dodatnih varnostnih mehanizmih.

Obstoječi 24.c člen je nepotreben, saj je vsebina o načinu nadomeščanja predsednika Vrhovnega sodišča Republike Slovenije že določena v matičnem zakonu, ki ureja sodišča. Ponavljanje iste vsebine je nepotrebno in pravnosistemsko nedopustno, zato se predlaga njegovo črtanje.

5. Delovnopравни status delavcev agencije

Na področju delovnoppravnega statusa delavcev agencije vključuje predlog sprememb in dopolnitev zakona več vidikov, pri čemer se prvi nanaša na postopke zaposlitve v agenciji. Postopki zaposlitve v agenciji se pomembno razlikujejo od zaposlitve v drugih organih javne uprave, čemur mora slediti tudi zakonodaja. Ob zadnji spremembi zakona, ki ureja položaj javnih uslužbencev, se je pričela uveljavljati centralizacija zaposlitve, ki za uslužbenca agencije in kandidate za zaposlitev v njej ne more veljati. Varovanje zaupnosti njihove identitete je namreč ključno za uspešno opravljanje dela. S predmetno spremembo 28. člena zakona se bodo tako nedvoumno določile pristojnosti agencije na področju zaposlovanja in s tem razmejila tudi vloga ministrstva, pristojnega za javno upravo.

Kadar bo to primerno, lahko agencija zaprosi ministrstvo, pristojno javno upravo, za strokovno pomoč pri posameznih fazah postopka, kot so pomoč pri presoji osebnih sposobnosti in veščin za opravljanje dela v drugem delu izbirnega postopka v javnem natečaju, pomoč pri razvoju sistema osebnih sposobnosti in veščin za opravljanje dela ter drugih orodij za ravnanje s kadri v organih državne uprave in druge naloge na področju ravnanja s kadri v skladu s pristojnostmi ministrstva, pristojnega za javno upravo.

Naslednja sprememba uvaja posebno ureditev glede časovne omejitve dnevne delovne obveznosti in dnevnega oziroma tedenskega počitka. Delo uradnih oseb agencije je specifično in ga je pogosto težko načrtovati vnaprej, saj je v marsičem odvisno od varnostno relevantnih dogodkov, na katere ni možno vplivati, ali pa so obveznosti vezane na sodelovanje s tajnimi sodelavci, kjer je nujno prilagajanje uslužbencev agencije. Zaradi tega se pojavljajo situacije, ko je treba delo nadaljevati tudi po izteku delovnega časa, posledično pa uslužbencu ni mogoče zagotoviti dnevnega počitka v skladu s splošnimi predpisi. Predlog spremembe zakona tako predvideva rešitev, da se zakonska omejitev dnevne delovne obremenitve spremeni v primerih, ko je to nujno zaradi izvajanja nalog agencije. Navedena sprememba bo omogočila, da se bo agencija lažje soočala s kritičnimi oziroma z nepričakovanimi varnostnimi situacijami, s tem pa bo tudi omogočeno zagotavljanje nacionalne varnosti države. Taka odreditev nadurnega dela bo mogoča le v izjemnih razmerah in situacijah, v katerih ni mogoče zagotoviti, da bi delo opravila druga uradna oseba agencije. Posledično ni možno niti, da bi uradna oseba imela možnost soglašati z odrejenim delom. Zaradi nujnosti je mogoče v takih primerih nadurno delo odrediti ustno, pisna odredba pa se pripravi in vroči naknadno.

V predlog zakona so vgrajena dodatne varovalke, ki bodo omejevale tovrstno odrejanje dela preko polnega delovnega časa, s čimer se bodo še vedno varovale pravice delavcev. Tako je določeno, da je taka odreditev dela dopustna le za najkrajši možni čas, uslužbencu pa mora delodajalec takoj po prenehanju razlogov, zaradi katerih je ta opravljal delo preko omejitev, določenih s splošnimi predpisi, zagotoviti sorazmerno daljši počitek, določene pa so tudi maksimalne tedenske in mesečne obremenitve, čez katere uslužbenca ni dovoljeno dodatno obremenjevati.

Tretja sprememba pa se nanaša na uvedbo stalne pripravljenosti na delovnih mestih, kjer obstaja dejanska možnost, da bo treba delo opraviti zunaj delovnega časa. Narava dela agencije je taka, da mora biti agencija pripravljena, da se v primeru izrednih dogodkov nemudoma odzove. V ta namen mora imeti na voljo tako osebje, ki takšne naloge nemudoma izvrši, kot tudi osebje, ki skrbi za to, da so sredstva za izvajanje nalog agencije stalno na voljo. Sprememba je povezana tudi s priporočilom Računskega sodišča Republike Slovenije, ki je po opravljenem nadzoru izdalo priporočilo, da se navedeni institut vključi v matični zakon agencije. Institut pripravljenosti za delo je kot poseben delovni pogoji urejen v novem osmem odstavku, v katerem je določeno, da mora biti uradna oseba agencije seznanjena z odrejeno pripravljenostjo za delo najmanj tri dni vnaprej po razporedu dela oziroma s posebno odredbo. Uradna oseba agencije mora biti za potrebe prihoda na delovno mesto ali kraj, kjer je treba opraviti nujno nalogo, dosegljiva po telefonu ali drugih komunikacijskih sredstvih.

6. Redakcijski popravki

Nomotehnično se popravlja določba obstoječega 4.a člena in črta obstoječi 24.c člen, saj je določba nepotrebna zaradi urejenosti v matičnem zakonu.

3. OCENA FINANČNIH POSLEDIC PREDLOGA ZAKONA ZA DRŽAVNI PRORAČUN IN DRUGA JAVNA FINANČNA SREDSTVA

Predlog zakona nima finančnih posledic za državni proračun in za druga javna finančna sredstva.

4. NAVEDBA, DA SO SREDSTVA ZA IZVAJANJE ZAKONA V DRŽAVNEM PRORAČUNU ZAGOTOVLJENA, ČE PREDLOG ZAKONA PREDVIDEVA PORABO PRORAČUNSKIH SREDSTEV V OBDOBJU, ZA KATERO JE BIL DRŽAVNI PRORAČUN ŽE SPREJET

Za izvajanje zakona dodatnih finančnih sredstev v sprejetem državnem proračunu ni treba zagotoviti.

5. PRIKAZ UREDITVE V DRUGIH PRAVNIH SISTEMIH IN PRILAGOJENOSTI PREDLAGANE UREDITVE PRAVU EVROPSKE UNIJE

Predloga zakona o spremembah Zakona o Slovenski obveščevalno-varnostni agenciji (EVA 2025-1524-0001) ni predmet usklajevanja s pravnim redom Evropske unije.

5.1 Prilagojenost predlagane ureditve pravu Evropske unije

V skladu s Pogodbo o delovanju Evropske unije in z določbo drugega odstavka 4. člena je področje nacionalne varnosti v izključni pristojnosti vsake države članice, torej v tem primeru Republike Slovenije.

Ostala področja, kot so npr. delovnopravno področje in finančno poslovanje agencije kot organa državne uprave, pa so skladna z veljavnimi pravnimi akti Republike Slovenije. Ti akti morajo biti zaradi članstva države v Evropski uniji harmonizirani in usklajeni s pravom Evropske unije.

Predlog zakona ni predmet usklajevanja s pravnim redom EU.

5.2 Primerjalnopravna ureditev

1. Republika Hrvaška

V Republiki Hrvaški področje delovanja obveščevalno-varnostnih služb celovito ureja Zakon o varnostno obveščevalnem sistemu Republike Hrvaške,⁸ ki ureja delovanje varnostno-obveščevalne agencije (Sigurnostno-obaveščajna agencija; v nadaljevanju: SOA), Vojaške varnostno-obveščevalne agencije, Sveta za nacionalno varnost, Sveta za koordinacijo varnostno-obveščevalnih agencij, Urada Sveta za nacionalno varnost, Zavoda za varnost informacijskih sistemov ter Operativno-tehnični center za nadzor telekomunikacij.

SOA, kot Slovenski obveščevalno-varnostni agenciji (Sovi) sorodna organizacija, ima podobno, čeprav nekoliko širše urejeno področje delovanja, in sicer: pridobivanje, analiza, obdelava in vrednotenje političnih, gospodarskih, znanstveno-tehnoloških in varnostnih podatkov v povezavi s tujino, ki so pomembne za hrvaško nacionalno varnost. Posebej so poudarjena nekatera področja delovanja, kot so terorizem in druge oblike organiziranega nasilja, obveščevalne dejavnosti tujih obveščevalnih služb in posameznikov, ekstremistične organizacije, grožnje najvišjim državnim predstavnikom, organizirani gospodarski kriminal, izdaja tajnih podatkov idr.

Pri pridobivanju podatkov ima SOA pravico vpogledati v vse evidence in registre, če pa je mogoče, se ji vzpostavi tudi trajen oddaljeni računalniški dostop do njih. Vsi dostopi oziroma vpogledi v podatke so sicer zabeleženi, vendar tako, da se ne razkriva identiteta osebe, ki je do podatkov dostopala, saj zakon vzpostavlja dolžnost varovanja tajnosti uslužbencev SOA, kot tudi nalaga dolžnost skrbnikom evidenc, da ne razkrivajo vpogledov (potencialnih interesov) SOA.

SOA lahko, če podatkov ni možno pridobiti drugače oziroma je njihova pridobitev povezana z nesorazmernimi ovirami, uporabi tudi posebne oblike pridobivanja podatkov, s katerimi se posega v zagotovljene človekove pravice in svoboščine, in sicer:

- tajni nadzor nad vsebino komunikacij;
- tajni nadzor podatkov o telekomunikacijskem prometu;
- tajni nadzor lokacije uporabnika;
- tajni nadzor mednarodnih telekomunikacij;
- tajni nadzor nad poštnimi in drugimi pošiljkami;
- tajni nadzor in tehnično snemanje v notranjosti objektov in zaprtih prostorih ter predmetov;
- tajno opazovanje in sledenje s sredstvi za zvočno in videodokumentiranje na odprtih in javnih mestih;
- tajni odkup predmetov.

Posebne oblike pridobivanja podatkov se odredijo z odredbo. Glede na intenzivnost posega v zasebnost posameznikov zakon določa, da odredbe za tajni nadzor vsebine komunikacij, tajni nadzor nad poštnimi in drugimi pošiljkami, tajni nadzor in tehnično snemanje v notranjosti objektov, zaprtih prostorih ter predmetov in tajni odkup predmetov odreja sodnik vrhovnega sodišča, vse ostale pa direktor SOA. Posebne oblike, ki jih odobravajo sodniki vrhovnega sodišča, so lahko uvedene največ za 4 mesece, vendar se lahko po potrebi podaljšajo. O podaljšanju odloča senat treh sodnikov vrhovnega sodišča.

Za svoje poslovanje lahko SOA izvaja metode prikritega poslovanja oziroma uporabe t. i. legendiranih nazivov ali tudi ustanavljanja tajnih družb oziroma družb s skritim ali fiktivnim lastništvom, pri čemer lahko sklepajo tajne dogovore z drugimi fizičnimi in pravnimi osebami za doseganje konspirativnosti njenega delovanja, tajnosti njenih uslužbencev in lastništva nad podjetji in stvarmi.

SOA lahko na podlagi pogodb o mednarodnem sodelovanju sodeluje tudi s tujimi obveščevalnimi službami in si z njimi izmenjuje podatke, opremo ali izvaja naloge z njenega delovnega področja. O sodelovanju oziroma prenehanju sodelovanja s tujo obveščevalno službo ali podobno organizacijo odloča Svet za nacionalno varnost na podlagi predloga direktorja SOA. Če je izkazana resna nevarnost za nacionalno varnost države, ki je pogodbeni partnerica, in ta nevarnost izvira od državljanov Republike Hrvaške, lahko tuji obveščevalni službi posreduje celo podatke o njem, s katerimi razpolaga.

⁸ Zakon o sigurnostno-obaveščajnom sustavu Republike Hrvatske, Klasa: 011-01/06-01/26, Urbroj: 71-05-03/1-06-2, sprejet 5. 7. 2006.

Na delovnopravnem področju hrvaški zakon prav tako določa nekatere izjeme od običajnega zaposlovanja uslužbencev, ki veljajo specifično za SOA. Poleg dodatkov, do katerih so njeni uslužbenci na podlagi specifik svoje zaposlitve upravičeni, velja tudi izjema od zahteve za javno objavo oziroma razpisa za prosta delovna mesta, obvezno varnostno preverjanje bodočega zaposlenega, odstop od dolžnosti pojasnitve razlogov za neizbiro kandidata za zaposlitev, zagotavljanje tajnosti svojih uslužbencev idr.

Nadzor nad delovanjem SOA izvajajo državni zbor, Urad Sveta za nacionalno varnost ter Svet za državljanski nadzor nad varnostno-obveščevalnimi agencijami. Slednji je sestavljen iz 7 članov z mandatom 4 leta, ki jih imenuje državni zbor. Vsi člani morajo biti strokovnjaki s svojega področja, pri čemer mora biti po vsaj en predstavnik pravne, politične in elektrotehnične stroke.

2. Zvezna republika Nemčija

Bundesnachrichtendienst (v nadaljevanju: BND) je zunanja obveščevalna služba Zvezne republike Nemčije, ki zbira politične, gospodarske in vojaške tuje obveščevalne podatke za varstvo Nemčije znotraj pravnega okvira. Kot višji zvezni organ so podrejeni zvezni vladi. Njihovo delo ureja poseben zakon, in sicer t. i. BND-Gesetz (v nadaljevanju: BND-zakon). BND nima policijskih pooblastil.

BND lahko obdeluje informacije, vključno z osebnimi podatki, razen v primeru, da je to prepovedano v skladu z zveznim zakonom, ki ureja osebne podatke. Razlog obdelave podatkov mora biti naveden. Poseben poudarek je na varovanju podatkov zaposlenih BND, objektov BND in virov, ki jih BND uporablja pri svojem delu ali za svoje delo. Hramba, sprememba in uporaba osebnih podatkov je dovoljena v obsegu zakonskih pooblastil BND, da se opravijo njene naloge. Popravek in brisanje osebnih podatkov je omejeno na deset let, omejitev procesiranja osebnih podatkov pa mora biti pregledana najkasneje po desetih letih. Posamezniki lahko zaprosijo BND, ali o njih zbirajo podatke, in BND jih mora o tem obvestiti. Zakon ureja tudi prenos osebnih podatkov k BND in od nje ter uporabo podatkov v združenih evidencah tako z domačimi kot s tujimi subjekti.

BND uporablja različne obveščevalne metode za izpolnjevanje svojega zakonskega poslanstva. Te metode, ki so zakonsko določene tako po vsebini kot obsegu, so:

- IMINT – slikovna inteligenca – pridobivanje podatkov iz satelitskih in zračnih slik;
- OSINT – odprtokodna inteligenca – pridobivanje podatkov iz javnih informacij, tako tiskanih kot digitalnih, v nacionalnem in tujih jezikih;
- SIGINT – obveščevalni signali – pregled različnih elektronskih komunikacij;
- HUMINT – človeška inteligenca – pridobivanje podatkov s človeškimi viri;
- SOCMINT – Social Media Intelligence – pridobivanje podatkov iz družbenih medijev kot odprtokodnega informacijskega sistema.
- GEOINT – geoprostorska inteligenca – pridobivanje podatkov z geografskih lokacij.

Prepovedano je zbiranje zasebnih podatkov posameznikov. Vsako zbiranje podatkov in uporaba le-teh mora upoštevati stroge zakonske okvire.

Zakon dovoljuje obdelavo osebnih podatkov tako na podlagi selektorjev kot tudi prometnih podatkov, ki ne temeljijo na selektorjih.

Zakon opredeljuje tudi neodvisni pravni pregled, in sicer ga izvaja neodvisna nadzorna komisija, ki opravi pravni pregled zbiranja SIGINT obveščevalnih podatkov. Komisijo sestavljata dva nadzorna organa, in sicer kvazi-sodni ter administrativno-pravni odbor. Zakon predpisuje pogoje za imenovanje v odbora ter njune pristojnosti. Komisija mora poročati nadzornemu odboru parlamenta.

BND sodeluje tudi v različnih platformah za sodelovanje, kot npr. v Skupnem centru za boj proti terorizmu (GTAZ), ki zagotavlja nemoteno izmenjavo informacij z domačimi agencijami. Tukaj si 40 nacionalnih varnostnih organov izmenjuje informacije o terorističnih osumljencih ali konkretnih grožnjah z napadi. Pomembna posebnost GTAZ je, da lahko obveščevalne službe in organi kazenskega pregona sodelujejo v skladu s pravilom ločevanja in brez izgube časa. S prispevanjem obveščevalnih podatkov Skupnemu centru za analizo in politiko nezakonitih migracij (GASIM) in Nacionalnemu centru za kibernetško obrambo BND bolje pomaga razumeti vzroke in smernice nezakonitih migracij in/ali odkriti kibernetški kriminal. Poleg tega je BND ustanovni član in tako zastopan v Pobudi za ekonomsko varnost, s čimer podpira podjetja pri preprečevanju tveganj v okviru

te pobude. BND je v stiku s približno 450 obveščevalnimi službami v več kot 160 državah. Tesno sodeluje z institucijami Evropske unije in Nata. To svetovno mrežo uporablja za izpolnjevanje svojega zakonskega poslanstva. Izmenjava informacij z drugimi obveščevalnimi službami o nadnacionalnih pojavih, kot sta mednarodni terorizem ali trgovina z orožjem, je posebej pomemben element nemške varnostne arhitekture.

3. Republika Avstrija

Osrednji avstrijski notranji obveščevalni organ in hkrati organ pregona je Direktorat za državno zaščito in obveščevalno službo (DSN), ki se ukvarja z notranjo varnostjo, s protiobveščevalnimi dejavnostmi ter z bojem proti ekstremizmu in terorizmu in je bil ustanovljen leta 2021. Poleg DNS so ustanovljeni še trije podobni organi. Prvi je Kriminalistična obveščevalna enota (BK), ki se osredotoča na organizirani kriminal in kriminaliteto belih ovratnikov ter služi kot nacionalna točka za mednarodno policijsko sodelovanje. Za zunanje grožnje in vojaško obveščevalno dejavnost pa sta ustanovljeni Agencija za strateško obveščevalno dejavnosti in Agencija za varnost oboroženih sil.

Delo obveščevalnih služb je primarno urejeno v Zakonu o varnostni in obveščevalni službi (SNG), del določb pa vsebuje tudi Zakon o varnostni policiji (SPG). V aprilu 2025 je bil v avstrijskem parlamentu vložen predlog spremembe SNG, ki zaradi svoje povezanosti z drugimi področji terja spremembo več zakonov. Predlog spremembe SNG je bil potrjen junija 2025. S spremembo zakonodaje bo imela varnostna in obveščevalna služba pooblastilo za prestrežanje komunikacij, vključno z zaščiteno oziroma s šifrirano komunikacijo, kadar je to nujno potrebno za preprečitev napada, ki ogroža ustavno ureditev in za izvedbo katerega je zagrožena zaporna kazen najmanj 10 let, oziroma kadar je to nujno potrebno po določbah njihovega Kazenskega zakonika in bi bila izvršitev naloge z uporabo drugih preiskovalnih metod neučinkovita, oziroma kadar je to nujno potrebno za izvedbo preiskovalnega ukrepa. Navedeno pooblastilo obsega prestrežanje sporočil in informacij, ki se pošiljajo, posredujejo ali sprejemajo v šifrirani obliki, s programom, ki se z uporabo tehničnih sredstev naloži na računalniški sistem posameznika, kadar bi bila izvedba naloge z uporabo drugih preiskovalnih ukrepov sicer neučinkovita.

Zakon določa več omejitev, in sicer je treba preiskavo zaključiti takoj, ko pogoji zanjo ne obstajajo več, pooblastilo pa se lahko izda za prihodnje ali tudi preteklo časovno obdobje, predvidoma potrebno za izpolnitev naloge. Za izvedbo tega pooblastila so podani še dodatni pogoji, in sicer se je treba posvetovati s pooblaščenecem za pravno varstvo ter mu dati možnost, da poda mnenje v treh dneh. Zahtevek se tako lahko predloži Zveznemu upravnemu sodišču šele po izteku tega roka ali po predložitvi ustrezne izjave pooblaščenca za pravno varstvo. Pooblaščenec za pravno varstvo je prav tako dolžan preveriti odobritev in nadzorovati izvajanje preiskave navedene ter predvsem preverjati, da se med izvajanjem preiskave odobritev ne prekorači ter da se preiskava izvaja le v tolikšnem obsegu, da je zagotovljena sorazmernost.

Pri izvedbi preiskovalnega ukrepa je treba tehnično zagotoviti, da se lahko prestrežajo izključno sporočila, ki so bila poslana, posredovana ali prejeta v obsegu in časovnem obdobju, ki ju opredeljuje odredba, da se na računalniškem sistemu, ki bo pod nadzorom, izvedejo zgolj spremembe, ki so nujno potrebne za prestrežanje komunikacij, in da se nameščeni program po zaključku preiskovalnega ukrepa odstrani ali onesposobi. Nameščeni program je treba v skladu z zmožnostmi tehnike zaščititi pred nepooblaščenno uporabo. Pridobljena sporočila je treba v skladu z zmožnostmi tehnike zaščititi pred spreminjanjem, nepooblaščenim brisanjem in nepooblaščenim dostopanjem.

Poleg tega je zagotovljeno tudi posebno pravno varstvo, ki ga izvaja pooblaščenec za pravno varstvo, ki ima dodatna pooblastila za nadzor nad odobritvami.

Obvezno je tudi obveščanje posameznika, ki je bil predmet nadzora, in ga seznaniti z razlogi, načinom in dolžino trajanja ter s pravno podlago za uvedene ukrepe, predvsem v primeru prestrežanja komunikacije. Poleg tega je treba seznaniti tudi tiste osebe, ki so poslale, posredovale, ali prejele

sporočilo, kadar je njihova identiteta znana ali jo je možno ugotoviti brez večjega truda. O opravljeni seznanitvi je treba obvestiti pooblaščenca za pravno varstvo.

4. Kraljevina Norveška

Obveščevalno-varnostni sistem v Kraljevini Norveški sestavljajo tri obveščevalne službe. Primarno vlogo ima Norveška obveščevalna služba (NIS), ki deluje pod okriljem ministrstva za obrambo. Deluje tako na civilnem kot vojaškem področju, izključno za področje zunanjih groženj in pridobivanje tujih obveščevalnih podatkov. Druga služba je Policijska varnostna agencija (PST), tretja pa Nacionalni varnostni organ (NSM), ki skupaj pokrivata področje notranje varnosti. PST je del ministrstva za pravosodje in javno varnost ter pokriva protiobveščevalno področje, boj proti terorizmu, organiziranemu kriminalu, ekstremizmu, NSM pa se ukvarja z bojem proti vohunjenju, sabotazam, terorizmu in hibridnim grožnjam.

Delovanje NIS ureja Zakon o obveščevalni službi, ki vsebuje tudi določbe glede načinov zbiranja informacij. NIS ima zakonsko možnost, da prestreza in zbira elektronske informacije, ki niso javno dostopne v računalniških ali podobnih sistemih ali v aplikacijah, ki so v lasti ali pa se pričakuje, da so v uporabi obveščevalnih tarč. Če obstaja razlog, da bo zbiranje vključevalo informacije, ki niso namenjene sporočanju, se zbiranje ne izvede, razen če je to nujno potrebno. Enako pooblastilo ima tudi PST v kriminalnih zadevah. Zakonodajna sprememba, ki to omogoča, je bila uveljavljena leta 2016.

Dovoljena je uporaba programske opreme, ki se namesti na napravo cilja in zaobide varnostne ovire na napravi. Branje podatkov se lahko izvede z uporabo tehničnih naprav, računalniških programov ali drugače; urejeno pa mora biti tako, da se po nepotrebnem ne zajamejo nobene informacije o uporabi računalniškega sistema od kogar koli drugega kot osumljenca. Branje mora biti izvedeno tako, da ni nepotrebnega tveganja za motnje v delovanju ali poškodbe opreme ali podatkov; vključuje pa lahko komunikacije, elektronsko shranjene podatke in druge informacije o uporabi računalniškega sistema ali uporabniškega računa.

Zagotovljen je tudi nadzor, in sicer *ex ante*, to je predhodna sodna pot, ki jo izvajajo sodišča, ter *ex post*, naknadna zunajsodna pot, ki jo izvajajo posebej imenovani nadzorni organi.

5. Danska

Danska ima za delovanje Danske varnostne in obveščevalne agencije (Politiet Efterretningstjeneste; v nadaljevanju: PET) sprejet Zakon o policijski obveščevalni službi.⁹ Zakon celovito ureja dejavnosti PET in določa njene naloge, in sicer preprečevanje, preiskovanje ter boj proti kaznivim dejanjem, ki so ali bi lahko bili grožnja Danski kot neodvisni, demokratični in varni družbi. Poleg tega zakon določa okvir, kdaj lahko PET zakonito zbira, obdeluje in razkriva podatke, pomembne za njeno delo.

Med naloge PET spadajo tudi priprava ocene ogroženosti, pomoč drugim enotam policije, obveščanje ministra, pristojnega za pravosodje, o zadevah, pomembnih za notranjo varnost države, pomembnejših zadevah v okviru dejavnosti obveščevalne službe in o pomembnih posameznih zadevah. Prav tako mora kot nacionalni varnostni organ svetovati in pomagati javnim organom in zasebnikom v varnostih zadevah, vključno s pomočjo pri preiskavah osebne varnosti. Varujejo osebe, organizacije in organe ter opravljajo druge naloge, ki so po veljavni zakonodaji dodeljene službi. Letno mora predložiti poročilo o svojem delovanju ministru za pravosodje.

PET zbira in pridobiva podatke, ki so lahko pomembni za delovanje službe. Drugi upravni organi morajo na zahtevo policijske obveščevalne službe posredovati podatke PET, če ta oceni, da se lahko domneva, da so pomembni za opravljanje nalog službe glede preprečevanja in preiskovanja kršitev. Uvede lahko preiskave proti fizičnim in pravnim osebam, če se lahko domneva, da so preiskave

⁹ Lov om Politiets Efterretningstjeneste (PET), sprejet z zakonodajnim dekretom, št. 1600 z dne 19. 12. 2014, z dvema amandmajema (dekret, št. 1881 z dne 29. 12. 2015 in dekret, št. 1727 z dne 27. 12. 2016).

pomembne za opravljanje nalog PET v zvezi s preprečevanjem in preiskovanjem kršitev 12. in 13. poglavja danskega kazenskega zakonika (op.: gre za kazniva dejanja zoper neodvisnost in varnost države ter zoper ustavo in najvišje organe države) oziroma so potrebni za opravljanje drugih nalog službe.

PET lahko obdeluje katere koli osebne podatke. Če obdelava poteka s soglasjem, se šteje, da so podatki pomembni za opravljanje nalog službe pri preprečevanju in preiskovanju kršitev 12. in 13. poglavja danskega kazenskega zakonika, ali pa so potrebni za opravljanje drugih nalog službe. Za obdelavo podatkov o pravnih osebah se ustrezno uporabljajo členi danskega Zakona o obdelavi osebnih podatkov. Enako velja za obdelavo vseh podatkov o pravnih osebah. PET mora, razen če zakon ali predpisi, sprejeti na podlagi zakona, določajo drugače, izbrisati podatke o fizičnih in pravnih osebah, ki so posredovani v okviru preiskav ali preiskav, usmerjenih zoper te osebe, kadar niso v zvezi s preiskavo. Izbris podatkov se lahko opusti, če je to potrebno zaradi bistvenih razlogov za opravljanje nalog policijske obveščevalne službe.

Če PET v zvezi s svojim delovanjem izve, da zadeve ali dokumenti itd. ne izpolnjujejo več pogojev iz tega zakona, jih je treba izbrisati, ne glede na to, ali je rok za izbris po zakonu že potekel. PET ni dolžan na lastno pobudo redno pregledovati zadev in dokumentov službe ipd. z namenom presoje, ali so izpolnjeni pogoji za izbris. Minister, pristojen za pravosodje, lahko predpiše, da mora policijska obveščevalna služba v določenih primerih izbrisati podatke v večjem obsegu, kot izhaja iz določb zakona.

PET lahko razkrije podatke obrambno-obveščevalni službi, če bi bilo razkritje pomembno za opravljanje nalog službe. Prav tako lahko posreduje osebne podatke (pod določenimi pogoji) drugim danskim upravnim organom, zasebnim podjetjem, tujim organom in mednarodnim organizacijam.

Fizična ali pravna oseba nima pravice dostopa do podatkov, ki jih PET obdeluje o njej, niti pravice do vedenja o tem, ali služba obdeluje podatke o njej. Če posebne okoliščine to upravičujejo, lahko policijska obveščevalna služba omogoči popoln ali delni dostop do informacij. Fizična ali pravna oseba lahko zahteva nadzor nad obveščevalnimi službami, da razišče, ali služba neupravičeno obdeluje podatke o zadevni osebi. Nadzor opravi pristojni inšpektorat, ki o ugotovitvah obvesti prijavitelja.

Določbe v zakonodaji o obveznosti posredovanja podatkov ne veljajo za podatke o prejemkih, ki jih zagotavljajo skladi v posebnem postopku revizije za PET. Takšni prejemki se ne vštevajo v obdavčljiv dohodek ali v osnovo za izračun socialnih prejemkov ipd.

Obveščevalno službo PET nadzoruje nadzorni organ, ki ga sestavlja pet članov, ki jih imenuje minister za pravosodje po pogajanjih z ministrom za obrambo.

6. Kraljevina Nizozemska

Delo nizozemske obveščevalno-varnostne službe (v nadaljevanju: AIVD) ureja Zakon o obveščevalnih in varnostnih službah iz leta 2017 (v nadaljevanju: Wiv 2017), ki je začel veljati 1. maja 2018. Vključuje tudi določila, ki zagotavljajo, da je njihovo delo čim bolj transparentno, saj je to, kar delajo, vidno, zato so javno odgovorni za svoja dejanja. Ta pravila so neposredna posledica Evropske konvencije o človekovih pravicah, ki zahteva, da je delo obveščevalnih in varnostnih služb "jasno, predvidljivo in dostopno" javnosti.

Wiv 2017 določa AIVD naslednjih šest glavnih nalog:

- a) Izvajati preiskave v zvezi z organizacijami in osebami, ki zaradi ciljev, ki jih zasledujejo, ali s svojimi dejavnostmi vzbujajo resen sum, da ogrožajo nadaljnji obstoj demokratičnega pravnega reda ali varnost ali druge vitalne interese države.
- b) Izvajanje varnostnih pregledov, kot je navedeno v Zakonu o varnostnih pregledih.
- c) Spodbujanje ukrepov za zaščito interesov iz (a), vključno z ukrepi za zaščito podatkov, katerih zaupnost je stvar nacionalne varnosti, in tistih delov vladnih služb in poslovnega sektorja, ki so po mnenju pristojnih ministrov ključnega pomena za ohranitev družbe.
- d) Izvajati preiskave v zvezi z drugimi državami.

- e) Pripraviti analize groženj in tveganj na skupno zahtevo ministra za notranje zadeve in odnose s kraljestvom ter ministra za pravosodje in varnost v korist zaščite oseb iz člena 4(3)(b) in 42(1)(c) Zakona o policiji iz leta 2012, kot tudi za varovanje in zaščito predmetov in storitev, določenih v skladu s 16. členom tega zakona.
- f) Na zahtevo osebe ali organa, ki ga z uredbo skupaj imenujejo zadevni ministri, za poročanje o podatkih, ki jih služba obdeluje v zvezi z osebami ali organi v primerih, določenih z navedeno uredbo.

Med pooblastila AIVD spadajo opazovanje in sledenje ljudem, uporaba agentov ter spremljanje in prisluškovanje kateri koli obliki telekomunikacij. Posebna preiskovalna pooblastila, znana tudi kot "posebni obveščevalni viri", se lahko uporabijo le, kadar je to nujno potrebno, da AIVD opravlja svoje naloge. Posebnih pooblastil ni mogoče uporabiti za dve od teh nalog: varnostne preglede in varovanje vitalnih sektorjev. Poleg tega AIVD ne sme sprejeti nobenega ukrepa, ki bi lahko resno posegel v osebno zasebnost, brez izrecnega predhodnega dovoljenja pristojnega ministra in zavezujoče sodbe neodvisne revizijske komisije. Wiv 2017 zahteva, da AIVD obvesti vse, proti katerim je uporabil posebno preiskovalno pooblastilo, ki krši njihovo ustavno pravico do zasebnosti doma ali tajnosti komunikacij.

Pet let po prenehanju uporabe posebnega obveščevalnega sredstva, kot so pregled pisem ali ciljno prisluškovanje, pristojni minister preveri, ali je zadevno osebo sedaj mogoče obvestiti. To se ne izvede, če bi obvestilo škodilo odnosom z drugimi državami ali razkrilo vire ali metode AIVD. Če osebi, zoper katero je bilo uporabljeno posebno preiskovalno pooblastilo, ni mogoče izdati poročila, je treba o tem obvestiti nadzorno komisijo z navedbo razlogov za neizdajo obvestila.

V skladu z Wiv 2017 lahko oseba od AIVD zahteva pregled vseh informacij, ki jih ima o njej ali o pokojnem zakoncu, partnerju, otroku ali staršu. Če je zahteva zavrnjena, ima prosilec pravico do pritožbe pri okrožnem sodišču v Haagu.

Posebna preiskovalna pooblastila, ki jih AIVD lahko uporabi pri svojih preiskavah, spremljata dve neodvisni regulatorni komisiji. Prva komisija, Komisija za preiskovalna pooblastila (Toetsingscommissie Inzet Bevoegdheden – TIB), predhodno preveri, ali je zahteva za uporabo posebnih obveščevalnih sredstev – npr. prisluškovanje komunikacijski napravi – zakonita ali ne (njihova sodba je pravnomočna). Druga neodvisna komisija, Nadzorni odbor za obveščevalne in varnostne službe (Commissie van Toezicht op de Inlichtingen-en Veiligheidsdiensten – CTIVD) spremlja skladnost z zakonom Wiv 2017 in Zakonom o varnostnem preverjanju (Wet Veiligheidsonderzoeken – WVO) za nazaj.

V skladu z zakonsko obveznostjo glede zaupnosti ima ta organ pravico pregledati vse informacije, ki jih želi. Prav tako redno poroča o zakonitosti obveščevalnega dela.

AIVD ima zakonsko obveznost, da do aprila vsako leto objavi letno poročilo. Ta poročila ne prikazujejo samo dejavnosti v preteklem letu, temveč opisujejo tudi področja zanimanja v tekočem letu.

6. PRESOJA POSLEDIC, KI JIH BO IMEL SPREJEM ZAKONA

6.1. Presoja administrativnih posledic

a) v postopkih oziroma poslovanju javne uprave ali pravosodnih organov:

Zakon ne bo imel posledic za poslovanje javne uprave ali pravosodnih organov.

b) pri obveznostih strank do javne uprave ali pravosodnih organov:

Zakon ne bo imel posledic na obveznosti strank do javne uprave ali pravosodnih organov.

6.2. Presoja posledic za okolje, vključno s prostorskimi in varstvenimi vidiki, in sicer za:

Zakon ne bo imel posledic za okolje.

6.3. Presoja posledic za gospodarstvo, in sicer za:

Zakon ne bo imel posledic za gospodarstvo.

6.4. Presoja posledic za socialno področje, in sicer za:

Zakon ne bo imel posledic na socialnem področju.

6.5. Presoja posledic za dokumente razvojnega načrtovanja, in sicer za:

Zakon ne bo imel posledic za dokumente razvojnega načrtovanja.

6.6. Presoja posledic za druga področja:

Zakon ne bo imel posledic na drugih področjih.

6.7. Izvajanje sprejetega predpisa:

a) Predstavitev sprejetega zakona:

Sprejeti zakon bo predstavljen na spletni strani Državne zbornice Republike Slovenije.

b) Spremljanje izvajanja sprejetega predpisa

V okviru svojih pristojnosti bodo izvajanje sprejetega predpisa spremljali nadzorni organi agencije.

6.8. Druge pomembne okoliščine v zvezi z vprašanji, ki jih ureja predlog zakona:

V zvezi z vprašanji, ki jih ureja predlog zakona, ni drugih pomembnih okoliščin.

7. PRIKAZ SODELOVANJA JAVNOSTI PRI PRIPRAVI PREDLOGA ZAKONA:

- **spletni naslov, na katerem je bil predpis objavljen**

Predlog zakona je bil javno objavljen na portalu e-Demokracija dne 22.9.2025 (<https://e-uprava.gov.si/drzava-in-drizba/e-demokracija/predlog-predpisov/predlog.predpisa.html?id=18192&lang=si>)

- **čas trajanja javne predstavitve, v katerem je bilo mogoče sporočiti mnenja, predloge in pripombe**

Javna obravnava je potekala do 22.10.2025.

- **datum in kraj morebitne javne obravnave ali druge oblike sodelovanja**
/

- **seznam subjektov, ki so sodelovali (imen in priimkov fizičnih oseb, ki niso poslovni subjekti, ne navajajte)**

Pripombe oziroma mnenja na predlog zakona so podali tri fizične osebe, Informacijski pooblaščenec dne ter Inštitut Državljan D, zavod za spodbujanje informacijske in medijske pismenosti.

8. PODATEK O ZUNANJEM STROKOVNJAKU OZIROMA PRAVNI OSEBI, KI JE SODELOVALA PRI PRIPRAVI PREDLOGA ZAKONA, IN ZNESKU PLAČILA ZA TA NAMEN:

Pri pripravi predloga zakona niso sodelovali zunanji strokovnjaki oziroma pravne osebe.

9. NAVEDBA, KATERI PREDSTAVNIKI PREDLAGATELJA BODO SODELOVALI PRI DELU DRŽAVNEGA ZBORA IN DELOVNIH TELES:

- Joško Kadivnik, direktor

II. BESEDILO ČLENOV

1. člen

V Zakonu o Slovenski obveščevalno-varnostni agenciji (Uradni list RS, št. 81/06 – uradno prečiščeno besedilo) se v 2. členu v prvem odstavku prva alineja spremeni tako, da se glasi:

»- iz tujine ali v povezavi z njo, pomembne za zagotavljanje varnostnih, političnih ali gospodarskih interesov Republike Slovenije;«.

2. člen

V 4.a členu se besedilo »Zakona o javnih uslužbencih (Uradni list RS, št. 56/02 in 110/02-ZDT-B)« nadomesti z besedilom »zakona, ki ureja sistem javnih uslužbencev«.

3. člen

12. člen se spremeni tako, da se glasi:

»12. člen

(1) Za namen varstva ustavne ureditve Republike Slovenije in zagotavljanje nacionalne varnosti agencija zbira, upravlja, obdeluje, shranjuje in posreduje (v nadaljnjem besedilu: obdeluje) osebne podatke, vključno s posebnimi vrstami osebnih podatkov iz drugega odstavka 14. člena tega zakona ter druge podatke, ki so potrebni za uresničevanje nalog iz 2. člena tega zakona.

(2) Agencija pred posredovanjem podatkov tujim obveščevalno-varnostnim službam ali mednarodnim organizacijam preveri, da država ali mednarodna organizacija, ki je prejemnica podatkov, zagotavlja primerljivo raven varstva osebnih podatkov, in si priskrbi zagotovila, da bo država ali mednarodna organizacija, ki je prejemnica podatkov, obdelovala podatke za dovoljene namene.

(3) Agencija obdeluje podatke, ki jih pridobi od tuje obveščevalno-varnostne službe ali mednarodne organizacije, za namene in v okviru omejitev, ki jih določi tuja obveščevalno-varnostna služba ali mednarodna organizacija.«.

4. člen

V 14. členu se v drugem odstavku za besedo »zaposlitev« beseda »in« nadomesti z vejico in doda besedilo »podobo obraza, govora oziroma glasu ter«.

Za tretjim odstavkom se doda nov, četrti odstavek, ki se glasi:

»(4) Biometrični podatki iz drugega odstavka tega člena se obdelujejo skupaj z že zbranimi podatki za primerjanje oziroma identifikacijo posameznikov, ko je to glede na okoliščine konkretne zadeve nujno in potrebno ali ko to izrecno izhaja iz odredbe za posebne oblike pridobivanja podatkov. Direktor agencije podrobneje določi obdelavo biometričnih podatkov v agenciji.«.

5. člen

16. člen se spremeni tako, da se glasi:

»16. člen

Upravljavci in obdelovalci zbirk podatkov morajo agenciji na njeno obrazloženo zahtevo brezplačno posredovati podatke ali omogočiti vpogled na predhodno dogovorjen način.«.

6. člen

18. člen se spremeni tako, da se glasi:

»18. člen

(1) Za dokumentarno gradivo agencije se uporabljajo predpisi s področja varstva dokumentarnega in arhivskega gradiva ter predpisi, ki urejajo področje tajnih podatkov, če ta zakon ne določa drugače.

(2) Dokumentarno gradivo iz razvida, razen tistega dela dokumentarnega gradiva, ki vsebuje podatke iz tretjega in četrtega odstavka tega člena, postane arhivsko gradivo in se preda Arhivu Republike Slovenije 50 let po zaključku posamezne zadeve.

(3) Dokumentarno gradivo, ki vsebuje podatke, ki omogočajo identifikacijo uradnih oseb agencije, oseb, ki sodelujejo z agencijo, ali naziva, ki ga agencija uporablja pri finančnem in materialnem poslovanju v razmerju do tretjih oseb, postane arhivsko gradivo in se preda Arhivu Republike Slovenije po 75 letih od pridobitve oziroma nastanka takega podatka.

(4) Dokumentarno gradivo, ki vsebuje podatke, za katere je tuja obveščevalno-varnostna služba ali mednarodna organizacija določila, da se jih ne sme posredovati tretji osebi, in podatki, ki omogočajo identifikacijo tajnih sodelavcev agencije ali pripadnikov tujih obveščevalno-varnostnih služb ali mednarodnih organizacij, agencija hrani trajno.«.

7. člen

23. člen se spremeni tako, da se glasi:

»23. člen

Če je podana velika verjetnost, da obstaja nevarnost za varnost države, lahko agencija pri opravljanju svojih nalog uporabi tudi naslednje posebne oblike pridobivanja podatkov:

- tehnično sredstvo za nadzor signala mobilne telefonije;
- kontrola pisem in drugih pošilk ter nadzorovanje in snemanje telekomunikacij;
- neposredni dostop do podatkov telekomunikacijskega sredstva za namen beleženja komunikacijskega prometa na samem sredstvu.«.

8. člen

Za 23. členom se doda nov 23.a člen, ki se glasi:

»23.a člen

(1) Uporabo tehničnega sredstva za nadzor signala mobilne telefonije dovoli na predlog direktorja agencije s pisno odredbo za vsak primer posebej predsednik Vrhovnega sodišča Republike Slovenije, če je podana velika verjetnost, da obstaja nevarnost za varnost države, ki se kaže v:

- aktivnostih zoper suverenost, neodvisnost, državno celovitost in strateške interese Republike Slovenije,
- aktivnostih, načrtih in pripravah za izvedbo mednarodnih terorističnih akcij zoper Republiko Slovenijo ter drugih nasilnih dejanjih proti državnemu organu in nosilcem javnih funkcij v Republiki Sloveniji ter tujini,
- posredovanju in pridobivanju podatkov in dokumentov, ki so v Republiki Sloveniji opredeljeni kot tajni podatki, nepooblaščenim osebam v tujini,
- pripravah na oborožen napad na Republiko Slovenijo ali na katerega od pomembnejših objektov v Republiki Sloveniji,
- obveščevalni dejavnosti posameznikov, organizacij in skupin v korist tujine ali
- mednarodni organizirani kriminalni dejavnosti in z njo povezanimi pripravljalnimi dejanji,

in je utemeljeno pričakovati, da bo na določenem območju in v določenem časovnem obdobju tako možno identificirati osebe, ki izvajajo navedene aktivnosti, oziroma ugotoviti komunikacijska ali druga tehnična sredstva, ki se uporabljajo za te aktivnosti, ter če identifikacije oseb ter ugotovitve komunikacijskih ali drugih tehničnih sredstev ni mogoče opraviti na milejši način oziroma bi bilo to povezano z nesorazmernimi težavami.

(2) V okviru posebne oblike pridobivanja podatkov iz tega člena ni dovoljeno prisluškovanje in snemanje elektronskih komunikacij ter ugotavljanje lokacije komunikacijskih sredstev tretjih oseb.

(3) Predlog in odredba morata vsebovati podatke o zadevi in osebah, na katere se ta posebna oblika pridobivanja podatkov nanaša, utemeljitev razlogov za njeno uporabo, podatke o načinu njenega izvajanja, o obsegu in trajanju ter morebitnih drugih okoliščinah, ki narekujejo njeno uporabo, ter utemeljitev, da podatkov ni mogoče pridobiti na milejši način oziroma bi bilo to povezano z nesorazmernimi težavami.

(4) Uporaba posebne oblike pridobivanja podatkov iz prvega odstavka tega člena se uporablja najkrajši možni čas za doseg namena iz prvega odstavka tega člena, vendar ne dlje kot 15 dni od prejema odredbe predsednika Vrhovnega sodišča Republike Slovenije, brez možnosti podaljšanja. O prenehanju mora direktor agencije pisno obvestiti predsednika Vrhovnega sodišča Republike Slovenije.

(5) Agencija obdeluje osebne podatke oseb, za katere ugotavlja, da ne sodelujejo pri izvajanju aktivnosti iz prvega odstavka tega člena (tretje osebe), v obsegu, ki je iz tehničnih razlogov neizogibno potreben za doseg namena iz prvega odstavka tega člena in na način, ki najmanj posega v njihove pravice. Agencija sme začasno uporabiti podatke tretjih oseb izključno za namene ugotavljanja identitete oseb, zoper katere so usmerjene aktivnosti iz prvega odstavka tega člena, in jih mora po zaključku teh aktivnosti nemudoma izbrisati.

(6) Po zaključku uporabe tehničnega sredstva za nadzor signala mobilne telefonije agencija v štirinajstih dneh pripravi poročilo o izvedeni aktivnosti in ga skupaj z zbranimi podatki posreduje v seznanitev predsedniku Vrhovnega sodišča Republike Slovenije. Predsednik Vrhovnega sodišča Republike Slovenije odredi brisanje podatkov, za katere oceni, da niso potrebni za doseg namena iz prvega odstavka tega člena.

(7) V 90 dneh po zaključitvi zadeve v razvidu obvesti direktor agencije osebo, na katero se je ta posebna oblika pridobivanja podatkov nanašala, da se ima pravico seznaniti s pridobljenim gradivom, v primerih večjega obsega tega gradiva pa s poročilom, ki obsega povzetek zbranega gradiva. Če je mogoče utemeljeno sklepati, da bo zaradi seznanitve z gradivom nastala nevarnost za življenje ali zdravje ljudi ali za nacionalno varnost, lahko direktor agencije odloči, da osebe z vsebino pridobljenega gradiva ne bo seznanil.

(8) Agencija najmanj enkrat na leto, praviloma do konca marca tekočega leta za preteklo leto, pripravi poročilo o nadzoru nad uporabo tehničnega sredstva za nadzor signala mobilne telefonije in z njim seznaniti predsednika Vrhovnega sodišča Republike Slovenije (periodično poročilo).

(9) Direktor agencije s soglasjem vlade podrobneje določi način uporabe tehničnega sredstva za nadzor signala mobilne telefonije.«.

9. člen

Za 24.b členom se dodata nova, a24.c in b24.c člen, ki se glasita:

»a24.c člen

(1) Uporabo tehničnega sredstva za neposredni dostop do podatkov telekomunikacijskega sredstva za namen beleženja komunikacijskega prometa na sredstvu dovoli na predlog direktorja agencije s pisno odredbo za vsak primer posebej predsednik Vrhovnega sodišča Republike Slovenije, če je podana velika verjetnost, da obstaja nevarnost za varnost države, ki se kaže v:

- neposrednih sedanjih ali predvidljivih prihodnjih tajnih aktivnostih zoper suverenost, neodvisnost, državno celovitost in strateške interese Republike Slovenije,
- neposrednih sedanjih ali predvidljivih prihodnjih aktivnostih, načrtih in pripravah za izvedbo mednarodnih terorističnih akcij zoper Republiko Slovenijo ter drugih nasilnih dejanjih proti državnemu organu in nosilcem javnih funkcij v Republiki Sloveniji ter tujini,
- neposrednem sedanjem ali predvidljivem prihodnjem posredovanju in pridobivanju podatkov in dokumentov, ki so v Republiki Sloveniji opredeljeni kot tajni podatki, nepooblaščenim osebam v tujini,
- neposrednih sedanjih ali predvidljivih prihodnjih pripravah na oborožen napad na Republiko Slovenijo ali na katerega od pomembnejših objektov v Republiki Sloveniji,
- neposredni sedanji ali predvidljivi prihodnji obveščevalni dejavnosti posameznikov, organizacij in skupin v korist tujine ali
- neposredni sedanji ali predvidljivi prihodnji mednarodni organizirani kriminalni dejavnosti in z njo povezanimi pripravljalnimi dejanji

in je utemeljeno pričakovati, da se v zvezi s to aktivnostjo uporablja določeno telekomunikacijsko sredstvo ali bo to sredstvo uporabljeno, pri tem pa je mogoče utemeljeno sklepati, da podatkov ni možno pridobiti drugače oziroma bi njihovo pridobivanje na drug način oziroma z drugo obliko lahko ogrozilo življenje ali zdravje ljudi oziroma bi pomenilo resno grožnjo nacionalni varnosti.

(2) Pri izvajanju posebne oblike pridobivanja podatkov iz tega člena ni dovoljen vstop v tuje stanovanje ali druge prostore.

(3) V okviru izvajanja posebne oblike pridobivanja podatkov iz tega člena ni dovoljeno poseganje v vsebino komunikacije z namenom njenega spreminjanja, dopolnjevanja ali kakršnega koli drugega predrugačenja.

(4) Predlog in odredba morata vsebovati podatke o osebi in telekomunikacijskem sredstvu, na katera se posebna oblika pridobivanja podatkov nanaša, utemeljitev razlogov in okoliščin za njegovo uporabo, ki vključuje časovno obdobje ter način in obseg izvajanja tega ukrepa, pri čemer se v predlogu in odredbi določno opredelijo nujno potrebne spremembe na telekomunikacijskem sredstvu, ki so potrebne za dostop do podatkov za namen beleženja komunikacijskega prometa.

(5) Posebna oblika pridobivanja podatkov iz tega člena se uporablja najkrajši možni čas za doseg namena iz prvega odstavka tega člena, vendar ne dlje kot en mesec od prejema odredbe predsednika Vrhovnega sodišča Republike Slovenije, z možnostjo podaljšanja, vendar skupno ne več kot tri mesece.

(6) Uporaba posebne oblike pridobivanja podatkov iz tega člena se odpravi takoj, ko prenehajo razlogi, zaradi katerih je odrejena oziroma po preteku časovnega obdobja, določenega v odredbi, pri čemer je treba tehnično zagotoviti, da se nameščeni program odstrani oziroma onesposobi. O prenehanju direktor agencije pisno obvesti predsednika Vrhovnega sodišča Republike Slovenije.

(7) Agencija obdeluje osebne podatke tretjih oseb v obsegu, ki je iz tehničnih razlogov neizogibno potreben za doseg namena iz prvega odstavka tega člena, in na način, ki najmanj posega v njihove pravice.

(8) Po zaključku uporabe posebne oblike pridobivanja podatkov iz tega člena agencija v štirinajstih dneh pripravi poročilo o izvedeni aktivnosti in ga skupaj z zbranimi podatki posreduje v seznanitev predsedniku Vrhovnega sodišča Republike Slovenije. Predsednik Vrhovnega sodišča Republike Slovenije odredi brisanje podatkov, za katere oceni, da niso potrebni za doseg namena iz prvega odstavka tega člena.

(9) V 90 dneh po zaključitvi zadeve v razvidu obvesti direktor agencije osebo, na katero se je posebna oblika pridobivanja podatkov iz tega člena nanašala, da ima pravico seznaniti se s pridobljenim gradivom, v primerih večjega obsega tega gradiva pa s poročilom, ki obsega povzetek zbranega gradiva. Če je mogoče utemeljeno sklepati, da bo zaradi seznanitve z gradivom nastala nevarnost za življenje ali zdravje ljudi ali za nacionalno varnost, lahko direktor agencije odloči, da osebe z vsebino pridobljenega gradiva ne bo seznanil.

(10) Agencija najmanj enkrat na leto, praviloma do konca marca tekočega leta za preteklo leto, pripravi poročilo o nadzoru nad uporabo tehničnega sredstva za neposredni dostop do podatkov telekomunikacijskega sredstva za namen beleženja komunikacijskega prometa na sredstvu in z njim seznanjeni predsednika Vrhovnega sodišča Republike Slovenije (periodično poročilo).

(11) Direktor agencije s soglasjem vlade podrobneje določi način uporabe tehničnega sredstva za neposredni dostop do podatkov telekomunikacijskega sredstva za namen beleženja komunikacijskega prometa na sredstvu.

b24.c člen

(1) Uporabo tehničnega sredstva za neposredni dostop do podatkov telekomunikacijskega sredstva za namen beleženja komunikacijskega prometa na sredstvu nadzira tudi pooblaščenec za nadzor.

(2) Agencija o nameri, da bo uporabila tehnično sredstvo za neposredni dostop do podatkov telekomunikacijskega sredstva za namen beleženja komunikacijskega prometa na sredstvu, obvesti pooblaščenca za nadzor in mu omogoči vpogled v vse podatke in postopke v zvezi s to posebno obliko pridobivanja podatkov, na njegovo zahtevo pa mu poda tudi ustrezna pojasnila.

(3) Pooblaščenec za nadzor o ugotovitvah nadzora ažurno obvešča predsednika Vrhovnega sodišča Republike Slovenije in direktorja agencije ter jima daje priporočila za ukrepanje v okviru njunih pristojnosti.

(4) Pooblaščenca za nadzor imenuje Vlada Republike Slovenije za dobo 5 let z možnostjo ponovnega imenovanja.

(5) Za pooblaščenca za nadzor je lahko imenovana oseba, ki ima ustrezno strokovno znanje in praktične sposobnosti ter izkušnje, in ki:

- je državljan Republike Slovenije;
- aktivno obvlada slovenski jezik;
- je poslovno sposoben;
- je star najmanj 40 let;
- ni v kazenskem postopku in ni obsojen za kaznivo dejanje, ki se preganja po uradni dolžnosti;
- je bil varnostno preverjen in njegovo imenovanje ne pomeni varnostnega tveganja za agencijo.

(6) Šteje se, da ima oseba ustrezno strokovno znanje, če ima najmanj izobrazbo, pridobljeno po študijskih programih prve stopnje oziroma izobrazbo, ki ustreza ravni izobrazbe, pridobljene po študijskih programih prve stopnje, in je v skladu z zakonom, ki ureja slovensko ogrodje kvalifikacij, uvrščena na 7. raven.

(7) Šteje se, da ima oseba ustrezne praktične sposobnosti in izkušnje, če ima najmanj 10 let delovnih izkušenj na področjih ustavnega prava, človekovih pravic ali nacionalne varnosti.

(8) Pooblaščenec za nadzor je upravičen do sejin in povrnitve stroškov v višini, kot je določena z uredbo, ki ureja sejnine in povračila stroškov v javnih skladih, javnih agencijah, javnih zavodih in javnih gospodarskih zavodih, in na način, ki je podrobneje urejen v internem aktu agencije.«.

10. člen

24.c člen se črta.

11. člen

V 28. členu se na koncu prvega odstavka doda besedilo »Postopke zaposlitve vodi agencija. Na zaprosilo agencije zagotavlja strokovno pomoč v postopkih zaposlitve ministrstvo, pristojno za javno upravo.«.

12. člen

V 34. členu se v prvem odstavku besedilo »posebnih delovnih razmerah« nadomesti z besedilom »manj ugodnem delovnem času«.

V drugem odstavku se besedilo »Posebne delovne razmere so« nadomesti z besedilom »Delo v manj ugodnem delovnem času je«.

Za tretjim odstavkom se dodajo novi četrti do deveti odstavki, ki se glasijo:

»(4) Ne glede na določbe zakona, ki ureja delovna razmerja, časovne omejitve dnevne delovne obveznosti, dnevni in tedenski počitek ter delo preko polnega delovnega časa, lahko v izjemnih, nujnih ali nepredvidenih primerih, ko ni mogoče drugače opraviti nalog agencije, nadrejeni odredi uradni osebi agencije, da dokonča začetno nalogo ali opravi nujno nalogo po poteku delovnega časa brez takšne prekinitve dela, ki bi uradni osebi agencije omogočila počitek. Soglasje uradne osebe agencije glede ukrepa iz tega odstavka ni potrebno.

(5) Delo preko polnega delovnega časa lahko traja največ 20 ur na teden oziroma 50 ur na mesec, pri čemer povprečen delovni teden, vključno z delom preko polnega delovnega časa, ne sme presegati 56 ur v sedemdnevem obdobju, izračunanem kot povprečje v posameznem referenčnem obdobju. Delo preko polnega delovnega časa nadrejeni odredi v pisni obliki praviloma pred potekom rednega delovnega časa. Če zaradi narave dela ali nujnosti opravljanja dela to ni mogoče, se lahko delo preko polnega delovnega časa v izjemnih in nujnih primerih odredi ustno. V tem primeru se pisna odreditev vroči uradni osebi agencije naknadno, najpozneje v osmih dneh po opravljenem delu.

(6) Odreditev dela po prejšnjem odstavku je dopustna le za najkrajši možni čas, ki je potreben za dokončanje ali opravo nujne naloge, s tem da je treba uradni osebi agencije takoj po prenehanju razlogov zagotoviti sorazmerno daljši počitek v skladu s splošnimi predpisi in kolektivno pogodbo za negospodarsko dejavnost.

(7) Druge oblike dela v manj ugodnem delovnem času se odredijo, če to terjajo delovne obveznosti oziroma je samo tako mogoče opraviti določene naloge, ki jih ni moč odlagati ali pa morajo biti opravljene v določenem roku.

(8) Uradni osebi agencije se lahko odredi tudi pripravljenost za delo, ki je poseben delovni pogoj, pri katerem mora biti uradna oseba agencije, ki ji je ta pripravljenost odrejena, v pripravljenosti za delo doma, kar pomeni, da je uradna oseba agencije za potrebe prihoda na delovno mesto ali kraj, kjer je treba opraviti nujno nalogo, dosegljiva po telefonu ali drugih komunikacijskih sredstvih. Uradna oseba agencije se seznani z odrejeno pripravljenostjo za delo najmanj tri dni vnaprej po razporedu dela ali s posebno odredbo.

(9) Delovna mesta, na katerih poteka delo v skladu z drugim in osim odstavkom tega člena, se določijo v aktu o notranji organizaciji in sistemizaciji delovnih mest.«.

Dosedanja četrti in peti odstavek se črtata.

PREHODNI IN KONČNA DOLOČBA

13. člen

Agencija sprejme interni akt:

- iz novega četrtega odstavka 14. člena zakona v šestih mesecih po uveljavitvi tega zakona;
- iz devetega odstavka novega 23.a člena zakona v enem letu po uveljavitvi tega zakona in pred pričetkom uporabe posebne oblike pridobivanja podatkov iz 23.a člena zakona;
- iz enajstega odstavka novega a24.c člena zakona v enem letu po uveljavitvi tega zakona in pred pričetkom uporabe posebne oblike pridobivanja podatkov iz a24.c člena zakona.

14. člen

Vlada Republike Slovenije imenuje pooblaščenca za nadzor iz novega b24.c člena v enem letu po uveljavitvi tega zakona in pred pričetkom uporabe posebne oblike pridobivanja podatkov iz a24.c člena zakona.

15. člen

Ta zakon začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije.

Št.

Ljubljana, dne

EVA: 2025-1524-0001

III. OBRAZLOŽITEV

K 1. členu

Z dopolnitvijo prve alineje prvega odstavka se širi pristojnost delovanja agencije na obveščevalnem področju in se smiselno izenačuje s pogojem za pridobivanje podatkov pri protiobveščevalni dejavnosti agencije, kot je opredeljena v drugi alineji prvega odstavka.

Agencija bo poleg podatkov iz tujine, ki so pomembni za zagotavljanje varnostnih, političnih in gospodarskih interesov države, lahko obdelovala tudi podatke v povezavi s tujino, ki so pomembni za zagotavljanje navedenih interesov države. Množična uporaba telekomunikacijskih sredstev, globalna narava kriminalno-obveščevalnih dejanj in spremembe na področju transnacionalnosti zahtevajo uvedbo sprememb tudi na obveščevalnem področju, na podlagi katerih bo agencija lahko obravnavala več varnostno relevantnih situacij. Dopolnitev se bo neposredno odražala na kvaliteti in kvantiteti obveščevalnih informacij, ki jih posreduje vodstvu države in drugim relevantnim deležnikom, s tem pa se bo nadalje pomembno prispevalo k zagotavljanju varnostnih, političnih in gospodarskih interesov Republike Slovenije ter tudi širšega mednarodnega okolja.

K 2. členu

Sprememba predstavlja nomotehnični popravek obstoječega 4.a člena.

K 3. členu

Agencija pri opravljanju nalog iz 2. člena tega zakona obdeluje vse vrste osebnih podatkov, vključno s posebnimi vrstami, kot so npr. biometrični ali občutljivi osebni podatki, kot so navedeni v drugem odstavku 14. člena, prav tako tudi podatke, ki niso opredeljeni kot osebni. Sprememba predmetnega člena predstavlja napolnilno določbo za dodano vrsto osebnih podatkov, ki je v naslednjem členu predloga zakona podrobneje opredeljena.

Prvi odstavek 12. člena je prenovljen zaradi večje jasnosti določb in poenotenja s terminologijo s področja varstva osebnih podatkov.

Z novima drugim in tretjim odstavkom se uvaja t. i. pravilo tretjega, na podlagi katerega je prejemnik neke informacije, ki je običajno označena s stopnjo tajnosti, dolžan pred njenim posredovanjem oziroma nadaljnjim razpolaganjem zunaj opredeljenega okvira uporabe prehodno pridobiti soglasje pošiljatelja. Pravilo povzema že uveljavljeno mednarodno prakso na področju izmenjave in posredovanja obveščevalnih oziroma varnostnih podatkov. To pravilo smiselno odseva določbi 34. in 36. člena Zakona o tajnih podatkih, ki na nacionalni ravni uveljavljata navedeno pravilo na področju tajnih podatkov.

K 4. členu

V povezavi z dopolnitvijo prvega odstavka 12. člena tega zakona in vključitvijo zakonske podlage za obdelavo posebne vrste osebnih podatkov se dopolnjuje tudi nabor osebnih podatkov o osebah, ki jih agencija sistematično operativno obravnava.

Posebne vrste osebnih podatkov se v kontekstu delovanja agencije nanašajo na biometrične podatke, in sicer bo zbirka podatkov agencije lahko vsebovala tudi podobo obraza, govora oziroma glasu. S tem bo agenciji omogočena uvedba modernejših pristopov pri obdelavi osebnih podatkov, prav tako pa bo pripomoglo k natančnejši in hitrejši obravnavi oseb, ki so predmet sistematične operativne obravnave agencije.

V novem, četrtem, odstavku, agencija podrobneje določi namen obdelave biometričnih podatkov, ki so navedeni v drugem odstavku tega člena, in sicer se bodo podatki lahko obdelovali skupaj z že zbranimi podatki za primerjanje oziroma identifikacijo relevantnih posameznikov. Ta obdelava je dodatno omejena še z enim pogojem, in sicer je uporaba navedenih biometričnih podatkov mogoča zgolj takrat, ko je to glede na okoliščine konkretne zadeve nujno in potrebno ali ko to izrecno izhaja iz odredbe za posebne oblike pridobivanja podatkov. Direktor agencije podrobneje določi obdelavo biometričnih podatkov v agenciji.

Agencija bo z ustreznimi internimi postopki še naprej zagotavljala varno in zakonito obdelavo osebnih podatkov, ki je neločljivo povezana tudi s standardi, ki jih zahtevata nacionalna in mednarodna zakonodaja s področja obravnave tajnih podatkov. Osební podatki se bodo obdelovali do zaključitve zadeve v razvidu, potem bodo izbrisani oziroma blokirani, kot izhaja iz nespremenjenega tretjega odstavka 14. člena.

K 5. členu

S celovito prenovo 16. člena se določa neposredna zakonska pravna podlaga, na podlagi katere bodo morali vsi upravljavci in obdelovalci osebnih podatkov, ne glede na sektor delovanja, agenciji na njeno obrazloženo zahtevo posredovati zahtevane podatke brezplačno. Pri opredelitvi upravljavca in obdelovalca osebnih podatkov se sledi opredelitvi v predpisih s področja varstva osebnih podatkov. Upravljavec osebnih podatkov je tako vsaka fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave.¹⁰ Obdelovalec osebnih podatkov je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca.¹¹ Zakonska določitev obeh kategorij je z vidika dela agencije nujno potrebna, saj se le tako zajamejo vsi relevantni deležniki, ki lahko agenciji posredujejo podatke, potrebne za opravljanje njenih nalog. S spremembo se določata tudi dva načina oziroma možnosti posredovanja zaprosenih podatkov, in sicer upravljavci ali obdelovalci podatkov agenciji posredujejo podatke oziroma omogočijo vpogled po predhodnem dogovoru. Gre za uvedbo možnosti elektronske izmenjave zaprosil, ki bi nadomestila klasično izmenjavo podatkov, njena prednost pa je predvsem hitrost pridobitve podatkov, ki je pogosto pomembna pri izvajanju nalog agencije. Elektronska izmenjava podatkov bi bila vzpostavljena na sistemih, ki takšno izmenjavo sploh dopuščajo, saj agencija pretežno posluje s podatki, ki so označeni s stopnjo tajnosti. Posredovanje zahtevkov in pridobivanje podatkov bo tudi v elektronskih sistemih potekalo ob skrbnem beleženju izmenjanih podatkov, revizijskih sledi in dnevnikov obdelav, pri čemer se bodo spoštovala določila predpisov s področja varstva osebnih in tajnih podatkov ter informacijske varnosti.

K 6. členu

S spremembo zakona se opredeljuje več kategorij dokumentarnega gradiva agencije in v skladu s specifikami posamezne kategorije se določajo roki dostopnosti oziroma kraj hrambe.

Splošno gradivo agencije se obravnava v skladu s predpisi s področja dokumentarnega in arhivskega gradiva ter s predpisi, ki urejajo področje tajnih podatkov, če ta zakon ne določa drugače. Gre za kategorijo dokumentov agencije, ki nastajajo pri njenem splošnem poslovanju kot organu v državni upravi. Rok za izročitev takšnega gradiva je določen v splošnem predpisu s področja dokumentarnega in arhivskega gradiva.

Dokumentarno gradivo iz razvida je posebna oblika dokumentarnega gradiva agencije, ki neposredno izhaja iz njene obveščevalne in protiobveščevalne dejavnosti oziroma mednarodnega sodelovanja. To gradivo se hrani v razvidu, ki je opredeljen kot urejena, ovrednotena in sistemizirana zbirka

¹⁰ 7. točka 4. člena Splošne uredbe

¹¹ 8. točka 4. člena Splošne uredbe

dokumentarnega gradiva. V skladu z ZSOVA ga oblikuje in vodi agencija v zvezi s pridobivanjem, z vrednotenjem in s sistematičnim urejanjem podatkov iz prvega in drugega odstavka 2. člena istega zakona. Za to kategorijo dokumentarnega gradiva velja, da se, razen dveh izjem, opredeljenih v nadaljnjih odstavkih, preda Arhivu Republike Slovenije 50 let po zaključku posamezne zadeve.

Prva izjema od prvega in drugega odstavka so identifikacijski podatki uradnih oseb agencije in oseb, ki z agencijo sodelujejo, ter podatki o nazivu, ki ga agencija uporablja za finančno in materialno poslovanje do tretjih oseb. Ti podatki postanejo arhivsko gradivo in se predajo Arhivu Republike Slovenije po 75 letih od pridobitve oziroma nastanka tega gradiva.

Druga izjema od prvega in drugega odstavka se nanaša na dokumentarno gradivo, ki vsebuje podatke, za katere je tuja obveščevalno-varnostna služba ali mednarodna organizacija določila omejitve nadaljnjega posredovanja, ter podatke, ki omogočajo identifikacijo tajnih sodelavcev agencije ali pripadnikov tujih obveščevalno-varnostnih služb ali mednarodnih organizacij. Podatke iz tega odstavka agencija hrani trajno, dostopnost do podatkov oziroma spremembo statusa v arhivsko gradivo pa se določa v skladu z omejitvami tuje službe oziroma mednarodne organizacije ter določili druge področne zakonodaje.

K 7. členu

Obstoječi 23. člen še vedno ohranja naravo napolilne določbe za posebno obliko pridobivanja podatkov, pri čemer se obstoječe pooblastilo kontrole pisem in drugih občil ter nadzorovanje in snemanje telekomunikacij dopolnjuje z novima oblikama pridobivanja podatkov, in sicer z uvedbo tehničnega sredstva za nadzor signala mobilne telefonije ter z uvedbo neposrednega dostopa do podatkov telekomunikacijskega sredstva in beleženja komunikacijskega prometa na sredstvu. Zaradi konsistentnosti se ohranja obstoječa terminologija t. i. oblik pridobivanja podatkov, četudi pomeni uvedba tehničnega sredstva za nadzor signala mobilne telefonije bolj način pridobivanja podatkov kot njegovo obliko.

Novi obliki pridobivanja podatkov sta dodani v obstoječi 23. člen, ker se za vsa tri navedena pooblastila agencije zahteva odobritev predsednika Vrhovnega sodišča Republike Slovenije.

K 8. členu

Predlog spremembe zakona uvaja možnost uporabe tehničnega sredstva za nadzor signala mobilne telefonije. Izpostavlja se več omejenosti tehničnega vidika sredstva kot uporabe z zaostritvijo zakonskih pogojev. Pridobitev tehničnih podatkov o mobilnih napravah še ne pomeni, da se bodo v skladu s tem zakonom obdelovali osebni podatki, saj cilj agencije v tako zgodnji fazi ni identifikacija oziroma povezovanje podatkov s konkretnimi posamezniki, temveč izločanje in osredotočanje na želene vsebine v skladu z zakonom. Prav s tem se omogoča najmanjši možni vpliv v zasebnost posameznikov, ki se jih po tem zakonu opredeljuje kot tretje osebe. Gre za uporabo tehničnega sredstva, ki bo omogočalo zgolj identifikacijo mobilnih komunikacijskih signalov, ne pa tudi vpogleda v vsebino komunikacij ali metapodatke. Rezultat uporabe take naprave bo presek mobilnih signalov, torej le tistih, ki se bodo pojavljali na posameznih varnostno relevantnih lokacijah oziroma situacijah, medtem ko se podatki o drugih signalih ne bodo obdelovali niti hranili. Dodatno omejitev pomeni kratko obdobje uporabe tehničnega sredstva za nadzor signala mobilne telefonije. Tehnično sredstvo je dovoljeno uporabljati 15 dni brez možnosti podaljšanja. Dodatno sistemsko varovalko pomeni prepoved uporabe tehničnega sredstva, ki omogoča ali bi lahko omogočalo prisluškovanje in snemanje elektronskih komunikacij ter prepoved ugotavljanja lokacije komunikacijskih sredstev tretjih oseb.

Agencija bo predmetno tehnično sredstvo uporabljala kot delovni pripomoček, saj po vsebini njegova uporaba pomeni predhodno fazo za nadaljnje ukrepe agencije. Agencija bo z njegovo uporabo

pridobila podatke, potrebne za razpoznavo številke komunikacijskega sredstva in številke za elektronsko komuniciranje, ter podatke o lokaciji komunikacijskega sredstva. Teh podatkov sicer z obstoječimi ukrepi ne bi mogla pridobiti ali bi bilo njihovo pridobivanje povezano z nesorazmernimi težavami, lahko pa tudi z ogrožanjem zdravja in življenja uslužbencev in sodelavcev agencije.

Posebno obliko pridobivanja podatkov odredi predsednik Vrhovnega sodišča Republike Slovenije za vsak primer posebej, kadar bodo izpolnjeni zakonsko določeni pogoji. Poleg sodne odobritve je določen tudi naknadni nadzor v obliki vmesnega poročila agencije o uporabi navedenega sredstva, ki bo posredovan predsedniku Vrhovnega sodišča Republike Slovenije. Z obveznostjo priprave takšnega poročila se bo dodatno vzpostavil interni nadzorni cikel na strani agencije, ki bo morala vzpostaviti periodično spremljanje in nadzor nad izvajanjem odredb predsednika Vrhovnega sodišča Republike Slovenije. Interno spremljanje in nadzor bosta pomenila neposredno kontrolo strokovnosti in zakonitosti izvajanja nalog agencije, medtem ko bo predsednik Vrhovnega sodišča Republike Slovenije vršil sodno kontrolo na več stopnjah – pred odobritvijo posamezne odredbe, po prenehanju odredbe s seznanitvijo o prenehanju oziroma zaključku uporabe ter tudi s t. i. periodičnim poročilom agencije. Obvestilna obveznost po zaključku zadeve v razvidu pa še dodatno krepi nadzor nad izvajanim ukrepom.

Agencija bo morala kot predlagateljica ukrepa v predlogu odredbe izkazati za vsak primer posebej obstoj velike verjetnosti, da obstaja nevarnost za varnost države, ki se kaže v alternativno naštetih aktivnostih. Aktivnosti izhajajo iz obstoječega 24. člena zakona, pri čemer je bil smiselno upoštevan blažji poseg v človekove pravice posameznikov, zato so aktivnosti v posameznih primerih splošneje opredeljene, da lahko zajamejo več potencialno relevantnih situacij.

Agencija bo morala v predlogu odredbe izkazati, da je utemeljeno pričakovati, da bo na določenem območju in v določenem časovnem obdobju tako možno identificirati osebe, ki izvajajo navedene aktivnosti, oziroma ugotoviti komunikacijska ali druga tehnična sredstva, ki se uporabljajo za te aktivnosti. Nadalje bo morala tudi utemeljiti, da teh podatkov ni mogoče opraviti na milejši način oziroma bi bilo to povezano z nesorazmernimi težavami.

Posebej je dodana omejitev, da v okviru predmetne posebne oblike pridobivanja podatkov ni dovoljeno prisluškovanje in snemanje elektronskih komunikacij ter ugotavljanje lokacije komunikacijskih naprav tretjih oseb.

Iz naslednjih odstavkov novega člena izhaja natančna opredelitev vsebine predloga in odredbe, kjer se smiselno sledi postopku, kot je predviden za obstoječ ukrep kontrole pisem in drugih pošilk ter nadzorovanja in snemanja telekomunikacij. Sledi časovna opredelitev trajanja ukrepa, in sicer je določen rok 15 dni brez možnosti podaljšanja. Tehnično sredstvo se preneha uporabljati takoj, ko prenehajo razlogi, zaradi katerih je bila odrejena njegova uporaba oziroma po preteku časovnega obdobja, določenega v odredbi. O prenehanju mora direktor agencije pisno obvestiti predsednika Vrhovnega sodišča Republike Slovenije.

V petem odstavku je določena omejitev, da lahko agencija obdeluje osebne podatke oseb, za katere ugotavlja, da ne sodelujejo pri izvajanju aktivnosti iz prvega odstavka, zgolj v obsegu, ki je iz tehničnih razlogov neizogibno potreben za doseg namena iz prvega odstavka tega člena in na način, ki najmanj posega v njihove pravice. Agencija sme začasno uporabiti podatke tretjih oseb izključno za namene ugotavljanja identitete oseb, zoper katere so usmerjene aktivnosti iz prvega odstavka, in jih mora po zaključku aktivnosti nemudoma izbrisati.

Po vsakem zaključku uporabe tehničnega sredstva mora agencija pripraviti poročilo o izvedeni aktivnosti in ga skupaj z zbranimi podatki posredovati v seznanitev predsedniku Vrhovnega sodišča Republike Slovenije. S to določbo se omogoča t. i. zapisniška sledljivost izvedbe ukrepa in pridobljenih

podatkov. Predsednik Vrhovnega sodišča Republike Slovenije odredi brisanje podatkov, za katere oceni, da niso potrebni za dosego namena iz prvega odstavka tega člena.

Po zaključitvi zadeve v razvidu direktor agencije obvesti posameznika, na katerega se je ukrep nanašal, da ima pravico, seznaniti se s pridobljenim gradivom, v primerih večjega obsega tega gradiva pa s poročilom, ki obsega povzetek zbranega gradiva. Dodana je omejitev te pravice, in sicer se lahko v primerih, kadar je mogoče utemeljeno sklepati, da bo zaradi seznaitve z gradivom nastala nevarnost za življenje ali zdravje ljudi ali za nacionalno varnost, direktor agencije odloči, da posameznika z vsebino pridobljenega gradiva ne bo seznanil. Takšno gradivo bo v skladu z določbami tega zakona, ki ureja dokumentarno gradivo agencije iz razvida, po poteku določenega roka postalo arhivsko gradivo.

Sledi določba z obveznostjo agencije, da najmanj enkrat na leto pripravi poročilo o nadzoru nad uporabo tehničnega sredstva za nadzor signala mobilne telefonije in z njim seznaniti predsednika Vrhovnega sodišča Republike Slovenije. Gre za t. i. periodično poročilo, ki predstavlja preplet internega in sodnega nadzora nad izvajanjem tega pooblastila agencije. Postopek uporabe tehničnega sredstva bo agencija opredelila v internem pravilniku, h kateremu bo soglasje podala Vlada Republike Slovenije.

K 9. členu

Novi a24.c člen predloga zakona uvaja možnost odobritve neposrednega dostopa do podatkov telekomunikacijskega sredstva za namen beleženja komunikacijskega prometa na sredstvu v Republiki Sloveniji in v tujini. Za opredelitev telekomunikacijskega sredstva se uporablja terminologija, kot je že sprejeta in uporabljena v obstoječem zakonu. Pri izvajanju predmetnega ukrepa telekomunikacijsko sredstvo torej pomeni nadpomenko, ki zajema vsa primerna tehnična sredstva in sisteme, ki omogočajo oddajanje, prenašanje, sprejemanje in usmerjanje vseh vrst sporočil v obliki signalov, glasu, slike ali zvokov. Beleženje komunikacijskega prometa pa pomeni beleženje vseh informacij, ki se izmenjajo ali prenesejo preko posamezne komunikacijske storitve oziroma elektronskih omrežij. Komunikacijski promet je sestavljen iz vsebine in morebitnih pripadajočih prometnih, lokacijskih in meta podatkov.

Ukrep odobri na predlog direktorja agencije za vsak primer posebej predsednik Vrhovnega sodišča Republike Slovenije. Pogoji za pridobitev odredbe za ta ukrep so sicer v osnovi enaki kot za odobritev kontrole pisem in drugih pošilk ter nadzorovanje in snemanje telekomunikacij iz obstoječega 24. člena ZSOVA, pri čemer pa je za odobritev neposrednega dostopa za namen beleženja telekomunikacijskega prometa na sredstvu treba nedvoumno izkazati okoliščine, ki bodo zahtevale takojšnje ukrepanje in nujno sprejetje ustreznih ukrepov za zaščito nacionalne varnosti. Agencija bo tako lahko predlagala uvedbo te posebne oblike pridobivanja podatkov le v primeru posebej opredeljenih situacij, ko bo podana velika verjetnost, da obstaja nevarnost za varnost države. Upošteva stopnjo invazivnosti ukrepa v ustavno zagotovljene človekove pravice je torej odobritev uporabe ukrepa neposredno povezana s primeri izjemnih varnostnih situacij, s čimer se omejuje uporabo sredstva, hkrati pa agenciji omogoča, da se v situacijah, ko nacionalni varnosti grozi neposredna sedanja oziroma predvidljiva prihodnja nevarnost, ustrezno odzove.

Agencija bo morala v predlogu odredbe jasno izkazati obstoj ene ali več od navedenih aktivnosti, hkrati pa utemeljiti prepričanje, da se v zvezi s to aktivnostjo uporablja določeno telekomunikacijsko sredstvo ali bo to sredstvo uporabljeno.

Dodaten pogoj je obrazložitev agencije, da je mogoče utemeljeno sklepati, da teh podatkov ni mogoče pridobiti drugače oziroma bi njihovo pridobivanje na drug način oziroma z drugo obliko lahko ogrozilo življenje ali zdravje ljudi oziroma bi pomenilo resno grožnjo nacionalni varnosti. Upošteva najvišjo

stopnjo invazivnosti ukrepa se torej tudi pri zadostitvi načela oziroma pogoja subsidiarnosti upošteva stopnja nevarnosti za javno varnost oziroma resna grožnja nacionalni varnosti.

Dokazni standard, kot je oblikovan in pripoznan pri delovanju obveščevalnih služb, je v primeru odobritve uporabe nove posebne oblike najstrožji. Zahtevana je *neposrednost* grozeče nevarnosti in hkrati njena *sedanjost*, ki je v določenih primerih, kadar takšna oblika ni možna ali mogoča, nadomeščena z visoko stopnjo predvidljivosti nastanka grozeče aktivnosti. S tem se pomembno oddaljimo od drugih aktivnosti, za katere se uporabljajo že obstoječe klasične metode pridobivanja podatkov na obveščevalnem področju.

Sledita dva izrecni omejitvi agencije, ki opredeljujeta način izvedbe ukrepa in s tem pomenita pomembni varovalki za poseganje v ustavne pravice zadevnih posameznikov. Izbrano tehnično sredstvo, ki bo uporabljeno za izvajanje neposrednega dostopa do podatkov telekomunikacijskega sredstva za namen beleženja komunikacijskega prometa na sredstvu, bo moralo delovati tako, da bo omogočena namestitvev in izvedba odobrene naloge brez vstopa v tuje stanovanje oziroma v druge prostore. Z izrecno prepovedjo vstopa v tuje stanovanje ali druge prostore pri izvajanju predmetne oblike pridobivanja podatkov se odpravlja dvom v zvezi z izvedbo ukrepa, saj agencija že sedaj nima zakonskega pooblastila za vstop v tuje stanovanje ali druge prostore, hkrati pa se varuje ustavna pravica nedotakljivosti stanovanja, kot izhaja iz 36. člena Ustave Republike Slovenije.

Prav tako v okviru izvajanja posebne oblike pridobivanja podatkov ni dovoljeno poseganje v vsebino komunikacije z namenom njenega spreminjanja, dopolnjevanja ali kakršnega koli drugačnega predruženja. S tem se dodatno izpostavlja obveznost agencije, da do podatkov zgolj dostopa in beleži promet, smiselno enako kot pri ukrepu iz 24. člena ZSOVA.

Iz četrtega odstavka novega člena izhaja natančna opredelitev vsebine predloga in odredbe, s katero se nadaljuje smiselno enako odobravanje ukrepov predsednika Vrhovnega sodišča Republike Slovenije, saj se sledi strukturi in že poznanemu postopku za odobritev ukrepa kontrole pisem in drugih pošilk ter nadzorovanja in snemanja telekomunikacij. V predlogu odredbe bo treba natančno opredeliti nujno potrebne spremembe na telekomunikacijskem sredstvu, ki so potrebne za dostop do podatkov za namen beleženja komunikacijskega prometa.

V petem odstavku sledi časovna opredelitev trajanja ukrepa. Tehnično sredstvo se uporablja najkrajši možni čas za doseg namena iz prvega odstavka tega člena, vendar ne dlje kot en mesec od prejema odredbe predsednika Vrhovnega sodišča Republike Slovenije. Možno je podaljšanje ukrepa, vendar skupno ne več kot tri mesece. V šestem odstavku sledi omejitev, da se uporaba tehničnega sredstva odpravi takoj, ko prenehajo razlogi, zaradi katerih je bila odrejena, oziroma po preteku časovnega obdobja, določenega v odredbi. Pri tem je agencija dolžna tehnično zagotoviti, da se nameščeni program odstrani oziroma onesposobi. O prenehanju direktor agencije pisno obvesti predsednika Vrhovnega sodišča Republike Slovenije.

Sledi omejitev, da lahko agencija obdeluje osebne podatke tretjih oseb zgolj v obsegu, ki je iz tehničnih razlogov neizogibno potreben za doseg namena iz prvega odstavka tega člena, in na način, ki najmanj posega v njihove pravice.

Po zaključku uporabe tehničnega sredstva agencija v štirinajstih dneh pripravi poročilo o izvedeni aktivnosti ter ga skupaj z zbranimi podatki posreduje v seznanitev predsedniku Vrhovnega sodišča Republike Slovenije. Le-ta odredi brisanje podatkov, za katere oceni, da niso potrebni za doseg namena iz prvega odstavka tega člena. Z navedenim se zadosti pogoju zapisniške sledljivosti.

Dodana je tudi posebna določba, na podlagi katere je pod določenimi pogoji o izvedbi ukrepa obveščen tudi nadzorovani posameznik, s čimer mu je dana možnost, da zahteva naknadno sodno varstvo. Po zaključitvi zadeve v razvidu direktor agencije v 90 dneh obvesti posameznika, na katerega

se je ukrep nanašal, da ima pravico, seznaniti se s pridobljenim gradivom, v primerih večjega obsega tega gradiva pa s poročilom, ki obsega povzetek zbranega gradiva. Dodana je omejitev te pravice, in sicer se lahko v primerih, kadar je mogoče utemeljeno sklepati, da bo zaradi seznanitve z gradivom nastala nevarnost za življenje ali zdravje ljudi ali za nacionalno varnost, direktor agencije odloči, da posameznika z vsebino pridobljenega gradiva ne bo seznanil. Takšno gradivo bo v skladu z določbami tega zakona, ki ureja dokumentarno gradivo agencije iz razvida, po poteku določenega roka postalo arhivsko gradivo.

Izvajanje nadzora nad predmetno obliko bo večstopenjsko. Poleg sodnega nadzora je uveden tudi t. i. periodični nadzor nad zakonitostjo uporabe tehničnega sredstva, ki je preplet internega in sodnega nadzora. Agencija bo najmanj enkrat na leto pripravila poročilo o nadzoru nad uporabo tehničnega sredstva in z njim seznanila predsednika Vrhovnega sodišča Republike Slovenije. Namen tega poročila je izvajanje rednega nadzora v agenciji, kjer se bo poleg zakonitosti (ki jo bo preveril že predsednik Vrhovnega sodišča Republike Slovenije pri vsakokratni odobritvi ukrepa) preverjala še strokovnost izvedbe, kar vključuje tudi hrambo podatkov in njihovo brisanje ter spoštovanje predpisov s področja tajnih podatkov. Predsedniku Vrhovnega sodišča Republike Slovenije bo vsaj enkrat na leto posredovano kumulativno poročilo z ugotovitvami internega nadzora. Od agencije bo lahko zahteval dodatne obrazložitve ali pojasnila, primarni namen pa je izboljševanje prakse agencije glede izvajanja predmetnega ukrepa. Posledično pomeni vključitev predsednika Vrhovnega sodišča Republike Slovenije v interni nadzorni mehanizem tudi povečanje pomembnosti tega instituta, saj bo z obveznostjo posredovanja ugotovitev "zunajni instituciji" agencija dodatno prispevala k transparentnosti izvajanja ukrepa in s tem k njegovi zakoniti in strokovni izvedbi. Kontinuiteta odobravanja ukrepa s strani ene sodne avtoritete in s tem združitev vseh potrebnih informacij (pretežno) v eni osebi, gotovo pa v eni funkciji, pomeni veliko prednost pri zagotavljanju zahtevane ravni utemeljenosti za odobritev ukrepa.

Drugo obliko nadzora predstavlja nov institut, tj. pooblaščenec za nadzor. V skladu s predlogom zakona mu bo agencija morala omogočiti vpogled v vse listine, podatke in postopke v zvezi z izvajanjem ukrepa. Tako bo lahko med izvajanjem te posebne oblike pridobivanja podatkov oziroma po zaključku le-tega presojal, ali se ukrep izvaja v skladu s tehničnimi, postopkovnimi in z zakonskimi zahtevami. O svojih ugotovitvah bo obveščal neposredno agencijo in predsednika Vrhovnega sodišča Republike Slovenije. Ob morebitnih ugotovljenih pomanjkljivostih bo ukrep v skladu z drugimi določbami tega člena odpravljen, o ugotovljenih nepravilnostih pri izvajanju ukrepov v posameznih zadevah pa bo periodično redno obveščena¹² tudi Komisija za nadzor obveščevalnih in varnostnih služb. Ta bo še vedno vršila tudi svoj nadzor, ki vključuje tudi preverjanje delovanja agencije v celoti ter izvajanje letnih programov in načrtov.

Pooblaščenca za nadzor bo za mandatno dobo 5 let imenovala Vlada Republike Slovenije. Imenovana oseba bo morala izpolnjevati taksativno naštetе pogoje, pri katerih pa so njihov najpomembnejši del zlasti 10-letne izkušnje na delovnih mestih, na katerih se zahteva strokovno znanje s področij ustavnega prava, človekovih pravic ali nacionalne varnosti. Navedeno bo imenovani osebi omogočilo ustrezno razumevanje delovanja obveščevalne službe ter njenih specifičnih metod in tehnik dela. Glede na to da bo imela takšna oseba dostop do najboljčutljivejših podatkov, bo morala najprej uspešno opraviti varnostno preverjanje, njeno imenovanje pa ne bo smelo pomeniti varnostnega tveganja za agencijo.

Postopek uporabe tehničnega sredstva bo agencija opredelila v internem pravilniku, h kateremu bo soglasje podala Vlada Republike Slovenije.

K 10. členu

¹² Osmo alinejo drugega odstavka 19. člena Zakona o parlamentarnem nadzoru obveščevalnih in varnostnih služb (Uradni list RS, št. 93/07 – uradno prečiščeno besedilo).

Določba obstoječega 24.c člen se črta, saj je nepotrebna, ker je vsebina o načinu nadomeščanja predsednika Vrhovnega sodišča Republike Slovenije že določena v matičnem zakonu, ki ureja sodišča. Ponavljanje enake vsebine je nepotrebno in pravnosistemsko nedopustno.

K 11. členu

Zaradi specifičnosti poklica uradnih osebe agencije se kandidati za zaposlitev iščejo med različnimi profili poklicev, z različno izobrazbo in delovnimi izkušnjami, zato javna objava ali razpis nista vedno najprimernejši obliki za iskanje in zaposlitev.. V primeru zaposlitve brez javne objave oziroma razpisa se še vedno izvedejo vsi postopki po ZSOVA (varnostno preverjanje) ter preverjanje pogojev za zasedbo delovnega mesta.

Podatki o zaposlenih v agenciji in nekdanjih zaposlenih so tajni podatek v skladu z zakonom, ki ureja tajne podatke. V primeru (javne) objave ali razpisa za delovno mesto v agenciji mora zato vse postopke voditi neposredno agencija in ne novi Center za kadre, ustanovljen na podlagi zakona, ki ureja sistem javnih uslužbencev.

Lahko pa agencija ministrstvo, pristojno javno upravo, zaprosi za strokovno pomoč pri posameznih fazah postopka, kot so pomoč pri presoji osebnih sposobnosti in veščin za opravljanje dela v drugem delu izbirnega postopka v javnem natečaju, pomoč pri razvoju sistema osebnih sposobnosti in veščin za opravljanje dela ter drugih orodij za ravnanje s kadri v organih državne uprave in druge naloge na področju ravnanja s kadri v skladu s pristojnostmi ministrstva, pristojnega za javno upravo.

K 12. členu

Spremembe in dopolnitve 34. člena obstoječega zakona se uvodoma nanašajo na nomotehnični popravek uporabljene terminologije, da bo ta v skladu z opredelitvijo v predpisih, ki se nanašajo na delovnopravna razmerja in sistem javnih uslužbencev.

Vzpostavlja se pravna podlaga za posebno ureditev pri spoštovanju določil delovnopravne zakonodaje na področju obveznega počitka ter omejitev glede tedenskih in mesečnih nadur. Nadaljnje opravljanje delovnih nalog se bo tako lahko odredilo v izjemnih primerih, ko bo posamezna izvršitev delovne naloge tako nujna za zagotovitev zakonskega cilja agencije, da bi njena prekinitve lahko pomenila nastanek neposredne škode agenciji ali nacionalni varnosti.

Navedene določbe se dodajajo zaradi zagotavljanja nemotenega opravljanja nalog agencije iz 2. člena zakona. Delovnopравни okviri iz splošne delovnopravne zakonodaje namreč niso primerni za delo uradnih oseb agencije, saj ne priznavajo posebnih razmer, v katerih mora delovati agencija, nanašajo pa se na omejitve (nad)urnega dela in obveznega počitka. Agencija se zaveda pomembnosti spoštovanja priznanih standardov (nad)urnega dela in počitka ter s tem vseh pravic delavcev, ki izvirajo iz tega konteksta, vendar pa potrebuje zakonsko izjemo, ki bo upravičevala morebitne presežke dogovorjenih kvot v izjemnih primerih. Izvedba nalog uradnih oseb agencije bo tudi takrat omejena na najkrajši možni delovni čas, o njihovi prekinitvi pa bo uradnim osebam zagotovljen ustrezen počitek.

Zakonska ureditev pripravljenosti na delo je potrebna zaradi priporočila Računskega sodišča Republike Slovenije, ki je v letu 2021 opravilo nadzor nad poslovanjem agencije. Računsko sodišče je agenciji naložilo, da poskrbi za ustrezno zakonsko opredelitev možnosti odreditve pripravljenosti na domu, ki je dosednji zakon ni vseboval.

Institut pripravljenosti na delo je kot poseben delovni pogoj urejen v novem osmem odstavku, v katerem je določeno, da mora biti uradna oseba agencije seznanjena z odrejeno pripravljenostjo za

delo najmanj tri dni vnaprej po razporedu dela oziroma s posebno odredbo. Uradna oseba agencije mora biti za potrebe prihoda na delovno mesto ali kraj, kjer je treba opraviti nujno nalogo, dosegljiva po telefonu ali drugih komunikacijskih sredstvih.

K 13. členu

S prehodno določbo se ureja sprejem internega akta iz novega četrtega odstavka 14. člena zakona, devetega odstavka novega 23.a člena in 11. odstavka novega a24.c člena. Prvi interni akt mora biti sprejet v šestih mesecih po uveljavitvi zakona, naslednja dva pa v enem letu po uveljavitvi zakona in pred pričetkom posamezne posebne oblike pridobivanja podatkov.

K 14. členu

S prehodno določbo se določa rok za imenovanje pooblaščenca za nadzor iz novega b24.c člena. Pooblaščenec mora biti imenovan v enem letu po uveljavitvi zakona in pred pričetkom uporabe posebne oblike pridobivanja podatkov iz a24.c člena zakona.

K 15. členu

Predlog določa petnajstdnevni *vacatio legis*.

IV. BESEDILO ČLENOV, KI SE SPREMINJAJO

2. člen

(1) Agencija pridobiva in vrednoti podatke ter posreduje informacije:

- iz tujine, pomembne za zagotavljanje varnostnih, političnih in gospodarskih interesov države;
- o organizacijah, skupinah in osebah, ki s svojo dejavnostjo iz tujine ali v povezavi s tujino ogrožajo ali bi lahko ogrozile nacionalno varnost države in njeno ustavno ureditev.

(2) Agencija sodeluje s pristojnimi državnimi organi in službami pri varnostnem preverjanju ter posreduje podatke, pomembne za varnost določenih oseb, delovnih mest, organov, objektov in okolišev.

(3) Agencija opravlja naloge na podlagi zakona v skladu s prednostnimi nalogami, ki jih določi vlada na podlagi nacionalnovarnostnega programa, ki ga sprejme Državni zbor.

4.a člen

Za postopek izbire direktorja agencije se ne uporabljajo določbe Zakona o javnih uslužbencih (Uradni list RS, št. 56/02 in 110/02-ZDT-B).

12. člen

(1) Agencija za uresničevanje nalog iz prvega in drugega odstavka 2. člena tega zakona zbira, obdeluje, shranjuje in posreduje osebne ter druge podatke in vodi ter uporablja evidence na podlagi predpisov o varstvu osebnih podatkov, če s tem zakonom za posamezne primere ni določeno drugače.

(2) Kadar agencija posreduje osebne podatke tujim obveščevalnim in varnostnim službam v skladu s tem zakonom, mora pred tem pridobiti zagotovila, da ima država, v katero podatke odnaša, urejeno varstvo osebnih podatkov in da bo tuja obveščevalna ali varnostna služba uporabila osebne podatke samo za namene, določene s tem zakonom.

14. člen

(1) Agencija v okviru razvida iz prejšnjega člena vodi zbirko podatkov o osebah, ki jih agencija sistematično operativno obravnava v določenem časovnem obdobju.

(2) Zbirka podatkov o osebah, ki jih agencija operativno obravnava, obsega: ime in priimek, psevdonim, rojstne podatke (dan, mesec, leto, kraj, država), naslov stalnega in/ali začasnega bivališča, državljanstvo, šolsko izobrazbo, poklic, zaposlitev in razlog za operativno obravnavo.

(3) Osebni podatki iz prvega odstavka tega člena se shranjujejo in uporabljajo do zaključitve zadeve v razvidu, potem se iz zbirke osebnih podatkov izbrišejo oziroma blokirajo.

16. člen

(1) Upravitelji zbirk osebnih podatkov morajo agenciji na obrazloženo pisno zahtevo direktorja agencije pisno posredovati osebne in druge podatke ali jih dati na vpogled.

(2) Državni organi in organizacije z javnimi pooblastili posredujejo osebne podatke brezplačno.

18. člen

Zaključena zadeva v razvidu se prenese v zbirko dokumentarnega gradiva agencije. Po roku, ki ga določita direktor agencije in direktor Arhiva Republike Slovenije in ki ne sme biti daljši od enega leta, se dokumentarno gradivo iz zbirke arhivsko uredi ter preda Arhivu Republike Slovenije.

23. člen

Agencija lahko pod pogoji, določenimi s tem zakonom, izjemoma pridobiva podatke tudi s kontrolo pisem in drugih občil ter z nadzorovanjem in s snemanjem telekomunikacij.

24.c člen

V primeru odsotnosti predsednika Vrhovnega sodišča Republike Slovenije opravlja njegove pristojnosti iz 24., 24.a in 24.b člena tega zakona podpredsednik Vrhovnega sodišča Republike Slovenije.

28. člen

(1) Delovno razmerje v agenciji se lahko sklene brez objave oziroma razpisa.

(2) Kandidatu, s katerim ne bo sklenjeno delovno razmerje, agencija ni dolžna sporočiti razlogov za svojo odločitev.

34. člen

(1) Uradne osebe agencije morajo na podlagi odredbe direktorja agencije ali osebe, ki jo za to pooblasti, opravljati delo v posebnih delovnih razmerah, kadar je to potrebno za izvajanje z zakonom določenih nalog.

(2) Posebne delovne razmere so:

- delo v neenakomernem delovnem času;
- delo v izmenah;
- delo ob sobotah, nedeljah, praznikih in drugih dela prostih dneh;
- delo preko polnega delovnega časa;
- popoldansko in nočno delo;
- delo v podaljšanem delovnem času;
- izraba in prekinitev dopusta glede na potrebe agencije.

(3) Delo v neenakomernem delovnem času oziroma izmenah vključuje opravljanje delovne obveznosti ob sobotah, nedeljah, praznikih in drugih dela prostih dneh ter delo v popoldanskem in nočnem času v okviru določene redne mesečne oziroma letne delovne obveznosti.

(4) Delovna mesta, na katerih poteka delo v skladu s prejšnjim odstavkom, se določijo v aktu o notranji organizaciji in sistemizaciji delovnih mest.

(5) Druge oblike dela v posebnih delovnih razmerah se odredijo, če to terjajo delovne obveznosti oziroma je samo tako mogoče opraviti določene naloge, ki jih ni moč odlagati ali pa morajo biti opravljene v določenem roku.