



Mnenje 28/2025 o osnutku izvedbenega sklepa Evropske komisije v skladu z Uredbo (EU) 2016/679 o ustreznem varstvu osebnih podatkov v Braziliji

Različica 1.0

Sprejeto 4. novembra 2025

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Povzetek

Evropska komisija je 5. septembra 2025 začela postopek za sprejetje osnutka izvedbenega sklepa (v nadaljnjem besedilu: osnutek sklepa) o ustreznem varstvu osebnih podatkov v Federativni republiki Braziliji (v nadaljnjem besedilu: Brazilija).

Evropska komisija je 5. septembra 2025 Evropski odbor za varstvo podatkov zaprosila za mnenje. Evropski odbor za varstvo podatkov je ustreznost ravni varstva, ki jo zagotavlja Brazilija, ocenil na podlagi proučitve samega osnutka sklepa in analize dokumentacije, ki je javno dostopna na uradnih spletnih mestih brazilskih organov.

Evropski odbor za varstvo podatkov se je osredotočil na oceno splošnih vidikov splošne uredbe o varstvu podatkov¹ v osnutku sklepa in na dostop javnih organov do osebnih podatkov, ki se prenašajo iz EGP za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter nacionalne varnosti, vključno s pravnimi sredstvi, ki so na voljo posameznikom v EGP. Ocenil je tudi, ali so zaščitni ukrepi, določeni v pravnem okviru v Braziliji, vzpostavljeni in učinkoviti.

Evropski odbor za varstvo podatkov je kot glavna referenčna dokumenta za to dejavnost uporabil referenčni dokument o ustreznosti, ki ga je 28. novembra 2017 sprejela Delovna skupina iz člena 29², kakor je bil nazadnje revidiran in ga je Evropski odbor za varstvo podatkov sprejel 6. februarja 2018 (v nadaljnjem besedilu: referenčni dokument o ustreznosti), in svoja Priporočila 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe.

Evropski odbor za varstvo podatkov pozitivno ugotavlja, da okvir za varstvo podatkov, zlasti splošni zakon o varstvu osebnih podatkov v Braziliji (*Lei Geral de Proteção de Dados Pessoais*, LGPD) skupaj s predsedniškimi odloki in zavezujočimi uredbami, ki jih je izdal brazilski nacionalni organ za varstvo podatkov (*Agencia Nacional de Proteção de Dados*, ANPD), določa zahteve (tudi v zvezi z načeli, pravicami posameznikov, na katere se nanašajo osebni podatki, prenosi, nadzorom in pravnim varstvom), ki so tesno usklajene s splošno uredbo o varstvu podatkov in sodno prakso Sodišča Evropske unije (v nadaljnjem besedilu: Sodišče).

Evropski odbor za varstvo podatkov je poleg tega ugotovil, da bi morala Evropska komisija v osnutku sklepa pojasniti nekatere vidike brazilskega pravnega okvira in pozorno spremljati njegov razvoj.

V zvezi z načelom odgovornosti in zahtevami za oceno učinka v zvezi z varstvom podatkov Evropski odbor za varstvo podatkov meni, da je obveznost izvedbe te ocene pomembna v primerih, ko bi lahko obdelava povzročila veliko tveganje za pravice in svoboščine posameznikov, ter da ocena učinka v zvezi z varstvom podatkov zajema oceno nujnosti in sorazmernosti obdelave. Zato poziva Evropsko komisijo, naj spremlja praktično izvajanje teh zahtev.

¹ 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.

² Delovna skupina iz člena 29, dokument WP 254 rev. 01, ki je bil sprejet 28. novembra 2017 ter kakor je bil nazadnje revidiran in sprejet 6. februarja 2018 ter ki ga je potrdil Evropski odbor za varstvo podatkov.

S splošnim zakonom o varstvu osebnih podatkov je v nekaterih primerih predvidena omejitev zagotavljanja informacij posameznikom, na katere se nanašajo osebni podatki, ali nadzornemu organu na podlagi „poslovne in industrijske skrivnosti“. Ob upoštevanju pomena zahtev glede preglednosti za možnost posameznikov, na katere se nanašajo osebni podatki, da nadzirajo, kako se njihovi podatki obdelujejo, in pomena obveznosti sodelovanja z nadzornim organom, zlasti za zagotavljanje informacij, potrebnih za njegove nadzorne naloge, Evropski odbor za varstvo podatkov poziva Evropsko komisijo, naj spremlja izvajanje teh omejitev v praksi, da bi bolje razumela njihov učinek na pravici do obveščenosti in dostopa ter na pooblastila nacionalnega organa za varstvo podatkov, če obstajajo.

Evropski odbor za varstvo podatkov v zvezi s pravili o nadaljnjem prenosu poziva Evropsko komisijo, naj v osnutku sklepa pojasni, ali se lahko prenosi v skladu s pogoji, enakovrednimi členu 49 splošne uredbe o varstvu podatkov, izvajajo le v izjemnih okoliščinah, ko ni mogoče uporabiti drugih instrumentov za prenos. Komisija je tudi pozvana, naj pojasni, ali so posamezniki, na katere se nanašajo osebni podatki, obveščeni o: morebitnih tveganjih prenosa, kadar ta temelji na njihovi privolitvi, in okoliščinah prenosa (trajanje in namen prenosa, ciljne države, odgovornosti udeleženih strani, pravice posameznikov, na katere se nanašajo osebni podatki, in sredstva za njihovo uveljavljanje), ne glede na uporabljeno orodje za prenos.

Poleg tega Evropski odbor za varstvo podatkov Evropsko komisijo poziva, naj podrobneje opredeli naloge nacionalnega sveta za varstvo osebnih podatkov in zasebnosti ter njegovo sodelovanje z nacionalnim organom za varstvo podatkov.

V zvezi z dostopom brazilskih javnih organov do osebnih podatkov, prenesenih upravljavcem in obdelovalcem v Braziliji za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter nacionalne varnosti (v nadaljnjem besedilu: vladni dostop), in njihovo uporabo s strani teh organov Evropski odbor za varstvo podatkov ugotavlja, da se splošni zakon o varstvu osebnih podatkov ne uporablja za obdelavo podatkov, ki se izvaja *izključno* za namene javne varnosti, nacionalne obrambe, državne varnosti ali preiskovanja in pregona kaznivih dejanj. Hkrati pozitivno ugotavlja, da brazilsko zvezno vrhovno sodišče v svoji sodni praksi splošni zakon o varstvu osebnih podatkov razlaga tako, da je njegova delna uporaba razširjena na obdelavo osebnih podatkov za kazenske preiskave in ohranjanje javnega reda.

Evropski odbor za varstvo podatkov glede na navedeno Komisijo poziva, naj v osnutku sklepa nadalje oceni in pojasni uporabo splošnega zakona o varstvu osebnih podatkov v primeru obdelave osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, vključno s preiskovalnimi in popravljivimi pooblastili nacionalnega organa za varstvo podatkov v razmerju do organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ter naj v okviru svoje obveznosti spremljanja skrbno upošteva vse pomembne spremembe v zvezi s tem.

Evropski odbor za varstvo podatkov ob upoštevanju dejstva, da imajo zvezne države široko diskrecijsko pravico pri opredeljevanju zadev nacionalne varnosti, kar omogoča izjeme zaradi nacionalne varnosti pri obdelavi osebnih podatkov, Komisijo poziva, naj v osnutku sklepa natančneje opiše in pojasni okvir pojma nacionalna varnost v skladu z brazilskim pravom. V zvezi s tem Komisijo poziva, naj nadalje pojasni, kako so izvzeta iz splošnega zakona o varstvu osebnih podatkov za namene nacionalne varnosti povezana z zbiranjem in izmenjavo podatkov med javnimi subjekti v okviru brazilskega obveščevalnega sistema (SISBIN).

Kazalo

1. UVOD	5
2. SPLOŠNI VIDIKI VARSTVA PODATKOV	6
2.1 Odgovornost in upravljanje podatkov	6
2.2 Področje uporabe in opredelitev pojmov	7
2.2.1 Stvarno področje uporabe in ozemeljska veljavnost splošnega zakona o varstvu osebnih podatkov	8
2.2.2 Opredelitev pojmov.....	8
2.3 Načela varstva podatkov in pravne podlage.....	9
2.3.1 Načela obdelave	9
2.3.2 Varnostni ukrepi in kršitve.....	11
2.3.3 Zakonitost obdelave.....	12
2.4 Pravice posameznikov.....	13
2.5 Omejitve nadaljnjih prenosov	13
2.6 Postopkovni in izvršilni mehanizmi	15
2.6.1 Neodvisen nadzor	16
2.6.2 Pravno varstvo	17
2.6.3 Sankcije	18
3. DOSTOP DO OSEBNIH PODATKOV, KI JIH IZ EVROPSKE UNIJE PRENESEJO JAVNI ORGANI V BRAZILIJ, IN NJIHOVA UPORABA.....	18
3.1 Dostop in uporaba s strani brazilskih javnih organov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.....	19
3.1.1 Pravni okvir na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj	19
3.1.2 Nujnost in sorazmernost	21
3.1.3 Nadaljnja uporaba podatkov in nadaljnji prenosi	22
3.1.4 Nadzor in pravno varstvo	23
3.2 Dostop in uporaba s strani brazilskih javnih organov za namene nacionalne varnosti	25

3.2.1 Obseg izjeme iz člena 4(III) splošnega zakona o varstvu osebnih podatkov in njena uporaba za kazniva dejanja zoper državno varnost.....	25
3.2.2 Pravni okvir za nacionalno varnost	26
3.2.3 Nadaljnji prenosi in mednarodni sporazumi	28
3.2.4 Nadzor in pravno varstvo	29
4. IZVAJANJE IN SPREMLJANJE OSNUTKA SKLEPA	30

Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 70(1), točka (s), Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljnjem besedilu: splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma o Evropskem gospodarskem prostoru (v nadaljnjem besedilu: EGP), zlasti Priloge XI in Protokola 37 k Sporazumu, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018³,

ob upoštevanju členov 12 in 22 svojega poslovnika –

SPREJEL NASLEDNJE MNENJE:

³ Sklice na „države članice“ v tem mnenju je treba razumeti kot sklice na „države članice EGP“.

1. UVOD

- (1) V poglavju V splošne uredbe o varstvu podatkov so določeni pogoji za prenose osebnih podatkov v tretjo državo ali mednarodno organizacijo. Prenosi osebnih podatkov se lahko izvedejo na podlagi sklepa Evropske komisije o ustreznosti (člen 45 splošne uredbe o varstvu podatkov) ali, če takega sklepa o ustreznosti ni, kadar upravljavec ali obdelovalec zagotovi ustrezne zaščitne ukrepe, vključno z izvršljivimi pravicami in pravnimi sredstvi za posameznika, na katerega se nanašajo osebni podatki (člen 46 splošne uredbe o varstvu podatkov). Če ni sklepa o ustreznosti ali ustreznih zaščitnih ukrepov, se prenos ali niz prenosov v tretjo državo ali mednarodno organizacijo izvede le pod določenimi pogoji (člen 49 splošne uredbe o varstvu podatkov).
- (2) Evropski odbor za varstvo podatkov opozarja, da so sklepi o ustreznosti, s katerimi je priznано neprekinjeno varstvo osebnih podatkov, ki se prenašajo iz EGP v tretje države ali mednarodne organizacije, zanesljivo orodje za prenos, s katerim se zagotavlja varstvo pravic posameznika, na katerega se nanašajo osebni podatki, kadar se podatki prenašajo zunaj EGP. V skladu z referenčnim dokumentom o ustreznosti⁴ in ustrezno sodno prakso Sodišča⁵ je treba izraz „ustrezna raven varstva“ iz člena 45(1) splošne uredbe o varstvu podatkov, čeprav tretji državi ni treba zagotoviti enake ravni varstva, kot je zagotovljena s pravnim redom Unije, v povezavi z Listino o temeljnih pravicah razumeti tako, da se z njim zahteva, da ta tretja država na podlagi svoje nacionalne zakonodaje ali mednarodnih zavez dejansko zagotavlja raven varstva temeljnih pravic in svoboščin, ki je v osnovi enakovredna ravni, zagotovljeni v Evropski uniji.
- (3) Brazilija je federativna republika, sestavljena iz zveze 26 zveznih držav in enega zveznega okrožja, kot je določeno v njeni zvezni ustavi (v nadaljnjem besedilu: ustava)⁶. Vsaka brazilska zvezna država ima tudi svojo ustavo, ki ne sme biti v nasprotju z zvezno ustavo. Zasebnost in varstvo podatkov sta v ustavi zaščitena kot temeljni pravici (členi 5(X), 5(XII) in 5(LXXIX) ustave)⁷, ustavno sodišče pa ju priznava vsem osebam, tudi tujcem, ne glede na to, ali te osebe prebivajo v Braziliji⁸ ali ne.
- (4) Glavni zakonodajni akt, ki ureja varstvo podatkov, je splošni zakon o varstvu osebnih podatkov ali *Lei Geral de Proteção de Dados* (LGPD) (zakon št. 13.709 z dne 14. avgusta 2018, nazadnje spremenjen z zakonom št. 14.460 z dne 25. oktobra 2022). Dopolnjujeta ga

⁴ Delovna skupina iz člena 29, dokument WP 254 rev. 01, ki je bil sprejet 28. novembra 2017 ter kakor je bil nazadnje revidiran in sprejet 6. februarja 2018 ter ki ga je potrdil Evropski odbor za varstvo podatkov, poglavje 3, točka C.

⁵ Sodba Sodišča z dne 6. oktobra 2015, Maximilian Schrems/Data Protection Commissioner (v nadaljnjem besedilu: sodba Schrems), C-362/14, in sodba Splošnega sodišča z dne 3. septembra 2025, Philippe Latombe/Evropska komisija (v nadaljnjem besedilu: sodba Latombe), T-553/23.

⁶ Glej uvodno izjavo 7 osnutka sklepa.

⁷ Glej uvodno izjavo 8 osnutka sklepa.

⁸ Glej uvodno izjavo 9 osnutka sklepa.

zavezujoča odloka (predsedniški odlok št. 10.474 z dne 26. avgusta 2020 in predsedniški odlok št. 11.758 z dne 30. oktobra 2023), ki sta pravno zavezujoča in izvršljiva⁹.

- (5) Brazilski okvir za varstvo podatkov poleg splošnega zakona o varstvu osebnih podatkov vključuje tudi zavezujoče uredbe, ki jih je izdal brazilski nacionalni organ za varstvo podatkov (*Agencia Nacional de Proteção de Dados*, ANPD)¹⁰. V teh uredbah so določena dodatna pravila o razlagi in uporabi splošnega zakona o varstvu osebnih podatkov¹¹. Na primer, uredba št. 4 z dne 24. februarja 2024 o uporabi upravnih sankcij, uredba št. 15 z dne 24. aprila 2024 o uradnem obveščanju o varnostnih incidentih (v nadaljnjem besedilu: uredba o obveščanju o varnostnih incidentih), uredba št. 19 z dne 23. avgusta 2024 o mednarodnem prenosu osebnih podatkov (v nadaljnjem besedilu: uredba o prenosu podatkov), uredba št. 2 z dne 27. januarja 2022 o uporabi splošnega zakona o varstvu osebnih podatkov za mala in srednja podjetja, uredba št. 18 z dne 15. julija 2024 o vlogi pooblaščenih oseb za varstvo podatkov (v nadaljnjem besedilu: uredba o pooblaščenih osebah za varstvo podatkov).
- (6) Evropski odbor za varstvo podatkov pozdravlja ustavno priznanje pravic do zasebnosti in varstva podatkov kot temeljnih pravic, ki se nadalje izvajajo z nacionalnim pravom. Poleg tega pozitivno ocenjuje mednarodne zaveze, ki jih je sprejela Brazilija¹².
- (7) Evropski odbor za varstvo podatkov ugotavlja, da lahko institucije, organi, uradi in agencije Evropske unije v skladu s členoma 47 in 94 Uredbe (EU) 2018/1725¹³ prenesejo osebne podatke v tretjo državo, na ozemlje, v sektor ali mednarodno organizacijo, za katere Evropska komisija v skladu s členom 45(3) Uredbe (EU) 2016/679 priznava, da zagotavljajo ustrezno raven varstva, če je prenos namenjen izključno opravljanju nalog v pristojnosti upravljavca, ne da bi bilo potrebno dodatno dovoljenje. Evropsko komisijo poziva, naj na to pravno možnost opozori v uvodnih izjavah osnutka sklepa.

2. SPLOŠNI VIDIKI VARSTVA PODATKOV

2.1 Odgovornost in upravljanje podatkov

- (8) V splošnem zakonu o varstvu osebnih podatkov je kot eno od splošnih načel, ki se uporabljajo za obdelavo osebnih podatkov, določeno načelo odgovornosti. V skladu z njim morajo upravljavci in obdelovalci¹⁴ sprejeti ustrezne tehnične in organizacijske ukrepe, da lahko uspešno izpolnjujejo svoje obveznosti glede varstva podatkov in dokažejo tako izpolnjevanje,

⁹ Glej uvodni izjavi 11 in 12 osnutka sklepa.

¹⁰ Vse zavezujoče uredbe, ki jih je izdal nacionalni organ za varstvo podatkov, so na voljo tukaj: https://www.gov.br/anpd/pt-br/acao-a-informacao/institucional/atos-normativos/regulamentacoes_anpd.

¹¹ Glej uvodno izjavo 13 osnutka sklepa.

¹² Glej uvodne izjave 8, 9 in 10 osnutka sklepa.

¹³ Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

¹⁴ Izvajalci obdelave v skladu s členom 5(IX) splošnega zakona o varstvu osebnih podatkov.

med drugim pristojnim nadzornim organom (člen 46 splošnega zakona o varstvu osebnih podatkov). Evropski odbor za varstvo podatkov ugotavlja, da taki ukrepi vključujejo imenovanje pooblaščenih oseb za varstvo podatkov (člen 41 splošnega zakona o varstvu osebnih podatkov), kot je podrobneje opredeljeno v uredbi nacionalnega organa za varstvo podatkov o pooblaščenih osebah za varstvo podatkov, oceno učinka v zvezi z varstvom podatkov (člen 38 splošnega zakona o varstvu osebnih podatkov) in vodenje evidence o dejavnostih obdelave podatkov (člen 37 splošnega zakona o varstvu osebnih podatkov). Poleg tega je v splošnem zakonu o varstvu osebnih podatkov navedeno, da lahko upravljavci in obdelovalci oblikujejo notranja pravila za dobro prakso in modele upravljanja, vključno z načrti za izobraževalne dejavnosti, mehanizmom notranjega nadzora in zmanjševanjem tveganj (člen 50 splošnega zakona o varstvu osebnih podatkov). Evropski odbor za varstvo podatkov pozitivno ugotavlja, da so taki instrumenti podobni tistim, ki so v splošni uredbi o varstvu podatkov predvideni za izvajanje načela odgovornosti, in pozdravlja tako tesno usklajenost.

- (9) Evropski odbor za varstvo podatkov ugotavlja, da glede ocene učinka v zvezi z varstvom podatkov splošni zakon o varstvu osebnih podatkov ne vključuje jasne obveznosti izvedbe ocene učinka v zvezi z varstvom podatkov v primerih, ko bi lahko obdelava povzročila veliko tveganje za pravice in svoboščine posameznikov, kadar se nanaša le na morebitno zahtevo nacionalnega organa za varstvo podatkov. V zvezi s tem ugotavlja, da nacionalni organ za varstvo podatkov v „pogosto zastavljenih vprašanjih“¹⁵ o oceni učinka v zvezi z varstvom podatkov priporoča izvedbo ocene učinka v zvezi z varstvom podatkov, kadar bi lahko postopek obdelave povzročil veliko tveganje. Poleg tega v splošnem zakonu o varstvu osebnih podatkov ocena nujnosti in sorazmernosti ni izrecno vključena v obseg ocene učinka v zvezi z varstvom podatkov. Vendar se v pogosto zastavljenih vprašanjih o oceni učinka v zvezi z varstvom podatkov upravljavcem in obdelovalcem priporoča, naj v ocenah učinka v zvezi z varstvom podatkov ocenijo nujnost in sorazmernost obdelave.
- (10) Glede na navedeno Evropski odbor za varstvo podatkov Evropsko komisijo poziva, naj spremlja praktično izvajanje teh zahtev, da bi preverila, ali se ocena učinka v zvezi z varstvom podatkov izvede, kadar bi lahko postopek obdelave povzročil veliko tveganje za pravice in svoboščine posameznikov, ter ali je v ocene učinka v zvezi z varstvom podatkov vključena tudi ocena nujnosti in sorazmernosti postopkov obdelave glede na namene.

2.2 Področje uporabe in opredelitev pojmov

- (11) Poglavje 3 referenčnega dokumenta o ustreznosti je namenjeno „vsebinskim načelom“ ter se nanaša na osnovne pojme in načela varstva podatkov. Sistem tretje države ali mednarodne organizacije mora vsebovati take osnovne pojme in načela, da se zagotovi raven varstva osebnih podatkov, ki je v osnovi enakovredna ravni, zagotovljeni s pravom EU. Ni nujno, da so povsem enaki izrazju splošne uredbe o varstvu podatkov, vendar morajo odražati pojme, določene v zakonodaji EU na področju varstva podatkov, in biti skladni z njimi. Referenčni

¹⁵ https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd.

dokument o ustreznosti se nanaša na naslednje pomembne pojme: „osebni podatki“, „obdelava“, „upravljavci podatkov“, „obdelovalec podatkov“, „prejemnik“ in „občutljivi podatki“. Ta vidik brazilskega prava bo obravnavan v naslednjih odstavkih.

2.2.1 Stvarno področje uporabe in ozemeljska veljavnost splošnega zakona o varstvu osebnih podatkov

- (12) Evropski odbor za varstvo podatkov pozdravlja, da je področje uporabe splošnega zakona o varstvu osebnih podatkov, tako stvarno kot teritorialno, zelo podobno področju uporabe, predvidenemu v okviru EU za varstvo podatkov.
- (13) Člen 4 splošnega zakona o varstvu osebnih podatkov iz svojega področja uporabe izključuje obdelavo za popolnoma osebne in neekonomske namene, take izjeme pa so predvidene tudi v splošni uredbi o varstvu podatkov (člen 2(2), točka (c), splošne uredbe o varstvu podatkov). Poleg tega nekateri drugi postopki obdelave delno ne spadajo na področje uporabe splošnega zakona o varstvu osebnih podatkov, zlasti obdelava za: javno varnost, nacionalno obrambo, državne zakonsko določene naloge ali preiskovanje in pregon kaznivih dejanj; novinarske in umetniške namene; akademske raziskave in zdravstvene raziskave (člen 3(III) splošnega zakona o varstvu osebnih podatkov). To je podrobneje opisano v oddelku 3.1 tega mnenja.
- (14) Evropski odbor za varstvo podatkov posebej v zvezi z delno uporabo splošnega zakona o varstvu osebnih podatkov za obdelavo osebnih podatkov v novinarske in umetniške namene ugotavlja, da je obseg izjeme enakovreden obsegu iz člena 85(2) splošne uredbe o varstvu podatkov¹⁶, tj. taka izjema se uporablja le, kadar se osebni podatki obdelujejo izključno za tak namen, vsa druga obdelava, ki jo izvajajo tisk, mediji in umetniške organizacije, pa spada na področje uporabe splošnega zakona o varstvu osebnih podatkov. Prav tako se še naprej uporabljajo nekatere izjeme, predvidene za obdelavo osebnih podatkov izključno v akademske namene, tj. člena 7 (zahteve za pravno podlago) in 11 (pravila o obdelavi občutljivih podatkov) splošnega zakona o varstvu osebnih podatkov¹⁷. Obseg teh izjem je tudi v skladu z obsegom iz člena 85(2) splošne uredbe o varstvu podatkov.

2.2.2 Opredelitev pojmov

- (15) Evropski odbor za varstvo podatkov pozitivno ocenjuje uskladitev z okvirom EU za varstvo podatkov v zvezi z opredelitvami, uporabljenimi v splošnem zakonu o varstvu osebnih podatkov, ki so skladne z opredelitvami, predvidenimi v splošni uredbi o varstvu podatkov. Natančneje, v splošnem zakonu o varstvu osebnih podatkov so „osebni podatki“,

¹⁶ Glej tudi uvodno izjavo 35 osnutka sklepa.

¹⁷ Glej tudi uvodni izjavi 32 in 33 osnutka sklepa.

„psevdonimizirane informacije“, „anonimni podatki“¹⁸, „obdelava podatkov“, „upravitelj podatkov“, „obdelovalec podatkov“ in „občutljivi podatki“ (člen 5 splošnega zakona o varstvu osebnih podatkov) opredeljeni podobno kot v splošni uredbi o varstvu podatkov, in sicer v uvodni izjavi 26, členu 4 in členu 9(1). Tudi druge opredelitve, na primer „posameznik, na katerega se nanašajo osebni podatki“, „pooblaščen oseba za varstvo podatkov“, „privolitev“, „ocena učinka v zvezi z varstvom podatkov“ in pojem „skupno upravljanje“¹⁹, so v osnovi enakovredne pojmom, kot so predvideni v splošni uredbi o varstvu podatkov.

2.3 Načela varstva podatkov in pravne podlage

2.3.1 Načela obdelave

- (16) V referenčnem dokumentu o ustreznosti je v skladu s splošno uredbi o varstvu podatkov določeno, da je treba podatke obdelovati zakonito, pošteno in legitimno. V skladu s členom 6 splošnega zakona o varstvu osebnih podatkov se morajo dejavnosti obdelave osebnih podatkov izvajati v dobri veri in ob upoštevanju naslednjih načel: namen, ustreznost, nujnost, prost dostop²⁰, kakovost podatkov, preglednost, varnost, preprečevanje, nediskriminacija in odgovornost.
- (17) Ob upoštevanju konceptov teh načel brazilski pravni sistem določa enaka načela obdelave podatkov, kot so določena v členu 5 splošne uredbi o varstvu podatkov. Na primer, v zvezi z omejitvijo namena splošni zakon o varstvu osebnih podatkov v členu 7, odstavek 7, določa, da se „naknadna obdelava osebnih podatkov iz odstavkov 3 (javno dostopni osebni podatki) in 4 (podatki, ki jih posameznik, na katerega se nanašajo osebni podatki, sam objavi) tega člena lahko izvaja za nove namene, če se upoštevajo zakoniti in določeni nameni za novo obdelavo in ohranitev pravic posameznika, na katerega se nanašajo osebni podatki, ter razlogi in načela, določeni v tem zakonu“.
- (18) Splošna uredba o varstvu podatkov jasno zahteva, da se taka nadaljnja obdelava izvede le, če je tak nov namen združljiv s prvotnim namenom. Zahteva po zagotavljanju združljivosti namenov (ter skladnosti z veljavnimi etičnimi standardi ter tehničnimi in pravnimi zaščitnimi ukrepi) je poudarjena v vodniku za obdelavo osebnih podatkov v akademске namene ter za izvajanje študij in raziskav, ki ga je izdal nacionalni organ za varstvo podatkov, ter v smernicah o zakonitem interesu. Nacionalni organ za varstvo podatkov v smernicah o zakonitem interesu pojasnjuje, kako mora upravitelj podatkov dokazati učinkovito povezavo med obema namenoma obdelave in upoštevati „legitimna pričakovanja“ posameznika, na katerega se

¹⁸ Člen 12 splošnega zakona o varstvu osebnih podatkov nadalje določa, da se anonimizirani podatki ne štejejo za osebne podatke, razen če je bila anonimizacija razveljavljena ali jo je mogoče razveljaviti z razumnimi prizadevanji. V tem členu je pojasnjeno, da bi bilo treba pri določanju, kaj se šteje za „razumno“, upoštevati objektivne dejavnike, kot so: (1) stroški in čas, potreben za razveljavitev; (2) razpoložljiva tehnologija in (3) izključna uporaba lastnih sredstev upravitelja.

¹⁹ Glej člen 42, odstavek 1(l), splošnega zakona o varstvu osebnih podatkov.

²⁰ „Prost dostop: zagotovilo posameznikom, na katere se nanašajo osebni podatki, da lahko enostavno in brezplačno pridobijo informacije o obliki in trajanju obdelave ter o celovitosti njihovih osebnih podatkov“ (člen 6, del IV, splošnega zakona o varstvu osebnih podatkov).

nanašajo osebni podatki. V navedenih smernicah je nadalje pojasnjeno, da lahko „analiza legitimnih pričakovanj [...] temelji na več dejavnikih, med katerimi je mogoče poudariti naslednje: (d) predvideni namen zbiranja podatkov in njegovo združljivost z obdelavo na podlagi zakonitega interesa“. Evropski odbor za varstvo podatkov pozdravlja tako pojasnilo nacionalnega organa za varstvo podatkov, ki pripomore k boljši uskladitvi zahtev glede omejitve namena.

- (19) Načelo omejitve hrambe iz splošne uredbe o varstvu podatkov določa, da se podatki hranijo le toliko časa, kolikor je potrebno za zagotovitev namenov, za katere se obdelujejo (člen 5(1), točka (e), splošne uredbe o varstvu podatkov). Čeprav člen 6 splošnega zakona o varstvu osebnih podatkov načela omejitve hrambe ne vključuje izrecno, bi ga bilo treba brati skupaj s členom 15 navedenega zakona, ki določa zahtevo v primeru prenehanja obdelave podatkov. V tem členu je načelo omejitve hrambe jasno povezano z načeloma „ustreznosti“ in „nujnosti“, ki spadata med splošna načela iz člena 6 splošnega zakona o varstvu osebnih podatkov. Evropski odbor za varstvo podatkov zaradi večje jasnosti spodbuja Evropsko komisijo, naj v osnutku sklepa pojasni součinkovanje členov 6 in 15 splošnega zakona o varstvu osebnih podatkov v zvezi z načelom omejitve hrambe.
- (20) Poleg tega člen 16 splošnega zakona o varstvu osebnih podatkov v zvezi z zahtevami glede omejitve hrambe določa pogoje za hrambo in izbris osebnih podatkov po koncu obdelave. V tem členu so predvideni tudi štirje nameni, za katere se lahko podatki hranijo po koncu obdelave podatkov: (1) za izpolnjevanje zakonskih ali regulativnih obveznosti; (2) za raziskovalne namene, pri čemer se, kadar je to mogoče, zagotovi anonimizacija podatkov; (3) kadar se prenesejo na tretje osebe v skladu z zahtevami iz splošnega zakona o varstvu osebnih podatkov ali (4) kadar jih uporablja izključno upravljavec podatkov, če so podatki anonimizirani in je dostop tretjih oseb do teh podatkov prepovedan. Evropski odbor za varstvo podatkov ugotavlja, da so ti primeri obdelave v skladu z načelom omejitve hrambe iz splošne uredbe o varstvu podatkov.
- (21) Namen načela preglednosti in pravičnosti je zagotoviti, da imajo posamezniki, na katere se nanašajo osebni podatki, nadzor nad svojimi osebnimi podatki, in v ta namen je treba posamezniku, na katerega se nanašajo osebni podatki, informacije praviloma zagotoviti proaktivno²¹. Hkrati splošni zakon o varstvu osebnih podatkov določa omejitve tega načela, kadar gre za „poslovno in industrijsko skrivnost“, kar lahko vpliva na to, da posamezniki, na katere se nanašajo osebni podatki, prejmejo informacije o obdelavi svojih podatkov, da bi lahko izvajali nadzor nad njo (npr. z vložitvijo pritožbe pri nacionalnem organu za varstvo podatkov). Vendar Evropska komisija v osnutku sklepa pojasnjuje, da bi bilo treba to omejitev razlagati ob upoštevanju brazilskega zakona o dostopu do informacij in predsedniškega odloka št. 7.721 z dne 16. maja 2012 ter da jo „je torej treba razlagati tako, da se pri obdelavi in drugem razkritju informacij ne sme razkriti poslovna skrivnost ali ustvariti konkurenčna prednost za druge akterje, medtem ko morajo biti izpolnjeni cilji varstva osebnih podatkov. To pomeni, da se ob upoštevanju načela preglednosti in v celotnem besedilu splošnega zakona

²¹ To je poudarjeno tudi v referenčnem dokumentu o ustreznosti, glej poglavje 3, točka A(7).

o varstvu osebnih podatkov omejitev ‚poslovne in industrijske skrivnosti‘ ne razume kot splošen razlog za zavrnitev zaradi skladnosti z zakonom, temveč je treba vzpostaviti posebne zaščitne ukrepe, da bi se pri razkritju informacij zagotovila zaščita teh interesov“²².

- (22) Glede na pomen načela preglednosti Evropski odbor za varstvo podatkov poziva Evropsko komisijo, naj spremlja izvajanje te določbe v praksi, da bi bolje razumela njen vpliv na pravico do obveščenosti in dostopa.

2.3.2 Varnostni ukrepi in kršitve

- (23) Splošni zakon o varstvu osebnih podatkov vključuje načeli varnosti in preprečevanja, ki zahtevata uporabo ukrepov za varstvo osebnih podatkov in preprečevanje škode, povezane s tako obdelavo (člen 6(VII) in (VII) splošnega zakona o varstvu osebnih podatkov), pri čemer je v njem tudi izrecno navedeno, da se v primeru neustreznega izvajanja varnostnih ukrepov obdelava podatkov šteje za nezakonito. Z zakonom se zahtevata izvajanje ukrepov, potrebnih za dokazovanje skladnosti pristopa, ki temelji na tveganju, s tem načelom (členi 44, 46 in 47 splošnega zakona o varstvu osebnih podatkov), ter upoštevanje zahtev za oceno kršitve in uradno obveščanje o njej (člena 48 in 49 splošnega zakona o varstvu osebnih podatkov). Evropski odbor za varstvo podatkov pozitivno ugotavlja, da so taka načela in obveznosti tesno usklajeni z načeli in obveznostmi iz splošne uredbe o varstvu podatkov.
- (24) Evropski odbor za varstvo podatkov pozdravlja, da je nacionalni organ za varstvo podatkov sprejel dodatno zavezujočo uredbo o uradnem obveščanju o varnostnih incidentih, v kateri je opredeljen pojem incident in so zagotovljene podrobnosti za oceno njegove resnosti (npr. kadar se šteje, da incident povzroča tveganja za posameznike, na katere se nanašajo osebni podatki, ali znatno vpliva na temeljne interese in pravice posameznikov, na katere se nanašajo osebni podatki, in ga je zato treba sporočiti nacionalnemu organu za varstvo podatkov in posamezniku, na katerega se nanašajo osebni podatki) ter podrobnosti o zahtevah glede uradnega obveščanja o incidentih²³. V zvezi s tem ugotavlja, da mora v skladu z uredbo o uradnem obveščanju o varnostnih incidentih upravljavec „nacionalni organ za varstvo podatkov o varnostnem incidentu [praviloma] obvestiti v treh delovnih dneh“²⁴, in poziva Evropsko komisijo, naj osnutek svojega sklepa ustrezno prilagodi (uvodna izjava 75)²⁵.
- (25) Evropski odbor za varstvo podatkov v zvezi z uradnim obveščanjem o kršitvah varnosti podatkov ugotavlja, da je v splošnem zakonu o varstvu osebnih podatkov navedeno, da tako uradno obveščanje (tako nacionalnega organa za varstvo podatkov kot posameznika, na katerega se nanašajo osebni podatki) med drugim vključuje informacije o tehničnih in varnostnih ukrepih, ki se uporabljajo za varstvo osebnih podatkov, sprejetih pred incidentom

²² Glej uvodno izjavo 81 osnutka sklepa.

²³ Glej uvodno izjavo 73–77 osnutka sklepa.

²⁴ Glej člena 6 in 9 uredbe o uradnem obveščanju o varnostnih incidentih.

²⁵ Glej uvodno izjavo 75 osnutka sklepa, v skladu s katerim je treba „[o] varnostnem incidentu [...] nacionalni organ za varstvo podatkov in posameznike, na katere se nanašajo osebni podatki, obvestiti v treh dneh (72 urah) po tem, ko je upravljavec zanj izvedel“.

in po njem, ob upoštevanju poslovnih in industrijskih skrivnosti (člen 6(III) in člen 9(II) splošnega zakona o varstvu osebnih podatkov). Odbor razume potrebo po učinkovitem zagotavljanju, da pravica do zasebnosti in varstva podatkov ne vpliva negativno na varstvo drugih pravic, in poziva Komisijo, naj spremlja izvajanje take omejitve, kadar so bile informacije o incidentu zagotovljene delno (ob upoštevanju poslovnih in industrijskih skrivnosti), ter njen morebitni vpliv na pooblastila nacionalnega organa za varstvo podatkov.

2.3.3 Zakonitost obdelave

- (26) Evropski odbor za varstvo podatkov ugotavlja, da sta načelo zakonitosti in njegovo izvajanje, kot je predvideno v splošnem zakonu o varstvu osebnih podatkov (člen 5(XII) ter členi 7, 8 in 10), tesno usklajena z načelom iz splošne uredbe o varstvu podatkov (člen 4(11) ter členi 6, 7 in 9), ter pozdravlja to uskladitev.

2.3.3.1 Zakoniti interes

- (27) Zahteve glede zakonitega interesa, ki se bo uporabljal kot pravna podlaga za obdelavo iz splošnega zakona o varstvu osebnih podatkov (člen 7(IX)), so usklajene s splošno uredbo o varstvu podatkov (člen 6(1), točka (f)). V splošnem zakonu o varstvu osebnih podatkov je tudi poudarjeno, da bi morale običajno prevladati temeljne pravice in svoboščine (vključno s pravico do varstva podatkov²⁶).
- (28) Evropski odbor za varstvo podatkov ugotavlja, da so v členu 10 splošnega zakona o varstvu osebnih podatkov navedeni zakoniti nameni, za katere bi se lahko uporabljala taka pravna podlaga. Eden od teh zakonitih namenov je podpora in spodbujanje dejavnosti upravljavca (člen 10(I) splošnega zakona o varstvu osebnih podatkov).
- (29) Čeprav se zdi, da je ta izraz širok, Evropski odbor za varstvo podatkov ugotavlja, da so pogoji za uporabo „zakonitega interesa“ podrobneje opredeljeni v vodniku „Pravne podlage za obdelavo osebnih podatkov – zakoniti interes“ (v nadaljnjem besedilu: vodnik o zakonitem interesu), ki ga je sprejel nacionalni organ za varstvo podatkov. V tem vodniku je pojasnjeno, da morajo biti za to, da se interes šteje za „zakonit“, izpolnjeni trije pogoji: (1) združljivost z brazilskim pravnim sistemom; (2) sklicevanje na določeno okoliščino in (3) obdelava je povezana z zakonitimi, posebnimi in izrecnimi nameni²⁷. Ti pogoji so podobni trem kumulativnim pogojem za zakonitost obdelave osebnih podatkov na podlagi te pravne podlage, ki jih je določilo Sodišče²⁸, in njihovi dodatni razlagi, ki jo je podalo Sodišče. Poleg tega so pogoji za „zakoniti interes“, določeni v vodniku o zakonitem interesu, podobni pogojem iz smernic, ki jih je sprejel Evropski odbor za varstvo podatkov²⁹. Evropski odbor za varstvo

²⁶ Glej odstavek 3 tega mnenja.

²⁷ Glej uvodno izjavo 52 osnutka sklepa.

²⁸ Na primer, sodba Sodišča z dne 7. decembra 2023, SCHUFA Holding AG, združeni zadevi C-26/22 in C-64/22, točke 75–80.

²⁹ Smernice 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1), točka (f), splošne uredbe o varstvu podatkov (različica 1.0), sprejete 8. oktobra 2024.

podatkov pozdravlja pristop nacionalnega organa za varstvo podatkov v zvezi z zakonitim interesom in njegovo uporabo za obdelavo.

2.4 Pravice posameznikov

- (30) Evropski odbor za varstvo podatkov pozdravlja, da so s splošnim zakonom o varstvu osebnih podatkov posameznikom zagotovljene podobne pravice, kot so določene v splošni uredbi o varstvu podatkov (pri obeh v poglavju III). V splošnem zakonu o varstvu osebnih podatkov so predvidene zlasti pravica do dostopa, pravica do popravka, pravica do prenosljivosti podatkov, pravica do omejitve obdelave, pravica do izbrisa, pravica do obveščenosti, pravica do zavrnitve ali preklica privolitve ter pravica do ugovora obdelavi in pravica do peticije (člena 9 in 18 splošnega zakona o varstvu osebnih podatkov).
- (31) S splošnim zakonom o varstvu osebnih podatkov je posameznikom, na katere se nanašajo osebni podatki, zagotovljena tudi pravica, da zahtevajo pregled odločitev, ki so sprejete izključno na podlagi avtomatizirane obdelave osebnih podatkov in vplivajo na njihove interese (člen 20 splošnega zakona o varstvu osebnih podatkov). Vsebina člena 20 splošnega zakona o varstvu osebnih podatkov v bistvu odraža člen 22 splošne uredbe o varstvu podatkov.
- (32) Evropski odbor za varstvo podatkov ugotavlja, da brazilski zakon o pravnem sredstvu *habeas data* v zvezi s pravicami posameznikov, na katere se nanašajo osebni podatki, vsebuje posebne določbe za odobritev pravice do dostopa in pravice do popravka v kratkem roku (deset oziroma 15 dni) na zahtevo posameznika, in pozdravlja ta vidik.
- (33) Evropski odbor za varstvo podatkov meni, da splošni zakon o varstvu osebnih podatkov določa zahteve za pravice posameznikov, na katere se nanašajo osebni podatki, ki so v osnovi enakovredne zahtevam iz splošne uredbe o varstvu podatkov.

2.5 Omejitve nadaljnjih prenosov

- (34) V referenčnem dokumentu o ustreznosti je pojasnjeno, da nadaljnji prenos ne sme ogroziti ravni varstva posameznikov, katerih osebni podatki se prenašajo na podlagi sklepa o ustreznosti, zato bi moral biti vsak nadaljnji prenos dovoljen „samo, če tudi za nadaljnjega uporabnika (tj. uporabnika nadaljnjega prenosa podatkov) veljajo predpisi (vključno s pogodbenimi določbami), ki zagotavljajo ustrezno raven varstva in upoštevajo zadevna navodila za obdelavo podatkov v imenu upravljavca podatkov“.
- (35) V zvezi z oceno ustreznosti brazilskega pravnega okvira in prakse nadaljnji prenos pomeni prenos osebnih podatkov od subjekta, ki deluje kot upravljavec na območju ozemeljske veljavnosti uporabe brazilskega splošnega zakona o varstvu osebnih podatkov, subjektu zunaj tega območja ozemeljske veljavnosti.
- (36) Zahteve glede nadaljnjega prenosa so določene v poglavju V splošnega zakona o varstvu osebnih podatkov, pri čemer jih je nacionalni organ za varstvo podatkov nadalje dopolnil s

sprejetjem „uredbe o prenosu podatkov“, ki vsebuje opredelitve pojmov „prenos“, „mednarodni prenos podatkov“, „uvoznik“ in „izvoznik“ ter vključuje podrobne zahteve za prenose.

- (37) Evropski odbor za varstvo podatkov pozitivno ugotavlja, da sta opredelitvi pojmov „prenos“ in „mednarodni prenos podatkov“ usklajeni z opredelitvama iz njegovih smernic 05/2021³⁰.
- (38) V skladu s splošnim zakonom o varstvu osebnih podatkov in uredbo o prenosu podatkov se lahko nadaljnji prenosi izvajajo le za zakonite, določene in izrecne namene ter kadar so vzpostavljeni posebni instrumenti ali pogoji (člen 33 splošnega zakona o varstvu osebnih podatkov in členi 9–33 uredbe o prenosu podatkov)³¹. Evropski odbor za varstvo podatkov pozdravlja, da so ti instrumenti podobni orodjem za prenos, predvidenim v poglavju V splošne uredbe o varstvu podatkov. Vendar poziva Evropsko komisijo, naj v osnutku sklepa pojasni, ali se lahko prenosi v skladu s členom 33(III)–(IX) splošnega zakona o varstvu osebnih podatkov izvedejo le v izjemnih okoliščinah, kadar pogoji iz člena 33(I) in (II) splošnega zakona o varstvu osebnih podatkov niso izpolnjeni³².
- (39) Vendar je v uredbi o prenosu podatkov določeno, da so mednarodni prenosi osebnih podatkov dovoljeni, „kadar je posameznik, na katerega se nanašajo osebni podatki, izrecno in razločljivo privolil v tak prenos, potem ko je bil predhodno obveščen o mednarodni naravi predvidene dejavnosti, pri čemer je njegova privolitev jasno ločena od privolitev za druge namene“. Ni jasno, ali ta zahteva vključuje obveznost obveščanja posameznikov, na katere se nanašajo osebni podatki, o morebitnih tveganjih mednarodnih prenosov, ki izhajajo iz neobstoja ustreznega varstva v tretji državi in neobstoja ustreznih zaščitnih ukrepov (npr. informacije, da v tretji državi morda ni nadzornega organa in/ali načel obdelave podatkov in/ali pravic posameznikov, na katere se nanašajo osebni podatki), kar je zahteva iz člena 49(1), točka (a), splošne uredbe o varstvu podatkov. Za Evropski odbor za varstvo podatkov in v skladu s splošno uredbo o varstvu podatkov je zagotavljanje teh informacij bistveno, da se posamezniku, na katerega se nanašajo osebni podatki, omogoči, da poda informirano privolitev ob popolnem poznavanju teh specifičnih dejstev o prenosu. Evropski odbor za varstvo podatkov zato poziva Evropsko komisijo, naj v osnutku sklepa pojasni, ali je posameznik, na katerega se nanašajo osebni podatki, obveščen o morebitnih tveganjih takega prenosa, ki izhajajo iz neobstoja ustreznega varstva v tretji državi in ustreznih zaščitnih ukrepov.
- (40) Poleg tega je v uredbi o prenosu podatkov določeno, da „upravljavec in obdelovalec sprejmeta učinkovite ukrepe, s katerimi lahko dokažeta spoštovanje pravil o varstvu osebnih podatkov in skladnost z njimi ter učinkovitost takih ukrepov na način, ki je združljiv s stopnjo tveganja obdelave in uporabljenim načinom mednarodnega prenosa“ (člen 4(2) uredbe o prenosu

³⁰ Odstavek 9 Smernic 05/2021 o medsebojnem vplivu uporabe člena 3 in določb o mednarodnih prenosih v skladu s poglavjem V Splošne uredbe o varstvu podatkov, sprejetih 14. februarja 2023.

³¹ Glej uvodne izjave 101–109 osnutka sklepa.

³² Člen 49 splošne uredbe o varstvu podatkov določa, da se odstopanja, predvidena v tem členu, lahko uporabijo le, če sklep o ustreznosti v skladu s členom 45(3) splošne uredbe o varstvu podatkov ni sprejet ali če niso sprejeti ustrezni zaščitni ukrepi v skladu s členom 46 splošne uredbe o varstvu podatkov.

podatkov). Evropski odbor za varstvo podatkov pozdravlja vključitev te obveznosti. Hkrati bi bilo koristno pojasniti, da bi bilo treba učinkovitost teh ukrepov oceniti tudi za zagotovitev, da lokalna zakonodaja zadevne tretje države ne bi ogrozila kontinuitete varstva posameznikov, na katere se nanašajo osebni podatki in katerih podatki se prenašajo³³. Evropski odbor za varstvo podatkov poziva Evropsko komisijo, naj pojasni, da se bo ta element upošteval tudi v scenarijih prenosa.

- (41) Evropski odbor za varstvo podatkov pozdravlja vključitev izrecne zahteve glede preglednosti v zvezi s posamezniki, na katere se nanašajo osebni podatki, tj. da imajo posamezniki, na katere se nanašajo osebni podatki, pravico prejeti pogodbeni instrument, ki se uporablja za nadaljnji prenos, ter opis takega prenosa, npr. trajanje in namen prenosa, ciljne države, odgovornosti udeleženih strani, pravice posameznikov, na katere se nanašajo osebni podatki, in sredstva za njihovo uveljavljanje (člen 16 uredbe o prenosu podatkov).
- (42) Vendar se zdi, da je tak obseg obveznosti glede preglednosti pomemben le, kadar se prenosi izvajajo na podlagi standardnih pogodbenih klavzul, ne pa tudi, kadar se uporabljajo druga orodja³⁴. Zato Evropski odbor za varstvo podatkov poziva Evropsko komisijo, naj pojasni, da ne glede na uporabljeno orodje za prenos veljajo enake obveznosti glede preglednosti.
- (43) Evropski odbor za varstvo podatkov poleg tega ugotavlja, da zahteve glede vsebine zavezujočih poslovnih pravil niso v celoti skladne z zahtevami iz splošne uredbe o varstvu podatkov, zlasti iz člena 47(2), točki (f) in (l), splošne uredbe o varstvu podatkov. Da bi zagotovili, da raven varstva, ki jo zagotavlja splošna uredba o varstvu podatkov, ne bi bila ogrožena, poziva Evropsko komisijo, naj v osnutku sklepa pojasni, da se bodo tudi ti elementi³⁵ upoštevali, kadar je treba to orodje za prenos uporabiti za nadaljnje prenose osebnih podatkov, prenesenih v Brazilijo na podlagi sklepa o ustreznosti.

2.6 Postopkovni in izvršilni mehanizmi

- (44) V skladu z referenčnim dokumentom o ustreznosti³⁶ in ustrezno sodno prakso Sodišča³⁷ mora sistem varstva podatkov, ki je v osnovi enakovreden modelu Evropske unije, določati: (i) neodvisen organ, ki bi moral nadzirati in izvrševati zakone o varstvu podatkov ter bi bil pooblaščen za preiskovanje in ukrepanje brez zunanjega vpliva. Sistemi varstva podatkov morajo zagotavljati (ii) da so upravljavci in obdelovalci podatkov odgovorni in se zavedajo

³³ Glej sodbo Latombe. Glej tudi sodbo Sodišča Evropske unije z dne 16. julija 2020 v zadevi C-311/18 (v nadaljnjem besedilu: sodba Schrems II).

³⁴ Uredba o prenosu podatkov na primer vključuje splošne zahteve glede preglednosti, kadar naj bi se uporabljala zavezujoča poslovna pravila, zlasti „vzpostavitev in izvajanje programa upravljanja zasebnosti, katerega namen je vzpostaviti odnos zaupanja s posameznikom, na katerega se nanašajo osebni podatki, s preglednimi ukrepi, ki zagotavljajo mehanizme za sodelovanje posameznika, na katerega se nanašajo osebni podatki“ (člen 25(V) uredbe o prenosu podatkov), ter preglednosti v zvezi z uveljavljanjem pravic posameznika, na katerega se nanašajo osebni podatki, in pravice do pritožbe (člen 26(VI) uredbe o prenosu podatkov).

³⁵ Odgovornost in sodelovanje z nadzornim organom (člen 47(2), točki (f) in (l), splošne uredbe o varstvu podatkov).

³⁶ Glej poglavje 3(C) referenčnega dokumenta o ustreznosti.

³⁷ Sodba Sodišča z dne 6. oktobra 2015, Schrems, C-362/14.

svojih odgovornosti, ter da so posamezniki, na katere se nanašajo osebni podatki, obveščeni o svojih pravicah. Vzpostaviti bi bilo treba učinkovite sankcije in postopke preverjanja, da se zagotovi spoštovanje pravil ter da (iii) upravljavci in obdelovalci podatkov dokazujejo skladnost, in sicer z ukrepi, kot so ocene učinka v zvezi z varstvom podatkov, evidenca dejavnosti obdelave in imenovanje pooblaščenih oseb za varstvo podatkov. Poleg tega (iv) mora sistem varstva podatkov zagotavljati podporo in pomoč posameznikom, na katere se nanašajo osebni podatki, pri uveljavljanju njihovih pravic in ustreznih mehanizmov pravnega varstva.

- (45) Evropski odbor za varstvo podatkov je v tem oddelku svojo oceno osredotočil na obstoj neodvisnega organa, ustreznega mehanizma pravnega varstva in učinkovitih sankcij.

2.6.1 Neodvisen nadzor

- (46) S splošnim zakonom o varstvu osebnih podatkov je bil kot nacionalni nadzorni organ, odgovoren za spremljanje in izvrševanje njegovih določb, ustanovljen brazilski nacionalni organ za varstvo podatkov (*Agencia Nacional de Proteção de Dados*, ANPD).
- (47) Evropski odbor za varstvo podatkov pozdravlja, da je bil nacionalnemu organu za varstvo podatkov podeljen status „organa posebne narave“, s katerim naj bi mu bila zagotovljena samostojnost, potrebna za polno izvajanje pravnih funkcij in pooblastil, ki so mu bile podeljene s splošnim zakonom o varstvu osebnih podatkov, zlasti z razveljavitvijo določb, po katerih je bilo delovanje in finančno poslovanje nacionalnega organa za varstvo podatkov odvisno od pooblastil, ki jih je podelila izvršna oblast.
- (48) Evropski odbor za varstvo podatkov prav tako pozdravlja spremembe brazilskega pravnega okvira, uvedene 15. septembra 2025, v skladu s katerimi je nacionalni organ za varstvo podatkov zdaj priznan kot **regulativna agencija**³⁸. Odbor razume, da je zato ena od glavnih sprememb ta, da bo nacionalni organ za varstvo podatkov svoj proračun predložil neposredno ministrstvu za načrtovanje in proračun, namesto da bi ga moral predložiti prek ministrstva za pravosodje. Proračun nacionalnega organa za varstvo podatkov ostaja ločena postavka v proračunu zveznih držav. Evropski odbor za varstvo podatkov razume, da je nacionalni organ za varstvo podatkov že neodvisno upravljal tudi svoj proračun in finance, vendar se je s tem, ko je postal regulativna agencija, poenostavil njegov upravni postopek.
- (49) Evropski odbor za varstvo podatkov pozdravlja tudi novo pristojnost nacionalnega organa za varstvo podatkov, ki je bil nedavno imenovan za organ, pristojen za zaščito otrok na spletu³⁹. Ugotavlja, da je nacionalni organ za varstvo podatkov v skladu s poglavjem IX splošnega zakona o varstvu osebnih podatkov dobro opremljen s potrebnimi in razpoložljivimi pooblastili in nalogami za zagotavljanje skladnosti s pravicami do varstva podatkov in spodbujanje

³⁸ Začasni ukrep št. 1.317/2025, na voljo na spletnem naslovu <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314>.

³⁹ Zakon št. 15.211/2025 o zaščiti otrok in mladostnikov v digitalnem okolju, na voljo na spletnem naslovu <https://www.in.gov.br/web/dou/-/lei-n-15.211-de-17-de-setembro-de-2025-656579619>.

ozaveščenosti, kot so preiskovalna pooblastila in pooblastila za sankcioniranje (člen 55-J splošnega zakona o varstvu osebnih podatkov).

- (50) V zvezi z osebjem in proračunom nacionalnega organa za varstvo podatkov, ki ima vlogo pri njegovi neodvisnosti, Evropski odbor za varstvo podatkov pozitivno ocenjuje nedavno odločitev o povečanju števila zaposlenih z več kot 200 novimi delovnimi mesti⁴⁰.
- (51) Evropski odbor za varstvo podatkov ugotavlja, da v skladu s členom 55-C splošnega zakona o varstvu osebnih podatkov nacionalni organ za varstvo podatkov (zdaj) sestavlja več organov⁴¹, vključno z nacionalnim svetom za varstvo osebnih podatkov in zasebnosti. Seznanjen je z njegovo sestavo, ki vključuje tudi predstavnike zvezne izvršilne, zakonodajne in sodne veje oblasti⁴². Ugotavlja tudi, da je v skladu s členom 58-B splošnega zakona o varstvu osebnih podatkov nacionalni svet za varstvo osebnih podatkov in zasebnosti med drugim odgovoren za (i) „predlaganje strateških smernic in zagotavljanje osnovnih informacij za pripravo nacionalne politike za varstvo osebnih podatkov in zasebnosti ter za dejavnosti nacionalnega organa za varstvo podatkov“ ter za (ii) „priporočanje ukrepov, ki jih mora izvesti nacionalni organ za varstvo podatkov“.
- (52) Evropski odbor za varstvo podatkov zlasti v zvezi s temi nalogami meni, da je treba bolje razumeti, kako se izvajajo ter v kolikšni meri predlogi in priporočila nacionalnega sveta za varstvo osebnih podatkov in zasebnosti vplivajo na delo nacionalnega organa za varstvo podatkov. Zato poziva Evropsko komisijo, naj podrobneje opredeli te naloge in interakcijo med nacionalnim svetom za varstvo osebnih podatkov in zasebnosti ter nacionalnim organom za varstvo podatkov, da bi bolje ocenila vpliv nacionalnega sveta za varstvo osebnih podatkov in zasebnosti na dejavnosti nacionalnega organa za varstvo podatkov.

2.6.2 Pravno varstvo

- (53) Evropski odbor za varstvo podatkov pozdravlja mehanizem pravnih sredstev, predviden v splošnem zakonu o varstvu osebnih podatkov, ki posameznikom, na katere se nanašajo osebni podatki, zagotavlja tudi pravico do vložitve pritožbe pri nacionalnem organu za varstvo podatkov in izpodbijanja njegove odločitve s predložitvijo pritožbe njegovemu upravnemu odboru. Posamezniki se lahko nato zoper odločitve upravnega odbora pritožijo na sodišče ter uveljavljajo pravna sredstva zoper nacionalni organ za varstvo podatkov zaradi neizpolnjevanja obveznosti iz splošnega zakona o varstvu osebnih podatkov. Razlika med pritožbenim instrumentom in instrumentom pravnega varstva iz osnutka sklepa ni jasno razvidna. Evropski odbor za varstvo podatkov poziva Komisijo, naj dodatno pojasni delovanje

⁴⁰ <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314>.

⁴¹ V skladu s členom 55-C splošnega zakona o varstvu osebnih podatkov nacionalni organ za varstvo podatkov sestavljajo: upravni odbor, najvišji organ upravljanja; nacionalni svet za varstvo osebnih podatkov in zasebnosti; urad disciplinske komisije; IV – urad varuha človekovih pravic; VI – urad za pravne zadeve ter VI – upravne enote in specializirane enote, potrebne za izvrševanje določb splošnega zakona o varstvu osebnih podatkov. Glej tudi uvodne izjave 126–130 osnutka sklepa.

⁴² Glej tudi uvodno izjavo 132 osnutka sklepa in člen 55-C splošnega zakona o varstvu osebnih podatkov.

teh dveh možnosti, vključno s tem, ali je uporaba pravnih sredstev omejena le na zavrnitev obravnave pritožbe ali na vsebinsko zavrnitev pritožbe.

- (54) Poleg tega pozdravlja zagotovitev pravice do odškodnine za premoženjsko in nepremoženjsko škodo ter kolektivnega pravnega varstva (člen 22 splošnega zakona o varstvu osebnih podatkov).

2.6.3 Sankcije

- (55) Evropski odbor za varstvo podatkov opozarja, da imajo lahko učinkovite in odvračilne sankcije pomembno vlogo pri zagotavljanju spoštovanja pravil o varstvu podatkov, saj je to znak visoke stopnje odgovornosti in ozaveščenosti, ki jo zagotavlja sistem. Odbor pozdravlja popravljalna pooblastila, ki jih ima nacionalni organ za varstvo podatkov in so se večkrat izvajala⁴³ ter vključujejo vrsto ukrepov, kot so opozorila, globe v višini do dveh odstotkov (2 %) bruto prihodkov zadevnega zasebnega pravnega subjekta, dnevne globe, blokiranje osebnih podatkov, povezanih s kršitvijo, do njihove ureditve, začasna prekinitev zadevnih dejavnosti obdelave podatkov in izbris zadevnih osebnih podatkov (člen 52 splošnega zakona o varstvu osebnih podatkov)⁴⁴. Komisijo poziva, naj spremlja njihovo dosledno uporabo, zlasti v zvezi s sankcijami.
- (56) Evropski odbor za varstvo podatkov pozitivno ugotavlja, da je nacionalni organ za varstvo podatkov izdal (zavezujočo) uredbo o sankcijah. V njej so sankcije razvrščene na različne ravni na podlagi objektivnih dejavnikov, kot so vrsta in obseg podatkov, ki se obdelujejo, ali vpliv na pravice posameznikov, na katere se nanašajo osebni podatki, določena pa je tudi metodologija za izračun glob, ki je v skladu z zahtevami iz člena 83 splošne uredbe o varstvu podatkov.

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

- (57) V skladu s členom 45(2) splošne uredbe o varstvu podatkov je ocena omejitev in zaščitnih ukrepov, ki jih brazilsko pravo določa glede dostopa brazilskih javnih organov do osebnih podatkov in njihove naknadne uporabe s strani teh organov, tj. osebnih podatkov, ki se za

⁴³ Glej nacionalni organ za varstvo podatkov, Register sankcij: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/deciso-es-em-processos-sancionadores-1/deciso-es-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.

⁴⁴ „Te sankcije se lahko izrečejo javnim ali zasebnim subjektom, razen glob in dnevnih glob, ki jih ni mogoče izreči javnim subjektom“ (uvodna izjava 135 osnutka sklepa).

namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter nacionalne varnosti (v nadaljnjem besedilu: vladni dostop) prenašajo upravljavcem in obdelovalcem v Braziliji, pomemben element preskusa „osnovne enakovrednosti“, kakor ga razlaga Sodišče.

- (58) Evropski odbor za varstvo podatkov pozitivno ocenjuje posebno pozornost in dejanske informacije, ki jih je v zvezi s tem vidikom zagotavlja Komisija v osnutku sklepa⁴⁵. Zato v tem mnenju ne povzema dejanskih ugotovitev in analiz. Namesto tega poseganje brazilskega sistema zaradi vladnega dostopa za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter nacionalne varnosti ocenjuje na podlagi štirih elementov, ki jih je opredelil v evropskih temeljnih jamstvih za nadzorne ukrepe, sprejetih 10. novembra 2020⁴⁶:

- jamstvo A – jasna, natančna in dostopna pravna pravila;
- jamstvo B – nujnost in sorazmernost glede legitimnih ciljev, ki se zasledujejo;
- jamstvo C – neodvisni nadzorni mehanizem;
- jamstvo D – posamezniku so na voljo učinkovita pravna sredstva.

3.1 Dostop in uporaba s strani brazilskih javnih organov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

3.1.1 Pravni okvir na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

- (59) Evropski odbor za varstvo podatkov ugotavlja, da sta dostop brazilskih organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj⁴⁷ do osebnih podatkov ter njihova naknadna uporaba s strani teh organov urejena s sistemom pravnih aktov različne pravne narave. Varstvo podatkov in zasebnost, vključno s tajnostjo korespondence in komunikacij, sta v členu 5 ustave določena kot temeljni pravici. Evropski odbor za varstvo podatkov zlasti pozdravlja, da obseg varstva teh pravic, podobno kot v EU, ni omejen le na brazilske državljane, temveč zajema tudi tujce, ne glede na to, ali prebivajo v Braziliji ali ne⁴⁸.
- (60) Poleg tega obstaja več specializiranih sektorskih zakonov, ki urejajo morebiten dostop do osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. V zvezi s takim dostopom do podatkov, prenesenih v Brazilijo iz EU, so zlasti pomembni kazenski zakonik, zakon o prestrežanju telefonskih komunikacij, okvir državljskih pravic za internet, zakon o zaupnosti finančnih ustanov, zakon o hudodelskih združbah in kazenskih preiskavah ter drugo. Evropski odbor za varstvo podatkov ugotavlja, da so ti pravni akti javno dostopni in bi se lahko šteli za dovolj jasne, da posameznikom, na katere se nanašajo osebni

⁴⁵ Glej uvodne izjave 152–217 osnutka sklepa.

⁴⁶ [Priporočila 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe](#).

⁴⁷ Glej seznam organov v uvodni izjavi 165 osnutka sklepa.

⁴⁸ Glej uvodni izjavi 8 in 9 osnutka sklepa.

podatki, nakazujejo okoliščine in pogoje, pod katerimi so javni organi pooblaščen za dostop do njihovih podatkov⁴⁹.

- (61) Pomemben pravni vir v Braziliji sta tudi sodna praksa brazilskega zveznega vrhovnega sodišča, za katero se zdi, da uporablja široko razlago obsega pravice do zasebnosti in pravice do varstva podatkov⁵⁰, ter sodna praksa Medameriškega sodišča za človekove pravice, pristojnega za razlago in uporabo Ameriške konvencije o človekovih pravicah, ki jo je Brazilija ratificirala leta 1992⁵¹.
- (62) Evropski odbor za varstvo podatkov ugotavlja, da je področje uporabe splošnega zakona o varstvu osebnih podatkov pri obdelavi osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj delno, kar lahko povzroči pravno negotovost.
- (63) Kot je Komisija priznala v osnutku sklepa, se splošni zakon o varstvu osebnih podatkov ne uporablja za obdelavo podatkov, ki se izvaja *izključno* za namene javne varnosti, nacionalne obrambe, državne varnosti ali preiskovanja in pregona kaznivih dejanj⁵². V skladu s členom 4(I) in (III) splošnega zakona o varstvu osebnih podatkov bo obdelava podatkov na teh področjih urejena s posebno zakonodajo, ki mora zajemati načela in pravice posameznikov, na katere se nanašajo osebni podatki, določene v splošnem zakonu o varstvu osebnih podatkov. Po podatkih Evropskega odbora za varstvo podatkov, ki jih je potrdila Komisija, Brazilija še ni sprejela posebne zakonodaje v zvezi z obdelavo osebnih podatkov na področju kazenskega pravosodja ter preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (npr. podobne direktivi EU o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj⁵³).
- (64) Evropski odbor za varstvo podatkov pozitivno ugotavlja, da brazilsko zvezno vrhovno sodišče v svoji sodni praksi⁵⁴ splošni zakon o varstvu osebnih podatkov razlaga tako, da je njegova delna uporaba razširjena na obdelavo osebnih podatkov za kazenske preiskave in ohranjanje javnega reda.
- (65) Evropski odbor za varstvo podatkov pozdravlja, da brazilski nadzorni organ, tj. nacionalni organ za varstvo podatkov, v celoti podpira to razlago in meni, da „neobstoj posebne zakonodaje varnostnim agencijam ne daje širokega in neomejenega pooblastila za obdelavo osebnih podatkov državljanov izključno za namene javne varnosti ter preiskovanja in pregona kaznivih dejanj brez kakršnih koli omejitev“⁵⁵. Hkrati ugotavlja, da se zdi, da ima nacionalni

⁴⁹ Glej sodbo ESČP v zadevi Zakharov, točka 229.

⁵⁰ Glej odločbo zveznega vrhovnega sodišča o neposredni tožbi zaradi neustavnosti 6649 (ADI 6649), september 2022.

⁵¹ Glej uvodno izjavo 10 osnutka sklepa.

⁵² Glej uvodni izjavi 30 in 31 osnutka sklepa.

⁵³ Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89).

⁵⁴ Glej odločbo zveznega vrhovnega sodišča o neposredni tožbi zaradi neustavnosti 6649 (ADI 6649), september 2022.

⁵⁵ Glej tehnično navodilo nacionalnega organa za varstvo podatkov št. 29/2024/FIS/CGF/ANPD, naslovljeno na ministrstvo za pravosodje in javno varnost, točka 5.4.1.29, na voljo na spletnem naslovu: [SEI/ANPD - 0132350 - Nota Técnica](#).

organ za varstvo podatkov v skladu s členom 4(III), odstavek 3, splošnega zakona o varstvu osebnih podatkov za nekatere posebne obdelave podatkov, ki se izvajajo izključno za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, trenutno predvsem svetovalno vlogo v razmerju do organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

- (66) Evropski odbor za varstvo podatkov poziva Komisijo, naj v osnutku sklepa nadalje oceni in pojasni uporabo splošnega zakona o varstvu osebnih podatkov v primeru obdelave osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, vključno s pooblastili nacionalnega organa za varstvo podatkov, ter naj pri prihodnjem spremljanju skrbno upošteva vse pomembne spremembe v zvezi s tem (glej tudi oddelek o nadzoru in pravnem varstvu).

3.1.2 Nujnost in sorazmernost

- (67) Evropski odbor za varstvo podatkov pozitivno ugotavlja, da je za dostop do komunikacijskih podatkov, tako vsebine kot metapodatkov, ter do drugih kategorij zaščiteneh zaupnih informacij, kot so bančni in davčni podatki, praviloma potrebna predhodna sodna odobritev.
- (68) Kar zadeva dostop do komunikacijskih podatkov, Evropski odbor za varstvo podatkov pozdravlja, da se v skladu z zakonom o prestrezanju telefonskih komunikacij in sodno prakso zveznega vrhovnega sodišča tak ukrep šteje za izjemnega in da zanj veljajo strogi pogoji, namenjeni zagotavljanju njegove nujnosti in sorazmernosti⁵⁶. Poleg tega brazilsko pravo kot preventivni ukrep proti morebitnim zlorabam določa, da prestrezanje komunikacij brez sodne odobritve ali za namen, ki ni dovoljen z zakonom, pomeni kaznivo dejanje, ki se kaznuje z zaporno kaznijo do štirih let⁵⁷.
- (69) Strogo izvajanje zaščitnih ukrepov za dostop do komunikacijskih podatkov je še zlasti pomembno, ker v Braziliji obstaja splošna obveznost hrambe podatkov za ponudnike storitev internetne povezave in spletnih aplikacijskih storitev, da dnevne povezave hranijo eno leto⁵⁸. Evropski odbor za varstvo podatkov sicer pozitivno ugotavlja, da je dostop do hranjenih podatkov mogoč le na podlagi sodne odobritve⁵⁹, vendar opozarja na strog pristop ter omejitve splošne in neselektivne hrambe komunikacijskih metapodatkov v EU⁶⁰ ter pozitivno ocenjuje dodatne informacije, ki jih je Komisija zagotovila v zvezi s tem, da v zadevni državi ni množične hrambe podatkov. Zato spodbuja Komisijo, naj med spremljanjem in pregledom osnutka sklepa posebno pozornost nameni pravni ureditvi in praksi v Braziliji v zvezi z dostopom do komunikacijskih podatkov.

⁵⁶ Glej uvodni izjavi 169 in 170 osnutka sklepa.

⁵⁷ Prav tam.

⁵⁸ Glej uvodno izjavo 173 osnutka sklepa.

⁵⁹ Prav tam.

⁶⁰ Za več informacij o hrambi podatkov glej izjavo Evropskega odbora za varstvo podatkov 5/2024 o priporočilih skupine na visoki ravni za dostop do podatkov za učinkovito preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ki je na voljo na spletnem naslovu https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlq_en.pdf.

- (70) Evropski odbor za varstvo podatkov pozitivno ugotavlja, da se podobni zaščitni ukrepi uporabljajo tudi v zvezi z dostopom organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj do davčnih in bančnih podatkov, tj. za dostop je potrebna predhodna sodna odobritev, dostop se dovoli le v zvezi s hudimi kaznivimi dejanji, v primeru zlorabe se izrečejo kazenske sankcije itd.
- (71) V skladu z osnutkom sklepa obstaja izjema od splošne zahteve po predhodni sodni odobritvi, in sicer za dostop organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj do nekaterih kategorij osebnih podatkov⁶¹. V skladu s členoma 15 in 16 zakona o hudodelskih združbah in kazenskih preiskavah lahko načelnik policije in državno tožilstvo brez sodne odobritve dostopata do evidenčnih podatkov preiskovane osebe o: „osebnih kvalifikacijah, poreklu in naslovu, ki jih hranijo volilno sodišče, telefonske družbe, finančne ustanove, ponudniki internetnih storitev in izdajatelji kreditnih kartic“⁶². Podobno bodo prevozna podjetja za obdobje petih let sodniku, državnemu tožilstvu ali načelniku policije omogočila neposreden in stalen dostop do podatkovnih zbirk o rezervacijah in evidenc potovanj⁶³.
- (72) Evropski odbor za varstvo podatkov ugotavlja, da je področje uporabe zakona o hudodelskih združbah in kazenskih preiskavah omejeno na preiskovanje in sankcioniranje organiziranih hudodelskih združb in terorističnih organizacij, ki pomenijo znatno tveganje za državljane in družbo, zaradi česar je lahko upravičeno resnejše poseganje v temeljni pravici do zasebnosti in varstva podatkov⁶⁴. Hkrati meni, da so informacije o teh izjemah, zagotovljene v uvodni izjavi 164 osnutka sklepa, zelo splošne in nepopolne. Iz informacij iz osnutka sklepa zlasti ni jasno, ali je v takem primeru dostop do osebnih podatkov predmet naknadnega sodnega nadzora glede nujnosti in sorazmernosti.
- (73) Glede na to Evropski odbor za varstvo podatkov poziva Komisijo, naj v osnutku sklepa dodatno pojasni in razloži obseg in naravo primerov, v katerih za dostop organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj do podatkov ni potrebna sodna odobritev, ter veljavne zaščitne ukrepe v brazilski zakonodaji. Meni tudi, da bi morala Komisija med spremljanjem osnutka sklepa posebno pozornost nameniti uporabi teh izjem v skladu z brazilskim pravom.

3.1.3 Nadaljnja uporaba podatkov in nadaljnji prenos

- (74) Evropski odbor za varstvo podatkov opozarja, da se zaradi nadaljnje uporabe ali izmenjave podatkov s prejemniki v Braziliji ali tretji državi ne sme ogroziti raven varstva, ki se zagotavlja za osebne podatke, prenesene iz EU/EGP v Brazilijo, tj. da bi morali biti nadaljnji prenos

⁶¹ Glej uvodno izjavo 164 osnutka sklepa.

⁶² Glej člen 15 zakona o hudodelskih združbah in kazenskih preiskavah.

⁶³ Glej člen 16 zakona o hudodelskih združbah in kazenskih preiskavah.

⁶⁴ Glej sodbe Sodišča z dne 6. oktobra 2020, La Quadrature du Net in drugi, združeni zadevi C-511/18 in C-512/18, ECLI:EU:C:2020:791, točke 95–98 z dne 2. oktobra 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, točke 54, 57 in 60, ter z dne 2. marca 2021, Prokuratuur (pogoji za dostop do podatkov o elektronskih komunikacijah), C-746/18, ECLI:EU:C:2021:152, točka 35.

dovoljeni le, če je zagotovljena neprekinjena raven varstva, ki je v osnovi enakovredna tisti, ki je zagotovljena s pravom EU.

- (75) V zvezi s tem Evropski odbor za varstvo podatkov pozitivno ugotavlja, da je brazilsko zvezno vrhovno sodišče odločilo, da izmenjava osebnih podatkov med javnimi organi (tudi kadar se izmenjujejo med organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter obveščevalnimi agencijami) predpostavlja: (1) opredelitev zakonitega, določenega in izrecnega namena obdelave podatkov; (2) združljivost obdelave z informiranimi nameni; (3) omejitev izmenjave na najnižjo potrebno, da bi se izpolnil informirani namen, ter popolno skladnost z zahtevami, zaščitnimi ukrepi in postopki, določenimi v splošnem zakonu o varstvu osebnih podatkov, če je to združljivo z javnim sektorjem⁶⁵.
- (76) Ne glede na to pomembno sodbo najvišjega sodišča v Braziliji Evropski odbor za varstvo podatkov glede na že omenjeno zapletenost, natančen obseg in načine uporabe splošnega zakona o varstvu osebnih podatkov za organe preprečevanja, odkrivanja in preiskovanja kaznivih dejanj poziva Komisijo, naj pozorno spremlja razvoj dogodkov in prakso na tem področju.
- (77) Glede nadaljnjega prenosa osebnih podatkov organom preprečevanja, odkrivanja in preiskovanja kaznivih dejanj v tretjih državah je v osnutku sklepa sklicevanje na člen 33(III) splošnega zakona o varstvu osebnih podatkov, ki določa, da se lahko mednarodni prenosi podatkov izvedejo, „kadar je to potrebno za mednarodno pravno sodelovanje med javnimi obveščevalnimi, preiskovalnimi in kazenskimi organi, v skladu z mednarodnimi pravnimi instrumenti“⁶⁶. Evropski odbor za varstvo podatkov meni, da je ta razlaga preveč splošna, in poziva Komisijo, naj v osnutku sklepa dodatno pojasni pogoje in zaščitne ukrepe, ki urejajo nadaljnje prenose.

3.1.4 Nadzor in pravno varstvo

- (78) Evropski odbor za varstvo podatkov opozarja, da je treba za vsak poseg v pravico do zasebnosti in varstva podatkov uporabljati učinkovit, neodvisen in nepristranski nadzorni sistem, ki ga mora zagotoviti bodisi sodnik bodisi drug neodvisni organ (npr. upravni organ ali parlamentarni organ)⁶⁷.
- (79) Evropski odbor za varstvo podatkov poleg tega ugotavlja, da v brazilskem okviru, kot ga je opisala Komisija, dejavnosti organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj nadzirajo različni organi: (i) sodstvo; (ii) nacionalni organ za varstvo podatkov in (iii) državno tožilstvo.

⁶⁵ Glej uvodno izjavo 187 osnutka sklepa.

⁶⁶ Prav tam.

⁶⁷ Priporočila 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe, sprejeta 10. novembra 2020, glej str. 12:

https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.

- (80) Sodni nadzor, kot je pojasnjeno zgoraj v oddelku o nujnosti in sorazmernosti⁶⁸, se uporablja v zvezi z zbiranjem osebnih podatkov in dostopom do njih, zlasti v obliki predhodnega pregleda in odobritve.
- (81) Kar zadeva vlogo nacionalnega organa za varstvo podatkov, je, kot je že pojasnjeno v oddelku 3.1.1 tega mnenja, v osnutku sklepa o ustreznosti opozorjeno, da se v skladu s členom 4(III) splošnega zakona o varstvu osebnih podatkov ta zakon ne uporablja za obdelavo osebnih podatkov, ki se izvaja *izključno* za namene (i) javne varnosti; (ii) nacionalne obrambe; (iii) državne varnosti ter (iv) preiskovanja in pregona kaznivih dejanj. Poleg tega člen 4(I) določa, da bo tovrstna obdelava urejena s posebno zakonodajo, ki mora med drugim zajemati splošna načela varstva in pravice posameznikov, na katere se nanašajo osebni podatki, kot so določeni v splošnem zakonu o varstvu osebnih podatkov. V odstavku 3 istega člena je priznana svetovalna vloga nacionalnega organa za varstvo podatkov v zvezi z izjemami iz odstavka III, kadar se izvajajo izključno za te namene, zlasti pooblastila nacionalnega organa za varstvo podatkov, da izdaja tehnična mnenja in priporočila ter od ustreznih upravljavcev zahteva ocene učinka v zvezi z varstvom podatkov.
- (82) Komisija se v osnutku sklepa⁶⁹ sklicuje na pomembno odločbo zveznega vrhovnega sodišča z dne 15. septembra 2022, v kateri je navedena uporaba splošnih načel varstva podatkov in pravic posameznikov, na katere se nanašajo osebni podatki, pri obdelavi osebnih podatkov s strani države za zagotavljanje javnih storitev. Navedena odločba se osredotoča na „izmenjavo osebnih podatkov“ med organi in subjekti javne uprave ter pri obveščevalnih dejavnostih, pa tudi na „dostop vladnih agencij in subjektov“ do matičnega registra državljanov. V zvezi z izvršilno vlogo nacionalnega organa za varstvo podatkov Evropski odbor za varstvo podatkov na podlagi dodatnih informacij, ki jih je predložila Komisija, razume, da je nacionalni organ za varstvo podatkov tako vlogo že opravljal v razmerju do policije ter ministrstva za pravosodje in javno varnost. To je potekalo na podlagi sodne prakse, ki z razširitvijo delne uporabe splošnih načel in pravic posameznikov, na katere se nanašajo osebni podatki, na obdelavo, ki se izvaja za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, določa, da je nacionalni organ za varstvo podatkov odgovoren za nadzor nad uporabo prava in njegovo izvrševanje tudi na tem področju.
- (83) Glede na navedeno Evropski odbor za varstvo podatkov poziva Komisijo, naj podrobneje opredeli izvršilno vlogo nacionalnega organa za varstvo podatkov, zlasti v zvezi z ustreznimi pravnimi podlagami ter njegovimi preiskovalnimi in popravljivimi pooblastili v razmerju do organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ter naj pozorno spremlja razvoj dogodkov na tem področju.
- (84) Nazadnje Evropski odbor za varstvo podatkov ugotavlja, da ima državno tožilstvo širše pristojnosti od nadzora nad pravili o varstvu podatkov in zasebnosti ter nalaganja sankcij za kršitve temeljnih pravic. Kot je že pojasnjeno v oddelku 3.1 tega mnenja, je na primer v skladu

⁶⁸ Glej oddelek 3.1.2 zgoraj.

⁶⁹ Glej uvodno izjavo 187 osnutka sklepa.

z zakonom o hudodelskih združbah in kazenskih preiskavah državno tožilstvo eden od organov, ki lahko brez sodne odobritve dostopa do evidenčnih podatkov preiskovane osebe. Evropski odbor za varstvo podatkov zato poziva Komisijo, naj v osnutku sklepa podrobneje opredeli in razloži vlogo in pooblastila državnega tožilstva v zvezi z nadzorom obdelave osebnih podatkov s strani brazilskih organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

- (85) V zvezi s pravnim varstvom Evropski odbor za varstvo podatkov pozitivno ugotavlja, da se pravni mehanizmi, opisani v prvem delu tega mnenja, in zlasti pravna sredstva, ki so posameznikom na voljo za uveljavljanje njihovih pravic do varstva podatkov in zasebnosti, uporabljajo tudi v zvezi z dejavnostmi organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

3.2 Dostop in uporaba s strani brazilskih javnih organov za namene nacionalne varnosti

3.2.1 Obseg izjeme iz člena 4(III) splošnega zakona o varstvu osebnih podatkov in njena uporaba za kazniva dejanja zoper državno varnost

- (86) Kot je uvodoma navedla Komisija, je s členom 4(III) splošnega zakona o varstvu osebnih podatkov „državna varnost“ izvzeta iz uporabe splošnega zakona o varstvu osebnih podatkov pri obdelavi osebnih podatkov, in sicer skupaj z javno varnostjo, nacionalno obrambo ter dejavnostmi preiskovanja in pregona kaznivih dejanj.
- (87) Evropski odbor za varstvo podatkov ugotavlja, da brazilska zakonodaja o „Seguranca Nacional“ (nacionalni varnosti), kot je določena v zakonu št. 14.197 z dne 1. septembra 2021 o spremembi kazenskega zakonika in razveljavitvi zakona o nacionalni varnosti iz leta 1983⁷⁰, izraža brazilski pojem nacionalne varnosti na podlagi izčrpnega seznama kaznivih dejanj⁷¹, ki se nanašajo na različne grožnje za integriteto brazilske države kot institucije (nacionalna suverenost, vohunjenje (člen 350-K), kazniva dejanja zoper demokratične institucije (člen 359-L in drugi). Določbe zakona št. 14.197 so postale sestavni del brazilskega kazenskega zakonika.
- (88) Glede na navedeno Evropski odbor za varstvo podatkov pričakuje, da bo obdelavo podatkov brazilskih organov pregona kaznivih dejanj iz zakona št. 14.197 urejala ureditev, ki se uporablja za dostop in uporabo s strani brazilskih javnih organov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, kot je opisano v poglavju 3.2 osnutka sklepa, zato ima enake pomisleke glede varstva podatkov, kot so navedeni v poglavju 3.1 tega mnenja.

⁷⁰ Zakon št. 14.197 z dne 1. septembra 2021, na voljo na spletnem naslovu https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm (2.10.2026).

⁷¹ Glej uvodno izjavo 200 osnutka sklepa.

Zato poziva Komisijo, naj v osnutku sklepa pojasni, ali je obdelava podatkov v zvezi s pregonom kaznivih dejanj iz zakona št. 14.197 dejansko urejena z ureditvijo varstva podatkov, ki se uporablja za dejavnosti preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ali z drugo ureditvijo. V slednjem primeru poziva Komisijo, naj dodatno pojasni pravila o varstvu podatkov, ki se uporabljajo za kazenski pregon teh kaznivih dejanj za namene nacionalne varnosti.

3.2.2 Pravni okvir za nacionalno varnost

- (89) Kodificirani pravni okvir, na katerem temeljijo ugotovitve iz osnutka sklepa v poglavju o vladnem dostopu za „namene nacionalne varnosti“, sestavljajo zakon št. 14.197 iz leta 2021, zakon št. 9.883 z dne 7. decembra 1999 o vzpostavitvi brazilskega obveščevalnega sistema in povezan odlok št. 4.376 iz leta 2002. Z zadnjima dvema zakonodajnima aktoma sta bila vzpostavljena brazilski obveščevalni sistem (*Sistema Brasileiro des Inteligência*, SISBIN) in njegovo delovanje. Sledita jim zavezujoči predsedniški odlok št. 8.793⁷² iz leta 2016, ki opredeljuje nacionalno obveščevalno politiko (tako imenovana *Política Nacional de Inteligência*), in splošni zakon o varstvu osebnih podatkov iz leta 2018.
- (90) V predsedniškem odloku št. 8.793 iz leta 2016 so opisani predmet, cilji in omejitve nacionalne obveščevalne politike. Dejavnosti na podlagi tega odloka so namenjene pridobivanju znanja v zvezi z dejstvi in situacijami, ki se pojavljajo na nacionalnem ozemlju ali zunaj njega ter imajo takojšen ali potencialni vpliv na postopek odločanja, vladne ukrepe ter varnost družbe in državne obveščevalne službe, in posredovanju tega znanja pristojnim organom. V teh okoliščinah se obveščevalni podatki nanašajo na vse informacije – in podatke –, ki so potrebni in se obdelujejo za podporo postopku odločanja izvršilne veje oblasti na tem področju.
- (91) V skladu s pravno podlago brazilskega obveščevalnega sistema, kot jo je predstavila Komisija, so bili brazilski obveščevalni sistem in njegovi subjekti vzpostavljeni kot osrednji mehanizem za izvajanje nacionalne obveščevalne politike ter so kot taki zadolženi za izvajanje dejavnosti na področju nacionalne varnosti ter javne varnosti in zaščite ter zaščite demokratičnih institucij. V ta namen brazilski obveščevalni sistem zagotavlja izmenjavo znanja in celostno načrtovanje dejavnosti⁷³. Zato se zdi, da pojem nacionalne varnosti v Braziliji glede na dejavnosti brazilskega obveščevalnega sistema ni omejen le na kazniva dejanja, kodificirana v zakonu št. 14.197, temveč bi ga bilo mogoče šteti za sestavni del širšega pojma nacionalne obveščevalne službe.
- (92) Brazilski obveščevalni sistem je bil prvotno vzpostavljen z osemnajstimi zveznimi subjekti, med katerimi je bilo trinajst ministrstev, nato pa je bil z odlokom št. 11.693 z dne 6. septembra 2023 o organizaciji in delovanju brazilskega obveščevalnega sistema razširjen na 48 tako

⁷² Glej uvodno izjavo 199 osnutka sklepa.

⁷³ V predsedniškem odloku št. 8.793, oddelek 5, je navedeno, da so brazilski obveščevalni sistem in organi, ki so vanj vključeni, izmenjava znanja v okviru brazilskega obveščevalnega sistema in celostno načrtovanje sodelovanja med člani brazilskega obveščevalnega sistema instrumenti za izvajanje nacionalne obveščevalne politike.

imenovanih agencij⁷⁴. Evropski odbor za varstvo podatkov ugotavlja, da sodelovanje v okviru brazilskega obveščevalnega sistema vključuje subjekte, ki presegajo klasične varnostne institucije, kot so ministrstvo za znanost (člen 4(IV)), kmetijstvo (člen 4(XV)) in energijo (člen 4(XVIII)) ter zvezni generalni tožilec (člen 4(XIX)).

- (93) Odlok št. 4.376 iz leta 2002 določa, da mora svetovalni svet brazilskega obveščevalnega sistema predlagati splošne standarde in postopke za izmenjavo „znanja in komunikacije“ v okviru brazilskega obveščevalnega sistema⁷⁵, odlok št. 11.693 iz leta 2023 pa določa, da mora osrednji organ brazilskega obveščevalnega sistema pripraviti tehnična orodja⁷⁶ za izmenjavo informacij in znanja, ter opisuje izmenjavo in uporabo podatkov, ki jih pridobijo subjekti, ki so del brazilskega obveščevalnega sistema. Vendar osnutek sklepa Komisije ne vsebuje nobenih dodatnih informacij o teh pravilih ali pravnih standardih, ki jih izda osrednji organ, na primer kadar si subjekti, ki so del brazilskega obveščevalnega sistema, medsebojno izmenjujejo osebne podatke.
- (94) Poleg tega se zdi, da obstajajo razlike v pojmi o občutljivosti informacij, saj je v skladu z upoštevnim pravom, ki ureja dejavnosti brazilskega obveščevalnega sistema, občutljivost povezana s stopnjo zaupnosti, dodeljeno informaciji⁷⁷, in omejitvijo namena v primerjavi s splošnimi načeli splošne uredbe o varstvu podatkov⁷⁸.
- (95) Kot je bilo že pojasnjeno, so s členom 4(III), točke (a)–(c), splošnega zakona o varstvu osebnih podatkov, ki je bil kodificiran šele po vzpostavitvi brazilskega obveščevalnega sistema in določitvi nacionalne obveščevalne politike, iz uporabe splošnega zakona o varstvu osebnih podatkov izvzete dejavnosti obdelave podatkov, ki se izvajajo izključno za namene javne varnosti, nacionalne obrambe in državne varnosti, še vedno pa se upoštevajo uveljavljena splošna načela varstva podatkov.
- (96) Kot je Komisija poudarila v osnutku sklepa, se krovni okvir brazilske ustave in sodelovanje Brazilije v Medameriškem sodišču za človekove pravice nanašata na pravni okvir za vladni dostop za namene nacionalnih obveščevalnih služb. Evropski odbor za varstvo podatkov poleg tega priznava, da imajo sodbe brazilskega zveznega vrhovnega sodišča pomembno vlogo tudi pri opredelitvi pravnega okolja⁷⁹. Dosedanje sodbe vrhovnega sodišča pomenijo jedrnat in ustrezno podporo nadaljnjemu razvoju varstva osebnih podatkov v skladu z brazilsko ustavo. Hkrati je treba opozoriti, da sodbe vrhovnega sodišča ne pojasnjujejo ali določajo splošnih abstraktnih pravil o varstvu podatkov za obdelavo osebnih podatkov, temveč razlagajo določbe in načela ustave in splošnega zakona o varstvu osebnih podatkov.

⁷⁴ Glej uvodno izjavo 202 osnutka sklepa.

⁷⁵ Glej člen 7(II) odloka št. 4.376.

⁷⁶ Glej člen 10(XI), na voljo na spletnem naslovu https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm (26. 9. 2025).

⁷⁷ Glej odlok št. 8.793 iz leta 2016, odlok št. 11.693 in uvodno izjavo 204 osnutka sklepa.

⁷⁸ Glej člen 6(I) splošnega zakona o varstvu osebnih podatkov, ki se nanaša na zakonite in posebne namene, medtem ko se s splošno uredbo o varstvu podatkov zahtevajo zakoniti in določeni nameni.

⁷⁹ Glej uvodno izjavo 203 osnutka sklepa.

- (97) Evropski odbor za varstvo podatkov se zaveda, da imajo zvezne države široko diskrecijsko pravico pri opredeljevanju zadev v zvezi z nacionalno varnostjo, kar omogoča izjeme v zvezi z nacionalno varnostjo pri obdelavi osebnih podatkov. V zvezi s tem opozarja na opredelitev Evropskega sodišča za človekove pravice, v skladu s katero se morajo grožnje nacionalni varnosti po svoji naravi, resnosti in posebnih okoliščinah razlikovati od splošnih tveganj za javno varnost ali od hudih kaznivih dejanj⁸⁰.
- (98) Kot razume Evropski odbor za varstvo podatkov, se v zvezi s podatki, ki jih obdelujejo subjekti, ki so del brazilskega obveščevalnega sistema, izvzetje iz člena 4(III) splošnega zakona o varstvu osebnih podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj uporablja le, če se obdelava izvaja *izključno* za namene javne varnosti, nacionalne obrambe in državne varnosti. Zdi se, da to velja zlasti za dejavnosti osrednjega organa brazilskega obveščevalnega sistema, tj. brazilске obveščevalne agencije (ABIN). Zato se splošni zakon o varstvu osebnih podatkov uporablja v celoti, razen če subjekt, ki je del brazilskega obveščevalnega sistema, deluje v imenu brazilске obveščevalne agencije za enega od teh namenov.
- (99) Evropski odbor za varstvo podatkov poziva Komisijo, naj potrdi to razumevanje ter v osnutku sklepa opiše in natančneje pojasni oris pojma nacionalne varnosti v skladu z brazilskim pravom, zlasti v zvezi z zbiranjem in izmenjavo podatkov med subjekti in s strani subjektov zaradi dejavnosti brazilskega obveščevalnega sistema ter v zvezi z izvajanjem nacionalne obveščevalne politike. V zvezi s tem poziva Komisijo, naj pojasni tudi, kako so izvzetja iz splošnega zakona o varstvu osebnih podatkov za namene nacionalne varnosti povezana z izvzetjem zaradi nacionalne varnosti na podlagi splošne uredbe o varstvu podatkov.

3.2.3 Nadaljnji prenosi in mednarodni sporazumi

- (100) V členu 33 splošnega zakona o varstvu osebnih podatkov so opredeljeni osnovni pogoji za mednarodni prenos podatkov. Člen 33(I) in (II) splošnega zakona o varstvu osebnih podatkov določa zahteve, podobne sklepu o ustreznosti, ali zahteve za dodatne zaščitne ukrepe v skladu s splošno uredbo o varstvu podatkov. Te zahteve so opuščene v členu 33(III), (VI) in (VII) splošnega zakona o varstvu osebnih podatkov, ki obravnava primere „pravnega sodelovanja med obveščevalnimi službami“, prenose, ki izhajajo iz „zaveze iz mednarodnih sporazumov o sodelovanju“, in prenose, „ki so potrebni za izvrševanje javnega reda ali zakonskega pooblastila javne službe“, tj. nacionalne varnosti in nacionalnih obveščevalnih služb. Zdi se, da je ta sklep v skladu s konceptom člena 4(III) splošnega zakona o varstvu osebnih podatkov, ki uporabo splošnega zakona o varstvu osebnih podatkov omejuje le na njegova načela v zvezi z zadevami javne varnosti, nacionalne obrambe in državne varnosti. Zato bi se lahko štelo, da bi bilo treba nadaljnje prenose za nacionalne obveščevalne namene izvajati v skladu s splošnimi načeli varstva podatkov iz splošnega zakona o varstvu osebnih

⁸⁰ Sodba ESČP z dne 25. maja 2021, Big Brother Watch in drugi proti Združenemu kraljestvu, točka 350.

podatkov, hkrati pa bi zanje veljale določbe o mednarodnem sodelovanju iz pravnih aktov o vzpostavitvi nacionalne obveščevalne politike in brazilskega obveščevalnega sistema.

- (101) Glede na navedeno Evropski odbor za varstvo podatkov priznava, da Brazilija osebne podatke morda mora posredovati in jih tudi dejansko posreduje tujim obveščevalnim službam za namene sodelovanja ali izvajanja nacionalne obveščevalne politike v skladu s ciljem preprečevanja in prepoznavanja groženj na podlagi zgoraj navedenega integriranega koncepta varnosti.
- (102) Kot je bilo že navedeno, Komisija opozarja na uporabo krovnega okvira brazilске ustave in jamstva pravnega sredstva *habeas data* za varstvo osebnih podatkov v okviru brazilskega obveščevalnega sistema, ki veljata tudi za nadaljnje prenose za namene nacionalne varnosti. Evropski odbor za varstvo podatkov poziva Komisijo, naj dodatno pojasni pravno podlago ter zaščitne ukrepe in pogoje za varstvo podatkov, ki jih morajo brazilska obveščevalna agencija in drugi člani brazilskega obveščevalnega sistema upoštevati pred razkritjem osebnih podatkov tujim partnerjem za nacionalne obveščevalne namene.
- (103) Evropski odbor za varstvo podatkov poleg tega ugotavlja, da Komisija v svojo oceno ustreznosti ni vključila premislekov o obstoju mednarodnih sporazumov, sklenjenih med Brazilijo in tretjimi državami ali mednarodnimi organizacijami. Ker splošni zakon o varstvu osebnih podatkov ne določa zavezujoče zakonodaje, ki bi presegala splošna načela varstva podatkov, bi lahko taki sporazumi vsebovali posebne določbe za mednarodni prenos osebnih podatkov, ki jih hranijo brazilska obveščevalna agencija ali drugi člani brazilskega obveščevalnega sistema, v tretje države. Evropski odbor za varstvo podatkov meni, da bo sklenitev dvostranskih ali večstranskih sporazumov s tretjimi državami za namene nacionalnih obveščevalnih služb verjetno vplivala na zadevni pravni okvir varstva podatkov.
- (104) Evropski odbor za varstvo podatkov zato poziva Komisijo, naj pojasni, ali taki mednarodni sporazumi za nacionalne obveščevalne namene obstajajo, in naj oceni njihov morebitni vpliv na raven varstva osebnih podatkov, prenesenih iz EGP v Brazilijo, v zvezi s primarno ocenjenim pravnim okvirom za obdelavo podatkov za nacionalne obveščevalne namene.

3.2.4 Nadzor in pravno varstvo

- (105) V osnutku sklepa o ustreznosti so predvideni različni organi za nadzor dejavnosti brazilskih nacionalnih varnostnih organov, zlasti (i) izvršilna veja oblasti, (ii) zakonodajna veja oblasti; (iii) nacionalni organ za varstvo podatkov in (iv) sodstvo. Evropski odbor za varstvo podatkov v zvezi z nacionalnim organom za varstvo podatkov opozarja na premisleke in ugotovitve iz oddelka 3.1.4 tega mnenja, ki veljajo tudi tukaj.
- (106) V skladu z osnutkom sklepa je zbornica za zunanje odnose in nacionalno obrambo vladnega sveta odgovorna za nadzor nad izvajanjem obveščevalne nacionalne policije, urad za institucionalno varnost pa za usklajevanje dejavnosti zvezne obveščevalne službe. Evropski odbor za varstvo podatkov ugotavlja, da se ta nadzor nanaša le na zagotavljanje ciljev, ki jih

mora doseči obveščevalni sistem, in na njihovo izvajanje, ne vključuje pa preiskovalnih pooblastil ali pooblastil za sankcioniranje ter ne zajema dejanske obdelave osebnih podatkov.

- (107) Dejansko je za nadzor nad obveščevalnimi dejavnostmi, vključno z njihovo zakonitostjo in učinkovitostjo, pristojen skupni odbor za nadzor obveščevalnih dejavnosti (CCAI) (zakonodajna veja oblasti). Evropski odbor za varstvo podatkov pozdravlja okrepitev strukture in pooblastil skupnega odbora za nadzor obveščevalnih dejavnosti, kar povečuje preglednost njegovih dejavnosti in organu omogoča izvajanje ustreznega nadzora, kot so naknadni pregledi, revizije in nadzor nad tekočimi operacijami. Poleg tega pozitivno ugotavlja, da lahko skupni odbor za nadzor obveščevalnih dejavnosti obravnava pritožbe posameznikov, na katere se nanašajo osebni podatki, v okviru svojih pristojnosti za preiskovanje pritožb o kršitvah temeljnih pravic in jamstev.
- (108) Pristojnost sodstva za obravnavanje zadev, ki jih državljani vložijo proti javnim organom, je pozitiven vidik, zlasti ker omogoča sodni nadzor nad dejavnostmi, ki se izvajajo v imenu nacionalne varnosti, ter med drugim zagotavlja skladnost z ustavnimi pravicami (vključno s pravico do varstva podatkov) in splošnim zakonom o varstvu osebnih podatkov. Evropski odbor za varstvo podatkov pozitivno ugotavlja, da je možnost pritožbe zagotovljena prek zveznega vrhovnega sodišča in nazadnje prek Medameriškega sodišča za človekove pravice.
- (109) Kot razume Evropski odbor za varstvo podatkov, so posameznikom, na katere se nanašajo osebni podatki, v okviru nacionalnih obveščevalnih dejavnosti zagotovljene (i) pravice, kot so določene v splošnem zakonu o varstvu osebnih podatkov (kot posledica odločbe zveznega vrhovnega sodišča z dne 15. septembra 2022); (ii) pravica do dostopa do osebnih podatkov in njihovega popravka prek ustavnopravnega sredstva *habeas data* ter (iii) pravica do odškodnine za premoženjsko in nepremoženjsko škodo.
- (110) Evropski odbor za varstvo podatkov pozdravlja obstoj takih pravic in dejstvo, da se je nanje mogoče sklicevati prek sodnih in upravnih mehanizmov, zlasti skupnega odbora za nadzor obveščevalnih dejavnosti, pa tudi dejstvo, da so te možnosti pravnega varstva dostopne vsem posameznikom, ne glede na državljanstvo.

4. IZVAJANJE IN SPREMLJANJE OSNUTKA SKLEPA

- (111) Evropski odbor za varstvo podatkov v zvezi s spremljanjem in pregledom osnutka sklepa ugotavlja, da mora Komisija v skladu s sodno prakso Sodišča „glede na to, da se raven varstva, ki jo zagotavlja tretja država, lahko spremeni, [...] po sprejetju [sklepa o ustreznosti] na podlagi člena [45 splošne uredbe o varstvu podatkov] redno preverjati, ali je ugotovitev v zvezi z ustrežno ravnijo varstva, ki ga zagotavlja zadevna tretja država, še zmeraj dejansko

in pravno utemeljena. Vsekakor je taka preveritev potrebna, kadar je na podlagi indiciev mogoče o tem dvomiti⁸¹.

- (112) Evropski odbor za varstvo podatkov ugotavlja, da bo v skladu s členom 45(3) splošne uredbe o varstvu podatkov pregled ugotovitve o ustreznosti potekal vsaj vsaka štiri leta⁸².
- (113) Evropski odbor za varstvo podatkov pozdravlja, da je v uvodni izjavi 230 osnutka sklepa predvideno njegovo sodelovanje na srečanju, ki bo organizirano med Komisijo in brazilskimi organi ter bo namenjeno izvedbi pregleda izvajanja sklepa o ustreznosti. Kar zadeva praktično sodelovanje Evropskega odbora za varstvo podatkov in njegovih predstavnikov pri pripravi in izvajanju prihodnjih rednih pregledov, Evropski odbor za varstvo podatkov ponovno poudarja, da bi mu bilo treba dovolj zgodaj pred pregledi pisno predložiti vso ustrezno dokumentacijo, vključno s korespondenco.

Za Evropski odbor za varstvo podatkov
predsednica

(Anu Talus)

⁸¹ Sodba Sodišča Schrems I, točka 76. Glej tudi člen 3(4) osnutka sklepa.

⁸² Glej uvodno izjavo 229 in člen 3(4) osnutka sklepa.