

Mnenje odbora (člen 64)



Mnenje št. 28/2024 o nekaterih vidikih varstva podatkov, povezanih z obdelavo osebnih podatkov v okviru modelov umetne inteligence

Sprejeto 17. decembra 2024

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Povzetek

Tehnologije umetne inteligence ustvarjajo številne priložnosti in koristi v najrazličnejših sektorjih in družbenih dejavnostih.

Splošna uredba o varstvu podatkov z zaščito temeljne pravice do varstva podatkov podpira te priložnosti in spodbuja druge temeljne pravice EU, vključno s pravico do svobode razmišljanja, izražanja in obveščanja, pravico do izobraževanja ali svobodo opravljanja gospodarske dejavnosti, in kot taka predstavlja pravni okvir, ki spodbuja odgovorne inovacije.

V zvezi s tem je irski nadzorni organ ob upoštevanju vprašanj o varstvu podatkov, ki se zastavljajo zaradi teh tehnologij, poslal EOVP prošnjo za izdajo mnenja o zadevah splošne uporabe v skladu s členom 64(2) Splošne uredbe o varstvu podatkov. Prošnja za mnenje se nanaša na obdelavo osebnih podatkov v okviru faz razvoja in uvajanja modelov umetne inteligence (v nadaljnjem besedilu: **modeli UI**). Natančneje, v prošnji za izdajo mnenja je bilo postavljeno naslednje vprašanje: (1) kdaj in kako se lahko model UI šteje za „anonimnega“, (2) kako lahko upravljavci dokažejo primernost zakonitega interesa kot pravne podlage v fazah razvoja in (3) uvajanja ter (4) kakšne so posledice nezakonite obdelave osebnih podatkov v fazi razvoja modela UI na njihovo nadaljnjo obdelavo ali delovanje modela UI.

V zvezi s prvim vprašanjem je v mnenju navedeno, da bi morali pristojni nadzorni organi trditve o anonimnosti modela UI presoditi za vsak primer posebej, saj EOVP meni, da modelov UI, ki so se učili iz osebnih podatkov, ni mogoče v vseh primerih šteti za anonimne. Da bi model UI veljal za anonimnega, morata biti (1) verjetnost neposrednega (in verjetnostnega) pridobivanja osebnih podatkov o posameznikih, katerih osebni podatki so bili uporabljeni za razvoj modela, in (2) verjetnost namernega ali nenamernega pridobivanja takih osebnih podatkov iz poizvedb zanemarljiva, pri čemer je treba upoštevati „*vsa sredstva, za katera je razumno verjetno, da jih bo*“ uporabil upravljavec ali druga oseba.

Da bi nadzorni organi opravili svojo presojo, bi morali pregledati dokumentacijo, ki jo je predložil upravljavec, da bi dokazal anonimnost modela. V zvezi s tem je v mnenju naveden nepredpisujoč in neizčrpen seznam metod, ki jih lahko upravljavci uporabijo pri dokazovanju anonimnosti in jih zato nadzorni organi upoštevajo pri presojanju upravljavčeve trditve o anonimnosti. To na primer zajema pristope, ki jih upravljavci sprejmejo v fazi razvoja, da bi preprečili ali omejili zbiranje osebnih podatkov, ki se uporabljajo za učenje, zmanjšali možnost identifikacije, preprečili njihovo izluščenje ali zagotovili najsodobnejšo odpornost na napade.

V zvezi z drugim in tretjim vprašanjem so v mnenju navedeni splošni premisleki, ki jih morajo nadzorni organi upoštevati pri presojanju, ali se lahko upravljavci sklicujejo na zakoniti interes kot ustrezno pravno podlago za obdelavo, ki se izvaja v okviru razvoja in uvajanja modelov UI.

V mnenju je poudarjeno, da med pravnimi podlagami, ki jih določa Splošna uredba o varstvu podatkov, ni hierarhije in da morajo upravljavci opredeliti ustrezno pravno podlago za svoje dejavnosti obdelave. Mnenje nato opozarja na tristopenjski preizkus, ki ga je treba opraviti pri presojanju uporabe zakonitega interesa kot pravne podlage, tj. (1) opredelitev zakonitega interesa, za katerega si prizadeva upravljavec ali tretja oseba; (2) analiza nujnosti obdelave za namene zakonitega(-ih) interesa(-ov), za katerega(-e) si prizadeva (imenovan tudi „preizkus nujnosti“); in (3) ocena, ali nad zakonitim(-i) interesom(-i) ne prevladajo interesi ali temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki (imenovan tudi „preizkus uravnoteženja“).

V zvezi s prvim korakom je v mnenju opozorjeno, da se interes lahko šteje za zakonit, če so izpolnjena naslednja tri kumulativna merila: interes (1) je zakonit, (2) je jasno in natančno izražen ter (3) je resničen in prisoten (tj. ni špekulativen). Tak interes lahko zajema na primer razvoj modela UI – razvoj storitve pogovornega agenta za pomoč uporabnikom ali njegovo uvedbo – za izboljšanje odkrivanja groženj v informacijskem sistemu.

V zvezi z drugim korakom je v mnenju poudarjeno, da presoja nujnosti vključuje upoštevanje: (1) ali bo dejavnost obdelave omogočila uresničevanje zakonitega interesa in (2) ali ne obstaja manj vsiljiv način za uresničevanje tega interesa. Pri presojanju ali je pogoj nujnosti izpolnjen, bi morali nadzorni organi posebno pozornost nameniti količini obdelanih osebnih podatkov in temu, ali je to sorazmerno z uresničevanjem zadevnega zakonitega interesa, tudi glede na načelo zmanjšanja količine podatkov.

V zvezi s tretjim korakom je v mnenju poudarjeno, da bi bilo treba preizkus uravnoteženja izvesti ob upoštevanju posebnih okoliščin vsakega primera. Nadalje vsebuje pregled elementov, ki jih lahko nadzorni organi upoštevajo pri presojanju, ali interesi, temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, prevladajo nad interesom upravljavca ali tretje osebe.

V mnenju so kot del tretjega koraka poudarjena posebna tveganja za temeljne pravice, ki se lahko pojavijo v fazah razvoja ali uvajanja modelov UI. Pojasnjuje tudi, da lahko obdelava osebnih podatkov, ki poteka v fazah razvoja in uvajanja modelov UI, na posameznike, na katere se nanašajo osebni podatki, vpliva na različne načine, ki so lahko pozitivni ali negativni. Pri ocenjevanju tovrstnega učinka lahko nadzorni organi upoštevajo naravo podatkov, ki jih obdelujejo modeli, kontekst obdelave in morebitne nadaljnje posledice obdelave.

V mnenju je dodatno poudarjena vloga razumnih pričakovanj posameznikov, na katere se nanašajo osebni podatki, pri preizkusu uravnoteženja. To je lahko pomembno zaradi zapletenosti tehnologij, ki se uporabljajo v modelih UI, in dejstva, da posamezniki, na katere se nanašajo osebni podatki, morda težko razumejo raznolikost njihovih potencialnih uporab in različnih vključenih dejavnosti obdelave. V zvezi s tem so lahko tako informacije, ki se zagotovijo posameznikom, na katere se nanašajo osebni podatki, kot kontekst obdelave eni od elementov, ki jih je treba upoštevati pri presojanju, ali lahko posamezniki, na katere se nanašajo osebni podatki, razumno pričakujejo, da bodo njihovi osebni podatki obdelani. V zvezi s kontekstom to lahko vključuje: ali so bili osebni podatki javno dostopni ali ne, naravo razmerja med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem (in ali med njima obstaja povezava), naravo storitve, okoliščine, v katerih so bili osebni podatki zbrani, vir, iz katerega so bili podatki zbrani (tj. iz katerega spletnega mesta ali storitve in njihove nastavitve zasebnosti), morebitne nadaljnje uporabe modela in ali se posamezniki, na katere se nanašajo osebni podatki, dejansko zavedajo, da so njihovi osebni podatki sploh na spletu.

V mnenju je tudi navedeno, da kadar se zdi, da interesi, pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, prevladajo nad zakonitimi interesi, ki jih želi uresničiti upravljavec ali tretja oseba, lahko upravljavec razmisli o uvedbi blažilnih ukrepov za omejitev vpliva obdelave na te posameznike, na katere se nanašajo osebni podatki. Blažilnih ukrepov se ne sme zamenjevati z ukrepi, ki jih mora upravljavec v vsakem primeru sprejeti po zakonu, da bi zagotovil skladnost s SUVP. Poleg tega bi morali biti ukrepi prilagojeni okoliščinam primera in značilnostim modela UI, vključno z njegovo predvideno uporabo. V zvezi s tem je v mnenju naveden neizčrpen seznam primerov blažilnih ukrepov v zvezi s fazo razvoja (tudi glede spletnega strganja) in fazo uvajanja. Blažilni ukrepi se lahko hitro razvijajo in bi morali biti prilagojeni okoliščinam primera. Zato morajo nadzorni organi še vedno oceniti ustreznost blažilnih ukrepov, ki se izvajajo za vsak primer posebej.

V zvezi s četrtem vprašanjem je v mnenju na splošno poudarjeno, da imajo nadzorni organi diskrecijska pooblastila za presojo morebitnih kršitev in izbiro ustreznih, potrebnih in sorazmernih ukrepov, pri

čemer upoštevajo okoliščine vsakega posameznega primera. V mnenju so nato obravnavani trije scenariji.

Po scenariju 1 se osebni podatki shranijo v modelu UI (kar pomeni, da modela ni mogoče šteti za anonimnega, kot je podrobno opisano v prvem vprašanju) in jih nato obdeluje isti upravljavec (na primer v okviru uvajanja modela). V mnenju je navedeno, da bi bilo treba, odvisno od okoliščin primera, za vsak primer posebej oceniti, ali faza razvoja in uvajanja vključuje ločene namene (ki tako pomenijo ločene dejavnosti obdelave) in v kolikšni meri pomanjkanje pravne podlage za prvotno dejavnost obdelave vpliva na zakonitost poznejše obdelave.

Po scenariju 2 se osebni podatki hranijo v modelu, v okviru uvajanja modela pa jih obdeluje drug upravljavec. V zvezi s tem je v mnenju navedeno, da bi morali nadzorni organi upoštevati, ali je upravljavec, ki uvaja model, v okviru svojih obveznosti glede odgovornosti za dokazovanje skladnosti s členom 5(1)(a) in členom 6 SUVP izvedel ustrezno oceno, da bi preveril, da model UI ni bil razvit z nezakonito obdelavo osebnih podatkov. Ta presoja bi morala na primer upoštevati vir osebnih podatkov in to, ali je bila obdelava v fazi razvoja predmet ugotovljene kršitve, zlasti če jo je ugotovil nadzorni organ ali sodišče, ter bi morala biti manj ali bolj podrobna glede na tveganja, ki jih povzroča obdelava v fazi uvajanja.

Upravljavec v okviru scenarija 3 nezakonito obdeluje osebne podatke za razvoj modela UI, nato pa zagotovi, da so anonimizirani, preden isti ali drug upravljavec začne drugo obdelavo osebnih podatkov v okviru uvajanja. V zvezi s tem je v mnenju navedeno, da če je mogoče dokazati, da nadaljnje delovanje modela UI ne vključuje obdelave osebnih podatkov, EOVP meni, da se SUVP ne bi uporabila. Zato nezakonitost začetne obdelave ne bi smela vplivati na nadaljnje delovanje modela. Poleg tega EOVP meni, da bi se v zvezi s temi postopki obdelave SUVP uporabljala, kadar upravljavci pozneje obdelujejo osebne podatke, zbrane med fazo uvajanja, potem ko je bil model anonimiziran. V teh primerih meni, da v zvezi s SUVP nezakonitost začetne obdelave ne bi smela vplivati na zakonitost obdelave, izvedene v fazi uvajanja.

Kazalo

1	Uvod	6
1.1	Povzetek dejstev	6
1.2	Dopustnost prošnje za mnenje na podlagi člena 64(2) Splošne uredbe o varstvu podatkov ..	8
2	Področje uporabe in ključni pojmi	9
2.1	Obseg mnenja	9
2.2	Ključni pojmi.....	10
2.3	Modeli UI v okviru mnenja	11
3	Ustreznost prošnje za mnenje	12
3.1	O naravi modelov umetne inteligence v zvezi z opredelitvijo osebnih podatkov	12
3.2	O okoliščinah, v katerih bi se lahko modeli UI šteli za anonimne, in s tem povezan prikaz ..	14
3.2.1	Splošni premislek o anonimizaciji v obravnavanem kontekstu	14
3.2.2	Elementi za oceno preostale verjetnosti identifikacije.....	16
3.3	O primernosti zakonitega interesa kot pravne podlage za obdelavo osebnih podatkov v okviru razvoja in uvajanja modelov umetne inteligence	19
3.3.1	Splošne ugotovitve.....	19
3.3.2	Razmisleki o treh korakih presoje zakonitega interesa v okviru razvoja in uvajanja modelov umetne inteligence	20
3.4	O morebitnem vplivu nezakonite obdelave pri razvoju modela umetne inteligence na zakonitost nadaljnje obdelave ali delovanja modela umetne inteligence	30
3.4.1.....	Scenarij 1 Upravljavec nezakonito obdeluje osebne podatke za razvoj modela, osebni podatki ostanejo v modelu in jih nato obdeluje isti upravljavec (na primer v okviru uvajanja modela).	32
3.4.2	Scenarij 2 Upravljavec nezakonito obdeluje osebne podatke za razvoj modela, osebni podatki ostanejo v modelu in jih obdeluje drug upravljavec v okviru uvajanja modela	32
3.4.3	Scenarij 3 Upravljavec nezakonito obdeluje osebne podatke za razvoj modela, nato pa zagotovi, da je model anonimiziran, preden isti ali drug upravljavec začne drugo obdelavo osebnih podatkov v okviru uvajanja	34
4	Končne pripombe	34

Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 63 in člena 64(2) 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 ali SUVVP),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu EGP, kakor je bil spremenjen s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018¹,

ob upoštevanju členov 10 in 22 svojega poslovnika,

ob upoštevanju naslednjega:

(1) Glavna vloga Evropskega odbora za varstvo podatkov (v nadaljnjem besedilu: „**odbor**“ ali „**EOVP**“) je zagotoviti dosledno uporabo SUVVP v celotnem Evropskem gospodarskem prostoru (v nadaljnjem besedilu: „**EGP**“). Člen 64(2) SUVVP določa, da lahko kateri koli nadzorni organ, predsednik odbora ali Komisija zahteva, da odbor prouči katero koli zadevo splošne uporabe ali z učinkom v več kot eni državi članici EGP in poda mnenje. Namen tega mnenja je proučiti zadevo splošne uporabe ali zadevo z učinkom v več kot eni državi članici EGP.

(2) Mnenje odbora se sprejme v skladu s členom 64(3) SUVVP v povezavi s členom 10(2) poslovnika EOVP v osmih tednih po odločitvi predsednika in pristojnega nadzornega organa, da je dokumentacija popolna. Po predsednikovi odločitvi se glede na kompleksnost vsebine to obdobje lahko podaljša za šest tednov.

SPREJEL NASLEDNJE MNENJE:

1 Uvod

1.1 Povzetek dejstev

1. Irski nadzorni organ (v nadaljnjem besedilu: **irski nadzorni organ** ali **nadzorni organ prosilec**) je 4. septembra 2024 zaprosil EOVP, da izda mnenje v skladu s členom 64(2) SUVVP v zvezi z modeli UI in obdelavo osebnih podatkov (v nadaljnjem besedilu: **prošnja za mnenje**).
2. Predsednik odbora in irski nadzorni organ sta 13. septembra 2024 dokumentacijo štela za popolno. Naslednji delovni dan, 16. septembra 2024, je bila predana sekretariatu EOVP. Predsednica odbora je glede na kompleksnost zadeve sklenila podaljšati zakonski rok v skladu s členom 64(3) SUVVP in členom 10(4) poslovnika EOVP.
3. Prošnja za mnenje obravnava nekatere elemente učenja, posodabljanja, razvoja in delovanja modelov UI, pri katerih so osebni podatki del zadevnega nabora podatkov. Irski nadzorni organ poudarja, da se prošnja za mnenje nanaša na ključna vprašanja, ki močno vplivajo na posameznike, na katere se nanašajo osebni podatki, in upravljavce v EGP ter da v tej fazi ni usklajenega stališča med nacionalnimi

¹ Sklice na „države članice“ v tem mnenju je treba razumeti kot sklice na „države članice EGP“. Sklicevanje na Unijo v tem mnenju je treba razumeti kot sklicevanje na EGP.

nadzornimi organi². Izrazje, ki se bo uporabljalo za namene tega mnenja, je navedeno v oddelkih 2.2 in 2.3 v nadaljevanju.

4. Irski nadzorni organ je postavil naslednja vprašanja:

Vprašanje 1: Ali se šteje, da končni model UI, ki se je učil z uporabo osebnih podatkov, v nobenem primeru ne ustreza opredelitvi osebnih podatkov (kot je določeno v členu 4(1) SUVP)?

Če je odgovor na vprašanje 1 pritrdilen:

- i. V kateri fazi postopkov obdelave, ki vodijo do modela UI, se osebni podatki ne obdelujejo več?
 - a) Kako je mogoče dokazati, da model UI ne obdeluje osebnih podatkov?
- ii. Ali obstajajo dejavniki, ki bi povzročili, da se delovanje končnega modela UI ne bi več štelo za anonimno?
 - a) Če je odgovor pritrdilen, kako je mogoče dokazati ukrepe, sprejete za ublažitev teh dejavnikov, njihovo preprečevanje ali zaščito pred njimi (da se zagotovi, da se v modelu UI ne obdelujejo osebni podatki)?

Če je odgovor na vprašanje 1 nikalen:

- i. Katere so okoliščine, v katerih bi se to lahko zgodilo?
 - a) Če je tako, kako je mogoče dokazati ukrepe, ki so bili sprejeti za zagotovitev, da model UI ne obdeluje osebnih podatkov?

Vprašanje 2: Kadar se upravljavec podatkov zanaša na zakonite interese kot pravno podlago za obdelavo osebnih podatkov za oblikovanje, posodabljanje in/ali razvoj modela UI, kako bi moral ta upravljavec dokazati ustreznost zakonitih interesov kot pravne podlage, tako v zvezi z obdelavo podatkov tretjih oseb kot podatkov prvih oseb?

- i. Katere vidike bi moral upravljavec upoštevati za zagotovitev, da so interesi posameznikov, na katere se nanašajo osebni podatki in katerih osebni podatki se obdelujejo, ustrezno uravnoteženi z interesi tega upravljavca v okviru:
 - a) podatkov tretjih oseb,
 - b) podatkov prvih oseb.

Vprašanje 3: Če se upravljavec podatkov zanaša na zakonite interese kot pravno podlago za obdelavo osebnih podatkov, ki se izvaja v okviru modela UI ali sistema UI, katerega del je model UI, kako naj upravljavec po učenju iz osebnih podatkov dokaže ustreznost zakonitih interesov kot pravne podlage?

Vprašanje 4: Če je bilo ugotovljeno, da je bil model UI ustvarjen, posodobljen ali razvit z uporabo nezakonito obdelanih osebnih podatkov, kakšen je morebitni vpliv tega na zakonitost nadaljnje ali poznejše obdelave ali delovanja modela UI, bodisi samostojno bodisi kot del sistema UI, če:

- i. model UI bodisi samostojno bodisi kot del sistema UI obdeluje osebne podatke?
- ii. niti model UI niti model UI kot del sistema UI ne obdelujeta osebnih podatkov?

² Prošnja za mnenje, str. 1.

1.2 Dopustnost prošnje za mnenje na podlagi člena 64(2) Splošne uredbe o varstvu podatkov

5. Člen 64(2) SUVP določa zlasti, da lahko kateri koli nadzorni organ zahteva, da odbor prouči katero koli zadevo splošne uporabe ali zadevo z učinkom v več kot eni državi članici in poda mnenje.
6. Nadzorni organ prosilec je na EOVP naslovil vprašanja o vidikih varstva podatkov v okviru modelov UI. V prošnji za mnenje je navedel, da čeprav številne organizacije zdaj uporabljajo modele UI, vključno z velikimi jezikovnimi modeli, njihovo delovanje, učenje in uporaba vzbujajo „številne obsežne pomisleke glede varstva podatkov“³, ki „vplivajo na posameznike, na katere se nanašajo osebni podatki, v EU/EGP“⁴.
7. V prošnji za mnenje so v bistvu postavljena vprašanja o (i) uporabi pojma osebnih podatkov, (ii) načelu zakonitosti s posebnim poudarkom na pravni podlagi zakonitega interesa v okviru modelov UI ter o (iii) posledicah nezakonite obdelave osebnih podatkov v fazi razvoja modelov UI na nadaljnjo obdelavo ali delovanje modela.
8. Zato odbor meni, da se prošnja za mnenje nanaša na „zadevo splošne uporabe“ v smislu člena 64(2) SUVP. Zadeva se nanaša zlasti na razlago in uporabo členov 4(1), 5(1)(a) in 6 SUVP v zvezi z obdelavo osebnih podatkov pri razvoju in uporabi modelov UI. Kot je poudaril nadzorni organ prosilec, uporaba teh določb za modele UI sproža sistemska, abstraktna in nova vprašanja⁵. Vse več organizacij hitro razvija in čedalje bolj uporablja modele UI, kar sproža posebna vprašanja in, kot je poudarjeno v prošnji za mnenje, „bo EOVP imel velike koristi od oblikovanja skupnega stališča o zadevah, obravnavanih v tej prošnji za mnenje, saj so tovrstne zadeve ključne za kratko- in srednjeročno načrtovano delo EOVP“⁶. Poleg tega tehnologije umetne inteligence ustvarjajo številne priložnosti in koristi v najrazličnejših sektorjih in družbenih dejavnostih. Hkrati je SUVP pravni okvir, ki spodbuja odgovorne inovacije. Iz tega sledi, da obstaja splošni interes za izvedbo te presoje v obliki mnenja EOVP, da se zagotovi dosledna uporaba nekaterih določb SUVP glede modelov UI.
9. Alternativni pogoj iz člena 64(2) SUVP, se nanaša na zadeve „z učinkom v več kot eni državi članici“. EOVP opozarja, da je treba izraz „učinki“ razlagati *latu sensu* in zato ni omejen le na pravne učinke⁷. Ker se vse več modelov UI uči in uporablja v vse več organizacijah v EGP, ti vplivajo na veliko število posameznikov, na katere se nanašajo osebni podatki, po vsem EGP, od katerih so nekateri že izrazili pomisleke svojemu pristojnemu nadzornemu organu⁸. Zato EOVP meni, da zadeva, ki jo je izpostavil nadzorni organ prosilec, izpolnjuje tudi ta pogoj.
10. Prošnja za mnenje vključuje pisno utemeljitev o ozadju in razlogih za predložitev vprašanj odboru, vključno z ustreznim pravnim okvirom. Zato odbor meni, da je prošnja za mnenje utemeljena v skladu s členom 10(3) Poslovnika EOVP.

³ Prošnja za mnenje, str. 1.

⁴ Prav tam.

⁵ Prošnja za mnenje, str. 2.

⁶ Prošnja za mnenje, str. 1. Kot je navedeno v delovnem programu EOVP za obdobje 2024–2025, sprejetem 8. oktobra 2024, ki je na voljo na naslovu https://www.edpb.europa.eu/system/files/2024-10/edpb_work_programme_2024-2025_en.pdf, namerava EOVP izdati, , med drugim, smernice o anonimizaciji, psevdonimizaciji in strganju podatkov v okviru generativne umetne inteligence.

⁷ EOVP, Notranji dokument 3/2019 o notranjih smernicah glede člena 64(2) SUVP, sprejet 8. oktobra 2019, odstavek 15, na voljo na spletnem naslovu https://www.edpb.europa.eu/system/files/2022-07/internaledpb_document_201903_art64.2_en.pdf.

⁸ Prošnja za mnenje, str. 1-2.

11. V skladu s členom 64(3) SUVP⁹ EOVP ne izda mnenja, če je že izdal mnenje o zadevi. EOVP ni izdal mnenja o isti zadevi in še ni predložil odgovorov na vprašanja, ki izhajajo iz prošnje za mnenje.
12. Odbor zato meni, da je prošnja za mnenje dopustna in da bi bilo treba vprašanja, ki izhajajo iz nje, analizirati v mnenju, sprejetem v skladu s členom 64(2) SUVP.

2 Področje uporabe in ključni pojmi

2.1 Obseg mnenja

13. Odbor se strinja z nadzornim organom prosilcem, da razvoj in uporaba modelov UI z vidika varstva podatkov odpirata temeljna vprašanja o varstvu podatkov. Vprašanja se nanašajo zlasti na: (i) kdaj in kako se lahko model UI šteje za „anonimnega“ (vprašanje 1 v prošnji za mnenje); (ii) kako lahko upravljavci dokažejo ustreznost zakonitega interesa kot pravne podlage v fazi razvoja (vprašanje 2 v prošnji za mnenje) in uvajanja (vprašanje 3 v prošnji za mnenje) ter (iii) ali ima nezakonita obdelava osebnih podatkov v fazi razvoja posledice za zakonitost nadaljnje obdelave ali delovanja modela UI (vprašanje 4 v prošnji za mnenje).
14. EOVP opozarja, da so nadzorni organi odgovorni za spremljanje uporabe SUVP in bi morali prispevati k njeni dosledni uporabi v vsej Uniji¹⁰. Zato je v pristojnosti nadzornih organov, da proučijo posamezne modele UI in pri tem presodijo vsak primer posebej.
15. To mnenje zagotavlja okvir, na podlagi katerega lahko pristojni nadzorni organi presodijo posebne primere, pri katerih bi se pojavila (nekatera) vprašanja iz prošnje za mnenje. To mnenje ni izčrpno, temveč vsebuje splošne premisleke o razlagi zadevnih določb, ki jih morajo pristojni nadzorni organi v največji možni meri upoštevati pri uporabi svojih preiskovalnih pooblastil. Čeprav je to mnenje naslovljeno na pristojne nadzorne organe in se nanaša na njihove dejavnosti in pooblastila, ne posega v obveznosti upravljavcev in obdelovalcev na podlagi SUVP. Upravljavci so v skladu z načelom odgovornosti iz člena 5(2) SUVP zlasti odgovorni za vsa načela v zvezi s svojo obdelavo osebnih podatkov in so zmožni dokazati skladnost z njimi.
16. V nekaterih primerih je mogoče v mnenju navesti nekaj primerov, vendar glede na širok obseg vprašanj, vključenih v prošnjo za mnenje, in različne vrste modelov UI, ki so v njem zajeti, v tem mnenju ne bodo obravnavani vsi možni scenariji. Tehnologije, povezane z modeli UI, se hitro razvijajo, zato bi bilo treba ugotovitve EOVP v tem mnenju razlagati ob upoštevanju tega.
17. **V tem mnenju niso analizirane spodaj navedene določbe, ki imajo lahko še vedno pomembno vlogo pri presojanju zahtev za varstvo podatkov, ki se uporabljajo za modele UI:**
 - **obdelava posebnih vrst podatkov:** EOVP opozarja na prepoved iz člena 9(1) SUVP v zvezi z obdelavo posebnih vrst podatkov in omejene izjeme iz člena 9(2) SUVP¹¹. V zvezi s tem je Sodišče Evropske unije (v nadaljevanju besedila: „SEU“) dodatno pojasnilo, da „*kadar se niz podatkov, ki vsebuje občutljive in neobčutljive podatke, [...] zbere v svežnju, ne da bi bilo mogoče podatkovne*

⁹ Člen 64(3) SUVP in člen 10(4) poslovnika EOVP.

¹⁰ Člen 51(1) in člen 51(2) SUVP.

¹¹ Glejte tudi Poročilo EOVP o delu, ki ga je opravila projektna skupina za ChatGPT, sprejeto 23. maja 2024, odstavek 18: „V zvezi z obdelavo posebnih vrst osebnih podatkov se mora za zakonitost obdelave poleg tega uporabljati ena od izjem iz člena 9(2). Načeloma je lahko ena od teh izjem člen 9(2)(e) Splošne uredbe o varstvu podatkov. Vendar samo dejstvo, da so osebni podatki javno dostopni, ne pomeni, da je „posameznik, na katerega se nanašajo osebni podatki, te podatke očitno objavil“ [...]“.

*elemente med zbiranjem ločiti, je treba obdelavo tega niza podatkov šteti za prepovedano v smislu člena 9(1) Splošne uredbe o varstvu podatkov, če vsebuje vsaj en občutljiv podatkovni element in se ne uporablja nobeno odstopanje iz člena 9(2) navedene uredbe*¹². Poleg tega je SEU poudarilo tudi, da je „za namene uporabe izjeme iz člena 9(2)(e) Splošne uredbe o varstvu podatkov pomembno ugotoviti, ali je posameznik, na katerega se nanašajo osebni podatki, izrecno in z jasnim pritrdilnim dejanjem nameraval zadevne osebne podatke dati na voljo širši javnosti“¹³. Te vidike bi bilo treba upoštevati pri obdelavi osebnih podatkov v okviru modelov UI, ki vključujejo posebne vrste podatkov.

- **Avtomatizirano sprejemanje odločitev, vključno z oblikovanjem profilov:** Postopki obdelave, ki se izvajajo v okviru modelov UI, lahko spadajo na področje uporabe člena 22 SUVP, ki upravljavcem nalaga dodatne obveznosti in zagotavlja dodatne zaščitne ukrepe posameznikom, na katere se nanašajo osebni podatki. EOVP v zvezi s tem opozarja na svoje smernice o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679¹⁴.
- **Združljivost namenov:** Člen 6(4) SUVP za nekatere pravne podlage določa merila, ki jih upravljavec upošteva pri ugotavljanju, ali je obdelava za drug namen združljiva z namenom, za katerega se prvotno zbirajo osebni podatki. Ta določba je lahko pomembna v okviru razvoja in uporabe modelov UI, njeno uporabnost pa bi morale oceniti nadzorni organi.
- **Ocene učinka v zvezi z varstvom podatkov** (člen 35 SUVP): Ocene učinka v zvezi z varstvom podatkov so pomemben element odgovornosti, kadar je verjetno, da bo obdelava v okviru modelov UI povzročila veliko tveganje za pravice in svoboščine fizičnih oseb¹⁵.
- **Načelo vgrajenega varstva podatkov** (člen 25(1) SUVP): Vgrajeno varstvo podatkov je bistveno varovalo, ki ga morajo nadzorni organi oceniti v okviru razvoja in uvajanja modela UI.

2.2 Ključni pojmi

18. EOVP želi uvodoma pojasniti izrazje in pojme, ki jih uporablja v tem mnenju, in sicer samo za namene tega mnenja:

- „**podatki prve osebe**“ se nanašajo na osebne podatke, ki jih je upravljavec zbral od posameznikov, na katere se nanašajo osebni podatki;
- „**podatki tretje osebe**“ se nanašajo na osebne podatke, ki jih upravljavci niso pridobili od posameznikov, na katere se nanašajo osebni podatki, temveč so jih zbrali ali prejeli od tretje osebe, na primer od posrednika podatkov ali s spletnim strganjem;

¹² Sodba SEU z dne 4. julija 2023 v zadevi C-252/21, *Meta v Bundeskartellamt* (ECLI:EU:C:2023:537), točka 89.

¹³ Sodba SEU z dne 4. julija 2023 v zadevi C-252/21, *Meta v Bundeskartellamt* (ECLI:EU:C:2023:537), točka 77.

¹⁴ Smernice delovne skupine iz člena 29 o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679, kakor so bile nazadnje spremenjene in sprejete 6. februarja 2018, ki jih je EOVP potrdil 25. maja 2018. Glejte tudi sodbo SEU z dne 7. decembra 2023 v zadevi C-634/21, *SCHUFA Holding in drugi* (ECLI:EU:C:2023:957).

¹⁵ Smernice delovne skupine iz člena 29 o oceni učinka v zvezi z varstvom podatkov in ugotavljanju, ali obdelava „verjetno povzroči veliko tveganje“ za namene Uredbe 2016/679, revidirane in sprejete 4. oktobra 2017, ki jih je EOVP potrdil 25. maja 2018.

- „**spletno strganje**“ je pogosto uporabljena tehnika zbiranja informacij iz javno dostopnih spletnih virov. Informacije, pridobljene na primer iz storitev, kot so novice, družbeni mediji, forumske razprave in osebne spletne strani, lahko vsebujejo osebne podatke.
- Prošnja za mnenje se nanaša na „**življenjski cikel**“ **modelov UI** ter na različne faze, med drugim v zvezi z „ustvarjanjem“, „razvojem“, „učenjem“, „posodobitvijo“, „izpopolnjevanjem“, „delovanjem“ ali „naknadnim učenjem“ modelov UI. EOVP priznava, da so v posameznih okoliščinah tovrstne faze lahko del razvoja in uvajanja modelov UI ter lahko vključujejo obdelavo osebnih podatkov za različne namene obdelave. Kljub temu EOVP meni, da je za namene tega mnenja pomembno poenotiti kategorizacijo faz, ki se bodo verjetno pojavile. EOVP se zato za namene tega mnenja sklicuje na „**fazo razvoja**“ in „**fazo uvajanja**“. Razvoj modela UI zajema vse faze pred kakršno koli uvedbo modela UI in med drugim vključuje razvoj kod, zbiranje osebnih podatkov za učenje, predhodno obdelavo osebnih podatkov za učenje in učenje iz osebnih podatkov. Uvedba modela UI zajema vse faze, povezane z njegovo uporabo, in lahko vključuje vse operacije, izvedene po fazi razvoja. EOVP se še naprej zaveda raznolikosti primerov uporabe in njihovih morebitnih posledic v smislu obdelave osebnih podatkov, zato bi morali nadzorni organi proučiti, ali so ugotovitve iz tega mnenja pomembne za obdelavo, ki jo ocenjujejo.
- EOVP poudarja tudi, da se izraz „**učenje**“ po potrebi nanaša na del faze razvoja, v kateri se modeli UI učijo iz podatkov, da lahko opravijo predvideno nalogo (kot je pojasnjeno v naslednjem poglavju tega mnenja).
- Pojem in področje uporabe **modelov UI**, kot ju EOVP razume za namene tega mnenja, sta podrobneje opredeljena v naslednjem posebnem poglavju.

2.3 Modeli UI v okviru mnenja

19. Akt EU o umetni inteligenci (v nadaljevanju besedila: „**Akt o UI**“)¹⁶ opredeljuje „sistem UI“ kot „sistem temelječ na napravah, ki je zasnovan za delovanje z različnimi stopnjami avtonomije in lahko po uvedbi izkaže prilagodljivost ter za eksplicitne ali implicitne cilje iz prejetih vhodnih podatkov sklepa, kako ustvariti izhodne podatke, kot so napovedi, vsebine, priporočila ali odločitve, ki lahko vplivajo na fizična ali virtualna okolja“¹⁷. V uvodni izjavi (12) Akta o UI je pojem „sistem UI“ dodatno pojasnjen. V skladu s tem je ključna značilnost sistemov UI njihova sposobnost sklepanja. Tehnike, ki omogočajo sklepanje pri gradnji sistema UI, vključujejo strojno učenje ter pristope, ki temeljijo na logiki in znanju.
20. Po drugi strani so „modeli UI“ v Aktu o UI le posredno opredeljeni: „Čeprav so modeli UI bistvene komponente sistemov UI, sami po sebi niso sistemi UI. Da bi modeli UI postali sistemi UI, jim je treba dodati dodatne komponente, kot je na primer uporabniški vmesnik. Modeli UI so običajno vključeni v sisteme UI in so njihov sestavni del“¹⁸.
21. EOVP razume, da je opredelitev modela UI, predlagana v prošnji za mnenje, ožja od opredelitve iz Akta o UI, saj se v njej izraz „model UI“ nanaša na „in zajema izdelek, ki je rezultat mehanizmov učenja, ki se uporabljajo z nizom podatkov za učenje, v okviru umetne inteligence, strojnega učenja, globokega

¹⁶ Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci).

¹⁷ Glejte člen 3(1) Akta o umetni inteligenci.

¹⁸Uvodna izjava 97 Akta o UI.

učenja ali drugih povezanih okoliščin obdelave“ in nadalje določa, da „Izraz se uporablja za modele UI, ki so namenjeni in za tiste, ki niso namenjeni nadaljnjemu učenju, izpopolnjevanju in/ali razvoju.“¹⁹

22. Na podlagi tega je EOVP sprejel to mnenje ob razumevanju, da se bo sistem UI zanašal na model UI, da bi opravil svoj predvideni cilj z vključitvijo modela v širši okvir (npr. sistem UI za storitve za stranke lahko uporabi model UI, ki se je učil iz podatkov o preteklih pogovorih, da zagotovi odgovore na poizvedbe uporabnikov).
23. Poleg tega so modeli UI (ali „**modeli**“), ki so pomembni za to mnenje, tisti, ki so bili razviti z učenjem. Tovrstno učenje je del faze razvoja, kjer se modeli učijo iz podatkov za opravljanje predvidene naloge. Zato je za učenje potreben nabor podatkov, iz katerega bo model prepoznal in se „naučil“ vzorce. V teh primerih bo model uporabil različne tehnike za izgradnjo slike znanja, pridobljenega iz nabora podatkov, iz katerih se je učil. To zlasti velja za strojno učenje.
24. V praksi je vsak model UI algoritem, katerega delovanje je določeno z nizom elementov. Modeli globokega učenja so na primer pogosto v obliki nevronskega omrežja z več plastmi, sestavljenih iz vozlišč, povezanih z robovi, ki imajo uteži, ki se med učenjem prilagodijo, da bi se naučili razmerij med vhodnimi vrednostmi in izhodnimi podatki. Značilnosti enostavnega modela poglobljenega učenja bi bile: (i) vrsta in velikost vsake plasti, (ii) teža, pripisana vsakemu robu (včasih imenovano „parametri“), (iii) aktivacijske funkcije²⁰ med plastmi in po možnosti (iv) druge operacije, ki se lahko zgodijo med plastmi. Na primer, pri učenju preprostega modela globokega učenja za razvrščanje slik bodo vhodne vrednosti („**slikovne pike**“) povezane z izhodnimi podatki, uteži pa se lahko prilagodijo tako, da bodo večino časa dale prave izhodne podatke.
25. Drugi primeri modelov globokega učenja so veliki jezikovni modeli in generativna umetna inteligenca, ki se uporabljajo npr. za generiranje človeku podobne vsebine in ustvarjanje novih podatkov.
26. **Na podlagi zgornjih premislekov področje uporabe tega mnenja v skladu s prošnjo za mnenje zajema le podskupino modelov UI, ki so rezultat učenja s pomočjo osebnih podatkov.**

3 Ustreznost prošnje za mnenje

3.1 O naravi modelov umetne inteligence v zvezi z opredelitvijo osebnih podatkov

27. V členu 4(1) SUVP so osebni podatki opredeljeni kot „*vse informacije, ki se nanašajo na določeno ali določljivo fizično osebo*“(tj. posameznika, na katerega se nanašajo osebni podatki). Poleg tega uvodna izjava 26 SUVP določa, da se načela varstva podatkov ne bi smela uporabljati za anonimizirane informacije, in sicer informacije, ki se ne nanašajo na določenega ali določljivega posameznika, ob upoštevanju „*vseh sredstev, za katera se razumno pričakuje, da jih bo upravljavec ali druga oseba uporabila*“. To med drugim pomeni: (i) podatki, ki niso bili nikoli povezani z določenim ali določljivim posameznikom, in (ii) osebni podatki, ki so bili anonimizirani tako, da posameznik, na katerega se nanašajo osebni podatki, ni ali ni več določljiv.

¹⁹ Prošnja za mnenje, str. 3.

²⁰ Tj. funkcije, ki na podlagi vhodnih vrednosti in uteži izračunajo izhodni podatek nevronskega vozlišča, ki bo nato poslan na naslednjo raven nevronskega omrežja.

28. V skladu s tem je mogoče na vprašanje 1²¹ iz prošnje za mnenje odgovoriti z analizo, ali bi lahko model UI, ki je rezultat učenja, ki vključuje obdelavo osebnih podatkov, v vseh primerih šteli za anonimnega. Glede na formulacijo vprašanja se bo EOVP v tem oddelku skliceval na postopek „učenja“ modela UI.
29. EOVP želi predvsem zagotoviti naslednje splošne ugotovitve. Modeli UI, ne glede na to, ali se učijo s pomočjo osebnih podatkov ali ne, so običajno zasnovani za napovedovanje ali oblikovanje sklepov, kar pomeni, da so zasnovani tako, da sklepajo. Poleg tega so tovrstni modeli pogosto zasnovani za sklepanje o posameznikih, ki se razlikujejo od tistih, katerih osebni podatki so bili uporabljeni za učenje modela UI. Vendar so nekateri modeli UI posebej zasnovani tako, da zagotavljajo osebne podatke o posameznikih, katerih osebni podatki so bili uporabljeni za njihovo učenje, ali pa so ti podatki na kakršen koli način na voljo. V teh primerih bodo takšni modeli UI neločljivo (in običajno nujno) vključevali informacije, ki se nanašajo na določeno ali določljivo fizično osebo, zato bodo vključevali obdelavo osebnih podatkov. Zato teh vrst modelov UI ni mogoče obravnavati kot anonimnih. To bi na primer veljalo za (i) generativni model, ki bi bil izpopolnjen s glasovnimi posnetki posameznika, da bi posnemal njegov glas, ali (ii) kateri koli model, ki bi bil zasnovan tako, da bi na zahtevo po informacijah o določeni osebi odgovoril z osebnimi podatki, iz katerih se je učil.
30. Na podlagi zgornjih premislekov se EOVP pri odgovoru na prvo vprašanje v prošnji za mnenje osredotoča na primer modelov UI, ki niso zasnovani tako, da bi zagotavljali osebne podatke, povezane s podatki, iz katerih so se učili.
31. EOVP meni, da lahko informacije iz nabora podatkov za učenje, vključno z osebnimi podatki, ostanejo „vgrajene“ v parametre modela, in sicer predstavljene z matematičnimi objekti, tudi če model UI ni bil namerno zasnovan tako, da bi iz podatkov za učenje pridobil informacije v zvezi z določeno ali določljivo fizično osebo. Lahko se razlikujejo od prvotnih podatkovnih točk učenja, vendar lahko še vedno ohranijo prvotne informacije iz teh podatkov, ki so na koncu lahko izpisljivi ali drugače neposredno ali posredno pridobljeni iz modela. Kadar je mogoče informacije v zvezi z določenimi ali določljivimi posamezniki, katerih osebni podatki so bili uporabljeni za učenje modela, pridobiti iz modela UI s sredstvi, za katera je razumno verjetno, da bodo uporabljena, se lahko sklepa, da tak model ni anonimen.
32. V zvezi s tem je v prošnji za mnenje navedeno, da „Obstoječe raziskovalne publikacije opozarjajo na nekatere potencialne ranljivosti, ki lahko obstajajo v modelih UI in zaradi katerih se lahko obdelujejo osebni podatki,²² ter na obdelavo osebnih podatkov, ki se lahko izvaja, ko se modeli uporabijo za uporabo z drugimi podatki, bodisi prek vmesnikov za programiranje aplikacij bodisi prek vmesnikov za pisanje pozivov „prompt““²³.
33. V istem duhu so raziskave na področju pridobivanja podatkov za učenje še posebej dinamične²⁴. Kaže, da je v nekaterih primerih mogoče uporabiti sredstva, za katera je razumno verjetno, da bodo osebne

²¹ „Ali se šteje, da končni model UI, ki se je učil z uporabo osebnih podatkov, v nobenem primeru ne ustreza opredelitvi osebnih podatkov (kot je določena v členu 4(1) SUVP)?“

²² Kot so napadi na sklepanje o članstvu ([OWASP](#)) in napadi na model z obratnim inženiringom ([OWASP](#) in [Veale et al.](#), 2018).

²³ Prošnja za mnenje, str. 1-2.

²⁴ V zvezi s tem glejte na primer: (i) Veale M., Binns R., Edwards L., 2018, *Algorithms that remember: model inversion attacks and data protection law*. Phil. Trans. R. Soc. A 376: 20180083, na voljo na <http://dx.doi.org/10.1098/rsta.2018.0083>; (ii) Brown H., Lee K., Mireshghallah F., Shokri R. in Tramèr F., *What Does it Mean for a Language Model to Preserve Privacy?*, 2022, ACM Digital Library, FAccT '22, 20 junij 2022, Seul, Republika Koreja, na voljo na <https://dl.acm.org/doi/abs/10.1145/3531146.3534642>; (iii) Vassilev A., Oprea A., Fordyce A., Anderson H., *Adversarial Machine Learning A Taxonomy and Terminology of Attacks and*

podatke pridobila iz nekaterih modelov UI, ali preprosto nenamerno pridobila osebne podatke z interakcijami z modelom UI (na primer kot del sistema UI). Stalna raziskovalna prizadevanja na tem področju bodo pripomogla k nadaljnji oceni preostalih tveganj regurgitacije²⁵ in izluščenja osebnih podatkov v vsakem danem primeru.

34. **Na podlagi zgornjih premislekov EOVP meni, da modelov UI, za učenje katerih so bili uporabljeni osebni podatki, ni mogoče v vseh primerih šteti za anonimne. Namesto tega bi bilo treba določitev, ali je model UI anonimen, na podlagi posebnih meril presoditi za vsak primer posebej.**

3.2 O okoliščinah, v katerih bi se lahko modeli UI šteli za anonimne, in s tem povezan prikaz

35. V zvezi z vprašanjem 1 iz prošnje za mnenje²⁶ naj EOVP pojasni, v kakšnih okoliščinah se lahko model UI, ki se je učil z uporabo osebnih podatkov, šteje za anonimnega. V zvezi z vprašanjem 1(i)(a) prošnje za mnenje²⁷ naj EOVP pojasni, katere dokaze in/ali dokumentacijo bi morali nadzorni organi upoštevati pri presoji, ali je model UI anonimen.

3.2.1 Splošni premislek o anonimizaciji v obravnavanem kontekstu

36. Uporaba izraza „katere koli informacije“ v opredelitvi pojma „osebni podatki“ v členu 4(1) SUVP izraža cilj, da se temu pojmu dodeli široko področje uporabe, ki zajema vse vrste informacij, pod pogojem, da se „nanašajo“ na posameznika, na katerega se nanašajo osebni podatki, ki je določen ali ga je mogoče neposredno ali posredno določiti.
37. Informacije se lahko nanašajo na fizično osebo, tudi če so tehnično organizirane ali kodirane (na primer samo v strojno berljivem formatu, lastniškem ali odprtem) na način, zaradi katerega povezava s to fizično osebo ni takoj očitna. V takih primerih se lahko za enostavno opredelitev, identifikacijo in izluščenje specifičnih podatkov uporabljajo programske aplikacije. To še zlasti velja za modele UI, pri katerih parametri predstavljajo statistične povezave med podatki za učenje in pri katerih je mogoče pridobiti točne ali netočne (ker so statistično povzeti) osebne podatke, bodisi neposredno iz povezav med podatki, vključenimi v model, bodisi s poizvedbo v tem modelu.
38. Ker modeli UI običajno ne vsebujejo zapisov, ki bi jih bilo mogoče neposredno izolirati ali povezati, temveč parametre, ki predstavljajo verjetnostne povezave med podatki, vsebovanimi v modelu, je mogoče iz modela izpeljati²⁸ informacije v realističnih scenarijih, kot je sklepanje o članstvu. Da bi se

Mitigations, januar 2024, National Institute of Standards and Technology, dostopno na <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf>; (iv) Carlini N., Tramèr F., Wallace E., Jagielski M., Herbert-Voss A., Lee K., Roberts A., Brown T., Song D., Erlingsson U., Oprea A., Raffel C., *Extracting Training Data from Large Language Models*, arXiv:2012.07805v2 [cs.CR] 15. junij 2021, dostopno na <https://arxiv.org/pdf/2012.07805>; (v) Fredrikson M., Jha S., Ristenpart T., *Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures*, ACM Digital Library, 12. oktober 2015, dostopno na <https://dl.acm.org/doi/abs/10.1145/2810103.2813677>; (vi) Zhang Y., Jia R., Pei H., Wang W., Li B., Song D., *The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks*, arXiv:1911.07135v2 [cs.LG] 18. april 2020, na voljo na <https://arxiv.org/pdf/1911.07135>.

²⁵ Pri sistemu UI, ki temelji na generativni umetni inteligenci, regurgitacija ustreza okoliščinam, v katerih bi izhodni podatki neposredno ustrezali podatkom, uporabljenim za učenje.

²⁶ „Kakšne so okoliščine, v katerih bi se to lahko zgodilo?“

²⁷ „Če je odgovor pritrdilen, kako je mogoče dokazati ukrepe, ki so bili sprejeti za zagotovitev, da model UI ne obdeluje osebnih podatkov?“

²⁸ (i) Carlini N., Chien S., Nasr M., Song S., Terzis A., Tramèr F., *Membership Inference Attacks From First Principles*, arXiv:2112.03570, na voljo na <https://arxiv.org/abs/2112.03570>;

torej nadzorni organ z upravljavcem strinjal, da se lahko določen model UI šteje za anonimnega, bi moral preveriti vsaj, ali je prejel zadostne dokaze, da z razumnimi sredstvi: (i) osebnih podatkov, povezanih s podatki, uporabljenimi za učenje, iz modela ni mogoče izluščiti²⁹; in (ii) se noben rezultat, pridobljen pri poizvedovanju v modelu, ne nanaša na posameznike, katerih osebni podatki so bili uporabljeni za učenje modela.

39. Nadzorni organi bi morali pri presoji, ali so ti pogoji izpolnjeni, upoštevati tri elemente.
40. Najprej bi morali upoštevati elemente, opredeljene v najnovejših mnenjih delovne skupine iz člena 29 in/ali smernicah EOVP o tej zadevi. Kar zadeva anonimizacijo na datum tega mnenja, bi morali nadzorni organi upoštevati elemente, vključene v mnenju delovne skupine iz člena 29 št. 05/2014 o anonimizacijskih tehnikah, v katerem je navedeno, da se lahko podatki štejejo za anonimne, če ni mogoče izločiti, povezati in izpeljati informacij iz domnevno anonimnega nabora podatkov³⁰. Prav tako navaja: „Če predlog ne izpolnjuje enega od meril, bi bilo treba opraviti temeljito oceno identifikacijskih tveganj“³¹. **Glede na zgoraj navedeno verjetnost pridobivanja in sklepanja EOVP meni, da je zelo verjetno, da bodo v zvezi z modeli UI nujne tako temeljite ocene identifikacijskih tveganj.**
41. Drugič, to oceno bi bilo treba izvesti ob upoštevanju „vseh sredstev, za katera se razumno pričakuje,“ da jih bo upravitelj ali druga oseba uporabila za identifikacijo posameznikov³², določitev teh sredstev pa bi morala temeljiti na objektivnih dejavnikih, kot je pojasnjeno v uvodni izjavi 26 SUVP, ki lahko vključujejo:
- a. značilnosti samih podatkov za učenje, modela UI in postopka učenja³³;

(ii) Crețu A.M., Guépin F., and De Montjoye Y.A., *Correlation inference attacks against machine learning models*. Sci. Adv.10, ead9260(2024). DOI:10.1126/sciadv.ad9260 na voljo na <https://www.science.org/doi/10.1126/sciadv.ad9260>;

(iii) Dana L., Pydi M. S., Chevalere Y., *Memorization in Attention-only Transformers* arXiv:2411.10115v1 [cs.AI] 15. november 2024, na voljo na: <https://arxiv.org/abs/2411.10115>;

(iv) Gehrke M., Liebenow J., Mohammadi E. in Braun T. et al. *Lifting in Support of Privacy-Preserving Probabilistic Inference*. Künstl Intell, 13. junij 2024, na voljo na: <https://doi.org/10.1007/s13218-024-00851-y>;

(v) Hu H., *Membership Inference Attacks and Defenses on Machine Learning Models Literature*, na voljo na: <https://github.com/HongshengHu/membership-inference-machine-learning-literature>;

(vi) Nasr M., Carlini N., Hayase J., Jagielski M., Cooper A. F., Ippolito D., Choquette-Choo C. A., Wallace E., Tramèr F., and Lee K., *Scalable Extraction of Training Data from (Production) Language Models*, arXiv:2311.17035 28. november 2023, na voljo na: <https://arxiv.org/abs/2311.17035>;

(vii) Shokri R., Stronati M., Song C., Shmatikov V., *Membership Inference Attacks against Machine Learning Models* arXiv:1610.05820v2 [cs.CR], 31 marec 2017, na voljo na <https://arxiv.org/abs/1610.05820>;

(viii) Staab R., Vero M., Mislav Balunović, Martin Vechev, 2024, *Beyond Memorization: Violating Privacy Via Inference with Large Language Models*, arXiv:2310.07298v2, 6. maj 2024, na voljo na <https://arxiv.org/abs/2310.07298>;

(ix) Wu F., Cui L., Yao S., Yu S., *Inference Attacks in Machine Learning as a Service: A Taxonomy, Review, and Promising Directions* arXiv:2406.02027v1 [cs.LG], 27. junij 2024, na voljo na <https://arxiv.org/abs/2406.02027v1>;

(x) Zhang J., Das D., Kamath G., Tramèr F., *Membership Inference Attacks Can't Prove that a Model Was Trained On Your Data* arXiv:2409.19798v1, [cs.LG], 29. september 2024, na voljo na <https://arxiv.org/abs/2409.19798>;

(xi) Zhou Z., Xiang J., Chen C. in Su S., *Quantifying and Analyzing Entity-Level Memorization in Large Language Models*, arXiv:2308.15727v2 [cs.CL] 5. november 2023, na voljo na <https://arxiv.org/abs/2308.15727>.

²⁹ Pridobivanje vključuje zlasti primer, v katerem se osebni podatki izpeljejo iz samega modela UI z malo ali brez uporabe vmesnikov za poizvedovanje.

³⁰ Mnenje delovne skupine iz člena 29 št. 5/2014, stran 24.

³¹ Mnenje delovne skupine iz člena 29 št. 5/2014, stran 24.

³² Sodba SEU z dne 19. oktobra 2016 v zadevi C-582/14, *Breyer proti Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), točka 43.

³³ To vključuje značilnosti, kot so edinstvenost zapisov v podatkih za učenje, natančnost informacij, združevanje, randomizacija in zlasti, kako te vplivajo na občutljivost za identifikacijo.

- b. kontekst, v katerem je model UI objavljen in/ali obdelan³⁴;
 - c. dodatne informacije, ki bi omogočale identifikacijo in so lahko na voljo zadevnim osebam;
 - d. stroške in čas, ki bi ga oseba potrebovala za pridobitev takih dodatnih informacij (če ji te še niso na voljo)³⁵; in
 - e. tehnologijo, ki je na voljo v času obdelave, ter tehnološki razvoj³⁶.
42. Tretjič, nadzorni organi bi morali proučiti, ali so upravljavci ocenili tveganje identifikacije s strani upravljavca in glede na različne vrste „*drugih oseb*“, vključno z nenamernimi tretjimi osebami, ki dostopajo do modela UI, tudi ob upoštevanju, ali se lahko upravičeno šteje, da lahko pridobijo dostop do zadevnih podatkov ali jih obdelujejo.
43. **Skratka, EOVP meni, da bi morala biti za to, da se model UI z uporabo razumnih sredstev šteje za anonimnega, tako (i) verjetnost neposrednega (tudi verjetnostnega) pridobivanja osebnih podatkov o posameznikih, katerih osebni podatki so bili uporabljeni za učenje modela, kot tudi (ii) verjetnost namernega ali nenamernega pridobivanja takih osebnih podatkov iz poizvedb, zanemarljiva³⁷ za katerega koli posameznika, na katerega se nanašajo osebni podatki. Nadzorni organi bi morali privzeto upoštevati, da bo pri modelih UI verjetno potrebna temeljita ocena verjetnosti identifikacije, da bi lahko prišli do zaključka o njihovi morebitni anonimni naravi. To verjetnost je treba oceniti ob upoštevanju „vseh sredstev, za katera je razumno verjetno,“ da jih bo upravljavec ali druga oseba uporabila, in upoštevati tudi nenamerno (ponovno) uporabo ali razkritje modela.**

3.2.2 Elementi za oceno preostale verjetnosti identifikacije

44. Čeprav se lahko ukrepi sprejmejo tako v fazi razvoja kot v fazi uvajanja, da bi se zmanjšala verjetnost pridobitve osebnih podatkov iz modela UI, bi bilo treba pri presoji njegove anonimnosti upoštevati tudi neposredni dostop do njega.
45. Poleg tega bi morali nadzorni organi za vsak primer posebej presoditi, ali so ukrepi, ki jih upravljavec izvaja za zagotovitev in dokazovanje anonimnosti modela UI, ustrezni in učinkoviti.
46. Zlasti lahko končna ocena nadzornega organa razlikuje med javno dostopnim modelom UI, ki je dostopen neznanemu številu ljudi z neznanim naborom metod za poskušanje pridobivanja osebnih podatkov, ter notranjim modelom UI, ki je dostopen samo zaposlenim. Čeprav bi morali nadzorni organi v obeh primerih preveriti, ali so upravljavci izpolnili svojo obveznost odgovornosti v skladu s členoma 5(2) in 24 SUVP, lahko „sredstva, za katera se razumno pričakuje, da jih bodo uporabile“ druge osebe, vplivajo na obseg in naravo možnih scenarijev, ki jih je treba upoštevati. Zato lahko nadzorni organi, odvisno od okvira razvoja in uvedbe modela, upoštevajo različne ravni preskušanja in odpornosti proti napadom.
47. V zvezi s tem EOVP v nadaljevanju navaja nepredpisujoč in neizčrpen seznam možnih elementov, ki jih lahko nadzorni organi upoštevajo pri presojanju trditve upravljavca o anonimnosti. Možni so tudi drugi pristopi, če zagotavljajo enakovredno raven varstva, zlasti ob upoštevanju najnovejšega tehnološkega razvoja.

³⁴To vključuje kontekstualne elemente, kot so omejitev dostopa samo na nekatere osebe in pravna varovala.

³⁵Sodba SEU z dne 7. marca 2024 v zadevi C-479/22 P, *OC proti Evropski komisiji* (ECLI:EU:C:2024:215), točka 50.

³⁶Sodba SEU z dne 7. marca 2024 v zadevi C-479/22 P, *OC proti Evropski komisiji* (ECLI:EU:C:2024:215), točka 50.

³⁷ Sodba SEU z dne 19. oktobra 2016 v zadevi C-582/14, *Breyer proti Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), točka 46, in sodba SEU z dne 7. marca 2024 v zadevi C-479/22 P, *OC proti Evropski komisiji* (ECLI:EU:C:2024:215), točka 51.

48. Prisotnost ali odsotnost spodaj navedenih elementov ni odločilno merilo za ocenjevanje anonimnosti modela UI.

3.2.2.1 Oblikovanje modela umetne inteligence

49. V zvezi z zasnovo modelov UI bi morali nadzorni organi oceniti pristope, ki jih upravljavci uporabljajo v fazi razvoja. V zvezi s tem bi bilo treba proučiti uporabo in učinkovitost štirih ključnih področij (opredeljenih spodaj).

Izbira virov

50. Prvo področje ocenjevanja vključuje preverjanje izbire virov, uporabljenih za učenje modela UI. To vključuje oceno vseh ukrepov, ki so jih izvedli nadzorni organi, da bi se izognili zbiranju osebnih podatkov ali ga omejili, med drugim (i) ustreznost meril za izbor, (ii) ustreznost in primernost izbranih virov glede na predvideni namen(-e) in (iii) ali so bili izključeni neustrezni viri.

Priprava in čim manjši obseg podatkov

51. Drugo področje ocenjevanja se nanaša na pripravo podatkov za fazo učenja. Nadzorni organi bi morali proučiti zlasti: (i) ali je bila upoštevana uporaba anonimnih in/ali osebnih podatkov, ki so bili psevdonimizirani, in (ii) če je bilo odločeno, da se takšni ukrepi ne uporabijo, razloge za to odločitev, ob upoštevanju predvidenega namena; (iii) strategije in tehnike za zmanjšanje količine podatkov, uporabljene za omejitev obsega osebnih podatkov, vključenih v postopek učenja, in (iv) vse postopke filtriranja podatkov, izvedene pred učenjem modela, namenjene odstranitvi nerelevantnih osebnih podatkov.

Metodološke izbire v zvezi z učenjem

52. Tretje področje ocenjevanja se nanaša na izbiro zanesljivih metod pri razvoju modelov UI. Nadzorni organi bi morali oceniti metodološke izbire, ki lahko znatno zmanjšajo ali odpravijo določljivost, med drugim tudi: (i) ali ta metodologija uporablja metode regularizacije za izboljšanje posploševanja modelov in zmanjšanje pretiranega prilagajanja; in, kar je bistveno, (ii) ali je upravljavec uporabil ustrezne in učinkovite tehnike ohranjanja zasebnosti (npr. diferencialna zasebnost).

Ukrepi v zvezi z izhodnimi podatki modela

53. Zadnje področje ocenjevanja se nanaša na vse metode ali ukrepe, dodane samemu modelu UI, ki morda ne vplivajo na tveganje neposrednega pridobivanja osebnih podatkov za model s strani oseb, ki do njega dostopajo neposredno, lahko pa zmanjšajo verjetnost pridobitve osebnih podatkov, povezanih s podatki za učenje, iz poizvedb.

3.2.2.2 Analiza modela umetne inteligence

54. Da bi nadzorni organi ocenili zanesljivost oblikovanega modela UI v zvezi z anonimizacijo, je prvi korak zagotoviti, da je bila zasnova razvita, kot je bilo načrtovano, in da je predmet učinkovitega upravljanja inženiringa. Nadzorni organi bi morali oceniti, ali so upravljavci opravili kakršno koli revizijo na podlagi dokumentov (notranjo ali zunanjo), ki vključuje oceno izbranih ukrepov in njihovega učinka za omejitev verjetnosti identifikacije. To bi lahko vključevalo analizo poročil o pregledih kod in teoretično analizo, ki bi dokumentirala ustreznost izbranih ukrepov za zmanjšanje verjetnosti ponovne identifikacije zadevnega modela.

3.2.2.3 Testiranje modelov umetne inteligence in odpornost na napade

55. Nazadnje, nadzorni organi bi morali upoštevati obseg, pogostost, količino in kakovost testiranj, ki jih je upravljavec opravil na modelu. Nadzorni organi bi morali zlasti upoštevati, da je uspešno testiranje, ki zajema splošno znane in najsodobnejše napade, lahko le dokaz za odpornost na te napade. Do datuma izdaje tega mnenja bi to lahko med drugim vključevalo strukturirano testiranje proti: (i) sklepanju o

lastnostih in članstvu; (ii) uhajanju podatkov; (iii) regurgitaciji podatkov, na katerih se je model učil; (iv) inverziji modela ali (v) napadom z rekonstrukcijo podatkov.

3.2.2.4 Dokumentacija

56. Členi 5, 24, 25 in 30 SUVP ter člen 35 SUVP v primerih verjetnega visokega tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, od upravljavcev zahtevajo, da ustrezno dokumentirajo svoje postopke obdelave. To velja tudi za vsako obdelavo, ki bi vključevala učenje modela UI, tudi če je cilj obdelave anonimizacija. Nadzorni organi bi morali upoštevati tovrstno dokumentacijo in vsako redno oceno posledičnih tveganj za obdelavo, ki jo izvajajo upravljavci, saj so to temeljni ukrepi za dokazovanje, da se osebni podatki ne obdelujejo.
57. **EOVP meni, da bi morali nadzorni organi upoštevati dokumentacijo, kadar koli je treba presoditi trditev o anonimnosti v zvezi z določenim modelom UI. Ugotavlja tudi, da če nadzorni organ po presoji trditve o anonimnosti, tudi glede na dokumentacijo, ne more potrditi, da so bili sprejeti učinkoviti ukrepi za anonimizacijo modela UI, bi lahko nadzorni organ menil, da upravljavec ni izpolnil svojih obveznosti glede odgovornosti iz člena 5(2) SUVP. Zato bi bilo treba upoštevati tudi skladnost z drugimi določbami te uredbe.**
58. V idealnem primeru bi morali nadzorni organi preveriti, ali dokumentacija upravljavca vključuje:
- vse informacije, povezane z oceno učinka v zvezi z varstvom podatkov, vključno z vsemi ocenami in odločitvami, na podlagi katerih je bilo ugotovljeno, da ta ocena ni potrebna;
 - kakršen koli nasvet ali povratne informacije, ki jih je dala pooblaščenca oseba za varstvo podatkov (kadar je bila imenovana ali bi morala biti imenovana);
 - informacije o tehničnih in organizacijskih ukrepih, sprejetih pri oblikovanju modela UI za zmanjšanje verjetnosti identifikacije, vključno z modelom groženj in ocenami tveganja, na katerih temeljijo ti ukrepi. To bi moralo vključevati posebne ukrepe za vsak vir naborov podatkov, uporabljenih za učenje, vključno z ustreznimi naslovi URL vira in opisi sprejetih ukrepov (ali ukrepov, ki so jih že sprejeli tretji ponudniki naborov podatkov);
 - tehnične in organizacijske ukrepe, sprejete v vseh fazah v celotnem življenjskem ciklu modela, ki so ali prispevali k pomanjkanju osebnih podatkov v modelu ali preverili njihovo pomanjkanje;
 - dokumentacijo, ki dokazuje teoretično odpornost modela UI proti tehnikam ponovne identifikacije, ter kontrole, namenjene omejevanju ali ocenjevanju uspešnosti in vpliva glavnih napadov (ponovna identifikacija, napadi na sklepanje o članstvu, uhajanje podatkov itd.). Vključujejo lahko zlasti: (i) razmerje med količino podatkov za učenje in številom parametrov v modelu, vključno z analizo njegovega vpliva na model³⁸; (ii) metrike verjetnosti ponovne identifikacije na podlagi trenutnega najnovejšega tehnološkega razvoja; (iii) poročila o tem, kako je bil model testiran (kdo, kdaj, kako in v kakšnem obsegu), in (iv) rezultate testov;

³⁸ Ricciato F., *A Cautionary Reflection on (Pseudo-)Synthetic Data from Deep Learning on Personal Data*, konferenca Privacy in Statistical Databases (PSD 2024), Antibes, Francija, september 2024, diapozitivi na voljo na https://cros.ec.europa.eu/system/files/2024-10/20240926_PSD2024_Ricciato_v6_1.pdf in Belkin M., Hsu D., Ma S., in Mandal S. (2019), *Reconciling modern machine-learning practice and the classical bias–variance trade-off*. Proceedings of the National Academy of Sciences (Postopki nacionalne akademije znanosti), 24. julij 2019, 116(32) 15849-15854, na voljo na: <https://www.pnas.org/doi/10.1073/pnas.1903070116>

- f. dokumentacijo, predloženo upravljavcem oziroma upravljavcem, ki uporabljajo model, in/ali posameznikom, na katere se nanašajo osebni podatki, zlasti dokumentacijo v zvezi z ukrepi, sprejetimi za zmanjšanje verjetnosti identifikacije in glede morebitnih preostalih tveganj.

3.3 O primernosti zakonitega interesa kot pravne podlage za obdelavo osebnih podatkov v okviru razvoja in uvajanja modelov umetne inteligence

59. Da bi odgovoril na drugo in tretje vprašanje v prošnji za mnenje, bo EOVP najprej podal splošne ugotovitve o nekaterih pomembnih vidikih, ki bi jih morali nadzorni organi ne glede na pravno podlago za obdelavo upoštevati pri presojanju, kako lahko upravljavci dokažejo skladnost s SUVP v okviru modelov UI. EOVP bo nato na podlagi Smernic št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP³⁹ proučil tri korake, ki jih zahteva presoja zakonitega interesa v okviru razvoja in uporabe modelov UI.

3.3.1 Splošne ugotovitve

60. EOVP opozarja, da SUVP ne vzpostavlja hierarhije med različnimi pravnimi podlagami, določenimi v njenem členu 6(1)⁴⁰.
61. Člen 5 SUVP določa načela v zvezi z obdelavo osebnih podatkov. EOVP poudarja tista, ki so pomembna za to mnenje in bi jih morali nadzorni organi upoštevati vsaj pri ocenjevanju določenih modelov UI ter najpomembnejših zahtev iz drugih določb SUVP, ob upoštevanju področja uporabe tega mnenja.
62. **Načelo odgovornosti** (člen 5(2) SUVP) – to načelo določa, da je upravljavec odgovoren za skladnost s SUVP in jo mora biti sposoben dokazati. V zvezi s tem bi bilo treba vloge in odgovornosti strank, ki obdelujejo osebne podatke v okviru razvoja ali uvajanja modela UI, oceniti pred začetkom obdelave, da se že na začetku opredelijo obveznosti upravljavcev ali skupnih upravljavcev in morebitnih obdelovalcev.
63. **Načela zakonitosti, poštenosti in preglednosti** (člen 5(1)(a) SUVP) – EOVP pri presoji zakonitosti obdelave v okviru modelov UI ob upoštevanju člena 6(1) SUVP meni, da je koristno razlikovati med različnimi fazami obdelave osebnih podatkov⁴¹. Načelo poštenosti, ki je tesno povezano z načelom preglednosti, zahteva, da se osebni podatki ne obdelujejo z nepoštenimi metodami ali z goljufijo ali na način, ki je „neupravičeno škodljiv, nezakonito diskriminatoren, nepričakovan ali zavajajoč za posameznika, na katerega se nanašajo osebni podatki“⁴². Glede na zapletenost vključenih tehnologij bi bilo zato treba informacije o obdelavi osebnih podatkov v modelih UI zagotoviti na dostopen, razumljiv in uporabniku prijazen način⁴³. Preglednost obdelave osebnih podatkov vključuje zlasti izpolnjevanje obveznosti obveščanja iz členov 12 do 14 SUVP⁴⁴, ki v primeru avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov, zahtevajo tudi smiselne informacije o

³⁹ Glejte Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024.

⁴⁰ Prav tam, točka 1.

⁴¹ Poročilo EOVP o delu, ki ga je opravila projektna skupina ChatGPT, sprejeto 23. maja 2024, odstavek 14.

⁴² Poročilo EOVP o delu, ki ga je opravila projektna skupina ChatGPT, sprejeto 23. maja 2024, odstavek 23; Smernice EOVP 4/2019 o členu 25: Vgrajeno in privzeto varstvo podatkov, različica 2.0, sprejete 20. oktobra 2020, odstavek 69; Smernice delovne skupine iz člena 29 o preglednosti na podlagi Uredbe (EU) 2016/679, revidirane in sprejete 11. aprila 2018, ki jih je EOVP potrdil 25. maja 2018, odstavek 2.

⁴³ Smernice delovne skupine iz člena 29 o preglednosti na podlagi Uredbe 2016/679, revidirane in sprejete 11. aprila 2018, ki jih je EOVP potrdil 25. maja 2018, odstavek 5.

⁴⁴ Glejte tudi uvodno izjavo 39 SUVP: „Načini zbiranja, uporabe, pregledovanja ali drug način obdelave ter obseg obdelave ali prihodnje obdelave osebnih podatkov, ki se nanašajo na posameznike, bi morali za posameznike biti pregledni [...]“.

vključeni logiki ter pomenu in predvidenih posledicah obdelave za posameznika, na katerega se nanašajo osebni podatki⁴⁵. Ob upoštevanju, da lahko razvojne faze modelov UI vključujejo zbiranje velikih količin podatkov iz javno dostopnih virov (na primer s tehnikami spletnega strganja), je zanašanje na izjemo iz člena 14(5)(b) SUVP strogo omejeno na primere, ko so zahteve iz te določbe v celoti izpolnjene⁴⁶.

64. **Načela omejitve namena in najmanjšega obsega podatkov** (člen 5(1)(b) in (c) SUVP) – V skladu z načelom najmanjšega obsega podatkov razvoj in uporaba modelov UI zahtevata, da morajo biti osebni podatki primerni, ustrezni in potrebni v zvezi z namenom. To lahko vključuje obdelavo osebnih podatkov, da bi se izognili tveganju morebitnih pristranskosti in napak, kadar je to jasno in izrecno opredeljeno v namenu in so osebni podatki za ta namen potrebni (npr. jih ni mogoče učinkovito doseči z obdelavo drugih podatkov, vključno s sintetičnimi ali anonimiziranimi podatki)⁴⁷. *Delovna skupina iz člena 29 je že poudarila, da „mora biti namen zbiranja jasno in natančno opredeljen [...]“*⁴⁸. Pri ocenjevanju, ali je zastavljeni namen zakonit, specifičen in izrecen ter ali je obdelava v skladu z načelom najmanjšega obsega podatkov, bi bilo treba najprej opredeliti zadevno dejavnost obdelave. Zlasti različni koraki v fazah razvoja ali uvajanja lahko pomenijo enake ali različne dejavnosti obdelave in lahko vključujejo zaporedne upravljavce ali skupne upravljavce. V nekaterih primerih je mogoče določiti namen, ki se bo uresničeval med uvajanjem modela UI v zgodnji fazi razvoja. Tudi če temu ni tako, bi moral biti že zdaj jasen določen okvir te uporabe, zato je treba upoštevati, kako ta okvir vpliva na namen razvoja. Pri pregledu namena obdelave v določeni fazi razvoja bi morali nadzorni organi od upravljavca(-ev) pričakovati določeno stopnjo podrobnosti in pojasnilo, kako te podrobnosti vplivajo na namen obdelave. To lahko vključuje na primer informacije o vrsti razvitega modela UI, njegovih pričakovanih funkcijah in vseh drugih pomembnih okoliščinah, ki so na tej stopnji že znane. Okoliščine uvajanja lahko na primer vključujejo tudi, ali se model razvija za notranje uvajanje, ali namerava upravljavec model po njegovem razvoju prodati ali distribuirati tretjim osebam, vključno s tem, ali je primarno namenjen uvajanju v raziskovalne ali komercialne namene.
65. **Pravice posameznikov, na katere se nanašajo osebni podatki** (poglavje III SUVP) – Ne glede na to, da morajo nadzorni organi zagotoviti spoštovanje vseh pravic posameznikov, na katere se nanašajo osebni podatki, ko upravljavci razvijajo in uporabljajo modele UI, EOVP opozarja, da kadar koli se upravljavec sklicuje na zakoniti interes kot pravno podlago, se uporablja pravica do ugovora iz člena 21 SUVP, ki jo je treba zagotoviti⁴⁹.

3.3.2 Razmisleki o treh korakih presoje zakonitega interesa v okviru razvoja in uvajanja modelov umetne inteligence

66. Da bi ugotovili, ali lahko določena obdelava osebnih podatkov temelji na členu 6(1)(f) SUVP, bi morali nadzorni organi preveriti, ali so upravljavci skrbno ocenili in dokumentirali, ali so izpolnjeni naslednji

⁴⁵ Člen 13(2)(f) SUVP in člen 14(2)(g) SUVP.

⁴⁶ Poročilo EOVP o delu, ki ga je opravila projektna skupina ChatGPT, sprejeto 23. maja 2024, odstavek 27.

⁴⁷ Poleg tega člen 10(5) Akta o UI določa posebna pravila za obdelavo posebnih vrst osebnih podatkov v zvezi s sistemi UI z visokim tveganjem za namen zagotavljanja odkrivanja in odpravljanja pristranskosti.

⁴⁸ Mnenje delovne skupine iz člena 29 št. 3/2013 o omejitvi namena (WP203), stran 15–16.

⁴⁹ V skladu s členom 21 SUVP upravljavec ne sme več obdelovati osebnih podatkov, če posameznik, na katerega se nanašajo osebni podatki, iz razlogov, povezanih z njegovim posebnim položajem, ugovarja obdelavi osebnih podatkov v zvezi z njim, razen če dokaže nujne zakonite razloge za obdelavo, ki prevladajo nad interesi, pravicami in svoboščinami posameznika, na katerega se nanašajo osebni podatki, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov. Zato morajo nadzorni organi upoštevati dva vidika: ali lahko upravljavec dokaže takšne nujne prevladujoče zakonite razloge in ali je mogoče uveljavljati pravico do ugovora.

trije kumulativni pogoji: (i) uresničevanje zakonitega interesa upravljavca ali tretje osebe; (ii) obdelava je potrebna za uresničevanje zakonitega interesa in (iii) nad zakonitim interesom ne prevladajo interesi ali temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki⁵⁰.

3.3.2.1 Prvi korak – Uresničevanje zakonitega interesa s strani upravljavca ali tretje osebe

67. Interes je širša korist, ki jo lahko ima upravljavec ali tretja oseba pri izvajanju določene dejavnosti obdelave⁵¹. Čeprav sta SUVP in Sodišče Evropske unije več interesov prepoznala kot zakonite⁵², bi morala biti presoja zakonitosti danega interesa rezultat analize vsakega primera posebej.
68. Kot je opozoril EOVP v svojih Smernicah o zakonitem interesu⁵³, se lahko interes šteje za zakonitega, če so izpolnjena naslednja tri kumulativna merila:
- interes je zakonit⁵⁴;
 - interes je jasno in natančno izražen in
 - Interes je resničen in prisoten, ne špekulativen.

69. Ob upoštevanju drugih dveh korakov, ki jih zahteva presoja zakonitega interesa, lahko naslednji primeri pomenijo zakonit interes v okviru modelov UI: (i) razvoj storitve pogovornega agenta za pomoč uporabnikom; (ii) razvoj sistema UI za odkrivanje goljufive vsebine ali vedenja; in (iii) izboljšanje odkrivanja groženj v informacijskem sistemu.

3.3.2.2 Drugi korak – Analiza nujnosti obdelave za uresničevanje zakonitega interesa

70. Drugi korak presoje je ugotavljanje, ali je obdelava osebnih podatkov potrebna za uresničitev zakonitega(-ih) interesa(-ov)⁵⁵ („preizkus nujnosti“).
71. V uvodni izjavi 39 je izrecno navedeno: „Osebni podatki bi se lahko obdelali le, če namena obdelave ne bi bilo mogoče razumno doseči z drugimi sredstvi.“. V skladu s Sodiščem Evropske unije in prejšnjimi smernicami EOVP bi bilo treba pogoj v zvezi z nujnostjo obdelave proučiti ob upoštevanju temeljnih

⁵⁰ Sodba SEU z dne 4. julija 2023 v zadevi C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), točka 106; sodba SEU z dne 11. decembra 2019 v zadevi C-708/18, *Asociația de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), točka 40. Glejte tudi Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 12 in naslednje. Kot je opozorjeno v teh smernicah, bi bilo treba to „presojo opraviti na začetku obdelave, v sodelovanju s pooblaščen osebo za varstvo podatkov (če je imenovana), upravljavec pa bi jo moral dokumentirati v skladu z načelom odgovornosti iz člena 5(2) SUVP“.

⁵¹ Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 14.

⁵² Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 16.

⁵³ Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 17.

⁵⁴ Sodba SEU z dne 4. oktobra 2024 v zadevi C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), točka 49, v kateri je SEU poudarilo, da zakoniti interes ne sme biti v nasprotju z zakonom. V zvezi s tem EOVP poudarja, da je treba pri presoji zakonitosti določenega interesa po potrebi upoštevati zakonodajne okvire. Glejte na primer: člen 26(3) in člen 28 Uredbe (EU) 2022/2065 Evropskega parlamenta in Sveta z dne 19. oktobra 2022 o enotnem trgu za digitalne storitve in spremembi Direktive 2000/31/ES (Zakon o digitalnih storitvah) o prepovedanem ciljnem oglaševanju mladoletnikom; člen 5(1) in (2) Akta o umetni inteligenci o prepovedanih praksah umetne inteligence (manipulativne prakse in prakse pod pragom zavesti); obdelava v nasprotju s pravicami intelektualne lastnine in določbami Direktive (EU) 2019/790 o avtorski in sorodnih pravicah na enotnem digitalnem trgu.

⁵⁵ Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavki 28–30.

pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki, ter v povezavi z načelom najmanjšega obsega podatkov iz člena 5(1)(c) SUVP⁵⁶.

72. Metodologija, na katero se sklicuje Sodišče Evropske unije, upošteva okvir obdelave ter učinke na upravljavca in posameznike, na katere se nanašajo osebni podatki. Ocena nujnosti torej vključuje dva elementa: (i) ali bo dejavnost obdelave omogočila izvajanje namena⁵⁷ in (ii) ali ni manj vsiljivega načina za izvajanje tega namena⁵⁸.
73. Na primer in odvisno od primera je treba nameravano količino osebnih podatkov, vključenih v modele UI, presoditi z vidika manj vsiljivih alternativ, ki so lahko razumno na voljo za enako učinkovito uresničevanje zakonitega interesa. Če je doseganje namena mogoče tudi z modelom UI, ki ne vključuje obdelave osebnih podatkov, se šteje, da obdelava osebnih podatkov ni nujna. To je za razvoj modelov UI še posebej pomembno. Pri presojanju ali je pogoj nujnosti izpolnjen, bi morali nadzorni organi posebno pozornost nameniti količini obdelanih osebnih podatkov in temu, ali je to sorazmerno z uresničevanjem zadevnega zakonitega interesa, tudi glede na načelo zmanjšanja količine podatkov.
74. Pri oceni nujnosti je treba upoštevati tudi širši okvir načrtovane obdelave osebnih podatkov. Obstoj sredstev, ki manj posegajo v temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, se lahko razlikuje glede na to, ali je upravljavec v neposrednem razmerju s posamezniki, na katere se nanašajo osebni podatki (podatki prve osebe), ali ne (podatki tretje osebe). Sodišče EU je navedlo nekaj premislekov, ki jih je treba upoštevati pri analizi nujnosti obdelave podatkov prve osebe za namen uresničevanja zakonitih interesov (čeprav v okviru razkritja takih podatkov tretjim osebam)⁵⁹.

⁵⁶ Sodba SEU z dne 4. julija 2023 v zadevi C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), točki 108 in 109, ki se sklicuje tudi na sodbo SEU z dne 11. decembra 2019 v zadevi C-708/18, *Asociația de Proprietari bloc M5A-Scara A* (ECLI:EU:C:2019:1064), točka 48; sodba SEU z dne 9. novembra 2010 v združeni zadevi C-92/09 in C-93/09, *Volker und Markus Schecke* (ECLI:EU:C:2010:662), točki 85 in 86; sodba SEU z dne 22. junija 2021, C-439/19, *Latvijas Republikas Saeima* (ECLI:EU:C:2021:504), točke 98, 109, 110 in 113. Glejte na primer: Smernice EOVP 3/2019 o obdelavi osebnih podatkov prek video naprav, različica 2.0, sprejete 29. januarja 2020, odstavki 24–26 in 73; Smernice EOVP 2/2019 o obdelavi osebnih podatkov v skladu s členom 6(1)(b) SUVP v okviru zagotavljanja spletnih storitev posameznikom, na katere se nanašajo osebni podatki, različica 2.0, sprejete 8. oktobra 2019, odstavki 23–25; Mnenje EOVP 11/2024 o uporabi prepoznavanja obraza za poenostavitev pretoka potnikov na letališču, različica 1.1, sprejeto 23. maja 2024, odstavek 27.

⁵⁷ Glejte sodbo SEU z dne 16. decembra 2008 v zadevi C-524/06, *Heinz Huber proti Bundesrepublik Deutschland* (ECLI:EU:C:2008:724), točka 66. V isti zadevi glej tudi sklepne predloge generalnega pravobranilca Poiaresa Madura v zadevi C-524/06, *Heinz Huber proti Bundesrepublik Deutschland* (ECLI:EU:C:2008:194), točka 16, v katerih je navedeno da „je v tem primeru ustrezno preverjanje učinkovitosti, ki ga mora uporabiti nacionalno sodišče. Vprašati se mora, ali obstajajo drugi načini obdelave podatkov, s katerimi bi lahko organi za priseljevanje izvrševali pravila o rezidentskem statusu. Če je odgovor na to vprašanje pritrdilen, bi bilo treba centralizirano shranjevanje in obdelavo podatkov za državljane Unije razglasiti za nezakonito. Ni nujno, da je alternativni sistem najučinkovitejši ali najprimernejši; dovolj je, da je sposoben ustrezno delovati. Drugače povedano, tudi če je centralni register učinkovitejši, priročnejši ali uporabniku prijaznejši od njegovih alternativ (kot so decentralizirani, lokalni registri), imajo slednji nedvomno prednost, če jih je mogoče uporabiti za navedbo statusa prebivališča državljanov Unije.

⁵⁸ Glejte sodbo Sodišča EU z dne 27. septembra 2017 v zadevi C-73/16, *Peter Puškár* (ECLI:EU:C:2017:725), točka 113: „Tako mora predložitevno sodišče preveriti, ali je oblikovanje spornega seznama in vključitev imen zadevnih oseb nanj primerno za uresničitev zastavljenih ciljev in ali teh ciljev ni mogoče uresničiti z drugimi, manj omejujočimi ukrepi.“; glej na primer sklepne predloge generalnega pravobranilca Rantos v zadevi C-252/21, *Meta proti Bundeskartellamt*, ECLI:EU:C:2022:704, točka 61, v kateri je navedeno: „[...] Zato je potrebna tesna povezava med obdelavo in uresničevanim interesom, če ni drugih možnosti, ki bi bolj spoštovale varstvo osebnih podatkov, saj ne zadostuje, da je obdelava zgolj koristna za upravljavca“.

⁵⁹ Sodba SEU z dne 4. oktobra 2024 v zadevi C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), točke 51–53.

75. Izvajanje tehničnih zaščitnih ukrepov za varstvo osebnih podatkov lahko prispeva tudi k izpolnjevanju preizkusa nujnosti. To bi lahko na primer vključevalo izvedbene ukrepe, kot so tisti, opredeljeni v oddelku 3.2.2, tako da anonimizacija ni dosežena, vendar to še vedno zmanjšuje enostavnost določljivosti posameznikov, na katere se nanašajo osebni podatki. EOVP ugotavlja, da lahko nekateri od teh ukrepov, kadar niso potrebni za uskladitev S SUVP, pomenijo dodatne zaščitne ukrepe, kot je dodatno analizirano v pododdelku „blažilni ukrepi“ v oddelku 3.3.2.3⁶⁰.

3.3.2.3 Tretji korak – preizkus uravnoteženja

76. Tretji korak ocenjevanja zakonitega interesa je „**uravnoteženje**“ (v tem dokumentu imenovan tudi „**preizkus uravnoteženja**“)⁶¹. V tem koraku je treba opredeliti in opisati različne nasprotujoče si pravice in interese⁶², tj. na eni strani interese, temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, na drugi strani pa interese upravljavca ali tretje osebe. Nato je treba proučiti posebne okoliščine primera, da se dokaže, da je zakoniti interes ustrezna pravna podlaga za zadevne dejavnosti obdelave⁶³.

Interesi, temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki

77. Člen 6(1)(f) SUVP določa, da bi moral upravljavec pri ocenjevanju različnih sestavnih delov v okviru preizkusa uravnoteženja upoštevati interese, temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Interesi posameznikov, na katere se nanašajo osebni podatki, so interesi, na katere lahko vpliva zadevna obdelava. V okviru faze razvoja modela UI lahko ti med drugim vključujejo interes za samodoločanje in ohranjanje nadzora nad lastnimi osebnimi podatki (npr. podatki, zbrani za razvoj modela). V okviru uvajanja modela UI lahko interesi posameznikov, na katere se nanašajo osebni podatki, med drugim vključujejo interese za ohranitev nadzora nad lastnimi osebnimi podatki (npr. podatki, obdelanimi po uvedbi modela), finančne interese (npr. kadar posameznik, na katerega se nanašajo osebni podatki, uporablja model UI za ustvarjanje prihodkov ali kadar ga posameznik uporablja v okviru svoje poklicne dejavnosti), osebne koristi (npr. kadar se model UI uporablja za izboljšanje dostopnosti do nekaterih storitev) ali socialno-ekonomske interese (npr. kadar model UI omogoča dostop do boljšega zdravstvenega varstva ali olajša uveljavljanje temeljne pravice, kot je dostop do izobraževanja)⁶⁴.
78. Natančneje ko je interes opredeljen glede na predvideni namen obdelave, bolje bo mogoče razumeti dejanske koristi in tveganja, ki jih je treba upoštevati pri uravnoteženju.
79. V zvezi s temeljnimi pravicami in svoboščinami posameznikov, na katere se nanašajo osebni podatki, lahko razvoj in uporaba modelov UI pomenita resna tveganja za pravice, zaščitene z Listino EU o temeljnih pravicah (v nadaljnjem besedilu: **Listina EU**), med drugim vključno s pravico do zasebnega in družinskega življenja (člen 7 Listine EU) in pravico do varstva osebnih podatkov (člen 8 Listine EU). Ta tveganja se lahko pojavijo v fazi razvoja, na primer kadar se osebni podatki postrgajo proti volji posameznikov, na katere se nanašajo osebni podatki, ali brez njihove vednosti. Ta tveganja se lahko

⁶⁰ Glejte Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 57.

⁶¹ Glejte Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavki 31 do 60.

⁶² Glejte Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 32.

⁶³ Glejte Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 32, ki se sklicujejo tudi sodbo SEU z dne 4. julija 2023 v zadevi C-252/21 *Meta proti Bundeskartellamt*, (ECLI:EU:C:2023:537), odstavek 110.

⁶⁴ Glejte Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 38.

pojaviijo tudi v fazi uvajanja, na primer kadar model (ali kot del modela) obdeluje osebne podatke na način, ki je v nasprotju s pravicami posameznikov, na katere se nanašajo osebni podatki, ali kadar je mogoče naključno ali z napadi (npr. sklepanje o članstvu, pridobivanje podatkov ali inverzija modela) sklepati, kateri osebni podatki so zbirki podatkov za učenje modela. Tovrstni primeri predstavljajo tveganje za zasebnost posameznikov, na katere se nanašajo osebni podatki in katerih podatki se lahko pojavijo v fazi uvajanja sistema UI (npr. tveganje izgube ugleda, kraja ali goljufija identitete, varnostno tveganje odvisno od narave podatkov).

80. Glede na zadevni primer lahko obstajajo tudi tveganja za druge temeljne pravice. Obsežno in neselektivno zbiranje podatkov z modeli UI v fazi razvoja lahko na primer pri posamezniku, na katerega se nanašajo osebni podatki, ustvari občutek nadzora, zlasti ob upoštevanju težav pri preprečevanju strganja javnih podatkov. To lahko posameznike privede do samocenzuriranja in pomeni tveganje za spodkopavanje njihove svobode izražanja (člen 11 Listine EU). V fazi uvajanja so tveganja za svobodo izražanja prisotna tudi, kadar se modeli UI uporabljajo za blokiranje objave vsebin s strani posameznikov, na katere se nanašajo osebni podatki. Poleg tega lahko model UI, ki ranljivim posameznikom priporoča neprimerno vsebino, predstavlja tveganje za njihovo duševno zdravje (člen 3(1) Listine EU). V drugih primerih lahko uporaba modelov UI povzroči tudi negativne posledice za posameznikovo pravico do zaposlitve (člen 15 Listine EU), na primer, če se prijave za zaposlitev predhodno izberejo z uporabo modela UI. Na enak način bi lahko model UI predstavljal tveganja za pravico do nediskriminacije (člen 21 Listine EU), če diskriminira posameznike na podlagi nekaterih osebnih značilnosti (kot je državljanstvo ali spol). Poleg tega lahko uporaba modelov UI predstavlja tudi tveganje za varnost in zaščito posameznika (npr. če se model UI uporablja z zlonamernim namenom) ter tveganje za njegovo telesno in duševno celovitost⁶⁵.
81. Uvedba modelov UI lahko na nekatere temeljne pravice vpliva tudi pozitivno, npr. model UI lahko podpira pravico do duševne celovitosti osebe (člen 3 Listine), na primer, kadar se uporablja za prepoznavanje škodljivih vsebin na spletu, ali kadar olajša dostop do nekaterih bistvenih storitev ali uresničevanje temeljnih pravic, kot sta dostop do informacij (člen 11 Listine EU) ali dostop do izobraževanja (člen 14 Listine EU).

Vpliv obdelave na posameznike, na katere se nanašajo osebni podatki

82. Obdelava osebnih podatkov, ki poteka med razvojem in uvajanjem modelov UI, lahko na posameznike, na katere se nanašajo osebni podatki, vpliva na različne načine, ki so lahko pozitivni ali negativni⁶⁶. Na primer, če dejavnost obdelave prinaša koristi za posameznika, na katerega se nanašajo osebni podatki, se lahko ti upoštevajo pri preizkusu uravnoteženja. Čeprav lahko obstoj tovrstnih koristi privede do ugotovitve nadzornega organa, da interesi upravljavca ali tretje osebe ne prevladajo nad interesi, temeljnimi pravicami in svoboščinami posameznikov, na katere se nanašajo osebni podatki, je taka ugotovitev lahko le rezultat analize vsakega primera posebej, pri kateri se upoštevajo vsi ustrezni dejavniki.
83. Na vpliv obdelave na posameznike, na katere se nanašajo osebni podatki, lahko vplivajo (i) narava podatkov, ki jih obdelujejo modeli, (ii) okoliščine obdelave in (iii) nadaljnje posledice, ki jih lahko ima obdelava⁶⁷.

⁶⁵ Glejte Smernice št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 46.

⁶⁶ Glejte Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 39.

⁶⁷ Glejte Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 32.

84. V zvezi s **naravo podatkov, ki se obdelujejo**, je treba opozoriti, da ima lahko obdelava nekaterih drugih kategorij osebnih podatkov – razen posebnih vrst osebnih podatkov ter podatkov v zvezi s kazenskimi obsodbami in prekrški, za katere velja dodatno varstvo v skladu s členoma 9 oziroma 10 SUVP – pomembne posledice za posameznike, na katere se podatki nanašajo. V zvezi s tem bi bilo treba šteti, da bi lahko obdelava nekaterih vrst osebnih podatkov, ki razkrivajo zelo zasebne informacije (npr. finančne podatke ali podatke o kraju nahajanja) za razvoj in uporabo modela UI, resno vplivala na posameznike, na katere se nanašajo osebni podatki. V fazi uvajanja so lahko posledice tovrstne obdelave za posameznike, na katere se nanašajo osebni podatki, na primer ekonomske (npr. diskriminacija pri zaposlovanju) in/ali v smislu ogrožanja časti in dobrega imena posameznika (npr. obrekovanje).
85. V zvezi z **okoliščinami obdelave je treba najprej opredeliti elemente**, ki bi lahko povzročili tveganja za posameznike, na katere se nanašajo osebni podatki (npr. način razvoja modela, način uvajanja modela in/ali ustreznost varnostnih ukrepov za varstvo osebnih podatkov). Narava modela in predvidena operativna uporaba imata ključno vlogo pri prepoznavanju tovrstnih morebitnih vzrokov.
86. Prav tako je treba oceniti resnost teh tveganj za posameznike, na katere se nanašajo osebni podatki. Med drugim se lahko prouči, kako se obdelujejo osebni podatki (npr. če so združeni z drugimi nabori podatkov), kakšen je obseg obdelave in količina obdelanih osebnih podatkov⁶⁸ (npr. skupni obseg podatkov, obseg podatkov na posameznika, na katerega se nanašajo osebni podatki, število posameznikov, na katere se nanašajo osebni podatki)⁶⁹, status posameznika, na katerega se nanašajo osebni podatki (npr. otroci ali drugi ranljivi posamezniki, na katere se nanašajo osebni podatki), in njihovo razmerje z upravljavcem (npr. če je posameznik, na katerega se nanašajo osebni podatki, stranka). Na primer, uporaba spletnega strganja v fazi razvoja lahko zaradi velike količine zbranih podatkov, velikega števila posameznikov, na katere se podatki nanašajo, in neselektivnega zbiranja osebnih podatkov ob odsotnosti zadostnih zaščitnih ukrepov povzroči znatne vplive na posameznike.
87. **Nadaljnje posledice**, ki bi jih obdelava lahko imela, bi bilo treba upoštevati tudi pri presojanju vpliva obdelave na posameznike, na katere se nanašajo osebni podatki. Nadzorni organi bi jih morali presoditi v vsakem primeru posebej ob upoštevanju zadevnih posebnih dejstev.
88. Tovrstne posledice lahko vključujejo (vendar niso omejene na) tveganje kršitve temeljnih pravic posameznikov, na katere se nanašajo osebni podatki, kot je opisano v prejšnjem podpoglavju⁷⁰. Tveganja se lahko razlikujejo po verjetnosti in resnosti ter so lahko posledica obdelave osebnih podatkov, ki bi lahko povzročila fizično, materialno ali nepremoženjsko škodo, zlasti kadar lahko obdelava povzroči diskriminacijo⁷¹.
89. Kadar uvedba modela UI vključuje obdelavo osebnih podatkov (i) posameznikov, na katere se nanašajo osebni podatki, katerih osebni podatki so vključeni v podatkovni niz, ki se uporablja v fazi razvoja, in (ii) posameznikov, na katere se nanašajo osebni podatki in katerih osebni podatki se obdelujejo v fazi uvajanja, bi morali nadzorni organi pri preverjanju preizkusa uravnoteženja, ki ga izvaja upravljavec,

⁶⁸ Glejte Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 43.

⁶⁹ Sodba SEU z dne 4. julija 2023 v zadevi C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), točka 116.

⁷⁰ Glejte podpoglavje „Interesi, temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki“ zgoraj.

⁷¹ Glejte oddelek 2.3 Smernic Evropskega odbora za varstvo podatkov št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024. Za dodatne primere glej tudi uvodno izjavo 75 SUVP.

razlikovati in upoštevati tveganja, ki vplivajo na interese, pravice in svoboščine vsake od teh kategorij posameznikov, na katere se nanašajo osebni podatki.

90. **Nazadnje bi bilo treba pri analizi morebitnih nadaljnjih posledic obdelave upoštevati tudi verjetnost, da se bodo te nadaljnje posledice uresničile.** Presojto te verjetnosti je treba opraviti ob upoštevanju veljavnih tehničnih in organizacijskih ukrepov ter posebnih okoliščin posameznega primera. Nadzorni organi lahko na primer proučijo, ali so bili izvedeni ukrepi za preprečevanje morebitne zlorabe modela UI. Pri modelih UI, ki se uvedejo za različne namene, kot je generativna umetna inteligenca, lahko to vključuje kontrole, ki čim bolj omejujejo njihovo uporabo za škodljive prakse, na primer oblikovanje globokih ponaredkov, klepetalni boti, ki se uporabljajo za dezinformacije, lažno predstavljanje in druge vrste goljufij, ter manipulativne umetne inteligence/sredstva umetne inteligence (zlasti kadar so antropomorfična ali zagotavljajo zavajajoče informacije).

Razumna pričakovanja posameznikov, na katere se nanašajo osebni podatki

91. Na podlagi uvodne izjave 47 SUVP, „[V] vsakem primeru bi bila za ugotovitev obstoja zakonitega interesa potrebna skrbna ocena, tudi glede tega, ali posameznik, na katerega se nanašajo osebni podatki, lahko v času zbiranja osebnih podatkov in v njegovem okviru razumno pričakuje, da se bodo ti obdelali v zadevni namen. Interesi in temeljne pravice posameznika, na katerega se nanašajo osebni podatki, bi zlasti lahko prevladali nad interesi upravljavca podatkov, kadar se osebni podatki obdelujejo v okoliščinah, ko posamezniki, na katere se nanašajo osebni podatki, razumno ne pričakujejo nadaljnje obdelave.“⁷².
92. Razumna pričakovanja imajo ključno vlogo pri preizkusu uravnoteženja, med drugim zaradi zapletenosti tehnologije, ki se uporablja v modelih UI, in dejstva, da posamezniki, na katere se nanašajo osebni podatki, morda težko razumejo različne možne uporabe modela UI in vključeno obdelavo podatkov⁷³. V ta namen se lahko informacije, ki se zagotovijo posameznikom, na katere se nanašajo osebni podatki, upoštevajo pri presoji, ali lahko posamezniki, na katere se nanašajo osebni podatki, razumno pričakujejo, da se bodo njihovi osebni podatki obdelovali. Čeprav lahko opustitev informacij prispeva k temu, da posamezniki, na katere se nanašajo osebni podatki, ne pričakujejo določene obdelave, zgolj izpolnjevanje zahtev glede preglednosti iz SUVP samo po sebi ne zadostuje za ugotovitev, da lahko posamezniki, na katere se nanašajo osebni podatki, razumno pričakujejo določeno obdelavo⁷⁴. Poleg tega zgolj zato, ker so informacije v zvezi s fazo razvoja modela UI vključene v upravljalčevo politiko varstva zasebnosti, to ne pomeni nujno, da lahko posamezniki, na katere se nanašajo osebni podatki, upravičeno pričakujejo, da se bo to zgodilo; namesto tega bi morali nadzorni organi to analizirati na podlagi posebnih okoliščin posameznega primera in ob upoštevanju vseh relevantnih dejavnikov.
93. Pri ocenjevanju razumnih pričakovanj posameznikov, na katere se nanašajo osebni podatki, v zvezi z obdelavo, ki poteka v fazi razvoja, je pomembno upoštevati elemente, navedene v Smernicah EOVP o

⁷² Glejte tudi sodbo SEU z dne 4. julija 2023 v zadevi C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), točka 112; sodbo SEU z dne 11. decembra 2019 v zadevi C-708/18, *Asociația de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), točka 58; in sodbo SEU z dne 4. oktobra 2024 v zadevi C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), točka 55.

⁷³ Na primer, SEU je v sodbi z dne 4. julija 2023 v zadevi C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), točka 123, ugotovilo, da „izboljšanja izdelka“ načeloma ni mogoče izključiti kot zakonitega interesa, ugotovilo pa je tudi, da je „dvomljivo, ali [...] da lahko glede obdelave podatkov iz postopka v glavni stvari cilj izboljšanja proizvoda ob upoštevanju obsega te obdelave in njenega znatnega vpliva na uporabnika ter okoliščine, da ta uporabnik ne more razumno pričakovati, da bo [...] te podatke obdelovala, prevlada nad interesi in temeljnimi pravicami takega uporabnika, zlasti če je ta otrok“.

⁷⁴ Smernice št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 53.

zakonitem interesu⁷⁵. Poleg tega je v okviru vsebine tega mnenja pomembno upoštevati širši okvir obdelave. To lahko vključuje, čeprav ni omejeno na to, ali so bili osebni podatki javno dostopni ali ne, naravo razmerja med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem (in ali med njima obstaja povezava), naravo storitve, okoliščine, v katerih so bili osebni podatki zbrani, vir, iz katerega so bili podatki zbrani (npr. spletno mesto ali storitev, kjer so bili osebni podatki zbrani, in njihove nastavitve zasebnosti), morebitne nadaljnje uporabe modela in vprašanje ali se posamezniki, na katere se nanašajo osebni podatki, dejansko zavedajo, da so njihovi osebni podatki sploh na spletu.

94. V fazi razvoja modela se lahko razumna pričakovanja posameznikov, na katere se nanašajo osebni podatki, razlikujejo glede na to, ali so posamezniki, na katere se nanašajo osebni podatki, objavili podatke, obdelane za razvoj modela, ali ne. Poleg tega se lahko razumna pričakovanja razlikujejo tudi glede na to, ali so podatke neposredno posredovali upravljavcu (npr. v okviru njihove uporabe storitve), ali če jih je upravljavec pridobil iz drugega vira (npr. prek tretje osebe ali s strganjem). V obeh primerih bi bilo treba pri presoji razumnih pričakovanj upoštevati ukrepe, sprejete za obveščanje posameznikov, na katere se nanašajo osebni podatki, o dejavnostih obdelave.
95. V fazi uvajanja modela UI je prav tako pomembno upoštevati razumna pričakovanja posameznikov, na katere se nanašajo osebni podatki, v okviru posebnih zmogljivosti modela. Na primer, za modele UI, ki se lahko prilagodijo v skladu s predloženimi vhodnimi podatki, je morda pomembno proučiti, ali so posamezniki, na katere se nanašajo osebni podatki, vedeli, da so predložili osebne podatke, na podlagi katerih je model UI lahko prilagodil odgovore njihovim potrebam in zagotovil storitve po meri. Poleg tega bi bilo morda pomembno tudi proučiti, ali bi ta dejavnost obdelave vplivala le na storitev, ki se zagotavlja posameznikom, na katere se nanašajo osebni podatki (npr. personalizacija vsebin za določenega uporabnika), ali pa bi se uporabljala za spremembo storitve, ki se zagotavlja vsem strankam (npr. za splošno izboljšanje modela). Tako kot v fazi razvoja je lahko zlasti pomembno proučiti, ali obstaja neposredna povezava med posamezniki, na katere se nanašajo osebni podatki, in upravljavcem. Tovrstna neposredna povezava lahko na primer upravljavcu omogoči, da posameznikom, na katere se nanašajo osebni podatki, brez težav zagotovi informacije o dejavnosti obdelave in modelu, kar bi nato lahko vplivalo na razumna pričakovanja teh posameznikov, na katere se nanašajo osebni podatki.

Blažilni ukrepi

96. Kadar se zdi, da interesi, pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, prevladajo nad zakonitim(-i) interesom(-i), za katerega(-e) si prizadeva upravljavec ali tretja oseba, lahko upravljavec razmisli o uvedbi blažilnih ukrepov za omejitev učinka obdelave na te posameznike, na katere se nanašajo osebni podatki. Blažilni ukrepi so zaščitni ukrepi, ki bi morali biti prilagojeni okoliščinam primera in odvisni od različnih dejavnikov, vključno s predvideno uporabo modela UI. Cilj teh blažilnih ukrepov bi bil zagotoviti, da interesi upravljavca ali tretje osebe ne bodo prevladani, tako da bi se upravljavec lahko skliceval na to pravno podlago.
97. Kot je opozorjeno v smernicah EOVP o zakonitem interesu, blažilnih ukrepov ne bi smeli zamenjevati z ukrepi, ki jih mora upravljavec v vsakem primeru sprejeti po zakonu, da zagotovi skladnost s SUVP, ne glede na to, ali obdelava temelji na členu 6(1)(f) SUVP⁷⁶. To je zlasti pomembno za ukrepe, ki na primer zahtevajo skladnost z načeli SUVP, kot je načelo najmanjšega obsega podatkov.

⁷⁵ Smernice št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavki 50–54.

⁷⁶ Smernice št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 57.

98. Seznam spodaj navedenih ukrepov je neizčrpen in nepredpisujoč, izvajanje ukrepov pa bi bilo treba obravnavati na podlagi presoje vsakega primera posebej. Čeprav se glede na okoliščine lahko zahteva, da so nekateri spodaj navedeni ukrepi skladni s posebnimi obveznostmi iz SUVP, se lahko v nasprotnem primeru upoštevajo kot dodatni zaščitni ukrepi. Poleg tega se nekateri spodaj navedeni ukrepi nanašajo na področja, ki se hitro razvijajo in na katerih prihaja do novih sprememb, nadzorni organi pa bi jih morali upoštevati pri obravnavi določenega primera.
99. **V zvezi s fazo razvoja modelov UI** se lahko sprejme več ukrepov za zmanjšanje tveganj, ki jih predstavlja obdelava podatkov prve in tretje osebe (vključno z zmanjšanjem tveganj, povezanih s praksami strganja spletnih strani). Na podlagi navedenega EOVP navaja nekaj primerov ukrepov, ki se lahko izvajajo za zmanjšanje tveganj, ugotovljenih v preizkusu uravnoteženja, in ki bi jih morali nadzorni organi upoštevati pri presoji posameznih modelov UI v vsakem primeru posebej.
100. **Tehnični ukrepi**
- a. Ukrepi iz oddelka 3.2.2, ki so primerni za ublažitev zadevnih tveganj, če ti ukrepi ne povzročijo anonimizacije modela in niso potrebni za izpolnjevanje drugih obveznosti iz SUVP ali na podlagi preizkusa nujnosti (drugi korak presoje zakonitega interesa).
101. Poleg teh lahko drugi ustrezni ukrepi vključujejo:
- b. ukrep psevdonimizacije, ki bi lahko na primer vključeval ukrepe za preprečevanje kakršne koli kombinacije podatkov, ki temeljijo na posameznih identifikatorjih. Ti ukrepi morda niso primerni, če nadzorni organ meni, da je upravljavec dokazal razumno potrebo po zbiranju različnih podatkov o določenem posamezniku za razvoj zadevnega sistema ali modela UI;
 - c. ukrep za prikrivanje osebnih podatkov ali njihovo zamenjavo z lažnimi osebnimi podatki v podatkovnem nizu za učenje (npr. zamenjava imen in e-poštnih naslovov z lažnimi imeni in lažnimi e-poštnimi naslovi). Ta ukrep je lahko zlasti primeren, kadar dejanska materialna vsebina podatkov ni pomembna za splošno obdelavo (npr. pri učenju velikih jezikovnih modelov).
102. **Ukrepi, ki olajšujejo uresničevanje pravic posameznikov:**
- a. Upoštevanje razumnega časovnega obdobja med zbiranjem nabora podatkov za učenje in njegovo uporabo. Ta dodatni zaščitni ukrep lahko posameznikom, na katere se nanašajo osebni podatki, omogoči uveljavljanje njihovih pravic v tem obdobju, pri čemer se razumno obdobje oceni glede na okoliščine posameznega primera.
 - b. Predlaganje brezpogojne „zavrnitve“ od samega začetka, na primer z zagotavljanjem diskrecijske pravice do ugovora posameznikom, na katere se nanašajo osebni podatki, pred začetkom obdelave, da se okrepi nadzor posameznikov nad njihovimi podatki, kar presega pogoje iz člena 21 SUVP⁷⁷.
 - c. Omogočanje posameznikom, na katere se nanašajo osebni podatki, da uveljavljajo svojo pravico do izbrisa, tudi če se posebni razlogi iz člena 17(1) SUVP ne uporabljajo⁷⁸.
 - d. Omogočanje posameznikom, na katere se nanašajo osebni podatki, da se pritožijo v zvezi z regurgitacijo ali pomnjenjem njihovih osebnih podatkov ter okoliščinami in sredstvi, s katerimi

⁷⁷ Prav tam.

⁷⁸ Prav tam.

lahko pritožbe ponovijo, kar upravljavcem omogoča, da ponovijo in ocenijo ustrezne tehnike odprave naučenih podatkov za obravnavo pritožb.

103. **Ukrepi za preglednost:** v nekaterih primerih bi lahko blažilni ukrepi vključevali ukrepe, ki zagotavljajo večjo preglednost v zvezi z razvojem modela UI. Nekateri ukrepi lahko poleg skladnosti z obveznostmi iz SUVP pomagajo premagovati asimetrijo informacij in posameznikom, na katere se nanašajo osebni podatki, omogočajo boljše razumevanje obdelave v razvojni fazi:
- a. Objava javnih in lahko dostopnih sporočil, ki presegajo informacije, zahtevane v skladu s členom 13 ali 14 SUVP, na primer z zagotavljanjem dodatnih podrobnosti o merilih zbiranja in vseh uporabljenih zbirkah podatkov, ob upoštevanju posebne zaščite otrok in ranljivih oseb.
 - b. Alternativne oblike obveščanja posameznikov, na katere se nanašajo osebni podatki, na primer: medijske kampanje z različnimi mediji za obveščanje posameznikov, na katere se nanašajo osebni podatki, informacijska kampanja po elektronski pošti, uporaba grafične vizualizacije, pogosto zastavljena vprašanja, oznake preglednosti in kartice modelov, katerih sistematizacija bi lahko strukturirala predstavitev informacij o modelih UI, ter letna poročila o preglednosti na prostovoljni osnovi.
104. **Posebni blažilni ukrepi v okviru spletnega strganja:** Glede na to, da, kot je navedeno zgoraj, pri spletnem strganju nastajajo posebna tveganja⁷⁹, bi lahko v tem okviru opredelili posebne blažilne ukrepe. Nadzorni organi jih lahko po potrebi poleg zgoraj navedenih blažilnih ukrepov upoštevajo tudi pri preiskovanju upravljavcev, ki izvajajo spletno strganje.
105. Posebni ukrepi, ki niso potrebni v okviru drugega koraka presoje zakonitega interesa, se lahko izkažejo za koristne za zmanjšanje tveganja v okviru spletnega strganja. Ti lahko vključujejo **tehnične ukrepe**, ki so:
- a. izključevanje vsebine podatkov iz publikacij, ki lahko vključujejo osebne podatke, ki pomenijo tveganje za določene osebe ali skupine oseb (npr. posameznike, ki bi lahko bili predmet zlorabe, predsodkov ali celo fizičnega poškodovanja, če bi bile informacije javno objavljene);
 - b. zagotavljanje, da se nekatere kategorije podatkov ne zbirajo ali da so nekateri viri izključeni iz zbiranja podatkov; to bi lahko na primer vključevalo nekatera spletišča, ki so še posebej vsiljiva zaradi občutljivosti njihove vsebine;
 - c. izključevanje zbiranja s spletnih mest (ali delov spletnih mest), ki jasno nasprotujejo spletnemu strganju in ponovni uporabi svoje vsebine za namen oblikovanja podatkovnih zbirk za učenje umetne inteligence (na primer z upoštevanjem datotek robots.txt ali ai.txt ali katerega koli drugega priznanega mehanizma za izražanje izključitve iz samodejnega pregledovanja ali strganja);
 - d. uvedba drugih ustreznih omejitev zbiranja, po možnosti vključno z merili, ki temeljijo na časovnih obdobjih.
106. V okviru spletnega strganja lahko primeri posebnih ukrepov, **ki olajšujejo uresničevanje pravic posameznikov in preglednosti**, vključujejo: oblikovanje seznama zavrnitve, ki ga upravlja upravljavec in ki posameznikom, na katere se nanašajo osebni podatki, omogoča, da ugovarjajo zbiranju svojih

⁷⁹ Te prakse lahko sprožijo tudi dodatna vprašanja, ki niso zajeta v tem mnenju, glej na primer Pagallo U., Ciani Sciolla J., *Anatomy of web data scraping: ethics, standards, and the troubles of the law* (Anatomija spletnega strganja podatkov: etika, standardi in težave z zakonodajo). *European Journal of Privacy Law & Technologies*, (2023) 2, str. 1-19, na voljo na: <https://doi.org/10.57230/EJPLT232PS>.

podatkov na nekaterih spletiščih ali spletnih platformah tako, da zagotovijo informacije, ki jih identificirajo na teh spletiščih, vključno pred zbiranjem podatkov⁸⁰.

107. **Posebni premisleki v zvezi z blažilnimi ukrepi v fazi uvajanja:** Čeprav so nekateri od zgoraj navedenih ukrepov glede na okoliščine lahko pomembni tudi za fazo uvajanja, EOVP v nadaljevanju navaja neizčrpen seznam dodatnih podpornih ukrepov, ki se lahko izvajajo in ki jih morajo nadzorni organi oceniti v vsakem primeru posebej.
- a. **Tehnični ukrepi** se lahko na primer sprejmejo za preprečevanje shranjevanja, regurgitacije ali ustvarjanja osebnih podatkov, zlasti v okviru generativnih modelov UI (kot so filtri izhodnih podatkov), in/ali za zmanjšanje tveganja nezakonite ponovne uporabe z modeli UI za splošni namen (npr. digitalno označevanje izdelkov, ustvarjenih z umetno inteligenco).
 - b. **Ukrepi, ki olajšajo ali pospešijo uveljavljanje pravic posameznikov** v fazi uvajanja, ki presegajo zakonske zahteve, zlasti in ne samo v zvezi z uveljavljanjem pravice do izbrisa osebnih podatkov iz izhodnih podatkov modela ali deduplikacijo ter tehnikami po učenju, ki poskušajo odstraniti ali prikriti osebne podatke.
108. Nadzorni organi bi morali pri proučevanju uporabe določenega modela UI proučiti, ali je upravljavec objavil izvedeni preizkus uravnoteženja, saj bi to lahko povečalo preglednost in pravičnost. Kot je navedeno v smernicah EOVP o zakonitem interesu, se lahko za druge ukrepe šteje, da posameznikom, na katere se nanašajo osebni podatki, zagotovijo informacije iz preizkusa uravnoteženja pred vsakršnim zbiranjem osebnih podatkov⁸¹. EOVP ponovno poudarja tudi⁸², da je element, ki ga je treba upoštevati, vprašanje, ali je upravljavec vključil pooblaščen osebo za varstvo podatkov, kjer je to ustrezno.

3.4 O morebitnem vplivu nezakonite obdelave pri razvoju modela umetne inteligence na zakonitost nadaljnje obdelave ali delovanja modela umetne inteligence

109. Ta del mnenja obravnava vprašanje 4 iz prošnje za mnenje. S tem vprašanjem se prosi za pojasnilo o morebitnem vplivu nezakonite obdelave v fazi razvoja na nadaljnjo obdelavo (na primer v fazi uvajanja modela UI) ali na delovanje modela. Namen vprašanja je obravnavati položaj, v katerem tak model UI obdeluje osebne podatke, ki se hranijo v njem (vprašanje 4(i) v prošnji za mnenje), in položaj, v katerem pri uvajanju modela UI ni več vključena obdelava osebnih podatkov (tj. model je anonimen) (vprašanje 4(ii) v prošnji za mnenje).
110. Pred obravnavo nekaterih specifičnih scenarijev EOVP navaja naslednje splošne premisleke.
111. Prvič, pojasnila v tem poglavju bodo osredotočena na obdelavo osebnih podatkov v fazi razvoja, ki se izvaja ob hkratnem neupoštevanju načela zakonitosti, kot je določeno v členu 5(1)(a) SUVP in členu 6 navedene uredbe (v nadaljnjem besedilu: **nezakonitost**)⁸³. Podobno bodo premisleki EOVP

⁸⁰Razen če upravljavec dokaže nujne zakonite razloge za obdelavo, ki prevladajo nad interesi, pravicami in svoboščinami posameznika, na katerega se nanašajo osebni podatki, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

⁸¹ Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 68.

⁸² Smernice EOVP št. 1/2024 o obdelavi osebnih podatkov na podlagi člena 6(1)(f) SUVP, različica 1.0, sprejete 8. oktobra 2024, odstavek 12.

⁸³ Sodba SEU z dne 4. maja 2023 v zadevi C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), točke 55-57.

osredotočeni na vpliv nezakonnosti obdelave v fazi razvoja na zakonitost naknadne obdelave ali delovanja modela (tj. skladnost s členoma 5(1)(a) in 6 SUVP). Vendar EOVP poudarja, da lahko obdelava, ki se izvaja v fazi razvoja, privede tudi do kršitev drugih določb SUVP, kot je pomanjkanje preglednosti za posameznike, na katere se nanašajo osebni podatki, ali vgrajenega in/ali privzetega varstva podatkov, ki v tem mnenju niso analizirani.

112. Drugič, pri obravnavi tega vprašanja ima ključno vlogo načelo odgovornosti, v skladu s katerim morajo biti upravljavci odgovorni za spoštovanje *med drugim* členov 5(1) in 6 SUVP⁸⁴ in to tudi dokazati. To velja tudi za potrebo po presoji, katera organizacija je upravljavec za zadevno dejavnost obdelave in ali nastanejo primeri skupnega upravljanja (ker so lahko neločljivo povezani)⁸⁵. Glede na pomen dejanskih okoliščin vsakega primera, tudi v zvezi z vlogo, ki jo ima vsaka stran, vključena v obdelavo, bi bilo treba premisleke EOVP razumeti kot splošne ugotovitve, ki bi jih morali nadzorni organi presojati v vsakem primeru posebej.
113. Tretjič, EOVP poudarja, da so nadzorni organi v skladu s členom 51(1) SUVP „*pristojni za spremljanje uporabe [SUVP], da se zaščitijo temeljne pravice in svoboščine posameznikov v zvezi z obdelavo ter olajša prost pretok osebnih podatkov v Uniji*“. Zato je v pristojnosti nadzornih organov, da presodijo zakonitost obdelave in izvajajo pooblastila, ki so jim dodeljena v SUVP v skladu z nacionalnim okvirom⁸⁶. V tovrstnih primerih imajo nadzorni organi diskrecijska pooblastila, da ocenijo morebitne kršitve in izberejo ustrezne, potrebne in sorazmerne ukrepe iz člena 58 SUVP, pri čemer upoštevajo okoliščine vsakega posameznega primera⁸⁷.
114. **Kadar se ugotovi kršitev, lahko nadzorni organi ob upoštevanju okoliščin posameznega primera naložijo popravne ukrepe, na primer naročijo upravljavcem, da sprejmejo ukrepe za odpravo nezakonnosti začetne obdelave.** Ti ukrepi lahko vključujejo na primer izrek globe, začasno omejitev obdelave, izbris dela nabora podatkov, ki je bil obdelan nezakonito, ali, če to ni mogoče, glede na zadevna dejstva in ob upoštevanju sorazmernosti ukrepa, odreditev izbrisa celotnega nabora podatkov, ki se je uporabil za razvoj modela UI, in/ali celotnega modela UI. Nadzorni organi lahko pri ocenjevanju sorazmernosti predvidenega ukrepa upoštevajo ukrepe, ki jih lahko upravljavec uporabi za odpravo nezakonnosti prvotne obdelave (npr. ponovno učenje).
115. EOVP tudi poudarja, da lahko posamezniki, na katere se nanašajo osebni podatki, v primeru nezakonnite obdelave osebnih podatkov zahtevajo izbris svojih osebnih podatkov v skladu s pogoji iz člena 17 Splošne uredbe o varstvu podatkov in da lahko nadzorni organi odredijo izbris osebnih podatkov ⁸⁸*po uradni dolžnosti*.

⁸⁴ Sodba SEU z dne 4. maja 2023 v zadevi C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), točka 53.

⁸⁵ Smernice EOVP št. 07/2020 o pojmi upravljavec in obdelovalec iz SUVP, različica 2.1, sprejete 7. julija 2021, točka 55.

⁸⁶ Morda bo treba upoštevati posebna nacionalna pravila. Glejte na primer člen 2-decies italijanskega zakonika o varstvu podatkov (zakonodajni odlok 196/2003), ki določa, da se podatki, obdelani v nasprotju s pravili o varstvu podatkov, ne smejo uporabljati. To ne posega v druge nacionalne pravne okvire, kot je kazenska zakonodaja.

⁸⁷ V zvezi s tem glej uvodno izjavo 129 SUVP ter sodbo SEU z dne 26. septembra 2024 v zadevi C-768-21, *TR proti Land Hessen* (ECLI:EU:C:2024:785), točka 37; sodbo SEU z dne 7. decembra 2023 v združenih zadevah C-26/22 in C-64/22, *SCHUFA Holding (Libération de reliquat de dette)* (ECLI:EU:C:2023:958), točka 57; in sodbo SEU z dne 14. marca 2024 v zadevi C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), točka 34.

⁸⁸ Glejte v zvezi s tem mnenje EOVP št. 39/2021 o tem, ali bi lahko člen 58(2)(g) SUVP služil kot pravna podlaga za nadzorni organ, da po uradni dolžnosti odredi izbris osebnih podatkov, če posameznik, na katerega se nanašajo osebni podatki, take zahteve ni predložil, odstavek 28. V zvezi s tem glejte tudi sodbo SEU z dne 14. marca 2024 v zadevi C-46/23 *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), točka 42.

116. Nadzorni organi lahko pri ocenjevanju, ali je ukrep ustrezen, potreben in sorazmeren, med drugim upoštevajo tveganja za posameznike, na katere se nanašajo osebni podatki, resnost kršitve, tehnično in finančno izvedljivost ukrepa ter obseg zadevnih osebnih podatkov.
117. Nazadnje, EOVP opozarja, da ukrepi, ki so jih nadzorni organi sprejeli na podlagi SUVP, ne posegajo v ukrepe, ki so jih pristojni organi sprejeli na podlagi Akta o UI in/ali drugih veljavnih pravnih okvirov (npr. zakonodaje o civilni odgovornosti).
118. V naslednjih poglavjih bo EOVP obravnaval tri scenarije, zajete v vprašanju 4 v prošnji za mnenje, pri katerih so razlike v tem, ali se osebni podatki, obdelani za razvoj modela, ohranijo v modelu in/ali nadaljnjo obdelavo izvaja isti ali drug upravljavec.

3.4.1 Scenarij 1 Upravljavec nezakonito obdeluje osebne podatke za razvoj modela, osebni podatki ostanejo v modelu in jih nato obdeluje isti upravljavec (na primer v okviru uvajanja modela).

119. Ta scenarij se nanaša na vprašanje 4(i) v prošnji za mnenje, če upravljavec nezakonito obdeluje osebne podatke (tj. tako, da ne upošteva členov 5(1)(a) in 6 SUVP) za razvoj modela UI, pri čemer model UI ohranja informacije v zvezi z določeno ali določljivo fizično osebo in zato ni anonimen. Osebne podatke nato naknadno obdeluje isti upravljavec (na primer v okviru uvajanja modela). V zvezi s tem scenarijem EOVP podaja naslednje ugotovitve.
120. Pooblastilo nadzornega organa, da naloži popravne ukrepe za začetno obdelavo (kot je pojasnjeno v odstavkih 113, 114 in 115 zgoraj), bi načeloma vplivalo na poznejšo obdelavo (npr. če nadzorni organ odredi upravljavcu, da izbriše osebne podatke, ki so bili obdelani nezakonito, mu takšni popravni ukrepi ne bi omogočili poznejše obdelave osebnih podatkov, ki so bili predmet ukrepov).
121. Glede vpliva nezakonite obdelave v fazi razvoja na nadaljnjo obdelavo (na primer v fazi uvajanja) EOVP opozarja, da morajo nadzorni organi analizirati vsak primer posebej, pri čemer upoštevajo posebne okoliščine vsakega primera.
122. **Ali fazi razvoja in uvajanja vključujeta ločene namene (in tako pomenita ločene dejavnosti obdelave) in v kolikšni meri pomanjkanje pravne podlage za začetno dejavnost obdelave vpliva na zakonitost nadaljnje obdelave, je treba presoditi za vsak primer posebej, odvisno od okoliščin primera.**
123. Na primer, zlasti ob upoštevanju pravne podlage iz člena 6(1)(f) SUVP, kadar nadaljnja obdelava temelji na zakonitem interesu, bi bilo treba pri presoji zakonitega interesa upoštevati dejstvo, da je bila prvotna obdelava nezakonita (npr. glede na tveganja za posameznike, na katere se nanašajo osebni podatki, ali dejstvo, da posamezniki, na katere se nanašajo osebni podatki, morda ne pričakujejo tovrstne nadaljnje obdelave). V teh primerih lahko nezakonitost obdelave v razvojni fazi vpliva na zakonitost nadaljnje obdelave.

3.4.2 Scenarij 2 Upravljavec nezakonito obdeluje osebne podatke za razvoj modela, osebni podatki ostanejo v modelu in jih obdeluje drug upravljavec v okviru uvajanja modela

124. Ta scenarij se nanaša na vprašanje 4(i) v prošnji za mnenje. Od scenarija 1 (v oddelku 3.4.1 tega mnenja) se razlikuje po tem, da osebne podatke v okviru uvajanja modela UI naknadno obdeluje drug upravljavec.
125. EOVP opozarja, da je ugotavljanje vlog, dodeljenih tem različnim akterjem v okviru varstva podatkov, bistven korak pri ugotavljanju, katere obveznosti veljajo v skladu s SUVP in kdo je odgovoren za te obveznosti, ter da bi bilo treba pri ocenjevanju odgovornosti vsake stranke na podlagi SUVP upoštevati

tudi primere skupnega upravljanja. Zato bi bilo treba spodnje ugotovitve šteti za splošne elemente, ki bi jih morali nadzorni organi po potrebi upoštevati. V zvezi s tem scenarijem 2 EOVP podaja naslednje ugotovitve.

126. Najprej je treba opozoriti, da mora v skladu s členom 5(1)(a) SUVP v povezavi s členom 5(2) SUVP vsak upravljavec zagotoviti zakonitost obdelave, ki jo izvaja, in biti sposoben to dokazati. Zato bi morali nadzorni organi presoditi zakonitost obdelave, ki jo izvaja (i) upravljavec, ki je prvotno razvil model UI, in (ii) upravljavec, ki je pridobil model UI in sam obdeluje osebne podatke.
127. Drugič, premislek iz točk 113, 114 in 115 zgoraj je v obravnavanem primeru upošteven glede pooblastila nadzornih organov, da posredujejo v zvezi s prvotno obdelavo. Člen 17(1)(d) SUVP (izbris nezakonito obdelanih podatkov) in člen 19 SUVP (obveznost obveščanja glede popravka ali izbrisa osebnih podatkov ali omejitve obdelave) sta lahko glede na okoliščine primera pomembna tudi v tem okviru, na primer v zvezi z obveščanjem, ki bi ga moral upravljavec, ki razvija model, opraviti pri upravljavcu, ki model uporablja.
128. Tretjič, v zvezi z morebitnim vplivom nezakonitosti prvotne obdelave na nadaljnjo obdelavo, ki jo izvaja drug upravljavec, bi morali nadzorni organi takšno oceno opraviti za vsak primer posebej.
129. **Nadzorni organi bi morali upoštevati, ali je upravljavec, ki uporablja model, v okviru svojih obveznosti glede odgovornosti⁸⁹ opravil ustrezno presojo, da dokaže skladnost s členom 5(1)(a) in členom 6 SUVP, da lahko ugotovijo, da model UI ni bil razvit z nezakonito obdelavo osebnih podatkov.** Pri taki presoji, ki jo izvedejo nadzorni organi, bi bilo treba upoštevati, ali je upravljavec ocenil nekatera od meril, kot so vir podatkov in ali je model UI posledica kršitve SUVP, zlasti če je tako odločil nadzorni organ ali sodišče, tako da upravljavec, ki je uvedel model, ne bi mogel zanikati, da je bila prvotna obdelava nezakonita.
130. Upravljavec bi moral na primer proučiti, ali podatki izvirajo iz kršitve varstva osebnih podatkov ali če je bila obdelava predmet ugotovitve o kršitvi s strani nadzornega organa ali sodišča. **Stopnja presoje upravljavca in raven podrobnosti, ki jo pričakujejo nadzorni organi, se lahko razlikujeta glede na različne dejavnike, vključno z vrsto in stopnjo tveganj, ki jih prinaša obdelava v modelu UI med njegovo uvedbo v zvezi s posamezniki, na katere se nanašajo osebni podatki, katerih podatki so bili uporabljeni za razvoj modela.**
131. EOVP ugotavlja, da Akt o UI od ponudnikov sistemov UI z visokim tveganjem zahteva, da pripravijo izjavo EU o skladnosti⁹⁰ in da ta izjava vsebuje izjavo, da je zadevni sistem UI skladen z zakonodajo EU o varstvu podatkov⁹¹. EOVP ugotavlja, da takšna lastna izjava morda ne pomeni dokončne ugotovitve o skladnosti na podlagi SUVP. Kljub temu jo lahko nadzorni organi upoštevajo pri proučevanju določenega modela UI.
132. Isti premisleki iz odstavka 123 zgoraj so pomembni tudi v tem primeru. Kadar nadzorni organi preverijo, ali in kako je upravljavec presodil ustreznost zakonitega interesa kot pravno podlago za obdelavo, ki jo izvaja, bi bilo treba nezakonitost prvotne obdelave upoštevati v okviru presoje zakonitega interesa, na primer z oceno morebitnih tveganj, ki lahko nastanejo za posameznike, na katere se nanašajo osebni podatki in katerih osebni podatki so bili nezakonito obdelani, da bi razvili model. V okviru preizkusa uravnoteženja je treba ustrezno upoštevati različne vidike, bodisi tehnične narave (npr. obstoj filtrov ali omejitev dostopa, nameščenih med razvojem modela, ki jih poznejši upravljavec ne more zaobiti ali

⁸⁹ Člena 5(2) in 24(1) SUVP.

⁹⁰ Člen 16(g) in člen 47 Akta o UI.

⁹¹ Priloga V, točka 5 Akta o UI.

nanje vplivati in ki bi lahko preprečili dostop do osebnih podatkov ali njihovo razkritje) bodisi pravne narave (npr. naravo in resnost nezakonnosti prvotne obdelave).

3.4.3 Scenarij 3 Upravljapec nezakonito obdeluje osebne podatke za razvoj modela, nato pa zagotovi, da je model anonimiziran, preden isti ali drug upravljapec začne drugo obdelavo osebnih podatkov v okviru uvajanja

133. Ta scenarij se nanaša na vprašanje 4(ii) v prošnji za mnenje in se nanaša na primer, ko upravljapec nezakonito obdeluje osebne podatke za razvoj modela UI, vendar to stori na način, ki zagotavlja anonimizacijo osebnih podatkov, preden isti ali drug upravljapec začne drugo obdelavo osebnih podatkov v okviru uvajanja. Prvič, EOVP opozarja, da so nadzorni organi pristojni in imajo pooblastila za posredovanje v zvezi z obdelavo, povezano z anonimizacijo modela, in obdelavo, ki se izvaja v fazi razvoja. Zato lahko nadzorni organi glede na posebne okoliščine posameznega primera uvedejo korektivne ukrepe za to začetno obdelavo (kot je pojasnjeno v odstavkih 113, 114 in 115 zgoraj).
134. Če je mogoče dokazati, da naknadno delovanje modela UI ne vključuje obdelave osebnih podatkov, EOVP meni, da se SUVP ne bi uporabljala⁹². Zato nezakonitost začetne obdelave ne bi smela vplivati na nadaljnje delovanje modela. Vendar EOVP poudarja, da zgolj trditev o anonimnosti modela ne zadostuje za njegovo izzetje iz uporabe SUVP, in ugotavlja, da bi jo morali nadzorni organi presoditi ob upoštevanju ugotovitev, ki jih je EOVP predložil za obravnavo prvega vprašanja v prošnji za mnenje, v vsakem primeru posebej.
135. **Kadar upravljavci naknadno obdelujejo osebne podatke, zbrane v fazi uvajanja, potem ko je bil model anonimiziran, bi se v zvezi s temi dejavnostmi obdelave uporabljala SUVP. V teh primerih, kar zadeva SUVP, nezakonitost začetne obdelave ne bi smela vplivati na zakonitost obdelave, ki se izvaja v fazi uvajanja.**

4 Končne pripombe

136. To mnenje je namenjeno vsem nadzornim organom in bo v skladu s členom 64(5)(b) SUVP na voljo javnosti.

Za Evropski odbor za varstvo podatkov

Predsednica

Anu Talus

⁹² Uvodna izjava 26 SUVP.