

Mišljenje Odbora (članak 64.)



Mišljenje 28/2024 o određenim aspektima zaštite podataka povezanima s obradom osobnih podataka u kontekstu modela umjetne inteligencije

Doneseno 17. prosinca 2024.

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Sažetak

Tehnologije umjetne inteligencije stvaraju brojne mogućnosti i prednosti u širokom rasponu sektora i društvenih aktivnosti.

Štiteći temeljno pravo na zaštitu podataka, Općom uredbom o zaštiti podataka podupiru se te mogućnosti i promiču druga temeljna prava EU-a, uključujući pravo na slobodu mišljenja, izražavanja i informiranja, pravo na obrazovanje ili slobodu poduzetništva. Na taj je način Opća uredba o zaštiti podataka pravni okvir kojim se potiču odgovorne inovacije.

U tom kontekstu, uzimajući u obzir pitanja o zaštiti podataka koja proizlaze iz tih tehnologija, irsko nadzorno tijelo zatražilo je od Europskog odbora za zaštitu podataka da izda mišljenje o pitanjima opće primjene u skladu s člankom 64. stavkom 2. Opće uredbe. Zahtjev se odnosi na obradu osobnih podataka u kontekstu faza razvoja i uvođenja modela umjetne inteligencije („UI”). Podrobnije, u zahtjevu se tražilo sljedeće: (1) kad i kako se UI model može smatrati „anonimnim”; (2) kako voditelji obrade mogu dokazati primjerenost legitimnog interesa kao pravne osnove u fazama razvoja i (3) uvođenja; i (4) koje su posljedice nezakonite obrade osobnih podataka u fazi razvoja UI modela na naknadnu obradu ili rad UI modela.

Kad je riječ o prvom pitanju, u mišljenju se navodi da bi nadležna nadzorna tijela trebala ocjenjivati tvrdnje o anonimnosti UI modela ovisno o pojedinačnom slučaju jer EDPB smatra da se UI modeli trenirani s pomoću osobnih podataka ne mogu u svim slučajevima smatrati anonimnima. Kako bi se UI model smatrao anonimnim, (1) vjerojatnost izravnog (uključujući probabilističko) izdvajanja osobnih podataka koji se odnose na pojedince čiji su osobni podatci upotrijebljeni za razvoj modela i (2) vjerojatnost dobivanja, namjerno ili nenamjerno, takvih osobnih podataka na temelju upita, trebala bi biti beznačajna, uzimajući u obzir „*sva sredstva za koja postoji razumna vjerojatnost da će ih upotrebljavati voditelj obrade ili druga osoba upotrebljavati*”.

Kako bi provela svoju procjenu, nadzorna tijela trebala bi pregledati dokumentaciju koju je dostavio voditelj obrade u svrhu dokazivanja anonimnosti modela. U tom pogledu, u mišljenju se navodi nepreskriptivan i neiscrpan popis metoda koje voditelji obrade mogu koristiti pri dokazivanju anonimnosti i koje stoga nadzorna tijela mogu uzeti u obzir pri procjeni tvrdnje voditelja obrade o anonimnosti. To obuhvaća, na primjer, pristupe koje voditelji obrade primjenjuju tijekom faze razvoja kako bi spriječili ili ograničili prikupljanje osobnih podataka koji se upotrebljavaju za treniranje, smanjili njihovu prepoznatljivost, spriječili njihovo izdvajanje ili pružili jamstvo u pogledu najsuvremenije otpornosti na napade.

Kad je riječ o drugom i trećem pitanju, u mišljenju se iznose opća razmatranja koja nadzorna tijela trebaju uzeti u obzir prilikom procjene mogu li se voditelji obrade osloniti na legitimni interes kao odgovarajuću pravnu osnovu za obradu koja se provodi u kontekstu razvoja i uvođenja UI modela.

U mišljenju se podsjeća na to da ne postoji hijerarhija među pravnim osnovama predviđenih Općom uredbom i da voditelji obrade trebaju utvrditi odgovarajuću pravnu osnovu za svoje aktivnosti obrade. U mišljenju se zatim podsjeća na test u tri koraka koji bi se trebao provesti pri procjeni upotrebe legitimnog interesa kao pravne osnove, tj. (1) utvrđivanje legitimnog interesa koji voditelj obrade ili treća strana nastoje ostvariti; (2) analiza nužnosti obrade za potrebe legitimnog(ih) interesa koji se nastoji ostvariti (koji se također naziva „test nužnosti”); i (3) procjena da legitimni interesi nisu podređeni interesima ili temeljnim pravima i slobodama ispitanika (koji se također naziva „test ravnoteže”).

Kad je riječ o prvom koraku, u mišljenju se podsjeća na to da se interes može smatrati legitimnim ako su ispunjena sljedeća tri kumulativna kriterija: interes je (1) zakonit, (2) jasno i precizno artikuliran te (3) stvaran i prisutan (tj. nije spekulativan). Takav interes može, primjerice, obuhvaćati razvoj UI modela – s pomoću razvoja usluge razgovornog agenta za pomoć korisnicima ili tijekom njegova uvođenja – poboljšanje otkrivanja prijetnji u informacijskom sustavu.

Kad je riječ o drugom koraku, u mišljenju se podsjeća da procjena nužnosti podrazumijeva uzimanje u obzir sljedećega: (1) hoće li aktivnost obrade omogućiti ostvarivanje legitimnog interesa i (2) postoji li manje intruzivan način ostvarivanja tog interesa. Pri procjeni je li uvjet nužnosti ispunjen, nadzorna tijela trebala bi obratiti posebnu pozornost na količinu obrađenih osobnih podataka i je li ona proporcionalna za ostvarivanje predmetnog legitimnog interesa, također s obzirom na načelo smanjenja količine podataka.

Kad je riječ o trećem koraku, u mišljenju se podsjeća na to da bi se test ravnoteže trebao provesti uzimajući u obzir specifične okolnosti svakog slučaja. U njemu se zatim daje pregled elemenata koje nadzorna tijela mogu uzeti u obzir pri procjeni toga jesu li interesi voditelja obrade ili treće strane podređeni

interesima, temeljnim pravima i slobodama ispitanika.

U okviru trećeg koraka u mišljenju se ističu specifični rizici za temeljna prava koji se mogu pojaviti u fazama razvoja ili uvođenja UI modela. Pojašnjava se i da obrada osobnih podataka koja se odvija tijekom faza razvoja i uvođenja UI modela može na različite načine utjecati na ispitanike, što može biti pozitivno ili negativno. Kako bi procijenila takav učinak, nadzorna tijela mogu uzeti u obzir prirodu podataka koje modeli obrađuju, kontekst obrade i moguće naknadne posljedice obrade.

U mišljenju se dodatno naglašava uloga razumnih očekivanja ispitanika u testu ravnoteže. To može biti važno zbog složenosti tehnologija koje se upotrebljavaju u UI modelima i činjenice da bi ispitanicima moglo biti teško razumjeti raznolikost njihovih potencijalnih upotreba, kao i različite uključene aktivnosti obrade. U tom pogledu informacije pružene ispitanicima i kontekst obrade mogu biti među elementima koje treba uzeti u obzir kako bi se procijenilo mogu li ispitanici razumno očekivati da će se njihovi osobni podatci obrađivati. Kad je riječ o kontekstu, to može uključivati sljedeće: jesu li osobni podatci bili javno dostupni ili ne, prirodu odnosa između ispitanika i voditelja obrade (i postoji li poveznica između njih), prirodu usluge, kontekst u kojem su osobni podatci prikupljeni, izvor iz kojeg su podatci prikupljeni (tj. mrežno mjesto ili usluga na kojoj su osobni podatci prikupljeni i postavke privatnosti koje nude), moguće daljnje upotrebe modela i jesu li ispitanici zapravo svjesni da su njihovi osobni podatci uopće dostupni na internetu.

U mišljenju se podsjeća i na to da, ako se čini da interesi, prava i slobode ispitanika nadilaze legitimne interese voditelja obrade ili treće strane, voditelj obrade može razmotriti uvođenje mjera ublažavanja kako bi se ograničio učinak obrade na te ispitanike. Mjere ublažavanja ne treba miješati s mjerama koje je voditelj obrade ionako zakonski obavezan donijeti kako bi osigurao usklađenost s Općom uredbom. Osim toga, mjere bi trebale biti prilagođene okolnostima slučaja i značajkama UI modela, uključujući njegovu predviđenu upotrebu. U tom pogledu, u mišljenju se navodi ne iscrpan popis primjera mjera ublažavanja u odnosu na fazu razvoja (također u pogledu ekstrakcije podataka s interneta, eng. *web scraping*) i fazu uvođenja. Mjere ublažavanja mogu biti podložne brzom razvoju i trebale bi biti prilagođene okolnostima slučaja. Stoga nadzorna tijela i dalje moraju procjenjivati primjerenost mjera ublažavanja koje se provode na pojedinačnoj osnovi.

Kad je riječ o četvrtom pitanju, u mišljenju se općenito podsjeća na to da nadzorna tijela imaju diskrecijske ovlasti za procjenu mogućeg(ih) kršenja i odabir primjerenih, nužnih i proporcionalnih

mjera, uzimajući u obzir okolnosti svakog pojedinačnog slučaja. U mišljenju se zatim razmatraju tri scenarija.

U 1. scenariju osobni podatci zadržavaju se u UI modelu (što znači da se model ne može smatrati anonimnim, kako je detaljno navedeno u prvom pitanju) i naknadno ih obrađuje isti voditelj obrade (na primjer u kontekstu uvođenja modela). U mišljenju se navodi da bi se pitanje uključuju li faze razvoja i uvođenja odvojene svrhe (što bi činilo odvojene aktivnosti obrade) i u kojoj bi mjeri nepostojanje pravne osnove za početnu aktivnost obrade utjecalo na zakonitost naknadne obrade, trebalo ocjenjivati ovisno o pojedinačnom slučaju i o kontekstu samog slučaja.

U 2. scenariju osobni podatci zadržavaju se u modelu i obrađuje ih drugi voditelj obrade u kontekstu uvođenja modela. U tom pogledu u mišljenju se navodi da bi nadzorna tijela trebala uzeti u obzir je li voditelj obrade koji uvodi model proveo primjerenu procjenu u okviru svojih obveza odgovornosti za dokazivanje usklađenosti s člankom 5. stavkom 1. točkom (a) i člankom 6. Opće uredbe kako bi se utvrdilo da UI model nije razvijen nezakonitom obradom osobnih podataka. Tom bi se procjenom trebali uzeti u obzir, na primjer, izvor osobnih podataka i je li obrada u fazi razvoja bila predmet utvrđivanja povrede, posebno ako ju je utvrdilo nadzorno tijelo ili sud, te bi trebala uključivati manje ili više detalja, ovisno o rizicima koji proizlaze iz obrade u fazi uvođenja.

U okviru 3. scenarija voditelj obrade nezakonito obrađuje osobne podatke kako bi razvio UI model, a zatim osigurava da su anonimizirani prije nego što isti ili drugi voditelj obrade pokrene drugu obradu osobnih podataka u kontekstu uvođenja. U tom se pogledu u mišljenju navodi da, ako se može dokazati da daljnji rad UI modela ne podrazumijeva obradu osobnih podataka, EDPB smatra da se Opća uredba tada ne bi primjenjivala. Stoga nezakonitost početne obrade ne bi trebala utjecati na daljnji rad modela. Nadalje, EDPB smatra da bi se, kada voditelji obrade naknadno obrađuju osobne podatke prikupljene tijekom faze uvođenja, nakon što je model anonimiziran, Opća uredba o zaštiti podataka primjenjivala bi se u odnosu na te postupke obrade. U mišljenju se iznosi stajalište da bi se u tim slučajevima, kad je riječ o Općoj uredbi o zaštiti podataka, nezakonitost početne obrade ne bi trebala utjecati na zakonitost obrade provedene u fazi uvođenja.

Sadržaj

1	Uvod	6
1.1	Sažetak činjenica	6
1.2	Dopuštenost zahtjeva za mišljenje na temelju članka 64. stavka 2. Opće uredbe	8
2	Područje primjene i ključni pojmovi	9
2.1	Područje primjene mišljenja	9
2.2	Ključni pojmovi	10
2.3	Modeli umjetne inteligencije u kontekstu mišljenja.....	11
3	O osnovanosti zahtjeva	12
3.1	O prirodi UI modela u odnosu na definiciju osobnih podataka	12
3.2	O okolnostima u kojima se UI modeli mogu smatrati anonimnima i o dokazima povezanim s time 14	
3.2.1	Opće razmatranje o anonimizaciji u predmetnom kontekstu	14
3.2.2	Elementi za procjenu preostale vjerojatnosti identifikacije	16
3.3	O primjerenosti legitimnog interesa kao pravne osnove za obradu osobnih podataka u kontekstu razvoja i uvođenja UI modela	19
3.3.1	Općenita opažanja.....	19
3.3.2	Razmatranja o trima koracima procjene legitimnog interesa u kontekstu razvoja i uvođenja UI modela	21
3.4	O mogućem učinku nezakonite obrade u razvoju UI modela na zakonitost naknadne obrade ili rada UI modela	30
3.4.1	Scenarij 1. Voditelj obrade nezakonito obrađuje osobne podatke za razvijanje modela, osobni podatci zadržani su u modelu i naknadno ih obrađuje isti voditelj obrade (na primjer u kontekstu uvođenja modela)	32
3.4.2	Scenarij 2. Voditelj obrade nezakonito obrađuje osobne podatke za razvijanje modela, osobni podatci zadržani su u modelu i obrađuje ih drugi voditelj obrade u kontekstu uvođenja modela 32	
3.4.3	Scenarij 3. Voditelj obrade nezakonito obrađuje osobne podatke kako bi razvio model, a zatim osigurava da je model anonimiziran, prije nego što isti ili drugi voditelj obrade započne drugu obradu osobnih podataka u kontekstu uvođenja	33
4	Završne napomene.....	34

Europski odbor za zaštitu podataka,

uzimajući u obzir članak 63. i članak 64. stavak 2. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (u daljnjem tekstu: „Opća uredba o zaštiti podataka“),

uzimajući u obzir Sporazum o Europskom gospodarskom prostoru, a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.¹,

uzimajući u obzir članak 11. i članak 22. svojeg Poslovnika,

budući da:

1. Glavna je uloga Europskog odbora za zaštitu podataka (dalje u tekstu: **Odbor** ili **EDPB**) osigurati dosljednu primjenu Opće uredbe o zaštiti podataka u cijelom Europskom gospodarskom prostoru (**EGP**). Člankom 64. stavkom 2. Opće uredbe o zaštiti podataka propisano je da svako nadzorno tijelo, predsjednik Odbora ili Komisija mogu zatražiti da svaki predmet opće primjene ili s učincima u više od jedne države članice EGP-a pregleda Odbor kako bi dao mišljenje. Cilj ovog mišljenja je ispitati predmet opće primjene ili s učincima u više od jedne države članice EGP-a.

2. Mišljenje Odbora donosi se na temelju članka 64. stavka 3. Opće uredbe u vezi s člankom 10. stavkom 2. Poslovnika EDPB-a u roku od osam tjedana od trenutka kada su predsjednik i nadležna nadzorna tijela odlučili da je dokumentacija potpuna. Odlukom predsjednika taj se rok može produljiti za dodatnih šest tjedana, uzimajući u obzir složenost predmeta.

DONIO JE SLJEDEĆE MIŠLJENJE

1 Uvod

1.1 Sažetak činjenica

1. Dana 4. rujna 2024. irsko nadzorno tijelo („**irsko nadzorno tijelo**” ili „**nadzorno tijelo koje podnosi zahtjev**”) zatražilo je od Odbora da izda mišljenje u skladu s člankom 64. stavkom 2. Opće uredbe o zaštiti podataka u vezi s modelima umjetne inteligencije i obradom osobnih podataka („**zahtjev**”).
2. Predsjednik Odbora i irsko nadzorno tijelo smatrali su da je dokumentacija potpuna 13. rujna 2024. Sljedeći radni dan, 16. rujna 2024., tajništvo EDPB-a objavilo je dokumentaciju. S obzirom na složenost predmeta, predsjednik Odbora odlučio je produljiti zakonski rok u skladu s člankom 64. stavkom 3. Opće uredbe i člankom 10. stavkom 4. Poslovnika EDPB-a.
3. Zahtjev se odnosi na određene elemente treniranja, ažuriranja, razvoja i rada UI modela u kojima su osobni podatci dio relevantnog skupa podataka. Irsko nadzorno tijelo ističe da se zahtjev odnosi na ključna pitanja koja imaju velik utjecaj na ispitanike i voditelje obrade u EGP-u te da u ovoj fazi ne

¹ Upućivanja na „države članice” u ovom mišljenju treba tumačiti kao upućivanja na „države članice EGP-a”. Upućivanja na „Uniju” u ovom mišljenju treba tumačiti kao upućivanja na „EGP”.

postoji usklađeno stajalište među nacionalnim nadzornim tijelima ². Terminologija koja će se upotrebljavati za potrebe ovog mišljenja navedena je u odjeljcima 2.2. i 2.3. u nastavku.

4. Irsko nadzorno tijelo postavilo je sljedeća pitanja:

1. pitanje: Smatra li se da konačni UI model, koji je treniran s pomoću osobnih podataka, u nijednom slučaju ne odgovara definiciji osobnih podataka (kako je utvrđeno u članku 4. stavku 1. Opće uredbe o zaštiti podataka)?

Ako je odgovor na 1. pitanje potvrđan:

- i. U kojoj se fazi postupaka obrade koji vode do UI modela više ne obrađuju osobni podatci?
 - a) Kako se može dokazati da UI model ne obrađuje osobne podatke?
- ii. Postoje li čimbenici koji bi doveli do toga da se rad konačnog UI modela više ne smatra anonimnim?
 - a) Ako je to slučaj, kako se mogu dokazati mjere poduzete za ublažavanje, sprečavanje ili zaštitu od tih čimbenika (kako bi se osiguralo da UI model ne obrađuje osobne podatke)?

Ako je odgovor na prvo pitanje negativan:

- i. Koje su okolnosti u kojima bi se to moglo dogoditi?
 - a) Ako je to slučaj, kako se mogu dokazati mjere koje su poduzete kako bi se osiguralo da UI model ne obrađuje osobne podatke?

2. pitanje: Ako se voditelj obrade podataka za izradu, ažuriranje i/ili razvoj UI modela oslanja na legitimne interese kao pravnu osnovu za obradu osobnih podataka, na koji bi način trebao dokazati primjerenost legitimnih interesa kao pravne osnove, u odnosu na obradu podataka trećih strana, ali i u odnosu na podatke prve strane?

- i. Koja bi razmatranja taj voditelj obrade trebao uzeti u obzir kako bi osigurao da su interesi ispitanika, čiji se osobni podatci obrađuju, primjereno uravnoteženi s interesima tog voditelja obrade u kontekstu:
 - a) podataka trećih strana
 - b) podataka prve strane

3. pitanje: Nakon treniranja, ako se voditelj obrade podataka oslanja na legitimne interese kao pravnu osnovu za obradu osobnih podataka koja se odvija u okviru UI modela ili UI sustava čiji je UI model sastavni dio, kako bi voditelj obrade trebao dokazati primjerenost legitimnih interesa kao pravne osnove?

4. pitanje: Ako se utvrdi da je UI model izrađen, ažuriran ili razvijen s pomoću nezakonito obrađenih osobnih podataka, kakav to ima učinak, ako postoji, na zakonitost daljnje ili naknadne obrade ili rada UI modela, samostalno ili kao dio UI sustava, u sljedećim slučajevima:

- i. ako UI model samostalno ili kao dio sustava umjetne inteligencije obrađuje osobne podatke?
- ii. ako ni UI model ni UI model kao sastavni dio UI sustava ne obrađuju osobne podatke?

²Zahtjev, str. 1.

1.2 Dopuštenost zahtjeva za mišljenje na temelju članka 64. stavka 2. Opće uredbe

5. Člankom 64. stavkom 2. Opće uredbe posebno je predviđeno da Odbor pregleda svaki predmet opće primjene ili s učincima u više od jedne države članice kako bi dao mišljenje.
6. Nadzorno tijelo koje je podnijelo zahtjev uputilo je EDPB-u pitanja o aspektima zaštite podataka u kontekstu UI modela. U zahtjevu je navedeno da, iako mnoge organizacije sada upotrebljavaju UI modele, uključujući velike jezične modele („LLM-ovi”), njihov rad, treniranje i upotreba izazivaju „*niz dalekosežnih zabrinutosti u pogledu zaštite podataka*”³, što „*utječe na ispitanike u cijelom EU-u/EGP-u*”⁴.
7. U zahtjevu se, u osnovi, postavljaju pitanja o i. primjeni pojma osobnih podataka; ii. načelu zakonitosti, posebno u pogledu pravne osnove legitimnog interesa u kontekstu UI modela; kao i o iii. posljedicama nezakonite obrade osobnih podataka u fazi razvoja UI modela, na naknadnu obradu ili rad modela.
8. Odbor smatra da se zahtjev odnosi na „*predmet opće primjene*” u smislu članka 64. stavka 2. Opće uredbe. Konkretno, pitanje se odnosi na tumačenje i primjenu članka 4. stavka 1., članka 5. stavka 1. točke (a) i članka 6. Opće uredbe u vezi s obradom osobnih podataka u razvoju i uvođenju UI modela. Kako je istaknulo nadzorno tijelo koje je podnijelo zahtjev, primjena tih odredbi na UI modele otvara sistemska, apstraktna i nova pitanja⁵. Zbog brzog razvoja i uvođenja UI modela u sve više organizacija javljaju se specifična pitanja i, kako je istaknuto u zahtjevu, ⁶„*Europski odbor za zaštitu podataka imaće velike koristi od postizanja zajedničkog stajališta o pitanjima koja su postavljena u ovom zahtjevu, pri čemu su ta pitanja ključna za planirani rad Odbora u kratkoročnom i srednjoročnom razdoblju*”. Osim toga, UI tehnologije stvaraju brojne mogućnosti i koristi u širokom rasponu sektora i društvenih aktivnosti. Osim toga, Opća uredba o zaštiti podataka pravni je okvir koji potiče odgovorne inovacije. Iz toga slijedi da postoji opći interes za donošenje te procjene u obliku mišljenja Odbora kako bi se osigurala dosljedna primjena određenih odredbi Opće uredbe o u kontekstu UI modela.
9. Alternativni uvjet koji je naveden u članku 64. stavku 2. Opće uredbe odnosi se na pitanja „*s učincima u više od jedne države članice*”. Odbor podsjeća da se pojam „učinci” treba tumačiti *lato sensu* i stoga nije ograničen samo na pravne učinke⁷. Budući da se sve više UI modela trenira i upotrebljava ih sve veći broj organizacija u EGP-u, oni utječu na velik broj ispitanika diljem EGP-a, od kojih su neki već izrazili zabrinutost svojem nadležnom nadzornom tijelu⁸. Stoga EDPB smatra da pitanje koje je postavilo nadzorno tijelo koje podnosi zahtjev također ispunjava taj uvjet.
10. Zahtjev uključuje pisano obrazloženje o pozadini i razlozima za podnošenje pitanja Odboru, uključujući o relevantnom pravnom okviru. Stoga Odbor smatra da je zahtjev obrazložen u skladu s člankom 10. stavkom 3. Poslovnika EDPB-a.

³Zahtjev, str. 1.

⁴Ibid.

⁵Komunikacija, str. 2.

⁶Zahtjev, str. 1. Kako je navedeno u Programu rada Europskog odbora za zaštitu podataka za razdoblje 2024.–2025. donesenom 8. listopada 2024., dostupnom na https://www.edpb.europa.eu/system/files/2024-10/edpb_work_programme_2024-2025_en.pdf, Odbor planira objaviti, *među ostalim*, smjernice o anonimizaciji, pseudonimizaciji i ekstrakciji podataka u kontekstu generativne umjetne inteligencije.

⁷Europski odbor za zaštitu podataka, Interni dokument 3/2019 o unutarnjim smjernicama o članku 64. stavku 2. Opće uredbe o zaštiti podataka, donesen 8. listopada 2019., točka 15., dostupno na https://www.edpb.europa.eu/system/files/2022-07/internaledpb_document_201903_art64.2_en.pdf:

⁸Zahtjev, str. 1.–2.

11. U skladu s člankom 64. stavkom 3. Opće uredbe, EDPB ne izdaje mišljenje ako je već dao mišljenje o tom pitanju⁹. EDPB nije izdao mišljenje o istom pitanju i još nije dostavio odgovore na pitanja koja proizlaze iz zahtjeva.
12. Iz tih razloga Odbor smatra da je zahtjev dopušten i da bi pitanja koja proizlaze iz njega trebalo analizirati u ovom mišljenju („**Mišljenje**”) donesenom u skladu s člankom 64. stavkom 2. Opće uredbe.

2 Područje primjene i ključni pojmovi

2.1 Područje primjene mišljenja

13. Odbor se slaže s nadzornim tijelom koje podnosi zahtjev da, sa stajališta zaštite podataka, razvoj i uvođenje UI modela postavlja temeljna pitanja u vezi sa zaštitom podataka. Pitanja se posebno odnose na: i. kada se i kako UI model može smatrati „anonimnim” (prvo pitanje u zahtjevu); ii. kako voditelji obrade mogu dokazati primjerenost legitimnog interesa kao pravne osnove u razvoju (drugo pitanje u zahtjevu) i fazama uvođenja (treće pitanje u zahtjevu); i iii. ima li nezakonita obrada osobnih podataka u fazi razvoja posljedice na zakonitost naknadne obrade ili rada UI modela (četvrto pitanje u zahtjevu).
14. EDPB podsjeća da su nadzorna tijela odgovorna za praćenje primjene Opće uredbe i da bi trebala doprinijeti njezinoj dosljednoj primjeni u cijeloj Uniji¹⁰. Stoga je u nadležnosti nadzornih tijela da istraže određene UI modele i da pritom provode procjene ovisno o pojedinačnom slučaju.
15. Ovim se mišljenjem nadležnim nadzornim tijelima pruža okvir za procjenu posebnih slučajeva u kojima bi se mogla pojaviti (neka od) pitanja postavljenih u zahtjevu. Cilj ovog mišljenja nije da bude iscrpno, nego da pruži opća razmatranja o tumačenju relevantnih odredbi koje nadležna nadzorna tijela trebaju u najvećoj mogućoj mjeri uzeti u obzir u primjeni svojih istražnih ovlasti. Iako je ovo mišljenje upućeno nadležnim nadzornim tijelima i odnosi se na njihove aktivnosti i ovlasti, njime se ne dovode u pitanje obveze voditelja obrade i izvršitelja obrade u skladu s Općom uredbom. Konkretno, u skladu s načelom odgovornosti sadržanim u članku 5. stavku 2. Opće uredbe, voditelji obrade odgovorni su za sva načela koja se odnose na njihovu obradu osobnih podataka i moraju moći dokazati usklađenost s njima.
16. U nekim slučajevima se u mišljenju mogu navesti pojedini primjeri, ali uzimajući u obzir širok opseg pitanja uključenih u zahtjev, kao i različite vrste UI modela koji su u njemu obuhvaćeni, u ovom mišljenju neće se razmatrati svi mogući scenariji. Tehnologije povezane s UI modelima podložne su brzom razvoju; u skladu s tim, razmatranja EDPB-a u ovom mišljenju trebalo bi tumačiti imajući to u vidu.
17. **U ovom se mišljenju ne analiziraju odredbe u nastavku, koje i dalje mogu imati važnu ulogu u procjeni zahtjeva za zaštitu podataka koji se primjenjuju na UI modele:**
 - **Obrada posebnih kategorija podataka:** EDPB podsjeća na zabranu iz članka 9. stavka 1. Opće uredbe u pogledu obrade posebnih kategorija podataka i na ograničene iznimke iz članka 9. stavka 2. Opće uredbe¹¹. U tom je pogledu Sud Europske unije („Sud”) **dodatno pojasnio da „ako**

⁹ Članak 64. stavak 3. Opće uredbe i članak 10. stavak 4. Poslovnika EDPB-a.

¹⁰ Članak 51. stavak 1. Opće uredbe o zaštiti podataka i članak 51. stavak 2. Opće uredbe o zaštiti podataka.

¹¹ Vidjeti i Izvješće Europskog odbora za zaštitu podataka o radu radne skupine ChatGPT, doneseno 23. svibnja 2024., točku 18.: „Kad je riječ o obradi posebnih kategorija osobnih podataka, također se mora primjenjivati jedna od iznimaka iz članka 9. stavka 2. kako bi obrada bila zakonita. U načelu, jedna od tih iznimaka može biti članak 9. stavak 2. točka (e) Opće uredbe o zaštiti podataka. Međutim, sama činjenica da su osobni podatci javno dostupni ne znači da je „osoba čiji se podatci obrađuju očito objavila takve podatke” [...]”.

se skup podataka koji sadržava i osjetljive i neosjetljive podatke [...] prikuplja skupno, a da u trenutku prikupljanja nije moguće međusobno razdvojiti podatke, obrada tog skupa podataka mora se smatrati zabranjenom u smislu članka 9. stavka 1. Opće uredbe o zaštiti podataka ako sadržava barem jedan osjetljivi podatak i ne primjenjuje se nijedno odstupanje iz članka 9. stavka 2. te uredbe”¹². Nadalje, Sud EU-a također je naglasio da je „za potrebe primjene iznimke iz članka 9. stavka 2. točke (e) Opće uredbe o zaštiti podataka važno utvrditi je li ispitanik namjeravao, izričito i jasnom potvrdnom radnjom, predmetne osobne podatke učiniti dostupnima široj javnosti”¹³. Ta bi se razmatranja trebala uzeti u obzir kada obrada osobnih podataka u kontekstu UI modela uključuje posebne kategorije podataka.

- **Automatizirano donošenje odluka, uključujući izradu profila:** Postupci obrade koji se provode u kontekstu UI modela mogu biti obuhvaćeni područjem primjene članka 22. Opće uredbe, kojim se voditeljima obrade nameću dodatne obveze i pružaju se dodatne zaštitne mjere za ispitanike. EDPB u tom pogledu podsjeća na svoje Smjernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679¹⁴.
- **Usklađenost svrha:** U članku 6. stavku 4. Opće uredbe navode se, za određene pravne osnove, kriteriji koje voditelj obrade mora uzeti u obzir kako bi utvrdio je li obrada u drugu svrhu u skladu sa svrhom u koju su osobni podatci prvotno prikupljeni. Ta odredba može biti relevantna u kontekstu razvoja i uvođenja UI modela, a njezinu bi primjenjivost trebala ocijeniti nadzorna tijela.
- **Procjene učinka na zaštitu podataka** (članak 35. Opće uredbe): Procjene učinka na zaštitu podataka važan su element odgovornosti jer će obrada u kontekstu UI modela vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca,¹⁵.
- **Načelo tehničke zaštite podataka** (članak 25. stavak 1. Opće uredbe o zaštiti podataka): Tehnička zaštita podataka ključna je zaštitna mjera koju nadzorna tijela procjenjuju u kontekstu razvoja i uvođenja UI modela.

2.2 Ključni pojmovi

18. Kao uvodnu napomenu, EDPB želi pojasniti terminologiju i pojmove koje upotrebljava u ovom mišljenju, i to samo za potrebe ovog mišljenja:

- „**Podatci prve strane**” odnosi se na osobne podatke koje je voditelj obrade prikupio od ispitanika.
- „**Podatci trećih strana**” odnose se na osobne podatke koje voditelji obrade nisu dobili od ispitanika, nego su prikupljeni ili primljeni od treće strane, primjerice od informacijskog posrednika ili su prikupljeni ekstrakcijom podataka s interneta (eng. *web scraping*).

¹²Presuda Suda EU-a od 4. srpnja 2023., predmet C-252/21, „Meta protiv Bundeskartellamt” (ECLI:EU:C:2023:537), točka 89.

¹³Presuda Suda EU-a od 4. srpnja 2023., predmet C-252/21, „Meta protiv Bundeskartellamt” (ECLI:EU:C:2023:537), točka 77.

¹⁴Radna skupina iz članka 29. („WP29”) Smjernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679, kako su zadnje revidirane i donesene 6. veljače 2018., koje je Europski odbor za zaštitu podataka potvrdio 25. svibnja 2018. Vidjeti i presudu Suda EU-a od 7. prosinca 2023., predmet C-634/21, *SCHUFA Holding i dr.* (ECLI:EU:C:2023:957).

¹⁵Dokument Radne skupina iz članka 29. Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik” u smislu Uredbe 2016/679, donesene 4. listopada 2017., koje je potvrdio EDPB 25. svibnja 2018.

- „**Ekstrakcija podataka s interneta**” uobičajena je tehnika za prikupljanje informacija iz javno dostupnih internetskih izvora. Informacije izvučene putem, primjerice, usluga kao što su vijesti, društveni mediji, rasprave na forumima i osobna mrežna mjesta mogu sadržavati osobne podatke.
- Zahtjev se odnosi na „**životni ciklus**” **UI modela**, kao i na različite faze koje se, među ostalim, odnose na „stvaranje”, „razvoj”, „treniranje”, „ažuriranje”, „doradu”, „rad” ili „naknadno treniranje” UI modela. EDPB prima na znanje da se, ovisno o okolnostima, takve faze mogu odvijati tijekom razvoja i uvođenja UI modela te da mogu uključivati obradu osobnih podataka u različite svrhe obrade. Međutim, za potrebe ovog mišljenja EDPB smatra da je važno pojednostavniti kategorizaciju faza koje će se vjerojatno odvit. Stoga EDPB za potrebe ovog mišljenja upućuje na „**fazu razvoja**” i na „**fazu uvođenja**”. Razvoj UI modela obuhvaća sve faze prije uvođenja UI modela i uključuje, među ostalim, razvoj koda, prikupljanje osobnih podataka za treniranje, prethodnu obradu osobnih podataka za treniranje, kao i samo treniranje. Uvođenje UI modela obuhvaća sve faze koje se odnose na upotrebu UI modela i može uključivati sve operacije koje se provode nakon faze razvoja. EDPB i dalje je svjestan različitih slučajeva upotrebe i njihovih mogućih posljedica u smislu obrade osobnih podataka. Stoga bi nadzorna tijela trebala razmotriti jesu li opažanja iz ovog mišljenja relevantna za obradu koju procjenjuju.
- EDPB također ističe da se, prema potrebi, pojam „**treniranje**” odnosi na dio faze razvoja u kojem UI modeli uče iz podataka kako bi obavljali zadaću za koju su namijenjeni (kako je objašnjeno u sljedećem odjeljku ovog mišljenja).
- Pojam i područje primjene **UI modela**, kako ih EDPB shvaća za potrebe ovog mišljenja, detaljnije su utvrđeni u sljedećem posebnom odjeljku.

2.3 Modeli umjetne inteligencije u kontekstu mišljenja

19. U Aktu EU-a o umjetnoj inteligenciji („**Akt o umjetnoj inteligenciji**”) „UI sustav”¹⁶ definiran je kao „*strojni sustav dizajniran za rad s promjenjivim razinama autonomije i koji nakon uvođenja može pokazati prilagodljivost te koji, za eksplicitne ili implicitne ciljeve, iz ulaznih vrijednosti koje prima, zaključuje kako generirati izlazne vrijednosti kao što su predviđanja, sadržaj, preporuke ili odluke koji mogu utjecati na fizička ili virtualna okruženja*”¹⁷. U uvodnoj izjavi 12. Akta o umjetnoj inteligenciji dodatno se objašnjava pojam „UI sustav”. Ključna značajka UI sustava njihova je sposobnost izvođenja zaključaka. Tehnike koje omogućuju zaključivanje pri izgradnji UI sustava uključuju pristupe strojnog učenja i pristupe temeljene na logici i znanju.
20. S druge strane, „UI modeli” definirani su samo neizravno u Aktu o umjetnoj inteligenciji: „*Iako su UI modeli ključne komponente UI sustava, oni sami po sebi nisu UI sustavi. UI modeli zahtijevaju dodavanje dodatnih komponenti kao što je korisničko sučelje, kako bi postali UI sustavi. UI modeli obično su integrirani u UI sustave i čine njihov sastavni dio.*”¹⁸.
21. EDPB razumije da je definicija UI modela koja je predložena u zahtjevu uža od one iz Akta o umjetnoj inteligenciji jer se odnosi na „UI model” koji „*obuhvaća proizvod koji proizlazi iz mehanizama treniranja koji se primjenjuju na skup podataka za treniranje, u kontekstu umjetne inteligencije, strojnog učenja,*

¹⁶ Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji).

¹⁷ Članak 3. stavak 1. Akta o umjetnoj inteligenciji.

¹⁸Uvodna izjava 97. Akta o umjetnoj inteligenciji.

dubokog učenja ili drugog konteksta u vezi s obradom” i dodatno navodi da se „pojam primjenjuje na UI modele koji su namijenjeni za daljnje treniranje, doradu i/ili razvoj, kao i UI modele koji nisu”.¹⁹

22. Na temelju toga EDPB je usvojio ovo mišljenje pod uvjetom da će se sustav umjetne inteligencije (UI sustav) oslanjati na UI model kako bi ostvario svoj predviđeni cilj uključivanjem modela u širi okvir (npr. UI sustav za korisničku podršku može upotrebljavati UI model treniran na prijašnjim podatcima iz razgovora kako bi pružio odgovore na upite korisnika).
23. Nadalje, UI modeli (ili „**modeli**”) relevantni za ovo mišljenje jesu oni modeli razvijeni u okviru postupka treniranja. Takav postupak treniranja dio je faze razvoja kada modeli uče iz podataka kako bi obavljali zadaću za koju su namijenjeni. Stoga je za postupak treniranja potreban skup podataka iz kojeg će model utvrditi i „naučiti” obrasce. U tim će slučajevima model upotrebljavati različite tehnike kako bi se stvorio prikaz znanja izdvojenog iz skupa podataka za treniranje. To je posebno slučaj sa strojnim učenjem.
24. U praksi je svaki UI model algoritam čije je funkcioniranje određeno skupom elemenata. Na primjer, modeli dubokog učenja često su u obliku neuronske mreže s višestrukim slojevima koje se sastoje od čvorišta povezanih rubovima koji imaju težinske faktore koji se prilagođavaju tijekom treniranja kako bi se naučili odnosi između ulaznih i izlaznih podataka. Značajke jednostavnog modela dubokog učenja bile bi sljedeće: i. vrsta i veličina svakog sloja, ii. težinski faktor pripisan svakom rubu (ponekad se nazivaju „parametri”), iii. aktivacijske funkcije²⁰ između slojeva i, po mogućnosti, iv. druge operacije koje se mogu dogoditi između slojeva. Na primjer, pri treniranju jednostavnog modela dubokog učenja za razvrstavanje slika, ulazni podatci („**slikovni pikseli**”) bit će povezani s izlaznim podatcima, a težinski se faktori mogu prilagoditi kako bi se većinu vremena dobio pravi rezultat.
25. Drugi primjeri modela dubokog učenja uključuju velike jezične modele i generativnu umjetnu inteligenciju, koji se upotrebljavaju za npr. stvaranje sadržaja nalik ljudskom sadržaju i stvaranje novih podataka.
26. **Na temelju prethodno navedenih razmatranja, u skladu sa zahtjevom, područje primjene ovog mišljenja obuhvaća samo podskup UI modela koji su rezultat treniranja takvih modela s osobnim podatcima.**

3 O osnovanosti zahtjeva

3.1 O prirodi UI modela u odnosu na definiciju osobnih podataka

27. U članku 4. stavku 1. Opće uredbe osobni podatci definirani su kao „*znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi*” (tj. ispitanika). Nadalje, u uvodnoj izjavi 26. Opće uredbe navodi se da se načela zaštite podataka ne bi trebala primjenjivati na anonimne informacije, odnosno informacije koje se ne odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, uzimajući u obzir „*sva sredstva*” koja voditelj obrade ili bilo koja druga osoba „*mogu po svemu sudeći upotrijebiti*”. To uključuje: i. podatke koji nikada nisu bili povezani s osobom čiji je identitet utvrđen ili se može utvrditi i ii. osobne podatke koji su anonimizirani tako da se identitet ispitanika ne može utvrditi ili se više ne može utvrditi.

¹⁹ Zahtjev, str. 3.

²⁰ Tj. funkcije koje na temelju ulaznih podataka i težinskih faktora izračunavaju izlazne podatke neuronskog čvora koji će se zatim poslati na sljedeći sloj neuronske mreže.

28. U skladu s tim,²¹ na prvo pitanje u zahtjeva može se odgovoriti analizom treba li se UI model koji proizlazi iz treniranja koje uključuje obradu osobnih podataka u svim slučajevima smatrati anonimnim. Na temelju formuliranja pitanja EDPB će u ovom odjeljku upućivati na postupak „treniranja” UI modela.
29. Prije svega, EDPB želi iznijeti sljedeća opća razmatranja. UI modeli, bez obzira na to jesu li trenirani s pomoću osobnih podataka ili ne, obično su osmišljeni za donošenje predviđanja ili izvođenje zaključaka, tj. osmišljeni su za zaključivanje. Nadalje, UI modeli trenirani s pomoću osobnih podataka često su osmišljeni tako da donose zaključke o pojedincima koji se razlikuju od onih čiji su se osobni podatci upotrebljavali za treniranje UI modela. Međutim, neki su UI modeli posebno osmišljeni za pružanje osobnih podataka o pojedincima čiji su osobni podatci upotrijebljeni za treniranje modela ili na neki način za stavljanje takvih podataka na raspolaganje. U tim će slučajevima takvi UI modeli sami po sebi (i obično nužno) uključivati informacije koje se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi te će stoga uključivati obradu osobnih podataka. Stoga se te vrste UI modela ne mogu smatrati anonimnima. To bi bio slučaj za, primjerice, i. generativni model dorađen na glasovnim snimkama pojedinca kako bi se oponašao njegov glas ili ii. bilo koji model osmišljen da na traženje informacija o određenoj osobi odgovori s osobnim podacima korištenima u treniranju.
30. Na temelju prethodno navedenih razmatranja, u odgovoru na prvo pitanje iz zahtjeva EDPB usredotočuje se na situaciju s UI modelima koji nisu osmišljeni za pružanje osobnih podataka povezanih s podacima za treniranje.
31. EDPB smatra da, čak i ako UI model nije namjerno osmišljen kako bi iz podataka za treniranje proizveo informacije koje se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, informacije iz skupa podataka za treniranje, uključujući osobne podatke, i dalje mogu biti „apsorbirane” u parametrima modela, odnosno prikazane putem matematičkih objekata. Mogu se razlikovati od izvornih točaka podataka za treniranje, ali i dalje mogu zadržati izvorne informacije o tim podacima, koje se u konačnici mogu izdvojiti ili na drugi način dobiti, izravno ili neizravno, iz modela. Kad god se informacije koje se odnose na pojedince čiji je identitet utvrđen ili se može utvrditi, a čiji su osobni podatci upotrijebljeni za treniranje modela, mogu dobiti iz UI modela sa sredstvima za koja je razumno vjerojatno da će se upotrebljavati, može se zaključiti da takav model nije anoniman.
32. U tom se pogledu u zahtjevu navodi da „*postojeće istraživačke publikacije naglašavaju neke moguće slabe točke koje mogu postojati u UI modelima i koje bi mogle dovesti do obrade osobnih podataka,*²² *kao i do obrade osobnih podataka koja se može dogoditi kada se modeli upotrebljavaju za upotrebu s drugim podacima, bilo putem aplikacijskih programskih sučelja (API) ili sučelja za upit (eng. prompt interfaces)*”²³.
33. Isto tako, istraživanje o izdvajanju podataka za treniranje posebno je dinamično²⁴. Ono pokazuje da je u nekim slučajevima moguće upotrijebiti sredstva za koja je razumno vjerojatno da će izdvojiti osobne

²¹ „Smatra li se da konačni UI model, koji je treniran s pomoću osobnih podataka, u nijednom slučaju ne odgovara definiciji osobnih podataka (kako je utvrđeno u članku 4. stavku 1. Opće uredbe o zaštiti podataka)?”

²² Kao što su napadi radi otkrivanja korištenih podataka za treniranje (eng. *membership inference attack*) ([OWASP](#)) i napadi na inverziju modela (napadi eng. *model inversion attacks*) ([OWASP](#) i [Veale et al](#), 2018.).

²³ Zahtjev, str. 1.–2.

²⁴ Vidjeti, u tom pogledu, primjerice: 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, dostupno na <http://dx.doi.org/10.1098/rsta.2018.0083>; ii. Brown H., Lee K., Miresghallah F., Shokri R. i Tramèr F., *What Does it Mean for a Language Model to Conserve Privacy?* 2022., ACM Digital Library, FAccT’22, 20. lipnja 2022., Seul, Republika Koreja, dostupno 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 Mitigations*,

podatke iz nekih UI modela ili jednostavno slučajno dobiti osobne podatke putem interakcija s UI modelom (na primjer kao dio UI sustava). Kontinuirani istraživački napor u tom području pomoći će u daljnjoj procjeni preostalih rizika od regurgitacije²⁵ i izdvajanja osobnih podataka u svakom pojedinom slučaju.

34. **Na temelju prethodno navedenih razmatranja, EDPB smatra da se UI modeli trenirani na osobnim podacima ne mogu u svim slučajevima smatrati anonimnima. Umjesto toga, utvrđivanje anonimnosti UI modela trebalo bi se procjenjivati od slučaja do slučaja na temelju posebnih kriterija.**

3.2 O okolnostima u kojima se UI modeli mogu smatrati anonimnima i o dokazima povezanim s time

35. Kad je riječ o pitanju 1. iz zahtjeva²⁶, od EDPB-a se traži da pojasni okolnosti u kojima se UI model, koji je treniran s pomoću osobnih podataka, može smatrati anonimnim. Kad je riječ o pitanju 1. točki (i) podtočki (a) zahtjeva²⁷, od EDPB-a se traži da pojasni koje bi dokaze i/ili dokumentaciju nadzorna tijela trebala uzeti u obzir pri procjeni anonimnosti UI modela.

3.2.1 Opće razmatranje o anonimizaciji u predmetnom kontekstu

36. Upotreba izraza „*svi podatci*” u definiciji „*osobnih podataka*” u članku 4. stavku 1. Opće uredbe odražava cilj da se tom pojmu dodijeli široko područje primjene koje obuhvaća sve vrste informacija pod uvjetom da se „*odnose*” na ispitanike, čiji je identitet utvrđen ili se može utvrditi izravno ili neizravno.
37. Informacije se mogu odnositi na pojedinca čak i ako su tehnički organizirane ili kodirane (na primjer, u isključivom strojno čitljivom formatu, bilo vlasničkom ili otvorenom) na način da povezanost s tim pojedincem nije odmah očigledna. U takvim se slučajevima softverske aplikacije mogu upotrebljavati za jednostavno utvrđivanje, prepoznavanje i izdvajanje određenih podataka. To se posebno odnosi na UI modele u kojima parametri predstavljaju statističke odnose između podataka za treniranje i u kojima bi moglo biti moguće izdvojiti točne ili netočne (zbog statističke izvedenosti) osobne podatke, ili izravno iz veze među podacima uključenima u model ili postavljanjem upita tom modelu.
38. Budući da UI modeli obično ne sadržavaju zapise koji mogu biti izravno izolirani ili povezani, nego parametre koji predstavljaju probabilističke povezanosti među podacima sadržanima u modelu, u realističnim scenarijima moguće je izvesti zaključke o²⁸ informacijama iz modela, kao što je utvrđivanje

siječanj 2024., National Institute of Standards and Technology, dostupno 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. lipnja 2021., dostupno na <https://arxiv.org/pdf/2012.07805>; v. Fredrikson M., Jha S., Ristenpart T., *Model Inversion Attacks, Model Inversion Information and Basic Countermeasures*, ACM Digital Library, 12. listopada 2015., dostupno 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. travnja 2020., dostupno na <https://arxiv.org/pdf/1911.07135>.

²⁵ Kad je riječ o UI sustavu koji se temelji na generativnoj umjetnoj inteligenciji, regurgitacija odgovara situaciji u kojoj bi se rezultati izravno odnosili na podatke za treniranje.

²⁶ „Koje su okolnosti u kojima bi se to moglo dogoditi?”

²⁷ „Ako je odgovor potvrđan, kako se mogu dokazati koraci koji su poduzeti kako bi se osiguralo da UI model ne obrađuje osobne podatke?”

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

pripadnosti. Stoga, kako bi se nadzorno tijelo složilo s voditeljem obrade da se određeni UI model može smatrati anonimnim, nadzorno bi tijelo trebalo barem provjeriti je li primilo dostatne dokaze, uz razumna sredstva: i. da se osobni podatci povezani s podacima za treniranje ne mogu ²⁹ izdvojiti iz modela i ii. da se rezultati dobiveni pretraživanjem modela ne odnose na ispitanike čiji su osobni podatci upotrijebljeni za treniranje modela.

39. Nadzorna tijela trebala bi uzeti u obzir tri elementa prilikom procjene jesu li ti uvjeti ispunjeni.
40. Kao prvo, nadzorna tijela trebala bi uzeti u obzir elemente utvrđene u najnovijim mišljenjima Radne skupine iz članka 29. i/ili smjernicama EDPB-a o tom pitanju. Kad je riječ o anonimizaciji na datum ovog mišljenja, nadzorna tijela trebala bi uzeti u obzir elemente iz mišljenja 05/2014 Radne skupine iz članka 29. o tehnikama anonimizacije („mišljenje 5/2014 Radne skupine iz članka 29.”), u kojem se navodi da se podatci mogu smatrati anonimnima ako nije moguće izdvojiti pojedine informacije, povezati informacije i donijeti zaključke o informacijama iz skupa podataka koji se smatra anonimnim³⁰. U njemu se navodi i da, „kad god prijedlog ne ispunjava jedan od kriterija, trebala bi se provesti temeljita procjena identifikacijskih rizika”³¹. **S obzirom na prethodno navedenu vjerojatnost izdvajanja i izvođenja zaključaka, EDPB smatra da će UI modeli vrlo vjerojatno zahtijevati takvu temeljitu procjenu rizika u vezi s identifikacijom.**
41. Kao drugo, tu bi procjenu trebalo provesti uzimajući u obzir „sva sredstva koja voditelj obrade ili druga osoba razumno mogu upotrijebiti” za identifikaciju pojedinaca³², a određivanje tih sredstava trebalo bi se temeljiti na objektivnim čimbenicima, kako je objašnjeno u uvodnoj izjavi 26. Opće uredbe o zaštiti podataka, koji mogu uključivati:

(ii) Crețu A.M., Guépin F., i De Montjoye Y.A., *Correlation inference attacks against machine learning models*. Sci. Adv.10, eadj9260(2024). DOI:10.1126/sciadv.adj9260 dostupno na <https://www.science.org/doi/10.1126/sciadv.adj9260>

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

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

(v) Hu H., *Membership Inference Attacks and Defenses on Machine Learning Models Literature*, dostupno 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. studenog 2023., dostupno 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. ožujka 2017., dostupno 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. svibnja 2024., dostupno 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. lipnja 2024., dostupno na <https://arxiv.org/abs/2406.02027v1>

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

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

²⁹ Izdvajanje posebno uključuje slučaj u kojem se osobni podatci izvode iz samog UI modela, uz malu ili nikakvu upotrebu sučelja za upite.

³⁰ Mišljenje 5/2014 Radne skupine iz članka 29., stranica 24.

³¹ Mišljenje 5/2014 Radne skupine iz članka 29., stranica 24.

³² Presuda Suda EU-a od 19. listopada 2016., predmet C-582/14, *Breyer protiv Savezne Republike Njemačke* (ECLI:EU:C:2016:779), točka 43.

- a. značajke samih podataka za treniranje, UI modela i postupka treniranja³³
 - b. kontekst u kojem se UI model objavljuje i/ili obrađuje³⁴
 - c. dodatne informacije koje bi omogućile identifikaciju i koje bi mogle biti dostupne određenoj osobi
 - d. troškove i vrijeme koje bi osoba trebala za dobivanje takvih dodatnih informacija (ako joj one već nisu dostupne)³⁵ i
 - e. tehnologiju dostupnu u trenutku obrade, kao i tehnološki razvoj³⁶.
42. Kao treće, nadzorna tijela trebala bi razmotriti jesu li voditelji obrade procijenili rizik identifikacije od strane voditelja obrade i različitih vrsta „*drugih osoba*“, uključujući nenamjerne treće strane koje pristupaju UI modelu, također uzimajući u obzir može li se razumno smatrati da mogu pristupiti predmetnim podacima ili ih obrađivati.
43. **Ukratko, EDPB smatra da bi, kako bi se UI model smatrao anonimnim, s pomoću razumnih sredstava, i. vjerojatnost izravnog (uključujući probabilističkog) izdvajanja osobnih podataka u vezi s pojedincima čiji su osobni podatci korišteni za uvježbavanje modela, kao i ii. vjerojatnost pribavljanja, namjerno ili ne, takvih osobnih podataka na temelju upita, trebala biti beznačajna³⁷ za bilo kojeg ispitanika. Nadzorna tijela trebala bi automatski uzeti u obzir da će UI modeli vjerojatno zahtijevati temeljitu evaluaciju vjerojatnosti identifikacije kako bi se došlo do zaključka o njihovoj mogućoj anonimnoj prirodi. Tu bi vjerojatnost trebalo procijeniti uzimajući u obzir „*sva sredstva za koja je razumno vjerojatno da će ih voditelj obrade ili druga osoba upotrebljavati*“, a trebalo bi uzeti u obzir i nenamjernu (ponovnu) uporabu ili otkrivanje modela.**

3.2.2 Elementi za procjenu preostale vjerojatnosti identifikacije

44. Iako bi se mogle poduzeti mjere i u fazi razvoja i u fazi uvođenja kako bi se smanjila vjerojatnost dobivanja osobnih podataka iz UI modela, u procjeni anonimnosti UI modela također bi trebalo razmotriti izravan pristup modelu.
45. Osim toga, nadzorna tijela trebala bi procijeniti, od slučaja do slučaja, jesu li mjere koje je proveo voditelj obrade, kako bi osigurao i dokazao da je UI model anoniman, primjerene i učinkovite.
46. Konkretno, zaključak procjene nadzornog tijela može se razlikovati između javno dostupnog UI modela, koji je dostupan nepoznatom broju osoba s nepoznatim rasponom metoda za pokušaj izdvajanja osobnih podataka, i unutarnjeg UI modela koji je dostupan samo zaposlenicima. Iako bi u oba slučaja nadzorna tijela trebala provjeriti jesu li voditelji obrade ispunili svoju obvezu odgovornosti iz članka 5. stavka 2. i članka 24. Opće uredbe, „*sredstva za koja je razumno vjerojatno da će ih druge osobe upotrebljavati*“ mogu utjecati na raspon i prirodu mogućih scenarija koje treba razmotriti. Stoga,

³³ To uključuje značajke kao što su jedinstvenost zapisa u podacima za treniranje, preciznost informacija, objedinjavanje, randomizacija, a posebno način na koji one utječu na osjetljivost na identifikaciju.

³⁴ To uključuje kontekstualne elemente, kao što su ograničavanje pristupa samo na pojedine osobe i pravne zaštitne mjere.

³⁵ Presuda Suda EU-a od 7. ožujka 2024., predmet C-479/22 P, *OC protiv Europske komisije* (ECLI:EU:C:2024:215), točka 50.

³⁶ Presuda Suda EU-a od 7. ožujka 2024., predmet C-479/22 P, *OC protiv Europske komisije* (ECLI:EU:C:2024:215), točka 50.

³⁷ Presuda Suda EU-a od 19. listopada 2016., predmet C-582/14, *Breyer protiv Savezne Republike Njemačke* (ECLI:EU:C:2016:779), točka 46., i presuda Suda EU-a od 7. ožujka 2024., predmet C-479/22 P, *OC protiv Europske komisije* (ECLI:EU:C:2024:215), točka 51.

ovisno o kontekstu razvoja i uvođenja modela, nadzorna tijela mogu razmotriti različite razine testiranja i otpornosti na napade.

47. U tom pogledu EDPB u nastavku navodi nepreskriptivan i neiscrpan popis mogućih elemenata koje nadzorna tijela mogu uzeti u obzir pri procjeni tvrdnje voditelja obrade o anonimnosti. Drugi pristupi mogu biti mogući ako pružaju jednaku razinu zaštite, posebno uzimajući u obzir najnovija dostignuća.
48. Prisutnost ili odsutnost elemenata navedenih u nastavku nije odlučujući kriterij za procjenu anonimnosti UI modela.

3.2.2.1 Izrada UI modela

49. Kad je riječ o osmišljavanju UI modela, nadzorna tijela trebala bi ocijeniti pristupe koje su voditelji obrade poduzeli tijekom faze razvoja. U tom bi pogledu trebalo razmotriti primjenu i učinkovitost četiriju ključnih područja (navedenih u nastavku).

Odabir izvora

50. Prvo područje procjene uključuje ispitivanje odabira izvora koji se upotrebljavaju za treniranje UI modela. To uključuje evaluaciju, koju provode nadzorna tijela, svih koraka poduzetih kako bi se izbjeglo ili ograničilo prikupljanje osobnih podataka, uključujući, među ostalim, i. primjerenost kriterija odabira; ii. relevantnost i prikladnost odabranih izvora s obzirom na predviđenu svrhu; i iii. jesu li isključeni neprimjereni izvori.

Priprema podataka i smanjenje količine podataka

51. Drugo područje evaluacije odnosi se na pripremu podataka za fazu treniranja. Nadzorna tijela trebala bi posebno ispitati: i. je li razmotrena upotreba anonimnih i/ili osobnih podataka koji su pseudonimizirani; i ii. ako je odlučeno da se neće upotrijebiti takve mjere, razloge za tu odluku, uzimajući u obzir predviđenu svrhu; iii. strategije smanjenja količine podataka koje se primjenjuju za ograničavanje količine osobnih podataka uključenih u postupak treniranja; i iv. sve postupke filtriranja podataka koji se provode prije treniranja modela kako bi se uklonili nevažni osobni podatci.

Metodološki odabiri u pogledu treniranja

52. Treće područje evaluacije odnosi se na odabir pouzdanih metoda u razvoju UI modela. Nadzorna tijela trebala bi procijeniti metodološke odluke kojima se može znatno smanjiti ili ukloniti prepoznatljivost, uključujući, među ostalim, sljedećega: i. primjenjuju li se u toj metodologiji metode reguliranja kako bi se poboljšala generalizacija modela i smanjila prekomjerna prilagodba i, što je najvažnije, ii. je li voditelj obrade primijenio primjerene i učinkovite tehnike zaštite privatnosti (npr. diferencijalna privatnost).

Mjere koje se odnose na izlazne vrijednosti modela

53. Posljednje područje evaluacije odnosi se na sve metode ili mjere dodane samom UI modelu koje možda neće utjecati na rizik od izravnog izdvajanja osobnih podataka za model od strane bilo koga tko mu izravno pristupa, ali koje bi mogle smanjiti vjerojatnost dobivanja osobnih podataka povezanih s podacima o treniranju iz upita.

3.2.2.2 Analiza UI modela

54. Kako bi nadzorna tijela procijenila pouzdanost osmišljenog UI modela u pogledu anonimizacije, prvi je korak osigurati da je dizajn razvijen kako je planirano i da podliježe učinkovitom inženjerskom upravljanju. Nadzorna tijela trebala bi ocijeniti jesu li voditelji obrade proveli ikakve revizije temeljene na dokumentima (unutarnje ili vanjske) koje uključuju evaluaciju odabranih mjera i njihova učinka kako bi se ograničila vjerojatnost identifikacije. To bi moglo uključivati analizu izvješća o pregledima kodova, kao i teoretsku analizu kojom se dokumentira primjerenost odabranih mjera za smanjenje vjerojatnosti ponovne identifikacije predmetnog modela.

3.2.2.3 Testiranje UI modela i otpornost na napade

55. Naposljetku, nadzorna tijela trebala bi uzeti u obzir opseg, učestalost, količinu i kvalitetu testova koja je voditelj obrade proveo na modelu. Nadzorna tijela posebno bi trebala uzeti u obzir činjenicu da uspješno testiranje koje obuhvaća općepoznate i najsuvremenije napade može biti samo dokaz otpornosti na te napade. Do datuma donošenja ovog mišljenja to bi moglo uključivati, među ostalim, strukturirano testiranje u odnosu na: i. zaključivanje o pripadnosti i članstvu; ii. eksfiltracija; iii. regurgitacija podataka za treniranje; iv. inverzija modela; ili v. rekonstrukcijski napadi.

3.2.2.4 Dokumentacija

56. Člancima 5., 24., 25. i 30. Opće uredbe te, u slučajevima vjerojatno visokog rizika za prava i slobode ispitanika, člankom 35. Opće uredbe, od voditelja obrade zahtijeva se da na odgovarajući način dokumentiraju svoje postupke obrade. To se odnosi i na svaku obradu koja bi uključivala treniranje UI modela, čak i ako je cilj obrade anonimizacija. Nadzorna tijela trebala bi uzeti u obzir takvu dokumentaciju i svaku redovitu procjenu posljedičnih rizika za obradu koju provode voditelji obrade jer su to temeljni koraci kojima se dokazuje da se osobni podatci ne obrađuju.
57. **EDPB smatra da bi nadzorna tijela trebala uzeti u obzir dokumentaciju kad god je potrebno ocijeniti tvrdnju o anonimnosti u pogledu određenog UI modela. EDPB primjećuje da, ako nadzorno tijelo nakon procjene tvrdnje o anonimnosti, uključujući s obzirom na dokumentaciju, ne može potvrditi da su poduzete učinkovite mjere za anonimnost UI modela, nadzorno tijelo moglo bi smatrati da voditelj obrade nije ispunio svoje obveze odgovornosti u skladu s člankom 5. stavkom 2. Opće uredbe. Stoga bi trebalo razmotriti i usklađenost s drugim odredbama Opće uredbe.**
58. U idealnom bi slučaju nadzorna tijela trebala provjeriti uključuje li dokumentacija voditelja obrade:
- sve informacije koje se odnose na procjene učinka na zaštitu podataka, uključujući sve procjene i odluke kojima je utvrđeno da procjena učinka na zaštitu podataka nije potrebna
 - sve savjete ili povratne informacije koje dostavi **službenik za zaštitu podataka** (ako je službenik za zaštitu podataka imenovan ili je trebao biti imenovan)
 - informacije o tehničkim i organizacijskim mjerama koje su poduzete tijekom osmišljavanja UI modela kako bi se smanjila vjerojatnost identifikacije, uključujući model prijetnje i procjene rizika na kojima se te mjere temelje. To bi trebalo uključivati posebne mjere za svaki izvor skupova podataka za treniranje, uključujući relevantne URL-ove izvora i opise poduzetih mjera (ili koje su već poduzeli pružatelji skupova podataka trećih strana)
 - tehničke i organizacijske mjere poduzete u svim fazama tijekom životnog ciklusa modela, koje su doprinijele nedostatku osobnih podataka u modelu ili je njima provjeren nedostatak osobnih podataka
 - dokumentaciju kojom se dokazuje teoretska otpornost UI modela na tehnike ponovne identifikacije, kao i kontrole osmišljene za ograničavanje ili procjenu uspjeha i učinka glavnih napada (regurgitacija, napadi radi otkrivanja korištenih podataka za treniranje (eng. *membership inference attack*), eksfiltracija itd.)). To posebno može uključivati: i. omjer između količine podataka za treniranje i broja parametara u modelu, uključujući analizu učinka na

model³⁸; ii. parametre o vjerojatnosti ponovne identifikacije na temelju najnovijih dostignuća; iii. izvješća o tome kako je model testiran (tko, kada, kako i u kojoj mjeri) i iv. rezultate testova

- f. dokumentaciju dostavljenu voditeljima obrade koji primjenjuju model i/ili ispitanicima, posebno dokumentaciju koja se odnosi na mjere poduzete za smanjenje vjerojatnosti identifikacije i u vezi s mogućim preostalim rizicima.

3.3 O primjerenosti legitimnog interesa kao pravne osnove za obradu osobnih podataka u kontekstu razvoja i uvođenja UI modela

59. Kako bi odgovorio na 2. i 3. pitanje u zahtjevu, EDPB će prvo iznijeti opće primjedbe o nekim važnim aspektima koje bi nadzorna tijela trebala uzeti u obzir, neovisno o pravnoj osnovi obrade, prilikom procjene načina na koji voditelji obrade mogu dokazati usklađenost s Općom uredbom u kontekstu UI modela. Na temelju Smjernica 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka³⁹ EDPB će zatim razmotriti tri koraka koja se zahtijevaju procjenom legitimnog interesa u kontekstu razvoja i uvođenja UI modela.

3.3.1 Općenita opažanja

60. EDPB podsjeća da se Općom uredbom ne uspostavlja nikakva hijerarhija između različitih pravnih osnova utvrđenih u članku 6. stavku 1. Opće uredbe⁴⁰.
61. U članku 5. Opće uredbe utvrđena su načela koja se odnose na obradu osobnih podataka. EDPB ističe ona koja su važna za ovo mišljenje i koje bi nadzorna tijela trebala uzeti u obzir barem pri procjeni određenih UI modela, kao i najrelevantnije zahtjeve iz drugih odredaba Opće uredbe, uzimajući u obzir područje primjene ovog mišljenja.
62. **Načelo odgovornosti** (članak 5. stavak 2. Opće uredbe) – Ovo načelo predviđa da voditelj obrade mora biti odgovoran za usklađenost s Općom uredbom i biti sposoban dokazati usklađenost. U tom pogledu, uloge i odgovornosti strana koje obrađuju osobne podatke u kontekstu razvoja ili uvođenja UI modela trebalo bi procijeniti prije početka obrade kako bi se definirale obveze voditelja obrade ili zajedničkih voditelja obrade te izvršitelja obrade (ako postoje) od samog početka.
63. **Načela zakonitosti, poštenosti i transparentnosti** (članak 5. stavak 1. točka (a) Opće uredbe o zaštiti podataka) – pri procjeni zakonitosti obrade u kontekstu UI modela, s obzirom na članak 6. stavak 1. Opće uredbe, EDPB smatra da je korisno razlikovati različite faze obrade osobnih podataka⁴¹. Načelom poštenosti, koje je usko povezano s načelom transparentnosti, zahtijeva se da se osobni podatci ne obrađuju nepoštenim metodama ili prijevarom, ili na način koji je „*neopravdano štetan, nezakonito diskriminirajući, neočekivan ili obmanjujući za ispitanika*”⁴². S obzirom na složenost uključenih

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

³⁹ Vidjeti Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024.

⁴⁰ Ibid., točka 1.

⁴¹ Izvješće EDPB-a o radu radne skupine ChatGPT, doneseno 23. svibnja 2024., točka 14.

⁴² Izvješće EDPB-a o radu radne skupine ChatGPT, doneseno 23. svibnja 2024., točka 23.; Smjernice EDPB-a 4/2019 Smjernice 4/2019 o članku 25. Tehnička i integrirana zaštita podataka, verzija 2.0, donesene

tehnologija, informacije o obradi osobnih podataka u UI modelima trebalo bi stoga pružati na pristupačan i razumljiv način prilagođen korisnicima⁴³. Transparentnost u pogledu obrade osobnih podataka posebno uključuje usklađenost s obvezama pružanja informacija utvrđenima u člancima od 12. do 14. Opće uredbe⁴⁴, koje također zahtijevaju, u slučaju automatiziranog donošenja odluka, uključujući izradu profila, smislene informacije o tome o kojoj je logici riječ, kao i važnost i predviđene posljedice obrade za ispitanika⁴⁵. Imajući na umu da faze razvoja UI modela mogu uključivati prikupljanje velikih količina podataka iz javno dostupnih izvora (kao što su tehnike ekstrakcije podataka s interneta), oslanjanje na iznimku predviđenu člankom 14. stavkom 5. točkom (b) Opće uredbe strogo je ograničeno na slučajeve u kojima su zahtjevi iz te odredbe u potpunosti ispunjeni⁴⁶.

64. **Načela ograničavanja svrhe i smanjenja količine podataka** (članak 5. stavak 1. točke (b) i (c) Opće uredbe) – U skladu s načelom smanjenja količine podataka, razvoj i uvođenje UI modela zahtijeva da osobni podatci budu primjereni, relevantni i nužni u odnosu na svrhu. To može uključivati obradu osobnih podataka kako bi se izbjegli rizici od mogućih pristranosti i pogrešaka ako je to jasno i posebno utvrđeno u okviru svrhe i ako su osobni podatci nužni u tu svrhu (npr. ne mogu se učinkovito postići obradom drugih podataka, uključujući sintetičke ili anonimizirane podatke)⁴⁷. Radna skupina iz članka 29. već je naglasila da „*svrha prikupljanja mora biti jasno i posebno utvrđena [...]*”⁴⁸. Kada se procjenjuje je li svrha koja se želi postići zakonita, specifična i izričita te je li obrada u skladu s načelom smanjenja količine podataka, prvo treba utvrditi predmetnu aktivnost obrade. Konkretno, različite faze u fazama razvoja ili uvođenja mogu predstavljati iste ili različite aktivnosti obrade i mogu uključivati uzastopne voditelje obrade ili zajedničke voditelje obrade. U nekim je slučajevima moguće utvrditi svrhu koja će se nastojati ostvariti tijekom uvođenja UI modela u ranoj fazi razvoja. Čak i ako to nije slučaj, određeni kontekst za to uvođenje trebao bi već biti jasan te bi stoga trebalo razmotriti kako taj kontekst utječe na svrhu razvoja. Prilikom preispitivanja svrhe obrade u određenoj fazi razvoja nadzorna tijela trebala bi očekivati određeni stupanj detaljnosti od voditelja obrade i objašnjenje načina na koji te detaljnosti utječu na svrhu obrade. To može uključivati, na primjer, informacije o vrsti razvijenog UI modela, njegovim očekivanim funkcionalnostima i bilo koji drugi relevantni kontekst koji je već poznat u toj fazi. Kontekst uvođenja također bi mogao uključivati, na primjer, razvija li se model za interno uvođenje, namjerava li voditelj obrade prodati ili distribuirati model trećim stranama nakon njegova razvoja, uključujući i to je li model prvenstveno namijenjen za primjenu u istraživačke ili komercijalne svrhe.
65. **Prava ispitanika** (poglavlje III. Opće uredbe) – Neovisno o potrebi da nadzorna tijela osiguraju poštovanje svih prava ispitanika kada voditelji obrade razvijaju i primjenjuju UI modele, EDPB podsjeća

20. listopada 2020., točka 69.; Smjernice Radne skupine iz članka 29. o transparentnosti na temelju Uredbe 2016/679, revidirane i donesene 11. travnja 2018., koje je EDPB potvrdio 25. svibnja 2018., stavak 2.

⁴³Smjernice Radne skupine iz članka 29. o transparentnosti na temelju Uredbe 2016/679, revidirane i donesene 11. travnja 2018., koje je EDPB potvrdio 25. svibnja 2018., stavak 5.

⁴⁴Vidjeti i uvodnu izjavu 39. Opće uredbe, u kojoj se navodi „*Za pojedince bi trebalo biti transparentno kako se osobni podaci koji se odnose na njih prikupljaju, upotrebljavaju, daju na uvid ili na drugi način obrađuju, kao i do koje se mjere ti osobni podaci obrađuju ili će se obrađivati[...]*”.

⁴⁵Članak 13. stavak 2. točka (f) Opće uredbe o zaštiti podataka i članak 14. stavak 2. točka (g) Opće uredbe o zaštiti podataka.

⁴⁶Izvješće EDPB-a o radu radne skupine ChatGPT, doneseno 23. svibnja 2024., točka 27.

⁴⁷Osim toga, člankom 10. stavkom 5. Akta o umjetnoj inteligenciji predviđaju se posebna pravila za obradu posebnih kategorija osobnih podataka u vezi s visokorizičnim UI sustavima u svrhu osiguravanja otkrivanja i ispravljanja pristranosti.

⁴⁸Mišljenje 3/2013 Radne skupine iz članka 29. o ograničavanju svrhe (WP203), str. 15.–16.

da se, kad god se voditelj obrade poziva na legitimni interes kao na pravnu osnovu, primjenjuje pravo na prigovor u skladu s člankom 21. Opće uredbe te bi ga trebalo osigurati⁴⁹.

3.3.2 Razmatranja o trima koracima procjene legitimnog interesa u kontekstu razvoja i uvođenja UI modela

66. Kako bi se utvrdilo može li se određena obrada osobnih podataka temeljiti na članku 6. stavku 1. točki (f) Opće uredbe, nadzorna tijela trebala bi provjeriti jesu li voditelji obrade pažljivo procijenili i dokumentirali jesu li ispunjena sljedeća tri kumulativna uvjeta: i. ostvarivanje legitimnog interesa od strane voditelja obrade ili treće strane; ii. obrada je nužna za ostvarivanje legitimnog interesa; i iii. legitimni interes nije podređen interesima ili temeljnim pravima i slobodama ispitanika⁵⁰.

3.3.2.1 Prvi korak – ostvarivanje legitimnog interesa od strane voditelja obrade ili treće strane

67. Interes je širi interes ili korist koju voditelj obrade ili treća strana mogu imati u sudjelovanju u posebnoj aktivnosti obrade⁵¹. Iako su Opća uredba i Sud EU-a prepoznali nekoliko interesa kao legitimne⁵², procjena legitimnosti određenog interesa trebala bi biti rezultat analize svakog pojedinačnog slučaja.
68. Kao što je EDPB podsjetio u svojim Smjernicama o legitimnom interesu⁵³, interes se može smatrati legitimnim ako su ispunjena sljedeća tri kumulativna kriterija:
- a. interes je zakonit⁵⁴
 - b. interes je jasno i precizno artikuliran i
 - c. interes je stvaran i prisutan, a ne špekulativan.

⁴⁹U skladu s člankom 21. Opće uredbe, ako ispitanik na temelju svoje posebne situacije uloži prigovor na obradu osobnih podataka koji se odnose na njega, voditelj obrade više ne smije obrađivati osobne podatke osim ako voditelj obrade dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva. Stoga su dva aspekta koja nadzorna tijela moraju uzeti u obzir sposobnost voditelja obrade da dokaže postojanje takvih uvjerljivih i jačih legitimnih razloga i može li se ostvariti pravo na prigovor.

⁵⁰ Presuda Suda EU-a od 4. srpnja 2023., predmet C-252/21, *Meta protiv Bundeskartellamt* (ECLI:EU:C:2023:537), točka 106.; presuda Suda EU-a od 11. prosinca 2019., predmet C-708/18, *Asociația de Proprietari bloc M5A-Scara A* (ECLI:EU:C:2019:1064), točka 40. Vidjeti i Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., točke 12. i dalje. Kao što se podsjeća u ovim Smjernicama, „procjenu bi trebalo provesti na početku obrade, uz sudjelovanje službenika za zaštitu podataka (ako je imenovan), a voditelj obrade trebao bi je dokumentirati u skladu s načelom odgovornosti utvrđenim u članku 5. stavku 2. Opće uredbe”.

⁵¹ Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., stavak 14.

⁵² Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., stavak 16.

⁵³ Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., stavak 17.

⁵⁴ Sud EU-a, presuda od 4. listopada 2024., predmet C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), točka 49., u kojoj je Sud EU-a naglasio da legitimni interes ne može biti u suprotnosti sa zakonom. U tom pogledu EDPB naglašava da bi, ovisno o slučaju, trebalo uzeti u obzir zakonodavne okvire pri procjeni zakonitosti određenog interesa. Vidjeti primjerice: članak 26. stavak 3. i članak 28. Uredbe (EU) 2022/2065 Europskog parlamenta i Vijeća od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama) o zabranjenom ciljanom oglašavanju maloljetnicima; članak 5. stavci 1. i 2. Akta o umjetnoj inteligenciji o zabranjenim praksama u području umjetne inteligencije (manipulativne prakse i ispod praga svijesti); obrada kojom se krše prava intelektualnog vlasništva i odredbe Direktive (EU) 2019/790 o autorskom i srodnim pravima na jedinstvenom digitalnom tržištu.

69. Podložno dvama drugim koracima koji se zahtijevaju procjenom legitimnog interesa, sljedeći primjeri mogu predstavljati legitiman interes u kontekstu UI modela: i. razvoj usluge razgovornog agenta kako bi se pomoglo korisnicima; ii. razvoj UI sustava za otkrivanje prijevarg sadržaja ili ponašanja; i iii. poboljšanje otkrivanja prijetnji u informacijskom sustavu.

3.3.2.2 Drugi korak – Analiza nužnosti obrade za ostvarivanje legitimnog interesa

70. Drugi korak procjene sastoji se od utvrđivanja je li obrada osobnih podataka nužna u svrhu legitimnih interesa koji se nastoje ostvariti⁵⁵ („test nužnosti”).
71. U uvodnoj izjavi 39. Opće uredbe navodi se sljedeće: „Osobni podaci trebali bi se obrađivati samo ako se svrha obrade opravdano ne bi mogla postići drugim sredstvima”. U skladu sa smjernicama Suda EU-a i prethodnim smjernicama EDPB-a, uvjet koji se odnosi na nužnost obrade trebalo bi ispitati s obzirom na temeljna prava i slobode ispitanika te u vezi s načelom smanjenja količine podataka iz članka 5. stavka 1. točke (c) Opće uredbe⁵⁶.
72. Metodologija na koju upućuje Sud EU-a uzima u obzir kontekst obrade, kao i učinke na voditelja obrade i ispitanike. Procjena nužnosti stoga uključuje dva elementa: i. hoće li aktivnost obrade omogućiti ostvarivanje te svrhe⁵⁷; i ii. postoji li manje intruzivan način ostvarivanja te svrhe⁵⁸.
73. Primjerice, i ovisno o slučaju, planiranu količinu osobnih podataka uključenih u UI model treba procijeniti imajući u vidu manje intruzivne alternative koje bi razumno mogle biti dostupne kako bi se jednako učinkovito postigla svrha legitimnog interesa koji se nastoji ostvariti. Ako je ostvarivanje te svrhe moguće i s pomoću UI modela koji ne podrazumijeva obradu osobnih podataka, trebalo bi

⁵⁵Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., točke 28.–30.

⁵⁶Sud EU-a, presuda od 4. srpnja 2023., predmet C-252/21, *Meta protiv Bundeskartellamt* (ECLI:EU:C:2023:537), točke 108. i 109., u kojem se također upućuje na Sud EU-a, presudu od 11. prosinca 2019., predmet C-708/18, *Asociația de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), točka 48.; Sud EU-a, presuda od 9. studenoga 2010., spojeni predmeti C-92/09 i C-93/09, *Volker i Markus Schecke* (ECLI:EU:C:2010:662), točke 85. i 86.; presuda Suda EU-a od 22. lipnja 2021., predmet C-439/19, *Latvijas Republikas Saeima* (ECLI:EU:C:2021:504), točke 98., 109., 110. i 113. Vidjeti također, na primjer: Smjernice 3/2019 EDPB-a o obradi osobnih podataka putem videouređaja, verzija 2.0, donesene 29. siječnja 2020., točke 24.–26. i 73.; Smjernice EDPB-a 2/2019 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (b) Opće uredbe o zaštiti podataka u kontekstu pružanja internetskih usluga ispitanicima, verzija 2.0, donesene 8. listopada 2019., točke 23.–25.; Mišljenje EDPB-a 11/2024 o upotrebi prepoznavanja lica radi ubrzavanja protoka putnika u zračnim lukama, verzija 1.1, doneseno 23. svibnja 2024., točka 27.

⁵⁷Vidjeti presudu Suda EU-a od 16. prosinca 2008., predmet C-524/06, *Heinz Huber protiv Savezne Republike Njemačke* (ECLI:EU:C:2008:724), točka 66. U istom predmetu vidjeti Mišljenje nezavisnog odvjetnika M. Poiaresa Madura u predmetu C-524/06, *Heinz Huber protiv Savezne Republike Njemačke* (ECLI:EU:C:2008:194), točka 16., u kojem se navodi: „odgovarajući test ovdje je test učinkovitosti, a na nacionalnom je sudu da ga primijeni. Mora se postaviti pitanje postoje li drugi načini obrade podataka kojima bi tijela nadležna za imigraciju mogla provoditi pravila o boravišnom statusu. Ako je odgovor na to pitanje potvrđan, centraliziranu pohranu i obradu podataka za građane Unije trebalo bi proglasiti nezakonitom. Nije potrebno da alternativni sustav bude najučinkovitiji ili najprimjereniji; dovoljno je da može funkcionirati na odgovarajući način. Drugim riječima, čak i ako je središnji registar učinkovitiji, praktičniji ili jednostavniji za korištenje od njegovih alternativa (kao što su decentralizirani, lokalni registri), jasno je da prednost treba dati potonjima ako se mogu upotrijebiti za navođenje boravišnog statusa građana Unije.

⁵⁸Vidjeti presudu Suda EU-a od 27. rujna 2017., predmet C-73/16, *Peter Puškár* (ECLI:EU:C:2017:725), točka 113.: „Stoga je na sudu koji je uputio zahtjev da provjeri jesu li izrada sporne evidencije i uključivanje u nju imena predmetnih osoba primjereni za ostvarivanje ciljeva koji se njome žele postići i postoje li blaža sredstva za postizanje tih ciljeva.”; vidjeti i, na primjer, mišljenje nezavisnog odvjetnika Rantosa u predmetu C-252/21, *Meta protiv Bundeskartellamt*, ECLI:EU:C:2022:704, točku 61., u kojem se navodi: „[...] Stoga je nužno postojanje uske veze između obrade i interesa koji se ostvaruje, u nedostatku alternativa kojima se više poštuje zaštita osobnih podataka, s obzirom na to da nije dovoljno da je obrada korisna samo voditelju obrade.

smatrati da obrada osobnih podataka nije nužna. To je posebno važno za razvoj UI modela. Pri procjeni je li uvjet nužnosti ispunjen, nadzorna tijela trebala bi obratiti posebnu pozornost na količinu obrađenih osobnih podataka i je li ona proporcionalna za ostvarivanje predmetnog legitimnog interesa, također s obzirom na načelo smanjenja količine podataka.

74. Pri procjeni nužnosti trebalo bi uzeti u obzir i širi kontekst planirane obrade osobnih podataka. Postojanje sredstava koja su manje intruzivna za temeljna prava i slobode ispitanika može se razlikovati ovisno o tome je li voditelj obrade u izravnom odnosu s ispitanicima (podatci prve strane) ili ne (podatci trećih strana). Sud EU-a naveo je neka razmatranja koja treba uzeti u obzir pri analizi nužnosti obrade podataka prve strane u svrhu legitimnih interesa koji se nastoje ostvariti (iako u kontekstu otkrivanja takvih podataka trećim stranama)⁵⁹.
75. Provedba tehničkih zaštitnih mjera za zaštitu osobnih podataka također može doprinijeti ispunjavanju testa nužnosti. To bi moglo uključivati, na primjer, provedbene mjere kao što su one utvrđene u odjeljku 3.2.2. na način da se ne postigne anonimizacija, ali kojima se i dalje smanjuje jednostavnost identifikacije ispitanika. EDPB napominje da neke od tih mjera, ako nisu potrebne za usklađivanje s Općom uredbom, mogu predstavljati dodatne zaštitne mjere, kako je dodatno analizirano u pododjeljku „mjere ublažavanja” u odjeljku 3.3.2.3⁶⁰.

3.3.2.3 Treći korak – Test ravnoteže

76. Treći korak procjene legitimnog interesa jest „**ispitivanje ravnoteže**” (koje se u ovom dokumentu naziva i „**testom ravnoteže**”)⁶¹. Taj se korak sastoji od utvrđivanja i opisivanja različitih suprotstavljenih prava i interesa⁶² o kojima je riječ, tj., s jedne strane, interesa, temeljnih prava i sloboda ispitanika, a s druge strane interesa voditelja obrade ili treće strane. Potom bi trebalo razmotriti posebne okolnosti slučaja kako bi se dokazalo da je legitimni interes odgovarajuća pravna osnova za predmetne aktivnosti obrade⁶³.

Interesi ispitanika, temeljna prava i slobode

77. Člankom 6. stavkom 1. točkom (f) Opće uredbe predviđa se da bi voditelj obrade pri procjeni različitih sastavnica u kontekstu testa ravnoteže trebao uzeti u obzir interese, temeljna prava i slobode ispitanika. Interesi ispitanika su oni na koje predmetna obrada može utjecati. U kontekstu faze razvoja UI modela oni mogu uključivati, ali nisu ograničeni na, interes za samoodređenje i zadržavanje kontrole nad vlastitim osobnim podacima (npr. podatci prikupljeni za razvoj modela). U kontekstu uvođenja UI modela interesi ispitanika mogu uključivati, ali nisu ograničeni na interese zadržavanja kontrole nad vlastitim osobnim podacima (npr. podacima koji se obrađuju nakon uvođenja modela), financijske interese (npr. ako ispitanik upotrebljava UI model za ostvarivanje prihoda ili ga upotrebljava pojedinac u kontekstu svoje profesionalne djelatnosti), osobne koristi (npr. ako se UI model upotrebljava za poboljšanje dostupnosti određenih usluga) ili socioekonomske interese (npr. ako UI model omogućuje

⁵⁹ Sud EU-a, presuda od 4. listopada 2024., predmet C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), točke 51.–53.

⁶⁰ Vidjeti Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., točka 57.

⁶¹ Vidjeti Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., točke od 31. do 60.

⁶² Vidjeti Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., točka 32.

⁶³ Vidjeti Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0., donesene 8. listopada 2024., točka 32., u kojima se upućuje i na Sud EU-a, presuda od 4. srpnja 2023., predmet C-252/21, *Meta protiv Bundeskartellamt* (ECLI:EU:C:2023:537), točka 110.

pristup boljoj zdravstvenoj zaštiti ili olakšava ostvarivanje temeljnog prava kao što je pristup obrazovanju)⁶⁴.

78. Što je interes preciznije definiran s obzirom na predviđenu svrhu obrade, to će on na bolji način omogućiti da se jasno uvide stvarne koristi i rizici koje treba uzeti u obzir u testu ravnoteže.
79. Kad je riječ o temeljnim pravima i slobodama ispitanika, razvoj i uvođenje UI modela mogu predstavljati ozbiljan rizik za prava zaštićena Poveljom EU-a o temeljnim pravima („**Povelja EU-a**”), uključujući, ali ne ograničavajući se na pravo na privatni i obiteljski život (članak 7. Povelje EU-a) i pravo na zaštitu osobnih podataka (članak 8. Povelje EU-a). Ti se rizici mogu pojaviti tijekom faze razvoja, na primjer ako se osobni podatci izvlače protivno željama ispitanika ili bez njihova znanja. Ti se rizici mogu pojaviti i u fazi uvođenja, na primjer ako se osobni podatci obrađuju s pomoću modela (ili kao njegov dio) na način koji je u suprotnosti s pravima ispitanika ili ako je moguće zaključiti, slučajno ili korištenjem napada (npr. radi otkrivanja korištenih podataka za treniranje, izvlačenje ili na inverziju modela), koji su osobni podatci sadržani u bazi podataka za učenje. Takve situacije predstavljaju rizik za privatnost ispitanika čiji se podatci mogu pojaviti u fazi uvođenja UI sustava (npr. rizik od narušavanja ugleda, krađa identiteta ili prijevара, sigurnosni rizik ovisno o prirodi podataka).
80. Ovisno o predmetnom slučaju, mogu postojati i rizici za druga temeljna prava. Na primjer, opsežno i neselektivno prikupljanje podataka s pomoću UI modela u fazi razvoja može stvoriti osjećaj nadzora za ispitanike, posebno uzimajući u obzir poteškoće u sprječavanju izvlačenja javnih podataka. To može navesti pojedince na autocenzuru i predstavljati rizik od ugrožavanja njihove slobode izražavanja (članak 11. Povelje EU-a). U fazi uvođenja prisutni su i rizici za slobodu izražavanja u slučajevima u kojima se UI modeli upotrebljavaju za blokiranje objave sadržaja ispitanika. Osim toga, UI model kojim se ranjivim pojedincima preporučuje neprimjeren sadržaj može predstavljati rizik za njihovo mentalno zdravlje (članak 3. stavak 1. Povelje EU-a). U drugim slučajevima uvođenje UI modela može dovesti i do štetnih posljedica za pravo pojedinca na rad (članak 15. Povelje EU-a), na primjer kada su prijave za posao odabrane s pomoću UI modela. Na isti bi način UI model mogao predstavljati rizik za pravo na nediskriminaciju (članak 21. Povelje EU-a) ako diskriminira pojedince na temelju određenih osobnih karakteristika (kao što su državljanstvo ili spol). Nadalje, uvođenje UI modela može predstavljati i rizik za sigurnost i zaštitu pojedinca (npr. ako se UI model upotrebljava sa zlom namjerom), kao i rizik za njegov fizički i duhovni integritet⁶⁵.
81. Uvođenje UI modela također može pozitivno utjecati na određena temeljna prava, npr. modelom se može podržati pravo osobe na duhovni integritet (članak 3. Povelje), na primjer kada se UI model upotrebljava za utvrđivanje štetnog sadržaja na internetu; ili model može olakšati pristup određenim osnovnim uslugama ili olakšati ostvarivanje temeljnih prava, kao što su pristup informacijama (članak 11. Povelje EU-a) ili pristup obrazovanju (članak 14. Povelje EU-a).

Učinak obrade podataka na ispitanike

82. Obrada osobnih podataka koja se odvija tijekom razvoja i uvođenja UI modela može na različite načine utjecati na ispitanike, što može biti pozitivno ili negativno⁶⁶. Primjerice, ako aktivnost obrade podrazumijeva koristi za ispitanika, one se mogu uzeti u obzir u testu ravnoteže. Iako postojanje takvih koristi može dovesti do zaključka nadzornog tijela da interesi voditelja obrade ili treće strane nisu

⁶⁴Vidjeti Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., točka 38.

⁶⁵ Smjernice 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0., donesena 8. listopada 2024., točka 46.

⁶⁶Vidjeti Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., točka 39.

podređeni interesima, temeljnim pravima i slobodama ispitanika, takav zaključak može biti samo rezultat analize svakog pojedinačnog slučaja, uzimajući u obzir sve odgovarajuće čimbenike.

83. Na učinak obrade na ispitanike mogu utjecati i. priroda podataka obrađenih u modelima; ii. kontekst obrade; i iii. daljnje posljedice koje obrada može imati⁶⁷.
84. Kad je riječ o **prirodi obrađenih podataka**, valja podsjetiti da, osim posebnih kategorija osobnih podataka i podataka koji se odnose na osuđujuće presude i kaznena djela koja uživaju dodatnu zaštitu u skladu s člancima 9. i 10. Opće uredbe, obrada nekih drugih kategorija osobnih podataka može dovesti do znatnih posljedica za ispitanike. U tom kontekstu treba smatrati da bi obrada određenih vrsta osobnih podataka kojima se otkrivaju vrlo privatne informacije (npr. financijski podatci ili podatci o lokaciji) za razvoj i uvođenje UI modela mogla imati ozbiljan učinak na ispitanike. U fazi uvođenja posljedice takve obrade za ispitanike mogu, na primjer, biti gospodarske (npr. diskriminacija u kontekstu zapošljavanja) i/ili povezane s ugledom (npr. kleveta).
85. Kad je riječ o **kontekstu obrade**, prvo je potrebno utvrditi elemente koji bi mogli stvoriti rizike za ispitanike (npr. način na koji je model razvijen, način na koji se model može primijeniti i/ili jesu li sigurnosne mjere koje se upotrebljavaju za zaštitu osobnih podataka primjerene). Priroda modela i predviđene operativne uporabe imaju ključnu ulogu u utvrđivanju takvih potencijalnih uzroka.
86. Također je potrebno procijeniti ozbiljnost tih rizika za ispitanike. Može se, među ostalim, razmotriti kako se osobni podatci obrađuju (npr. ako se kombiniraju s drugim skupovima podataka), koliki je opseg obrade i količina obrađenih osobnih podataka⁶⁸ (npr. ukupna količina podataka, količina podataka po ispitaniku, broj pogođenih ispitanika),⁶⁹ status ispitanika (npr. djeca ili drugi ranjivi ispitanici) i njihov odnos s voditeljem obrade (npr. ako je ispitanik klijent). Na primjer, upotreba ekstrakcije podataka s interneta u fazi razvoja može, u nedostatku dostatnih zaštitnih mjera, dovesti do znatnih učinaka na pojedince zbog velike količine prikupljenih podataka, velikog broja ispitanika i neselektivnog prikupljanja osobnih podataka.
87. **Dodatne posljedice** koje bi obrada mogla imati trebalo bi uzeti u obzir i pri procjeni učinka obrade na ispitanike. Nadzorna tijela trebala bi ih procjenjivati ovisno o pojedinačnom slučaju, uzimajući u obzir konkretne činjenice o kojima je riječ.
88. Takve posljedice mogu uključivati (ali nisu ograničene na) rizike od kršenja temeljnih prava ispitanika, kako je opisano u prethodnom pododjeljku⁷⁰. Rizici se mogu razlikovati po vjerojatnosti i ozbiljnosti te mogu proizlaziti iz obrade osobnih podataka koja bi mogla dovesti do fizičke, materijalne ili nematerijalne štete, osobito ako obrada može dovesti do diskriminacije⁷¹.
89. Ako uvođenje UI modela podrazumijeva obradu osobnih podataka i. ispitanika čiji su osobni podatci uključeni u skup podataka koji se upotrebljava u fazi razvoja i ii. ispitanika čiji se osobni podatci obrađuju u fazi uvođenja, nadzorna tijela trebala bi pri provjeri testa ravnoteže koji provodi voditelj

⁶⁷Vidjeti Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., točka 32.

⁶⁸Vidjeti Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., točka 43.

⁶⁹ Presuda Suda EU-a od 4. srpnja 2023., predmet C-252/21., *Meta protiv Bundeskartellamta* (ECLI:EU:C:2023:537), točka 116.

⁷⁰ Vidjeti prethodni pododjeljak „Interesi, temeljna prava i slobode ispitanika”.

⁷¹ Vidjeti odjeljak 2.3. Smjernica EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0., donesenih 8. listopada 2024. Vidjeti i uvodnu izjavu 75. Opće uredbe o zaštiti podataka.

obrade razlikovati i uzeti u obzir rizike koji utječu na interese, prava i slobode svake od tih kategorija ispitanika.

90. **Naposljetku, u analizi mogućih daljnjih posljedica obrade trebalo bi razmotriti i vjerojatnost nastanka tih daljnjih posljedica.** Procjenu takve vjerojatnosti trebalo bi provesti uzimajući u obzir postojeće tehničke i organizacijske mjere te posebne okolnosti slučaja. Na primjer, nadzorna tijela mogu razmotriti jesu li provedene mjere za izbjegavanje moguće zlouporabe UI modela. Kad je riječ o UI modelima koji se mogu upotrebljavati u razne svrhe, kao što je generativna umjetna inteligencija, to može uključivati kontrole kojima se u najvećoj mogućoj mjeri ograničava njihova upotreba za štetne prakse, na primjer: stvaranje uvjerljivih krivotvorenih sadržaja (eng. *deepfake*), botova za razgovor (eng. *chatbotova*) koji se upotrebljavaju za dezinformacije, krađu identiteta i druge vrste prijevara te manipulativne umjetne inteligencije/UI agenata (posebno ako su antropomorfni ili ako pružaju obmanjujuće informacije).

Razumna očekivanja ispitanika

91. Na temelju uvodne izjave 47. Opće uredbe o zaštiti podataka, „[U] svakom slučaju postojanje legitimnog interesa zahtijevalo bi pažljivu procjenu, među ostalim i toga može li ispitanik u vrijeme i u kontekstu prikupljanja osobnih podataka razumno očekivati obradu u dotičnu svrhu. Interesi i temeljna prava ispitanika posebno bi mogli nadvladati interes voditelja obrade ako se osobni podaci obrađuju u okolnostima u kojima ispitanici razumno ne očekuju daljnju obradu⁷².“
92. Razumna očekivanja imaju ključnu ulogu u testu ravnoteže, među ostalim zbog složenosti tehnologije koja se upotrebljava u UI modelima i činjenice da bi ispitanicima moglo biti teško razumjeti raznolikost mogućih uporaba UI modela i uključene obrade podataka⁷³. U tu se svrhu mogu razmotriti informacije pružene ispitanicima kako bi se procijenilo mogu li ispitanici razumno očekivati da će se njihovi osobni podatci obrađivati. Međutim, iako izostavljanje informacija može doprinijeti tome da ispitanici ne očekuju određenu obradu, samo ispunjenje zahtjeva u pogledu transparentnosti utvrđenih u Općoj uredbi nije dovoljno kako bi se smatralo da ispitanici mogu razumno očekivati određenu obradu⁷⁴. Nadalje, samo zato što su informacije koje se odnose na fazu razvoja UI modela uključene u politiku zaštite privatnosti voditelja obrade, to ne znači nužno da ispitanici mogu razumno očekivati da će se to dogoditi, nego bi to nadzorna tijela trebala analizirati s obzirom na posebne okolnosti slučaja i uzimajući u obzir sve relevantne čimbenike.
93. Pri procjeni razumnih očekivanja ispitanika u pogledu obrade koja se odvija u fazi razvoja, važno je uputiti na elemente navedene u Smjernicama EDPB-a o legitimnom interesu⁷⁵. Nadalje, u okviru predmeta ovog mišljenja važno je razmotriti širi kontekst obrade. To može uključivati, iako nije ograničeno na to jesu li osobni podatci bili javno dostupni ili nisu, prirodu odnosa između ispitanika i

⁷² Vidjeti i presudu Suda EU-a od 4. srpnja 2023., predmet C-252/21, *Meta protiv Bundeskartellamt* (ECLI:EU:C:2023:537), točka 112.; Sud EU-a, presuda od 11. prosinca 2019., predmet C-708/18, *Asociația de Proprietari bloc M5A-Scara A* (ECLI:EU:C:2019:1064), točka 58.; Sud EU-a, presuda od 4. listopada 2024., predmet C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), točka 55.

⁷³ Na primjer, u presudi od 4. srpnja 2023., predmet C-252/21, *Meta protiv Bundeskartellamt* (ECLI:EU:C:2023:537), točka 123., iako je Sud EU-a utvrdio da se „poboljšanje proizvoda” u načelu ne može isključiti kao legitiman interes, utvrdio da je: „dvojbena [...] bi li cilj koji se odnosi na poboljšanje proizvoda mogao, uzimajući u obzir opseg te obrade i njezin značajan učinak na korisnika, i okolnost da potonji ne može razumno očekivati da te podatke obrađuje [...], prevladati nad interesima i temeljnim pravima takvog korisnika, to više kada je taj korisnik dijete.”.

⁷⁴ Smjernice 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0., donesena 8. listopada 2024., točka 53.

⁷⁵ Smjernice 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0., donesena 8. listopada 2024., točke 50.–54.

voditelja obrade (i postoji li veza između njih), prirodu usluge, kontekst u kojem su osobni podatci prikupljeni, izvor iz kojeg su podatci prikupljeni (npr. mrežno mjesto ili usluga na kojoj su osobni podatci prikupljeni i postavke privatnosti koje nude), moguće daljnje upotrebe modela te jesu li ispitanici zaista svjesni da su njihovi osobni podatci uopće dostupni na internetu.

94. U fazi razvoja modela, razumna očekivanja ispitanika mogu se razlikovati ovisno o tome objavljuju li ispitanici podatke koji se obrađuju za razvoj modela. Nadalje, razumna očekivanja mogu se razlikovati i ovisno o tome pružaju li podatke izravno voditelju obrade (npr. u kontekstu korištenja usluge) ili ih je voditelj obrade pribavio iz drugog izvora (npr. preko treće strane ili ekstrakcijom podataka). U oba bi slučaja prilikom procjene razumnih očekivanja trebalo bi uzeti u obzir korake poduzete kako bi se osobe čiji se podatci obrađuju obavijestile o aktivnostima obrade.
95. U fazi uvođenja UI modela jednako je važno uzeti u obzir razumna očekivanja ispitanika u kontekstu posebnih sposobnosti modela. Na primjer, kad je riječ o UI modelima koji se mogu prilagoditi u skladu s dostavljenim ulaznim podacima, može biti relevantno razmotriti jesu li ispitanici bili svjesni da su pružili osobne podatke kako bi UI model mogao prilagoditi svoje odgovore njihovim potrebama i kako bi mogli dobiti prilagođene usluge. Nadalje, također može biti važno razmotriti bi li ta aktivnost obrade utjecala samo na uslugu koja se pruža ispitanicima (npr. personalizacija sadržaja za određenog korisnika) ili bi se upotrebljavala za izmjenu usluge koja se pruža svim klijentima (npr. radi općenitog poboljšanja modela). Kao i u fazi razvoja, također može biti posebno važno razmotriti postoji li izravna veza između ispitanika i voditelja obrade. Takva izravna veza može, na primjer, omogućiti voditelju obrade da ispitanicima lako pruži informacije o aktivnosti obrade i modelu, što bi zatim moglo utjecati na razumna očekivanja tih ispitanika.

Mjere za smanjenje rizika

96. Ako se čini da interesi, prava i slobode ispitanika nadilaze legitimne interese voditelja obrade ili treće strane, voditelj obrade može razmotriti uvođenje mjera za ublažavanje kako bi se ograničio učinak obrade na te ispitanike. Mjere za ublažavanje su zaštitne mjere koje bi trebale biti prilagođene okolnostima slučaja i ovisiti o različitim čimbenicima, uključujući o predviđenoj upotrebi UI modela. Tim bi se mjerama ublažavanja nastojalo osigurati da interesi voditelja obrade ili treće strane ne budu podređeni, kako bi se voditelj obrade mogao osloniti na tu pravnu osnovu.
97. Kako je navedeno u Smjernicama EDPB-a o legitimnom interesu, mjere ublažavanja ne bi trebalo miješati s mjerama koje je voditelj obrade zakonski ionako obavezan donijeti kako bi osigurao usklađenost s Općom uredbom, neovisno o tome temelji li se obrada na članku 6. stavku 1. točki (f) Opće uredbe⁷⁶. To je posebno važno za mjere koje, primjerice, zahtijevaju usklađenost s načelima Opće uredbe, kao što je načelo smanjenja količine podataka.
98. Popis mjera naveden u nastavku nije iscrpan i nije preskriptivan, a provedbu mjera trebalo bi razmotriti na temelju procjene svakog pojedinačnog slučaja. Iako, ovisno o okolnostima, neke od mjera navedenih u nastavku mogu biti potrebne za usklađivanje s posebnim obvezama iz Opće uredbe, ako to nije slučaj, one se mogu uzeti u obzir kao dodatne zaštitne mjere. Osim toga, neke od mjera navedenih u nastavku odnose se na područja koja su podložna brzom razvoju i novim trendovima te bi ih nadzorna tijela trebala uzeti u obzir pri razmatranju određenog slučaja.
99. **Kad je riječ o fazi razvoja UI modela**, može se poduzeti nekoliko mjera za ublažavanje rizika koje predstavlja obrada podataka i prve strane i trećih strana (uključujući za ublažavanje rizika povezanih s praksama ekstrakcije podataka s interneta). Na temelju prethodno navedenog, EDPB pruža neke

⁷⁶ Smjernice 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0., donesena 8. listopada 2024., točka 57.

primjere mjera koje se mogu provesti kako bi se ublažili rizici utvrđeni u testu ravnoteže, a nadzorna tijela trebala bi ih uzeti u obzir pri procjeni određenih UI modela za svaki pojedinačni slučaj.

100. Tehničke mjere:

- a. Mjere navedene u odjeljku 3.2.2. koje su prikladne za ublažavanje postojećih rizika, ako te mjere ne dovode do anonimizacije modela i ne moraju biti u skladu s drugim obvezama iz Opće uredbe ili u okviru testa nužnosti (drugi korak procjene legitimnog interesa).

101. Osim tih mjera, druge relevantne mjere mogu uključivati:

- b. Mjere pseudonimizacije: to bi, na primjer, moglo uključivati mjere za sprječavanje bilo koje kombinacije podataka na temelju pojedinačnih identifikatora. Te mjere možda nisu primjerene ako nadzorno tijelo smatra da je voditelj obrade dokazao razumnu potrebu za prikupljanjem različitih podataka o određenom pojedincu za razvoj predmetnog UI sustava ili modela.
- c. Mjere za „maskiranje” osobnih podataka ili njihovu zamjenu lažnim osobnim podatcima u skupu podataka za treniranje (npr. zamjena imena i e-adresa lažnim imenima i lažnim e-adresama). Ta mjera može biti posebno primjerena ako stvarni materijalni sadržaj podataka nije relevantan za ukupnu obradu (npr. u treniranju velikih jezičnih modela).

102. Mjere kojima se olakšava ostvarivanje prava pojedinaca:

- a. Poštovanje razumnog vremenskog razdoblja između prikupljanja skupa podataka za treniranje i njegove upotrebe. Ta dodatna zaštitna mjera može ispitanicima omogućiti ostvarivanje prava tijekom tog razdoblja, pri čemu se razumno vremensko razdoblje procjenjuje ovisno o okolnostima svakog slučaja.
- b. Predlaganje bezuvjetnog „izuzeća” od samog početka, primjerice davanjem diskrecijskog prava na prigovor ispitanicima prije početka obrade, kako bi se ojačala kontrola pojedinaca nad svojim podatcima, što nadilazi uvjete iz članka 21. Opće uredbe⁷⁷.
- c. Omogućivanje ispitanicima da ostvare svoje pravo na brisanje čak i ako se ne primjenjuju posebni razlozi navedeni u članku 17. stavku 1. Opće uredbe o zaštiti podataka⁷⁸.
- d. Omogućivanje ispitanicima da podnesu zahtjeve u pogledu regurgitacije ili pamćenja osobnih podataka te okolnosti i načina s pomoću kojih se zahtjevi mogu reproducirati, čime se voditeljima obrade omogućuje da reproduciraju i procijene relevantne tehnike ispravljanja naučenih podataka za rješavanje tih zahtjeva.

103. Mjere transparentnosti: u nekim slučajevima mjere ublažavanja mogle bi uključivati mjere kojima se osigurava veća transparentnost u pogledu razvoja UI modela. Neke mjere, uz usklađenost s obvezama iz Opće uredbe, mogu pomoći u prevladavanju asimetrije informacija i omogućiti ispitanicima da bolje razumiju obradu koja je uključena u fazu razvoja:

- a. Objavljivanje javnih i lako dostupnih priopćenja koje nadilaze informacije koje se zahtijevaju na temelju članka 13. ili 14. Opće uredbe, primjerice pružanjem dodatnih pojedinosti o kriterijima prikupljanja i svim upotrijebljenim skupovima podataka, uzimajući u obzir posebnu zaštitu djece i ranjivih osoba.

⁷⁷ Ibid.

⁷⁸ Ibid.

- b. Alternativni oblici informiranja ispitanika, na primjer: medijske kampanje s različitim medijskim kućama za informiranje ispitanika, informacijska kampanja putem e-pošte, upotreba grafičke vizualizacije, često postavljana pitanja, oznake transparentnosti i kartice modela čija bi sistematizacija mogla strukturirati prikaz informacija o UI modelima te godišnja izvješća o transparentnosti na dobrovoljnoj osnovi.

104. **Posebne mjere ublažavanja u kontekstu ekstrakcije podataka s interneta:** S obzirom na to da, kako je prethodno navedeno, ekstrakcija podataka s interneta stvara posebne rizike⁷⁹, u tom bi se kontekstu mogle utvrditi posebne mjere ublažavanja. Ako je to relevantno, nadzorna tijela mogu ih, uz prethodno navedene mjere ublažavanja, uzeti u obzir i pri istrazi voditelja obrade koji provode ekstrakciju podataka s interneta.
105. Posebne mjere, ako nisu nužne u drugom koraku procjene legitimnog interesa, mogu se pokazati korisnima za ublažavanje rizika u kontekstu ekstrakcije podataka s interneta. One mogu uključivati **tehničke mjere**, kao što su:
- a. Isključivanje sadržaja podataka iz publikacija koji bi mogli uključivati osobne podatke koji uključuju rizike za određene osobe ili skupine osoba (npr. pojedinci koji bi mogli biti izloženi zlouporabi, šteti ili čak tjelesnim ozljedama ako su informacije javno objavljene).
 - b. Osiguravanje da se određene kategorije podataka ne prikupljaju ili da su određeni izvori isključeni iz prikupljanja podataka; to bi moglo uključivati, primjerice, određena mrežna mjesta koja su posebno intruzivna zbog osjetljivosti njihova sadržaja.
 - c. Isključivanje prikupljanja s mrežnih mjesta (ili dijelova mrežnih mjesta) koja se jasno protive ekstrakciji podataka s interneta i ponovnoj uporabi njihova sadržaja u svrhu izrade baza podataka za treniranje u području umjetne inteligencije (na primjer poštovanjem datoteka robots.txt ili ai.txt ili bilo kojeg drugog priznatog mehanizma za izričito isključivanje iz automatskog pretraživanja ili ekstrakcije podataka).
 - d. Uvođenje drugih relevantnih ograničenja prikupljanja, po mogućnosti uključujući kriterije koji se temelje na vremenskim razdobljima.
106. U kontekstu ekstrakcije podataka s interneta, primjeri posebnih mjera **kojima se olakšava ostvarivanje prava pojedinaca i transparentnost** mogu uključivati: izradu popisa izuzeća kojim upravlja voditelj obrade i koji ispitanicima omogućuje da podnesu prigovor na prikupljanje svojih podataka na određenim mrežnim mjestima ili internetskim platformama tako što im se pružaju informacije koje ih identificiraju na tim mrežnim mjestima, uključujući i prije pojave prikupljanja podataka⁸⁰.
107. **Posebna razmatranja u pogledu mjera ublažavanja u fazi uvođenja:** Iako neke od prethodno navedenih mjera mogu biti relevantne i za fazu uvođenja, ovisno o okolnostima, EDPB u nastavku dostavlja neiscrpan popis dodatnih mjera potpore koje se mogu provesti i koje bi nadzorna tijela trebala ocjenjivati ovisno o pojedinačnom slučaju.
- a. **Tehničke mjere** mogu se, primjerice, uvesti kako bi se spriječilo pohranjivanje, regurgitacija ili generiranje osobnih podataka, posebno u kontekstu generativnih UI modela (kao što su izlazni filtri), i/ili kako bi se ublažio rizik od nezakonite ponovne upotrebe UI modela opće namjene

⁷⁹ Te prakse također mogu pokrenuti dodatna pitanja koja nisu obuhvaćena ovim mišljenjem, vidjeti na primjer Pagallo U., Ciani Sciolla J., *Anatomy of web data scraping: ethics, standards, and the troubles of the law*. European Journal of Privacy Law & Technologies, (2023.) 2 str. 1.—19., dostupno na: <https://doi.org/10.57230/EJPLT232PS>.

⁸⁰ Osim ako voditelj obrade dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

(npr. digitalno označivanje vodenim žigovima izlaznih podataka generiranih umjetnom inteligencijom).

- b. **mjere kojima se olakšava ili ubrzava ostvarivanje prava pojedinaca** u fazi uvođenja, uz ono što je propisano zakonom, posebno, ali ne ograničavajući se na ostvarivanje prava na brisanje osobnih podataka iz modela izlaznih podataka ili deduplikaciju, kao i tehnike nakon treniranja kojima se pokušavaju ukloniti ili prikriti osobni podatci.

108. Pri istraživanju uvođenja određenog UI modela nadzorna tijela trebala bi razmotriti je li voditelj obrade objavio test ravnoteže koji je proveo jer bi se time mogla povećati transparentnost i poštenost. Kako je navedeno u Smjernicama EDPB-a o legitimnom interesu, mogu se razmotriti druge mjere da bi se ispitanicima pružile informacije iz testa ravnoteže prije svakog prikupljanja osobnih podataka⁸¹. EDPB također ponovno naglašava⁸² da je potrebno razmotriti je li voditelj obrade, gdje je to primjenjivo, uključio službenika za zaštitu podataka.

3.4 O mogućem učinku nezakonite obrade u razvoju UI modela na zakonitost naknadne obrade ili rada UI modela

109. Ovaj odjeljak mišljenja odnosi se na 4. pitanje u zahtjevu. Ovim se pitanjem traži pojašnjenje mogućeg učinka nezakonite obrade u fazi razvoja na naknadnu obradu (primjerice u fazi uvođenja UI modela) ili na rad modela. Pitanje se odnosi i na situaciju u kojoj takav UI model obrađuje osobne podatke koji su zadržani u modelu (pitanje 4. točka i. u zahtjevu), kao i na situaciju u kojoj nikakva obrada osobnih podataka više nije uključena u primjenu UI modela (tj. model je anoniman) (pitanje 4. točka ii. u zahtjevu).
110. Prije razmatranja određenih posebnih scenarija, EDPB navodi sljedeća opća razmatranja.
111. Kao prvo, pojašnjenja navedena u ovom odjeljku bit će usmjerena na obradu osobnih podataka u fazi razvoja koja se provodi, a da se pritom ne poštuje načelo zakonitosti kako je utvrđeno u članku 5. stavku 1. točki (a) Opće uredbe i posebno članku 6. Opće uredbe o zaštiti podataka (dalje u tekstu „**nezakonitost**”)⁸³. Isto tako, razmatranja EDPB-a usredotočit će se na učinak nezakonitosti obrade u fazi razvoja na zakonitost (tj. usklađenost s člankom 5. stavkom 1. točkom (a) i člankom 6. Opće uredbe) naknadne obrade ili rada modela. Međutim, EDPB ističe da obrada koja se provodi u fazi razvoja može dovesti i do kršenja drugih odredbi Opće uredbe, kao što je nedostatak transparentnosti prema ispitanicima ili tehnička i/ili integrirana zaštita podataka, koje se ne analiziraju u ovom mišljenju.
112. Kao drugo, pri rješavanju tog pitanja ključnu ulogu ima načelo odgovornosti, kojim se od voditelja obrade zahtijeva da budu odgovorni i dokažu usklađenost s, *među ostalim*, člankom 5. stavkom 1. i člankom 6⁸⁴. Opće uredbe o zaštiti podataka. To vrijedi i za potrebu da se procijeni koja je organizacija voditelj obrade za predmetnu aktivnost obrade i pojavljuju li se situacije zajedničkog vođenja obrade (jer one mogu biti usko povezane)⁸⁵. S obzirom na važnost činjeničnih okolnosti svakog slučaja, među

⁸¹ Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., stavak 68.

⁸² Smjernice EDPB-a 1/2024 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (f) Opće uredbe o zaštiti podataka, verzija 1.0, donesene 8. listopada 2024., stavak 12.

⁸³ Sud EU-a, presuda od 4. svibnja 2023., predmet C- 60/22, *Savezna Republika Njemačka* (ECLI:EU:C:2023:373), točke 55.–57.

⁸⁴ Sud EU-a, presuda od 4. svibnja 2023., predmet C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), točka 53.

⁸⁵ Smjernice EDPB-a 7/2020 o pojmovima voditelja i izvršitelja obrade u Općoj uredbi o zaštiti podataka, verzija 2.1, donesene 7. srpnja 2021., točka 55.

ostalim u pogledu uloge svake strane uključene u obradu, razmatranja EDPB-a trebala bi se tumačiti kao opća opažanja koja bi nadzorna tijela trebala procjenjivati ovisno o pojedinačnom slučaju.

113. Kao treće, EDPB ističe da su, u skladu s člankom 51. stavkom 1. Opće uredbe, nadzorna tijela „odgovorna za praćenje primjene [Opće uredbe o zaštiti podataka] kako bi se zaštitila temeljna prava i slobode pojedinaca u pogledu obrade i olakšao slobodan protok osobnih podataka unutar Unije”. Stoga je u nadležnosti nadzornih tijela da procijene zakonitost obrade i izvršavaju svoje ovlasti koje su im dodijeljene Općom uredbom u skladu sa svojim nacionalnim okvirom⁸⁶. U takvim slučajevima nadzorna tijela imaju diskrecijske ovlasti za procjenu mogućih kršenja i odabir primjerenih, nužnih i proporcionalnih mjera, među onima koje su navedene u članku 58. Opće uredbe, uzimajući u obzir okolnosti svakog pojedinačnog slučaja⁸⁷.
114. **Ako se utvrdi povreda, nadzorna tijela mogu izreći korektivne mjere, kao što je nalažanje voditeljima obrade, uzimajući u obzir okolnosti svakog slučaja, da poduzmu mjere kako bi se otklonila nezakonitost početne obrade.** To može uključivati, na primjer, izricanje novčane kazne, izricanje privremenog ograničenja obrade, brisanje dijela skupa podataka koji je nezakonito obrađen ili, ako to nije moguće, ovisno o činjenicama o kojima je riječ, uzimajući u obzir proporcionalnost mjere, davanje naloga za brisanje cijelog skupa podataka koji se upotrebljava za razvoj UI modela i/ili samog UI modela. Pri procjeni proporcionalnosti predviđene mjere nadzorna tijela mogu uzeti u obzir mjere koje voditelj obrade može primijeniti kako bi ispravio nezakonitost početne obrade (npr. ponovno treniranje).
115. EDPB ističe i da, kada se osobni podatci nezakonito obrađuju, ispitanici mogu zatražiti brisanje svojih osobnih podataka u skladu s uvjetima utvrđenima u članku 17. Opće uredbe te da nadzorna tijela mogu naložiti brisanje osobnih podataka *po službenoj dužnosti*⁸⁸.
116. Prilikom procjene je li mjera primjerena, nužna i proporcionalna, nadzorna tijela mogu, među ostalim elementima, razmotriti rizike koji nastaju za ispitanike, ozbiljnost kršenja, tehničku i financijsku izvedivost mjere te količinu uključenih osobnih podataka.
117. Naposljetku, EDPB podsjeća da se mjerama koje poduzimaju nadzorna tijela u skladu s Općom uredbom ne dovode u pitanje mjere koje su poduzela nadležna tijela na temelju Akta o umjetnoj inteligenciji i/ili drugih primjenjivih pravnih okvira (npr. zakonodavstvo o građanskopravnoj odgovornosti).
118. U sljedećim odjeljcima EDPB će razmotriti tri scenarija obuhvaćena 4. pitanjem u zahtjevu, pri čemu se razlike odnose na to zadržavaju li se u modelu osobni podatci koji se obrađuju radi razvoja modela i/ili provodi li naknadnu obradu isti ili drugi voditelj obrade.

⁸⁶ Možda će biti potrebno uzeti u obzir posebna nacionalna pravila. Vidjeti, na primjer, članak 2-decies talijanskog Zakona o zaštiti podataka (Zakonodavni dekret 196/2003) kojim se utvrđuje da se podatci koji se obrađuju protivno pravilima o zaštiti podataka ne mogu upotrebljavati. Time se ne dovode u pitanje drugi nacionalni pravni okviri, kao što su kazneni zakoni.

⁸⁷ Vidjeti u tom pogledu uvodnu izjavu 129. Opće uredbe o zaštiti podataka i presudu Suda Europske unije od 26. rujna 2024., predmet C-768 – 21, *TR protiv Land Hessen* (ECLI:EU:C:2024:785), točka 37.; presuda Suda EU-a od 7. prosinca 2023. u spojenim predmetima C-26/22 i C-64/22, *SCHUFA Holding (Libération de reliquat de dette)* (ECLI:EU:C:2023:958), točka 57.; i Sud EU-a, presuda od 14. ožujka 2024., predmet C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), točka 34.

⁸⁸ U tom pogledu, mišljenje EDPB-a 39/2021 o tome može li članak 58. stavak 2. točka (g) Opće uredbe o zaštiti podataka služiti kao pravna osnova na temelju koje nadzorno tijelo može po službenoj dužnosti naložiti brisanje osobnih podataka u situaciji u kojoj ispitanik nije podnio takav zahtjev, točka 28. Vidjeti u tom pogledu i presudu Suda EU-a od 14. ožujka 2024., predmet C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), točka 42.

3.4.1 Scenarij 1. Voditelj obrade nezakonito obrađuje osobne podatke za razvijanje modela, osobni podatci zadržani su u modelu i naknadno ih obrađuje isti voditelj obrade (na primjer u kontekstu uvođenja modela)

119. Taj se scenarij odnosi na pitanje 4. točku (i) u zahtjevu, u situaciji u kojoj voditelj obrade nezakonito obrađuje osobne podatke (tj. nepoštovanjem članka 5. stavka 1. točke (a) i članka 6. Opće uredbe o zaštiti podataka) radi razvoja UI modela, a UI model zadržava informacije koje se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi i stoga nije anoniman. Osobne podatke zatim naknadno obrađuje isti voditelj obrade (na primjer u kontekstu uvođenja modela). Kad je riječ o tom scenariju, EDPB navodi sljedeća razmatranja.
120. Ovlast nadzornog tijela da uvede korektivne mjere za početnu obradu (kako je objašnjeno u prethodnim točkama 113., 114. i 115.) u načelu bi utjecala na naknadnu obradu (npr. ako nadzorno tijelo naloži voditelju obrade da izbriše osobne podatke koji su nezakonito obrađeni, takve korektivne mjere ne bi omogućile potonjem da naknadno obradi osobne podatke koji su bili predmet mjera).
121. Kad je riječ posebno o učinku nezakonite obrade u fazi razvoja na naknadnu obradu (na primjer u fazi uvođenja), EDPB podsjeća da nadzorna tijela trebaju provesti analizu svakog pojedinačnog slučaja kojom se uzimaju u obzir posebne okolnosti svakog slučaja.
122. **Pitanje uključuju li faze razvoja i uvođenja zasebne svrhe (koje čine zasebne aktivnosti obrade) i mjeru u kojoj nedostatak pravne osnove za početnu aktivnost obrade utječe na zakonitost naknadne obrade trebalo bi procjenjivati ovisno o pojedinačnom slučaju i ovisno o kontekstu predmeta.**
123. Na primjer, s obzirom na pravnu osnovu članka 6. stavka 1. točke (f) Opće uredbe, ako se naknadna obrada temelji na legitimnom interesu, u procjeni legitimnog interesa trebalo bi uzeti u obzir činjenicu da je početna obrada bila nezakonita (npr. u pogledu rizika za ispitanike ili činjenice da ispitanici ne mogu očekivati takvu naknadnu obradu). U tim slučajevima nezakonitost obrade u fazi razvoja može utjecati na zakonitost naknadne obrade.

3.4.2 Scenarij 2. Voditelj obrade nezakonito obrađuje osobne podatke za razvijanje modela, osobni podatci zadržani su u modelu i obrađuje ih drugi voditelj obrade u kontekstu uvođenja modela

124. Taj se scenarij odnosi na pitanje 4. točku (i) zahtjeva. Razlikuje se od scenarija 1 (u odjeljku 3.4.1. ovog mišljenja) jer osobne podatke naknadno obrađuje drugi voditelj obrade u kontekstu uvođenja UI modela.
125. EDPB podsjeća da je utvrđivanje uloga dodijeljenih tim različitim akterima u okviru za zaštitu podataka ključan korak kako bi se utvrdilo koje se obveze na temelju Opće uredbe primjenjuju i tko je odgovoran za te obveze te da bi se situacije zajedničkog vođenja obrade trebale uzeti u obzir i pri procjeni odgovornosti svake strane na temelju Opće uredbe. Stoga bi se opažanja u nastavku trebala smatrati općim elementima koje bi nadzorna tijela, prema potrebi, trebala uzeti u obzir. Kad je riječ o spomenutom scenariju 2, EDPB navodi sljedeća razmatranja.
126. Prvo, treba podsjetiti da bi, u skladu s člankom 5. stavkom 1. točkom (a) Opće uredbe, uzimajući u obzir njezin članak 5. stavak 2., svaki voditelj obrade trebao osigurati zakonitost obrade koju provodi i moći je dokazati. Stoga bi nadzorna tijela trebala procijeniti zakonitost obrade koju provodi i. voditelj obrade koji je izvorno razvio UI model i ii. voditelj obrade koji je pribavio UI model i koji sam obrađuje osobne podatke.

127. Kao drugo, razmatranje iz prethodnih stavaka 113., 114. i 115. relevantno je u ovom slučaju u pogledu ovlasti nadzornih tijela da interveniraju u odnosu na početnu obradu. Članak 17. stavak 1. točka (d) Opće uredbe (brisanje nezakonito obrađenih podataka) i članak 19. Opće uredbe (obveza obavješćivanja u vezi s ispravkom ili brisanjem osobnih podataka ili ograničenjem obrade) mogu, ovisno o okolnostima slučaja, biti relevantni i u ovom kontekstu, na primjer u vezi s obavijesti koju bi voditelj obrade koji razvija model trebao uputiti voditelju obrade koji uvodi model.
128. Kao treće, kad je riječ o mogućem učinku nezakonitosti početne obrade na naknadnu obradu koju provodi drugi voditelj obrade, takvu bi procjenu nadzorna tijela trebala provoditi ovisno o pojedinačnom slučaju.
129. **Nadzorna tijela trebala bi uzeti u obzir je li voditelj obrade koji uvodi model proveo odgovarajuću procjenu, kao dio svojih obveza odgovornosti⁸⁹ kako bi dokazao usklađenost s člankom 5. stavkom 1. točkom (a) i člankom 6. Opće uredbe, kako bi utvrdio da UI model nije razvijen nezakonitom obradom osobnih podataka.** Pri takvoj evaluaciji nadzornih tijela trebalo bi uzeti u obzir je li voditelj obrade procijenio neke neiscrpne kriterije, kao što su izvor podataka, i je li UI model rezultat kršenja Opće uredbe, posebno ako ga je utvrdilo nadzorno tijelo ili sud, kako voditelj obrade koji uvodi model ne bi mogao zanemariti činjenicu da je početna obrada bila nezakonita.
130. Voditelj obrade trebao bi razmotriti, na primjer, jesu li podatci proizašli iz povrede osobnih podataka ili je obrada bila podložna utvrđenju povrede od strane nadzornog tijela ili suda. **Stupanj procjene voditelja obrade i razina detalja koje nadzorna tijela očekuju mogu se razlikovati ovisno o različitim čimbenicima, uključujući vrstu i stupanj rizika koji proizlaze iz obrade u UI modelu tijekom njegova uvođenja u odnosu na ispitanike čiji su podatci upotrijebljeni za razvoj modela.**
131. EDPB napominje da se Aktom o umjetnoj inteligenciji od pružatelja visokorizičnih UI sustava zahtijeva da pripreme izjavu EU-a o sukladnosti⁹⁰ i da takva izjava sadržava izjavu da je relevantni UI sustav u skladu sa zakonima EU-a o zaštiti podataka⁹¹. EDPB napominje da takva osobna izjava možda neće predstavljati konačan zaključak o usklađenosti u skladu s Općom uredbom. Bez obzira na to, nadzorna tijela mogu je uzeti u obzir pri ispitivanju određenog UI modela.
132. Ista razmatranja iznesena u točki 123. ove presude također su relevantna u ovom slučaju. Kada nadzorna tijela provjeravaju je li i na koji način voditelj obrade procijenio primjerenost legitimnog interesa kao pravne osnove za obradu koju provodi, nezakonitost početne obrade trebalo bi uzeti u obzir kao dio procjene legitimnog interesa, primjerice procjenom potencijalnih rizika koji bi mogli nastati za ispitanike čiji su osobni podatci nezakonito obrađeni radi razvoja modela. Različiti aspekti, bilo tehničke prirode (npr. postojanje filtara ili ograničenja pristupa postavljenih tijekom razvoja modela, koje naknadni voditelj obrade ne može zaobići ili na njih utjecati te koji bi mogli spriječiti pristup osobnim podacima ili njihovo otkrivanje) ili pravne prirode (npr. priroda i ozbiljnost nezakonitosti početne obrade) moraju se uzeti u obzir u okviru testa ravnoteže.

3.4.3 Scenarij 3. Voditelj obrade nezakonito obrađuje osobne podatke kako bi razvio model, a zatim osigurava da je model anonimiziran, prije nego što isti ili drugi voditelj obrade započne drugu obradu osobnih podataka u kontekstu uvođenja

133. Taj se scenarij odnosi na pitanje 4. točku ii. zahtjeva i odnosi se na slučaj u kojem voditelj obrade nezakonito obrađuje osobne podatke kako bi razvio UI model, ali to čini na način kojim se osigurava da

⁸⁹Članak 5. stavak 2. i članak 24. Opće uredbe o zaštiti podataka.

⁹⁰Članak 16. točka (g) i članak 47. Akta o umjetnoj inteligenciji.

⁹¹Prilog V. točka 5. Akta o umjetnoj inteligenciji.

su osobni podatci anonimizirani prije nego što isti ili neki drugi voditelj obrade pokrene drugu obradu osobnih podataka u kontekstu uvođenja. Prvo, EDPB podsjeća da su nadzorna tijela nadležna i ovlaštena intervenirati u pogledu obrade povezane s anonimizacijom modela, kao i obrade koja se provodi tijekom faze razvoja. Stoga nadzorna tijela mogu, ovisno o posebnim okolnostima slučaja, izreći korektivne mjere za tu početnu obradu (kako je objašnjeno u prethodnim točkama 113., 114., 115.).

134. Ako se može dokazati da daljnji rad UI modela ne podrazumijeva obradu osobnih podataka, EDPB smatra da se Opća uredba o zaštiti podataka ne bi primjenjivala⁹². Stoga nezakonitost početne obrade ne bi trebala utjecati na daljnji rad modela. Međutim, EDPB naglašava da sama tvrdnja o anonimnosti modela nije dovoljna da bi ga se izuzelo od primjene Opće uredbe te napominje da bi ga nadzorna tijela trebala procijeniti uzimajući u obzir, ovisno o pojedinačnom slučaju, razmatranja koja je EDPB iznio za rješavanje 1. pitanja iz zahtjeva.
135. **Kada voditelji obrade naknadno obrađuju osobne podatke prikupljene tijekom faze uvođenja, nakon što model bude anonimiziran, Opća uredba primjenjivala bi se u vezi s tim aktivnostima obrade. U tim slučajevima, kad je riječ o Općoj uredbi, nezakonitost početne obrade ne bi trebala utjecati na zakonitost obrade provedene u fazi uvođenja.**

4 Završne napomene

136. Ovo mišljenje upućuje se svim nadzornim tijelima i bit će objavljeno u skladu s člankom 64. stavkom 5. točkom (b) Opće uredbe.

Za Europski odbor za zaštitu podataka

Predsjednica

Anu Talus

⁹² Uvodna izjava 26. Opće uredbe o zaštiti podataka.