DOKUMENT JE ELEKTRONSKO PODPISAN!
Podpisnik: Ksenija Klampfer
Izdajatelj certifikata: SI-PASS-CA
Številka certifikata: 00DEF93E9F0000000057
Potek veljavnosti: 01. 04. 2027
Čas podpisa: 11. 03. 2026 10:00
Št. dokumenta: 631-12/2024-3150-83

REPUBLIKA SLOVENIJA
MINISTRSTVO za DIGITALNO PREOBRAZBO
Davčna ulica 1, 1000 Ljubljana

T: 01 555 58 00
E: gp.mdp@gov.si
www.mdp.gov.si

Številka: 631-12/2024-3150-83
Datum: 02. 03. 2026

SMERNICE ZA RAZVOJ, UVAJANJE IN UPORABO UMETNE INTELIGENCE V JAVNI UPRAVI

mag. Ksenija Klampfer
ministrica

Ljubljana, marec 2026

KAZALO VSEBINE

1 UVOD

1.1 Namen

Namen Smernic za razvoj, uvedbo in uporabo umetne inteligence v javni upravi (v nadaljevanju: *Smernice*) je organom javne uprave kot uvajalcem in ponudnikom sistemov umetne inteligence (v nadaljevanju: sistem UI) podati praktična, pravna in etična izhodišča za varno, odgovorno in učinkovito uvajanje UI v delovne procese in v storitve, ki jih zagotavljajo za državljane in podjetja, oziroma za razvijanje tovrstnih sistemov kot ponudnik. Predmetni dokument je namenjen tudi javnim uslužbencem, ki orodja UI, javno dostopna na svetovnem spletu, uporabljajo pri svojem delu. Smernice narekujejo varnostne zahteve in priporočila glede vpisovanja in obdelave varovanih podatkov v sisteme UI.

Dokument tako podrobneje opredeljuje postopek sprejemanja odločitve o uvedbi sistemov UI v informacijske rešitve v javni upravi in ob upoštevanju v nadaljevanju navedene zakonodaje narekuje *(1)* zagotavljanje varstva osebnih in drugih pravno varovanih podatkov, *(2)* zagotavljanje ustrezne ravni informacijsko-komunikacijske in kibernetske varnosti, *(3)* zaščito temeljnih pravic in svoboščin. Informacijske rešitve, ki vključujejo UI, morajo prispevati k izboljšanju učinkovitosti delovnih procesov in storitev za državljane in podjetja, pri njihovi implementaciji pa je treba zagotoviti, da ne temeljijo na diskriminatornih podatkih. Uvajanje UI mora stremeti tudi k večji preglednosti in odgovornosti ter k varni uporabi informacijsko-komunikacijskih tehnologij v javni upravi. Osrednji del dokumenta tako predstavlja opis procesa, ki mu mora organ javne uprave slediti, ko se odloča, kateri sistem UI v konkretnem primeru uporabiti oziroma ga razviti.

1.2 Relevantni predpisi in posebej problematična področja

Organ javne uprave mora pri sprejemanju odločitve o uvedbi sistema UI ali njegovem razvoju upoštevati predvsem naslednjo zakonodajo:

1. Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (v nadaljevanju: *Akt o umetni inteligenci*),
2. Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (v nadaljevanju: *Splošna uredba o varstvu podatkov*),
3. Zakon o izvajanju uredbe (EU) o določitvi harmoniziranih pravil o umetni inteligenci (Uradni list RS, št. 85/25; v nadaljevanju: *ZIUDHPUI*),
4. Zakon o varstvu osebnih podatkov (Uradni list RS, št. 163/22 in 40/25 – ZInfV-1; v nadaljevanju: *ZVOP-2*),

5. Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (Uradni list RS, št. 177/20ZVOPoKD, v nadaljevanju: ZVOPOKD),
6. Uredba (EU) 2022/868 Evropskega parlamenta in Sveta z dne 30. maja 2022 o evropskem upravljanju podatkov in spremembi Uredbe (EU) 2018/1724 (v nadaljevanju: Akt o upravljanju podatkov),
7. Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11, 8/20 in 18/23 – ZDU-1O; v nadaljevanju: *ZTP*),
8. Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (Uradni list RS, št. 30/06, 24/14 – odl. US in 51/14, v nadaljevanju: *ZVDAGA*),
9. Uredba o varstvu dokumentarnega in arhivskega gradiva (Uradni list RS, št. 42/17, v nadaljnjem besedilu: UVDAG),
10. Zakon o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljevanju: ZInfV-1),
11. Zakon o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15, 63/16 – ZKUASP, 59/19 in 130/22; v nadaljevanju: ZASP),
12. Zakon o kritični infrastrukturi (Uradni list RS, št. 102/24; v nadaljevanju: ZKI-1),
13. Okvirna Konvencija Sveta Evrope o umetni inteligenci, človekovih pravicah, demokraciji in pravni državi[1],
14. Etične smernice za zaupanja vredno umetno inteligenco[2],
15. Uredba o upravnem poslovanju (Uradni list RS, št. 9/18, 14/20, 167/20, 172/21, 68/22, 89/22, 135/22, 77/23 in 24/24, v nadaljevanju: UUP),

pri čemer so navedeni EU in nacionalni predpisi med seboj komplementarni.

Pri uvajanju sistema UI oziroma pri razvoju sistema UI mora biti organ javne uprave še posebej pozoren, v kolikor bi v procesu obdelave vstopali podatki s področja obrambe, Policije ali nacionalne varnosti.

1.3 Definicije dodatnih izrazov, uporabljenih v smernicah

1.3.1 Splošno

Izrazi, uporabljeni v tem dokumentu, imajo enak pomen, kot v pravnih aktih, ki jih definirajo.

1.3.2 Življenjski cikel sistema UI

Običajno zajema več faz, ki vključujejo: načrtovanje in oblikovanje, zbiranje in obdelavo podatkov, razvoj modela oziroma prilagoditev obstoječega/ih modela/ov za specifične naloge, testiranje, ocenjevanje, preverjanje in potrjevanje. Prehod v produkcijsko uporabo (implementacija) zahteva spremljanje in kontinuirano izboljševanje na podlagi novih podatkov in povratnih informacij. Konec

[1] Ang. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Vilnius, 5. IX. 2024, dostopne na povezavi: CETS 225 - Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (zajem na dan 28. 1. 2026),
[2] (Dostopne na povezavi: Etične smernice za zaupanja vredno umetno inteligenco | Shaping Europe's digital future; zajem dne 23. 9. 2025).

cikla predstavlja faza umika oz. ukinitve sistema UI. Te faze se pogosto izvajajo ponavljalno in niso nujno zaporedne.

1.3.3 Sistem UI

Sistem UI je v skladu z Aktom o umetni inteligenci opredeljen kot sistem temelječ na napravah, ki je zasnovan za delovanje z različnimi stopnjami avtonomije in lahko po uvedbi izkaže prilagodljivost ter za eksplicitne ali implicitne cilje iz prejetih vhodnih podatkov sklepa, kako ustvariti izhodne podatke, kot so napovedi, vsebine, priporočila ali odločitve, ki lahko vplivajo na fizična ali virtualna okolja.

Definicija ima tako sedem elementov, ki morajo biti izpolnjeni, da sistem lahko štejemo kot sistem umetne inteligence in sicer:

1. sistem mora temeljiti na napravah;
2. zasnovan je za delovanje z različnimi stopnjami avtonomije;
3. lahko po uvedbi izkaže prilagodljivost;
4. za eksplicitne ali implicitne cilje;
5. iz prejetih vhodnih podatkov sklepa, kako ustvariti izhodne podatke,
6. kot so napovedi, vsebine, priporočila ali odločitve;
7. izhodni podatki lahko vplivajo na fizična ali virtualna okolja.

V skladu s Smernicami o definiciji sistema UI[3] ni nujno, da so vsi pogoji izpolnjeni v celotnem življenjskem ciklu sistema UI, nekateri so lahko izpolnjeni le z fazi razvoja sistema UI ali pa v fazi uvajanja sistema UI, lahko pa so tudi podani kumulativno.

1.3.4 Različne vrste umetne inteligence

Smernice se nanašajo na vse vrste umetne inteligence, kot na primer: generativno, prediktivno, prepoznavanje slik.

V nadaljevanju so opisane glavne značilnosti generativne umetne inteligence in velikih jezikovnih modelov kot pojmov, ki se pogosto uporabljata v splošni teoriji obravnave UI kot tudi v pričujočih smernicah.

1.3.4.1 Generativna umetna inteligenca

Generativna UI je tehnologija, ki sodi na področje strojnega učenja in ne prave »inteligence«. V resnici ne razume konceptov, temveč ustvarja vsebino, ki je statistično najbolj verjetna (najboljši odgovor) glede na poziv oziroma poizvedbo. Pri njeni uporabi se za izboljšanje rezultatov

[3] Smernice so dostopne na: https://ec.europa.eu/newsroom/dae/redirection/document/118642 (zajem na dan 28. 1. 2026).

uporablja človeški nadzor in okrepljeno učenje, uporabniki sami pa morajo, če želijo izboljšati pridobljeni rezultat, zagotoviti povratne informacije ali spremeniti svoj poziv (prompt). V praksi se vedno bolj kaže, da se najboljši rezultati pridobijo, če uporabniki nadzorujejo nabor dokumentov, v katerih bodo iskali odgovore. Generativno UI je mogoče natančno prilagoditi ali namensko usposobiti in posledično uporabiti modele po meri tako, da ustrezajo potrebam delovnega procesa (za to se uporabi sprogramirane agente z zaporednimi, vzporednimi pozivi, vmesnimi obdelavami rezultatov, povratnimi zankami ipd.).

Primeri generativne UI:

- sistemi UI, ki temeljijo na velikih jezikovnih modelih (npr. ChatGPT, Claude, Gemini), ki generirajo besedilo,
- sistemi UI, ki temeljijo na difuzijskih modelih (npr. DALL-E, Modjourney, Stable Diffusion), ki generirajo slike, tekst – v - govor,
- sistemi UI (npr. ElevenLabs), ki generirajo govor ter
- sisteme UI, ki ustvarjajo video iz opisa (t. i. video generacije) (npr. Sora Open AI).

1.3.4.2 Veliki jezikovni modeli (LLM)

Veliki jezikovni modeli (LLM) so napredni sistemi UI, zasnovani za obdelavo, razumevanje in ustvarjanje besedila. Temeljijo na tehnikah globokega učenja in se usposabljajo na zbirkah podatkov, ki vsebujejo več milijard besed iz različnih virov, kot so spletna mesta, knjige in članki. To obsežno usposabljanje omogoča uporabo velikih jezikovnih modelov v informacijskih rešitvah na način, da precej učinkovito posnemajo razumevanje odtenkov jezika, slovnice, konteksta in celo nekaterih vidikov splošnega znanja. Veliki jezikovni modeli predstavljajo specifičen podtip generativne UI, specializiran za obdelavo in generiranja človeškega jezika, temeljijo na ogromnih količinah besedilnih podatkov in so usposobljenih za povzemanje, prevajanje, ustvarjanje besedil itd..

Informacijske rešitve, ki uporabljajo velike jezikovne modele, lahko opravljajo široko paleto nalog, kot so:

- odgovarjanje na vprašanja,
- povzemanje besedila,
- prevajanje jezikov,
- ustvarjanje vsebine (zlasti osnutkov),
- celo sodelovanje v interaktivnih pogovorih z uporabniki,
- povezujejo se lahko na primer s spletom in kot multimodalni sistem UI celo ustvarjajo slike, zvočne in video zapise, ipd.

Ker se LLM-ji še naprej razvijajo, imajo velik potencial za izboljšanje in avtomatizacijo različnih informacijskih rešitev v širši družbi, torej vrsti panog, od storitev za stranke in ustvarjanja vsebin

do izobraževanja in raziskav. Vendar pa njihova uporaba sproža tudi etične in družbene pomisleke, kot je pristransko vedenje (danes sicer vemo, da je to posledica diskriminatornih vhodnih podatkov) ali zloraba, ki jih je treba naslavljati vzporedno z napredkom tehnologije.

Zato je pomembno, da se morebitni uvajalci LLM zavedajo, da so bistveni dejavniki pri pripravi zbirk podatkov, na katerih se bodo izvajale obdelave, ki zagotavljajo kakovostne rezultate:

- kakovost, raznolikost in količina podatkov,
- nediskriminatornost podatkov,
- izbira ustreznih virov podatkov,
- uporaba sintetičnega ustvarjanja podatkov,
- avtomatizirano zbiranje podatkov.

V zvezi z velikimi jezikovnimi modeli (LLM) je potrebno izpostaviti tudi t. i. bazo znanja, ki v povezavi z UI označuje eksplicitno shranjeno zbirko podatkov in znanj o določenem področju, ki se uporablja za sklepanje in reševanje problemov. Baza znanja tako vključuje dejstva, pravila, koncepte in odnose med njimi (npr. med učnimi podatki, v pogovorih z UI, v dokumentih, ki jih sistem UI obdeluje). Podatki, ki se v tem okviru obdelujejo, so lahko tudi varovani podatki (vključno z osebnimi podatki) in jih je treba kot takšne obravnavati.

2 NAČELA ZA ZAUPANJA VREDNO UMETNO INTELIGENCO V JAVNI UPRAVI

Pri razvoju in uvajanju sistemov UI v poslovne procese je treba upoštevati načela, ki izhajajo iz Etičnih smernic za zaupanja vredno umetno inteligenco ter Okvirne konvencije Sveta Evrope o umetni inteligenci, človekovih pravicah, demokraciji in pravni državi (v nadaljevanju: Okvirna konvencija). V Etičnih smernicah je predstavljen sklop sedmih ključnih zahtev, ki bi jih morali izpolnjevati sistemi UI, da bi se šteli za zaupanja vredne, poudarki bistvenih načel so naslednji:

2.1 Človekovo delovanje in nadzor

Sistemi UI bi morali opolnomočiti ljudi, da bi lahko sprejemali informirane odločitve in spodbujali njihove temeljne pravice. Istočasno pa je treba zagotoviti, da končne odločitve sprejema človek, ki ima tudi možnost preverjanja vsakega dela postopka. Za zagotavljanje človeškega nadzora je nujno zagotoviti ustrezna znanja in orodja za zadovoljivo razumevanje sistemov UI in interakcijo z njimi ter jim po možnosti omogočiti, da razumno sami ocenijo ali izpodbijajo sistem.

2.2 Tehnična robustnost, zanesljivost in varnost

Sistemi UI morajo biti odporni in varni. Biti morajo varni, zagotoviti nadomestni načrt, če gre kaj narobe, ter biti točni, zanesljivi in ponovljivi. To je edini način za zmanjševanje in preprečevanje nenamerne škode.

Okvirna konvencija v zvezi s predmetnim načelom izpostavlja še spodbujanje zanesljivosti sistemov UI in zaupanja v njihove rezultate, vključno z zahtevami v zvezi z ustrezno kakovostjo in varnostjo skozi celoten življenjski cikel sistema UI.

2.3 Zasebnost in upravljanje podatkov

Sistemi UI morajo pri svojem delovanju spoštovati zasebnost posameznikov, katerih podatki se v sistemih obdelujejo, in v tem smislu za svoje rezultate uporabljati predvsem kakovostne podatke, do katerih lahko dostopajo le upravičene osebe.

Okvirna konvencija v zvezi s predmetnim načelom narekuje sprejetje ukrepov, s katerimi zagotovi, da se v zvezi z dejavnostmi v življenjskem ciklu sistema UI varujejo pravice posameznikov do zasebnosti in njihovi osebni podatki ter da se uvedejo učinkovita jamstva in zaščitni ukrepi za posameznike (oboje ob upoštevanju veljavnih nacionalnih in mednarodnih pravnih obveznosti).

2.4 Preglednost

Poslovni modeli podatkov, sistema UI in umetne inteligence morajo biti pregledni, za svoje delovanje pa morajo zagotavljati sledljivost. Sisteme UI in njihove odločitve je tudi treba pojasniti

na način, prilagojen deležniku, pri čemer mora biti slednji seznanjen, da so v stiku s sistemom UI, ter biti obveščeni o njegovih zmogljivostih in omejitvah.

Okvirna konvencija v zvezi s predmetnim načelom dodaja še, da morajo biti v zvezi z dejavnostmi v življenjskem ciklu sistemov UI, vključno z identifikacijo vsebin, ki jih ustvarjajo sistemi UI, vzpostavljene ustrezne zahteve glede preglednosti in nadzora, prilagojene posebnim okoliščinam in tveganjem.

2.5 Nediskriminacija in pravičnost

Sistemi UI morajo zagotavljati rezultate, ki omogočajo ne le zakonite, temveč tudi pravične odločitve. Stremeti morajo tudi k vzpostavitvam rešitev, ki bi lahko zagotavljale ugotavljanje njihove morebitne diskriminatornosti, ki bi izhajala iz predhodnih diskriminatornih odločitev. S spodbujanjem raznolikosti bi morali biti sistemi UI dostopni tudi osebam z različnimi oblikami oviranosti.

Okvirna konvencija v zvezi s predmetnim načelom še izpostavlja, da morajo dejavnosti v življenjskem ciklu sistemov UI spoštovati enakost, vključno z enakostjo spolov, in prepoved diskriminacije, kot je določeno v veljavni mednarodni in nacionalni zakonodaji. Pri vseh dejavnostih v življenjskem ciklu sistema UI je treba sprejeti ukrepe za premagovanje neenakosti z namenom doseganja poštenih, pravičnih in enakopravnih rezultatov v skladu s svojimi veljavnimi nacionalnimi in mednarodnimi obveznostmi na področju človekovih pravic.

2.6 Družbena in okoljska blaginja

Sistemi UI morajo biti trajnostni in okolju prijazni, njihova uporaba pa mora upoštevati zdravo življenjsko okolje za ljudi in druga živa bitja, s predhodnim razmislekom o njihovem družbenem vplivu.

2.7 Odgovornost

Ob uporabi sistemov UI morajo biti vzpostavljeni mehanizmi za zagotavljanje odgovornosti za sisteme UI in njihove rezultate. Zagotoviti je treba možnost revizije pridobljenih rezultatov, ki vključuje oceno algoritmov, podatkov in izvedenih postopkov. Zagotoviti je potrebno ustrezno dostopno pravno sredstvo.

Okvirna konvencija Sveta Evrope o umetni inteligenci, človekovih pravicah, demokraciji in pravni državi v zvezi s predmetnim načelom omenja še odgovornost za škodljive vplive na človekove pravice, demokracijo in pravno državo, ki te izhajajo iz dejavnosti v življenjskem ciklu sistemov umetne inteligence.

Okvirna konvencija poleg že navedenega posebej izpostavlja še naslednja načela:

2.8 Človekovo dostojanstvo in individualna avtonomija

Pri vseh dejavnostih v življenjskem ciklu sistemov UI je potrebno zagotoviti spoštovanje človekovega dostojanstva in individualne avtonomije.

2.9 Varne inovacije

Da bi spodbudili inovacije in hkrati preprečili negativne učinke na človekove pravice, demokracijo in pravno državo, se po potrebi omogoči vzpostavitev nadzorovanih okolij za razvoj, eksperimentiranje in testiranje sistemov umetne inteligence pod nadzorom svojih pristojnih organov.

Poleg navedenih načel predmetni dokument uvaja naslednje načelo, in sicer:

2.10 Javnost podatkov v javnem sektorju

Organi javnega sektorja pa morajo poleg spoštovanja vseh navedenih načel upoštevati, da državljani bistveno bolj zaupajo sistemom, ki jih lahko preverijo, kar pomeni, da morajo organi javnega sektorja v največji možni meri zagotavljati javnost podatkov, ter nuditi čim več informacij, kolikor je to mogoče, zaradi zagotavljanja tehnične varnosti informacijskih rešitev, o delovanju informacijskih rešitev in v njihovih okvirih sistemov UI.

3 SPREJEMANJE ODLOČITVE O UVEDBI UMETNE INTELIGENCE

Organ javne uprave pri sprejemanju odločitve o uvedbi ali razvoju sistema UI v posamezen proces zasleduje vsaj cilje smotrnosti, primernosti, ustreznosti, zakonitosti in trajnosti.

3.1 Sprejem odločitve

Sprejem odločitve mora temeljiti na naslednjih korakih:

- **a)** Ocena potreb (določitev področja, procesa, nalog, storitev, na katerem se bo uporabljal UI), ki se jo pripravi na podlagi kontrolnega vprašalnika,
- **b)** Financiranje in kadrovski viri (zagotovitev ustreznih finančnih sredstev za uvedbo UI – razvoj sistema UI, njegovo uvedbo in zagotavljanje podpore ter ocena števila zaposlenih, ki bodo pri uvedbi in kasneje pri uporabi sistema UI sodelovali),
- **c)** Zagotavljanje skladnosti (zagotovitev skladnosti z določbami Akta o umetni inteligenci, kar pomeni, da mora organ javne uprave poskrbeti, da je sistem UI, ki ga uvaja ali razvija skladen z uredbo EU na tem področju (podrobnejši opis v poglavju 3.5 tega dokumenta) in za primer, da v proces uvedbe ali razvoja sistema UI vstopajo osebni, tajni ali drugi varovani podatki oziroma se ti zagotavljajo iz več različnih virov ter v primeru, da bo navedeni sistem povezan z drugimi informacijskimi rešitvami pa je potrebno zagotoviti oziroma izdelati:
  - celovito oceno tveganj vključno z:
    - oceno učinkov v zvezi z varstvom osebnih podatkov[4], ki omogoča identifikacijo, analizo in določitev ukrepov za zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki;
    - varnostnim vrednotenjem po ZTP;
    - ocena po ZInfV-1;
    - proučitev vidika avtorskih in sorodnih pravic.
  - načrt za obvladovanje morebitnih tveganj.
- **d)** Obstoj kakovostnih podatkov, kot temelj za učinkovito uporabo UI, zato morajo organi javnega sektorja – v kolikor želijo zagotavljati dobre rešitve – vzpostaviti tudi zanesljive sisteme za zbiranje, upravljanje in izmenjavo podatkov.

Pri načrtovanju in razvoju informacijskih rešitev s področja UI je potrebno zagotoviti skladnost z najnovejšimi standardi s tega področja, kot na primer: ISO/IEC 42001:2023 (mednarodni standard namenjen vzpostavitvi sistema upravljanja umetne inteligence, AI Management System – AIMS). Standard organizacijam omogoča, da umetno inteligenco razvijajo in uporabljajo odgovorno, varno, etično in skladno z zakonodajo. Na podlagi ISO 42001 so bili razviti tudi nekateri odprtokodni modeli. Izbiro modela ali rešitve na področju UI, ki ne ustreza tovrstnim standardom, je potrebno posebej utemeljiti in odstopanje od standardov upoštevati pri oceni tveganj.

[4] Ocena učinka v zvezi z varstvom podatkov - IPRS

3.2 Kriteriji za uvedbo umetne inteligence v informacijske rešitve

3.2.1 Kontrolni vprašalnik za pripravo ocene potreb za uvajanje umetne inteligence

Ocena potreb se opravi na način, da se najprej opredeli naslednje:

- določitev področja na katerem se uvaja sistem UI,
- določitev procesa/naloge/storitve, v katerem se bo sistem UI uporabljal in čemu je sistem UI namenjen (opredelitev npr. ali gre za hitrejše pridobivanje podatkov, ali za pomoč pri sprejemanju odločitev, ipd.),
- kakšen je vpliv uvedbe sistema UI na porabo energije in drugih naravnih virov ter na emisije toplogrednih plinov v primerjavi z obstoječim načinom dela; ali je uvedba sistema UI skladna z nacionalnimi cilji razogljičenja in prilagajanja podnebnim spremembam.

Pri vsaki od alinej se opredelita tako trenutni način poslovanja in načrtovani način poslovanja.

Nato se oceni, ali proces resnično potrebuje podporo z UI, in sicer tako, da organ javne uprave navede in pojasni razloge za uvedbo umetnointeligenčne rešitve, pri čemer mora zagotoviti odgovore vsaj na naslednja vprašanja:

- ali je želene cilje mogoče doseči brez uporabe UI,
- kakšne so posledice, če se uporabe UI ne zagotovi:
    - z vidika izvajanja naloge: naloge sploh ne bi bilo mogoče opraviti,
    - s časovnega vidika: nalogo je / ni mogoče zagotoviti pravočasno ali učinkovito / nalogo je / ni mogoče zagotoviti bistveno hitreje,
    - s finančnega vidika se pripravi oceno stroškov in se ugotovi: stroški naloge so manjši / enaki / večji kot stroški ne uvedbe sistema UI oziroma umetnointeligenčne rešitve,
    - z vidika kakovosti: kakovost naloge, kot se opravlja brez uporabe UI je / ni dovolj visoka / pričakuje se izboljšanje kakovosti naloge, ipd.,
    - z vidika ciljev uspešnosti: izvajanje naloge brez uporabe UI lahko / ne more doseči ciljev uspešnosti.
- ali uvedba podpore z uporabo UI prinaša dodano vrednost oziroma, kaj je predvidena dodana vrednost, ki je ni mogoče izvesti v predvidenem obsegu na drug način, na primer:
    - odprava obstoječih zaostankov pri delu ali zadevah,
    - izboljšanje splošne kakovosti rezultatov dela/odločitev,
    - znižanje transakcijskih stroškov obstoječe informacijske rešitve,
    - sistem UI bistveno vpliva na hitrost izvajanja naloge (sistem UI opravlja naloge, ki jih ljudje ne bi mogli opraviti v razumnem času),
    - uporaba inovativnih pristopov, ki bi lahko vodili v razvoj na določenem področju,
    - optimizacija prometnih tokov v realnem času za zmanjšanje zastojev in emisij, napovedovanje potreb po javnem prevozu za boljšo prilagoditev voznih redov, avtomatska detekcija poškodb na prometni infrastrukturi, ipd.).

- kakšna je ocena stroškov izvajanja procesov, pri čemer se upošteva:
    - kako pogosto se izvajajo naloge v procesu, v katerega se uvaja sistem UI (dnevno, tedensko, mesečno, obdobno, letno),
    - stroške uvedbe sistema UI, v katerega se vključi stroške razvoja, uvedbe, pa tudi uporabe sistema (predvidena količina in cena elektrike),
    - kakšen je potreben čas za izvedbo procesa (naloge) pred in po uvedbi podpore z UI.
- kakšen je obseg (število) potrebnih izvajalcev obstoječega procesa pred in po uvedbi sistema UI ter oseb, ki bodo morale sodelovati pri uvedbi,
- kakšen bo vpliv uvedbe sistema UI v poslovni proces na zaposlene: bodisi z vidika njihovega števila bodisi z vidika njihovih vlog,
- ali je projekt realno izvedljiv glede na ocenjene vire, infrastrukturo ter časovno izvedljivost projekta,
- kakšen je vpliv uporabe sistema UI na porabo energije in naravne vire v primerjavi s pričakovano dodano vrednostjo (na primer: podnebni in okoljski učinki delovanja infrastrukture za delovanje sistemov UI; raba energije, emisije toplogrednih plinov ter porabo vode in surovin (npr. surovin in materialov, pri katerih je pomembna učinkovita raba ter podaljševanje življenjskega cikla IT opreme); kjer je to mogoče, se da prednost rešitvam, ki temeljijo na energetsko učinkovitih tehnologijah in obnovljivih virih energije[5]).

3.3 Priprava načrta za uvedbo UI

Ob pozitivni oceni potreb, torej če organ javne uprave ugotovi, da je uvedba UI smotrna, primerna, ustrezna, zakonita in trajna z vseh vidikov ocene potreb, ter da organ javne uprave razpolaga s finančnimi in kadrovskimi viri, pripravi načrt za uvedbo sistema UI, v okviru katerega zagotovi proučitev naslednjih vidikov:

a) Izbira ustrezne tehnologije (analiza in odločitev o izbiri ustreznega pristopa do uvedbe sistema UI, vključno z določitvijo infrastrukture, na katero s bo sistem namestil),

b) Seznam aktivnosti (izdelava in sprejem seznama aktivnosti za tehnično uvedbo sistema UI, vključno s pripravo dokumentov iz tega poglavja),

c) Merjenje uspešnosti (določitev kazalnikov za merjenje uspešnosti uvedbe in uporabe sistema UI),

d) Uporabniška izkušnja (obrazložitev razlogov, zakaj je rešitev intuitivna, uporabnikom prijazna in prilagojena njihovim potrebam),

e) Nadzor in spremljanje (vzpostavitev mehanizmov za nadzor in spremljanje rešitev z UI, kar vključuje tudi mehanizme za nadzor nad morebitno pristransko obravnavo vsebin, vključujoč vse oblike politične agitacije, ki bi prinašala prednost posamezni politični opciji ali stranki)),

[5] Takšen pristop je skladen z nacionalnimi cilji blaženja in prilagajanja podnebnim spremembam ter strateškimi dokumenti podnebne in energetske politike (npr. Podnebni zakon, Nacionalni energetski in podnebni načrt, NEPN).

f) Komunikacija (obveščajte interne in zunanje javnost o napredku in rezultatih uvajanja in uporabe sistema UI),

g) Izobraževanje zaposlenih (vzpostavitev sistema nenehnega usposabljanja in izobraževanja za zaposlene o UI ter spodbujanje razvoja znanj o UI).

Odločitev za uvedbo UI zahteva celovit pristop, ki uravnoteži koristi, stroške in tveganja, obenem pa upošteva širši kontekst organizacije in družbe. Priporočljivo je začeti z manjšim pilotnim projektom, da se predhodno potrdi ustreznost predvidena rešitve.

3.4 Začetek izvajanja projekta »razvoj in uvedba storitev, podprtih z UI«

Organ javne uprave pred pričetkom razvoja podpore z uporabo UI preveri, ali ima na voljo vse potrebne vire, identificira morebitna tveganja in ovire ter jih naslovi. Pri izvajanju razvoja in uvedbe sledi naslednjim usmeritvam:

- za učinkovito učenje jezikovnih modelov so potrebni kakovostni podatki,
- oblikovanje in sprejem postopkov in pravil za dostop do podatkov (shranjevanje, nepooblaščen dostop, sledljivost in revizijska sled uporabe podatkov),
- vključitev vodstva in področnih strokovnjakov že na začetku projekta.

Projekt praviloma sledi tipičnim korakom, kot so zapisani v nadaljevanju.

3.4.1 Zapis ciljev in določitev kazalnikov

Organ javne uprave natančno opredeli poslovni problem, ki ga namerava rešiti z razvojem storitve podprte z UI. V okviru analize določi merljive kazalnike za merjenje uspešnosti.

3.4.2 Analiza podatkov in njihova uporaba

Organ javne uprave zbere vse relevantne podatke iz obstoječih virov, oceni kakovost podatkov, njihovo popolnost, celovitost, točnost in konsistentnost. Izvede čiščenje podatkov, njihovo dopolnjevanje ter jih pripravi za modeliranje.

Izbere najustreznejši algoritem (npr. strojno učenje, globoko učenje, »fine tuning«).

3.4.2.1 Kakovost podatkov

Za zagotavljanje kakovosti podatkov je treba upoštevati:

a) točnost: podatki morajo biti pravilni in brez napak,

b) doslednost: podatki morajo biti usklajeni med različnimi viri in sistemi ter imeti enotno obliko za učinkovito obdelavo,

c) popolnost: podatki morajo vsebovati vse potrebne informacije,

d) ažurnost: podatki morajo biti posodobljeni (odražati morajo trenutno stanje),
e) relevantnost: podatki morajo biti povezani z nalogo, ki jo UI opravlja,
f) razložljivost:(izvor podatkov mora biti sledljiv za revizijo in razlago odločitev UI,
g) zanesljivost: podatki morajo biti pridobljeni iz zaupanja vrednih virov, da je zaupanje v UI rešitve,
h) ustreznost: podatki morajo biti primerni za namen, za katerega se uporabljajo.

Slaba kakovost podatkov privede do slabih ali zavajajočih rezultatov, kar vodi do slabih odločitev in lahko predstavljajo tveganje diskriminatornosti. Zato je pri uporabi UI bistveno vlagati čas in sredstva v vzpostavitev in vzdrževanje kakovostnih podatkovnih baz.

3.4.3 Razvoj in treniranje modela

Organ javne uprave pridobljene in verificirane podatke razdeli na učne, validacijske in testne sklope ter izvede treniranje modela in njegovo optimizacijo. Po zaključku razvoja modela preveri njegovo ustreznost, natančnost, robustnost in varnost.

3.4.4 Testiranje in validacija

Organ javne uprave z ključnimi uporabniki izvede validacijo modela na realnih podatkih in stresne teste ter preveri delovanje v različnih scenarijih, ter izvede vse ostale postopke, ki so namenjeni zagotavljanju odpornosti sistemov na zunanje posege in ranljivosti, ki bi lahko vplivale na varnost.

3.4.5 Implementacija in integracija

Organ javne uprave po uspešnem testiranju vzpostavi ustrezne vmesnike za uporabo modela ter integrira rešitev v obstoječe poslovne procese.

3.5 Zagotavljanje skladnosti

3.5.1 Določitev stopnje tveganja sistema UI glede na Akt o umetni inteligenci

Akt o umetni inteligenci vzpostavlja na tveganjih utemeljen pristop, v okviru katerega so sistemi umetne inteligence razvrščeni v različne stopnje tveganja, za vsako stopnjo pa so določene posebne obveznosti in zahteve, ki jih morajo izpolnjevati ponudniki, uvajalci in drugi relevantni akterji.

Akt o umetni inteligenci uvaja štiri stopnje tveganja za sisteme UI:

1. Nesprejemljivo tveganje (5. člen): posebno škodljive uporae UI, ki so v nasprotju z vrednotami EU, ker kršijo temeljne pravice in so prepovedane. Sem tako sodi uporaba UI za družbeno točkovanje, izkoriščanje ranljivosti oseb – uporaba subliminalnih tehnik, biometrična identifikacija na daljavo v realnem času v javno dostopnih prostorih s strani

organov kazenskega pregona (razen v okviru omejitev in pogojev iz Akta o umetni inteligenci, dovoljenih z nacionalno zakonodajo), biometrična kategorizacija fizičnih oseb na podlagi biometričnih podatkov za sklepanje o njihovi rasi, političnem prepričanju itd., ne ciljno zbiranje slik obrazov s spleta, prepoznavanje čustev na delovnem mestu in v izobraževalnih ustanovah ter individualno napovedno policijsko delo. Sistemi, ki predstavljajo nesprejemljivo tveganje, so prepovedani.

2. Visoko tveganje (6. člen in nasl.): Nekateri sistemi UI, opredeljeni v Aktu o umetni inteligenci, ki bi lahko negativno vplivali na varnost ljudi ali njihove temeljne pravice, kot te izhajajo iz Listine EU o temeljnih pravicah, se šteje, da pomenijo veliko tveganje. Gre za nekatere sisteme UI na področju izobraževanja, zaposlovanja, zagotavljanje delovanja kritične infrastrukture, dostopa do bistvenih javnih storitev, biometrije, migracij in azila, preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter s področja pravosodja in demokratičnih procesov. Ti sistemi UI vključujejo tudi varnostne elemente izdelkov, ki jih zajema sektorska zakonodaja EU iz Priloge I Akta o. Visoko tvegani sistemi UI morajo biti skladni z zahtevami, ki jih Akt o umetni inteligenci zanje predvideva (8. do 15. člen Akta o umetni inteligenci), ponudniki in uvajalci[6] tovrstnih sistemov UI pa morajo spoštovati obveznosti, ki jih zanje predpisuje Akt o umetni inteligenci (glej naslednje poglavje).
3. Omejeno tveganje (50. člen): Sistemi UI, ki ne sodijo med visokotvegane oziroma njihova uporaba ni nesprejemljiva, a imajo lahko določen vpliv na zaznavanje ali ravnanje uporabnikov, se uvrščajo med sisteme UI z omejenim tveganjem. Čeprav Akt o umetni inteligenci zanje ne določa enako strogih zahtev, kot za sisteme UI z visokim tveganjem, pa vendarle niso povsem izvzeti iz regulacije. Akt o umetni inteligenci uvajalce ali ponudnike sistemov UI zavezuje, da so uporabniki, kadar komunicirajo s sistemom UI, kadar imajo stik z vsebinami, prirejenimi ali ustvarjenimi s sistemi UI, ali kadar so izpostavljeni sistemom UI za prepoznavanje čustev ali biometrično kategorizacijo, o tem obveščeni oziroma, da so obveščeni o vsebini, ki jo ustvari ali z njo manipulira sistem UI.
4. Minimalno tveganje: vse druge sisteme UI je mogoče razviti in uporabiti brez dodatnih zahtev Akta o umetni inteligenci, morajo pa vseeno upoštevati drugo relevantno zakonodajo. V to kategorijo spada velika večina sistemov UI, ki se trenutno uporabljajo. V navedeno kategorijo se uvrščajo npr. filtri za neželeno pošto. Ponudniki se lahko prostovoljno odločijo, ali bodo uporabljali zahteve za zaupanja vredno UI, in se zavežejo izpolnjevanju prostovoljnih kodeksov ravnanja.

Pred uvedbo sistema UI mora organ javne uprave odgovoriti na vprašanje, v katero od zgoraj navedenih kategorij sodi sistem UI, ki ga namerava uporabiti oziroma razviti, sodi in zagotoviti njegovo skladnost s pravili Akta o umetni inteligenci.

[6] Akt o umetni inteligenci poleg obveznosti za ponudnike in uvajalce določa tudi obveznosti za pooblaščene zastopnike ponudnikov, uvoznike, distributerje visokotveganih sistemov UI.

V nadaljevanju dokument podrobno opredeljuje obveznosti, ki jih Akt o umetni inteligenci določa za ponudnike in uvajalce sistemov UI, in sicer tako za visokotvegane sisteme UI kot za sisteme, za katere je predpisana samo obveznost preglednosti. V zvezi s povzetimi obveznosti je potrebno izpostaviti, da ne gre za celovit seznam obveznosti in da se ta nahaja v Aktu o umetni inteligenci. Poglavje povzema še obveznost glede zagotavljanja pismenosti na področju UI in obveznost objave podatkov o sistemih UI na enotni informacijski točki ministrstva, pristojnega za upravljanje informacijsko-komunikacijskih sistemov (kot predvideno z ZIUDHPUI).

3.5.2 Obveznosti uvajalcev in ponudnikov sistemov UI po Aktu o umetni inteligenci

Dokument v nadaljevanju opredeljuje obveznosti za ponudnike in uvajalce sistemov UI, kot te izhajajo iz Akta o umetni inteligenci, pri čemer je treba opozoriti, da ne gre za zaključen obseg obveznost Akta o UI, ampak velja besedilo obveznosti kot izhaja iz Akta o UI.

3.5.2.1 Obveznosti za visokotvegane sisteme UI

3.5.2.1.1 Organ javne uprave kot uvajalec visokotveganega sistema UI

Organ javne uprave mora kot uvajalec visokotveganega sistema UI[7]:

- sprejeti ustrezne tehnične in organizacijske ukrepe, s katerimi se zagotovi uporaba sistema skladu s priloženimi navodili za uporabo na podlagi tretjega in šestega odstavka 26. člena Akta o umetni inteligenci (kot to zahteva prvi odstavek 26. člena Akta),
- dodeliti človeški nadzor fizičnim osebam, ki imajo potrebne kompetence, usposobljenost in pooblastila ter potrebno podporo (kot to zahteva drugi odstavek 26. člena Akta),
- v primeru, da izvaja nadzor nad vhodnimi podatki, zagotoviti, da so ti ustrezni in dovolj reprezentativni glede na predvideni namen sistema UI (kot to zahteva četrti odstavek 26. člena Akta),
- spremljati delovanje sistema UI na podlagi navodil za uporabo in po potrebi obvestiti ponudnike v skladu z določbo 72. člena Akta o umetni inteligenci, ki ureja spremljanje po dajanju na trg s strani ponudnikov in načrt spremljanja po dajanju na trg za visokotvegane sisteme UI (kot to zahteva prvi stavek petega odstavka 26. člena Akta),
- kadar ima razlog za domnevo, da bi uporaba visokotveganega sistema UI v skladu z navodili lahko povzročila, da bi sistem predstavljal tveganje v skladu s prvim odstavkom 79. člena Akta o umetni inteligenci, o tem brez nepotrebnega odlašanja obvestiti ponudnika ali distributerja in ustrezni organ za nadzor trga oziroma začasno prekiniti uporabo tega sistema (kot to zahteva drugi stavek petega odstavka 26. člena Akta),
- kadar odkrije resen incident, o tem takoj obvestiti ponudnika, uvoznika ali distributerja in ustrezne organe za nadzor trga ali, če ne more priti v stik s ponudnikom, poročati o resnem

[7] Obveznosti veljajo od 2. 8. 2026 dalje.

incidentu v skladu s 73. členom Akta o umetni inteligenci (kot to zahtevata tretji in četrti stavek petega odstavka 26. člena Akta),

- voditi dnevnike, ki jih sistem UI samodejno ustvari, če je ta dnevnik pod njegovim nadzorom, v obdobju, ki ustreza predvidenemu namenu sistema UI, in sicer vsaj šest mesecev, razen če je v veljavnem pravu Unije ali nacionalnem pravu, zlasti v pravu Unije o varstvu osebnih podatkov, določeno drugače (kot to zahteva šesti odstavek 26. člena Akta),
- pred dajanjem sistema UI v uporabo ali pred uporabo sistema UI na delovnem mestu, obvestiti predstavnike delavcev ali delavce, na katere se to nanaša, da se bo zanje uporabljal visokotvegani sistem UI (kot to zahteva sedmi odstavek 26. člena Akta),
- registrirati sistem UI v skladu s tretjim odstavkom 49. člena Uredbe 2024/1689/EU (kot to zahteva prvi stavek osmega odstavka 26. člena Akta),
- v primeru, da ugotovi, da sistem UI, ki ga namerava uporabiti, ni bil registriran v podatkovni zbirki Unije iz 71. člena Akta o umetni inteligenci, takega sistema ne sme uporabiti, o tem pa mora obvestiti ponudnika ali distributerja (kot to zahteva drugi stavek osmega odstavka 26. člena Akta)[8],
- v primeru uporabe visokotveganih sistemov UI iz Priloge III Akta o umetni inteligenci, ki sprejemajo odločitve ali pomagajo pri odločanju v zvezi s fizičnimi osebami, fizične osebe obvestiti, da se zanje uporablja navedeni sistem (kot to zahteva enajsti odstavek 26. člena Akta);
- pred uvedbo sistema UI iz Priloge III Akta o umetni inteligenci, razen za sisteme UI na področju kritične infrastrukture, izvesti oceno učinka, ki ga lahko uporaba takega sistema povzroči na temeljne pravice[9] (t. i. FRIA – ang. *»Fundamental Rights Impact Assessment«*) in o tem obvestiti ustrezen organ za nadzor trga (kot to zahteva prvi odstavek 27. člena Akta),
- vsaki prizadeti osebi, za katero velja odločitev, ki jo sprejme na podlagi izhodnih podatkov visokotveganega sistema UI iz Priloge III Akta, razen v primeru sistema iz 2. točke Priloge III, in ki ima pravne učinke ali na to osebo podobno znatno vpliva na način, ki ima po njenem mnenju negativne učinke na njeno zdravje, varnost in temeljne pravice, zagotoviti jasna in smiselna pojasnila o vlogi sistema UI v postopku odločanja in glavnih elementih sprejete odločitve (navedena obveznost ne velja v primeru, če je ta pravica določena v drugem pravu Unije – npr. pravu Unije o varstvu osebnih podatkov) (kot to zahteva prvi odstavek 86. člena Akta).

[8] Uvajalci takšnega sistema ne smejo uporabiti.

[9] HRIA sestavljajo: (1) opis delovnih postopkov uvajalca, v katerih se bo visoko tvegani sistem UI uporabljal v skladu s predvidenim namenom, (2) opis obdobja in pogostosti uporabe visoko tveganega sistema UI, (3) kategorije fizičnih oseb in skupin, na katere bo verjetno vplivala njegova uporaba v specifičnem kontekstu, posebna tveganja škode, opis izvajanja ukrepov za človeški nadzor in ukrepi, ki jih je treba sprejeti v primeru uresničitve teh tveganj, vključno z ureditvami za notranje upravljanje in pritožbene mehanizme.

3.5.2.2 Organ javne uprave kot uvajalec visokotveganega sistema UI za naknadno biometrično identifikacijo na daljavo

Organ javne uprave mora kot uvajalec v primeru uporabe visokotveganega sistema UI za naknadno biometrično identifikacijo na daljavo[10]:

- v okviru preiskave za ciljno iskanje osebe, ki je osumljena ali obsojena storitve kaznivega dejanja, predhodno ali brez nepotrebnega odlašanja in najpozneje v 48 urah, zaprositi sodni ali upravni organ, katerega odločitev je zavezujoča in predmet sodnega nadzora, za uporabo tega sistema, razen če se ta uporablja za prvotno identifikacijo morebitnega osumljenca na podlagi objektivnih in preverljivih dejstev, neposredno povezanih s kaznivim dejanjem (kot to zahteva prvi stavek prvega pododstavka desetega odstavka 26. člena Akta),
- uporabiti sistem UI na način, da je uporaba omejena na tisto, kar je nujno potrebno za preiskavo določenega kaznivega dejanja (kot to zahteva drugi stavek prvega pododstavka desetega odstavka 26. člena Akta),
- takoj prenehati uporabljati sistem UI, v primeru, ko je dovoljenje iz prvega pododstavka desetega odstavka 26. člena Akta o umetni inteligenci v zvezi s tem sistemom zavrnjeno, in izbrisati osebne podatke, povezane z njegovo uporabo (kot to zahteva drugi pododstavek desetega odstavka 26. člena Akta),
- ne sme uporabljati sistema UI za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj na neciljan način v povezavi s kaznivim dejanjem, kazenskim postopkom, resnično in sedanjo ali resnično in predvidljivo grožnjo kaznivega dejanja ali iskanjem določene pogrešane osebe (kot to zahteva prvi stavek tretjega pododstavka desetega odstavka 26. člena Akta),
- kot organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj izključno na podlagi izhodnih podatkov takega sistema ne sme sprejeti odločitve, ki ima negativen pravni učinek na osebo (kot to zahteva drugi stavek tretjega pododstavka desetega odstavka 26. člena Akta),
- v ustrezni policijski datoteki dokumentirati vsako uporabo takih sistemov (kot to zahteva peti pododstavek desetega odstavka 26. člena Akta),
- organom za nadzor trga in organu za varstvo podatkov predložiti letno poročilo o uporabi tovrstnih sistemov (kot to zahteva šesti pododstavek desetega odstavka 26. člena Akta),

3.5.2.3 Organ kot ponudnik visokotveganega sistema UI

Organ javne uprave mora kot ponudnik visokotveganega sistema UI[11]:

- zagotoviti, da je njegov sistemi UI skladen z zahtevami iz oddelka 2 poglavja III Akta o umetni inteligenci[12] (kot to zahteva (a) točka prvega odstavka 16. člena Akta),

---

[10] Obveznosti veljajo od 2. 8. 2026 dalje.
[11] Obveznosti veljajo od 2. 8. 2026 dalje.
[12] Zahteve za visokotvegane sisteme UI so opredeljene v 9. do 15. členu Akta o umetni inteligenci (vzpostavitev in vzdrževanje sistema za obvladovanje tveganja, zahteve glede podatkov in njihovega upravljanja, priprava tehnične dokumentacije, vodenje evidenc, zagotavljanje preglednosti in informacij uvajalcem, omogočati morajo človeški nadzor, dosegati morajo ustrezno raven točnosti, robustnosti in kibernetske varnosti).

— na sistemu ali, kadar to ni mogoče, na embalaži ali spremni dokumentaciji, navesti svoje ime, registrirano trgovsko ime in registrirano znamko ali naslov, na katerem je dosegljiv (kot to zahteva (b) točka prvega odstavka 16. člena Akta),
— vzpostaviti sistem upravljanja kakovosti v skladu s 17. členom Akta o umetni inteligenci (kot to zahteva točka (c) prvega odstavka 16. člena Uredbe 2024/1689/EU),
— hraniti dokumentacijo iz 18. člena Akta o umetni inteligenci (kot to zahteva točka (d) prvega odstavka 16. člena Akta),
— hraniti dnevnike, ki jih samodejno ustvarijo njegovi visokotvegani sistemi UI, kakor je navedeno v 19. členu Akta o umetni inteligenci, kadar je to pod njenim nadzorom (kot to zahteva točka (e) prvega odstavka 16. člena Akta,
— pred dajanjem na trg ali v uporabo zagotoviti, da sistem opravi ustrezen postopek ugotavljanja skladnosti iz 43. člena Akta o umetni inteligenci (kot to zahteva točka (f) prvega odstavka 16. člena Akta),
— pripraviti izjavo EU o skladnosti v skladu s 47. členom Akta o umetni inteligenci (kot to zahteva točka (g) prvega odstavka 16. člena Akta),
— na sistem UI ali, kadar to ni mogoče, na njegovo embalažo ali priloženo dokumentacijo namestiti oznake CE v skladu z 48. členom Akta o umetni inteligenci (kot to zahteva točka (h) prvega odstavka 16. člena Akta),
— registrirati sistem v skladu s prvim odstavkom 49. člena Akta o umetni inteligenci (kot to zahteva točka (i) prvega odstavka 16. člena Akta),
— Agenciji za komunikacijska omrežja in storitve (AKOS) predložiti podatke iz oddelka A Priloge VIII Akta o umetni inteligenci za potrebe vpisa v evidenco visokotveganih sistemov UI na področju kritične infrastrukture (kot to zahteva tretji odstavek 18. člena ZIUDHPUI),
— sprejeti potrebne korektivne ukrepe in zagotoviti informacije v skladu z 20. členom Akta o umetni inteligenci (kot to zahteva točka (j) prvega odstavka 16. člen Akta),
— na obrazloženo zahtevo ustreznega organa za nadzor trga dokazati skladnost visokotveganega sistema UI z zahtevami iz oddelka 2 poglavja III Akta o umetni inteligenci (kot to zahteva točka (k) prvega odstavka 16. člena Akta),
— zagotoviti, da sistem izpolnjuje zahteve glede dostopnosti v skladu z zakonom, ki ureja dostopnost spletišč in mobilnih aplikacij, ali zakonom, ki ureja dostopnost do proizvodov in storitev za invalide (kot to zahteva točka (l) prvega odstavka 16. člena Akta),
— na obrazloženo zahtevo pristojnih nacionalnih organov zagotoviti vse informacije ali dokumentacijo, potrebno za dokazovanje skladnosti sistema z zahtevami iz oddelka 2 poglavja III Akta o umetni inteligenci, v enem od uradnih jezikov Unije, ki ga določi zadevna država članica in ga pristojni nacionalni organ brez težav razume (kot to zahteva prvi odstavek 21. člena Akta),
— na obrazloženo zahtevo pristojnega nacionalnega organa omogočiti dostop do samodejno ustvarjenih dnevnikov visokotveganih sistemov UI iz prvega odstavka 12. člena Akta o umetni inteligenci, če so ti dnevniki pod njegovim nadzorom (kot to zahteva drugi odstavek 21. člena Akta),

- vzpostaviti ali dokumentirati sistem spremljanja po dajanju na trg na način, ki je sorazmeren z naravo tehnologij UI in tveganji visokotveganega sistema UI (kot to zahteva prvi odstavek 72. člena Akta),
- poročati organom za nadzor trga v državi članici, v katerih je prišlo do incidenta v zvezi sistemom, takoj, ko ugotovi obstoj vzročne zveze med sistemom UI in resnim incidentom ali razumno verjetnostjo take zveze oziroma najpozneje v 15 dneh po tem, ko izve za resen incident (kot to zahtevata prvi in drugi odstavek 73. člena Akta),
- poročati organom za nadzor trga o močno razširjeni kršitvi ali resnem incidentu nemudoma oziroma najpozneje v dveh dneh, ko je izvedel za ta incident (kot to zahteva tretji odstavek 73. člena Akta),
- poročati organom za nadzor trga o smrti osebe takoj, ko ugotovi ali posumi, da obstaja vzročna zveza med sistemom, UI in resnim incidentom, vendar najpozneje 10 dni po datumu, ko je izvedel za resen incident (kot to zahteva četrti odstavek 73. člena Uredbe 2024/1689/EU).

3.5.3 Obveznosti ponudnikov in uvajalcev nekaterih sistemov UI glede preglednosti[13]

Organ javne uprave mora kot ponudnik sistema UI, za katerega velja obveznost preglednosti, zagotoviti, da:

- je sistem UI, namenjen neposredni interakciji s fizičnimi osebami, zasnovan in razvit tako, da so zadevne fizične osebe obveščene, da so v interakciji s sistemom UI, razen če je to očitno z vidika razmeroma dobro obveščene, pozorne in preudarne fizične osebe ob upoštevanju okoliščin in konteksta uporabe oziroma gre za sisteme UI, ki so z zakonom odobreni za odkrivanje, preprečevanje, preiskovanje ali pregon kaznivih dejanj, razen če so ti sistemi na voljo javnosti za prijavo kaznivega dejanja (kot to zahteva prvi odstavek 50. člena Akta),
- so izhodni podatki sistemov UI, vključno s sistemi UI za splošne namene, ki ustvarjajo sintetično zvočno, slikovno, video ali besedilno vsebino, označeni v strojno berljivi obliki oziroma jih je mogoče prepoznati kot umetno ustvarjene ali prirejene (kot to zahteva prvi stavek drugega odstavka 50. člena Akta),
- so njegove tehnične rešitve učinkovite, interoperabilne, robustne oziroma zanesljive, kolikor je to tehnično izvedljivo, pri čemer mora upošteva posebnosti in omejitve različnih vrst vsebin, stroškov izvajanja ali splošno priznanih najsodobnejših tehnoloških dosežkov, kar se lahko odraža v ustreznih tehničnih standardih (kot to zahteva drugi stavek drugega odstavka 50. člena Akta),

Organ javne uprave mora kot uvajalec sistema UI, za katerega velja obveznost preglednosti, zagotoviti, da:

[13] Obveznosti veljajo od 2. 8. 2026 dalje.

- so fizične osebe obveščene o delovanju sistema UI za prepoznavanje čustev ali sistema za biometrično kategorizacijo, ki so mu izpostavljene, in da so njihovi osebni podatki obdelani v skladu s Splošno uredbo o varstvu podatkov in Uredbo (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES ter Direktivo (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ kot je to ustrezno (kot to zahteva tretji odstavek 50. člena Akta),
- v primeru uporabe sistema UI, ki ustvarja ali prireja slikovno, zvočno ali video vsebino, ki je globoki ponaredek, razkrije, da je bila vsebina umetno ustvarjena ali prirejena (četrti odstavek 50. člena Akta),
- v primeru uporabe sistema UI, ki ustvarja ali prireja besedilo, ki se objavi z namenom obveščanja javnosti o zadevah javnega interesa, razkrije, da je bilo besedilo umetno ustvarjeno ali prirejeno, razen če je bila uporaba zakonsko dovoljena za odkrivanje, preprečevanje, preiskovanje ali pregon kaznivih dejanj ali kadar je bila vsebina, ustvarjena z UI, predmet človeške preverbe ali uredniškega pregleda ali kadar ima uredniško odgovornost za objavo vsebine (kot to zahteva drugi pododstavek četrtega odstavka 50. člena Akta).

Poleg navedenega Akt o umetni inteligenci predpisuje še obveznost zagotavljanja pismenosti na področju UI, ki velja tako za ponudnike kot tudi uvajalce sistemov UI. Organ javne uprave mora tako sprejeti ukrepe za zagotovitev zadostne ravni pismenosti njegovega osebja in drugih oseb, ki se v njegovem imenu ukvarjajo z obratovanjem in uporabo sistemov UI, na področju UI, upoštevajoč njihovo tehnično znanje, izkušnje, izobrazbo in usposobljenost ter okolje, v katerem se bodo uporabljali sistemi UI, pa tudi oseb ali skupine oseb, v zvezi s katerimi se bodo uporabljali ti sistemi (4. člen Akta o umetni inteligenci).

V skladu z 21. členom ZIUDHPUI pa morajo državni organi in organi samoupravnih lokalnih skupnosti, javne agencije, javni skladi, javni zavodi in javni gospodarski zavodi ter druge osebe javnega prava, če so posredni uporabniki državnega proračuna ali proračuna lokalne skupnost - poleg obveznosti registracije sistema UI v podatkovni zbirki, ki jo vodi Evropska komisija - na enotni informacijski točki, ki jo zagotavlja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov, objaviti naslednje podatke o sistemih UI oziroma informacijskih rešitvah, ki vključujejo UI:

1. naziv organa, pri katerem je sistem UI v uporabi,
2. predvidena raba ter njeni cilji in učinki,
3. navedba osnovnih principov delovanja algoritmov pri odločanju sistema UI,

4. številka dokumenta in datum ocene učinka v zvezi z varstvom osebnih podatkov,
5. številka dokumenta in datum ocene učinka na temeljne pravice, ko gre za visokotvegane sisteme UI,
6. navedba možnosti glede pravnega varstva zoper odločanje sistema UI.

Navedeno obveznost morajo organi javnega sektorja izpolniti najkasneje ob uvedbi sistema UI oziroma informacijske rešitve, ki vključuje UI. Obveznost objave prej navedenih podatkov na enotni informacijski točki ne velja za sisteme UI oziroma informacijske rešitve, ki vključujejo UI, s področja preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, obrambe, nacionalne varnosti, migracij, azila in upravljanja nadzora meja ter sisteme UI, ki se uporabljajo izključno za vojaške, obrambne ali nacionalne varnostne namene.

3.5.4 Skladnost (s Splošno uredbo o varstvu podatkov in Aktom o umetni inteligenci ob uporabi storitev DRO)

Organ javne uprave mora pred začetkom uporabe posameznega sistema tudi dogovoriti vse potrebno s ponudnikom storitev ter si s tem zagotoviti skladnost s Splošno uredbo o varstvu podatkov in Aktom o umetni inteligenci in posledično zagotoviti zakonitost poslovanja.

3.5.4.1 Priprava in podpis posebnega dogovora s ponudnikom oblačnih storitev o obdelavi osebnih podatkov

V primeru uporabe katerihkoli storitev, katerih predmet je obdelava osebnih podatkov, je treba skleniti ustrezen dogovor o obdelavi osebnih podatkov. Ta dogovor je potreben tudi, če bo UI dostopala oz. obdelovala osebne podatke v oblaku (npr. z Microsoft za Azure, Oracle, ipd.).

3.5.4.2 Obdelava vsebin dokumentov uporabnikov, če bo umetna inteligenca dostopala do njih

Opredeljeno po vzpostavitvi pilotne postavitve za zagotavljanje UI v DRO.

3.5.4.3 Beleženje in uporaba vnesenih podatkov uporabnikov umetne inteligence pri nadaljnjih obdelavah

Opredeljeno po vzpostavitvi pilotne postavitve za zagotavljanje UI v DRO.

3.5.5 Varstvo osebnih podatkov

Kadar sistemi UI obdelujejo osebne podatke, je treba pri njihovem delovanju upoštevati tudi pravila varstva osebnih podatkov. V Sloveniji so ta primarno urejena s Splošno uredbo o varstvu osebnih podatkov, ZVOP-2 ter ZVOPOKD.

Podrobnejša pojasnila o zagotavljanju obveznosti na podlagi predpisov, ki določajo varstvo osebnih podatkov, na svoji spletni strani objavlja Informacijski pooblaščenec.

3.5.5.1 Odgovornost za zagotavljanje skladnosti sistemov UI s pravom varstva osebnih podatkov

Splošna uredba ločuje med dvema skupinama akterjev, ki sodelujejo pri obdelavi osebnih podatkov: upravljavci so pravne ali fizične osebe, ki sami ali skupaj (v tem primeru gre za skupne upravljavce) usmerjajo obdelavo z določanjem njenih ciljev in sredstev, lahko pa jo tudi prepustijo tretji osebi, ki v tem primeru nastopa v vlogi obdelovalca. Njihove vloge in posledično tudi odgovornosti v verigi obdelav podatkov se razlikujejo. V skladu z načelom odgovornosti so upravljavci odgovorni za zagotavljanje skladnosti z določbami Splošne uredbe in jo morajo biti sposobni tudi dokazati[14]. Organ javne uprave, ki bo najpogosteje nastopal v vlogi upravljavca podatkov, bo moral v začetni fazi uvajanja UI ustrezno oceniti vloge vseh sodelujočih akterjev in temu ustrezno opredeliti razmerja med njimi.

3.5.5.2 Opredelitev namena in pravne podlage obdelave podatkov

Od namena (cilja) obdelave podatkov bo odvisno, katere podatke upravljavec potrebuje za dosego opredeljenega namena (obdelava)in na kateri pravni podlagi, koliko časa jih bo hranil in kakšne ukrepe za zagotavljanje varnosti podatkov bo v tem času moral zagotoviti.

Uporaba orodij UI mora biti opredeljena v internih aktih organa. Temeljiti mora na pravni podlagi kot to določata 6. člen Splošne uredbe in drugi odstavek 6. člena ZVOP-2. Za obdelavo občutljivih podatkov (kot npr. podatkov o zdravstvenem stanju, za osebne podatke iz kazenskih in evidenc prekrškovnih evidenc itd.) ne zadostujejo zgolj navedene pravne podlage, temveč mora biti izpolnjena tudi ena izmed izjem iz drugega odstavka 9. člena Splošne uredbe.

3.5.5.3 Zbiranje podatkov in načelo najmanjšega obsega podatkov

Sistemi UI temeljijo na obdelavi velike količine (osebnih) podatkov, ki so lahko pridobljeni posebej za namen učenja sistema UI ali pa so bili zbrani za kakšen drug namen in se ponovno uporabijo. Takšna ponovna uporaba je dopustna le, če je združljiva z namenom, za katerega so bili podatki prvotno zbrani.

Na glede na to, kako so bili osebni podatki zbrani, morajo biti zadevni posamezniki obveščeni o ključnih okoliščinah obdelave podatkov, kot so nameni obdelave, pravne podlage, roki hrambe in pravice posameznikov.

---

[14] Npr. da sistem UI obdeluje osebne podatke na ustreznem zakonitem temelju, da njihov obseg ni prekomeren, da je posamezniku, na katerega se podatki nanašajo, zagotovil vse zahtevane informacije in omogočil učinkovito izvrševanje njegovih pravic, ter da je zagotovil vse tehnične in organizacijske ukrepe za varnost podatkov.

Načelo najmanjšega obsega podatkov od upravljavcev zahteva, da so podatki relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo. Če podatki niso potrebni za zasledovane namene, jih upravljavec za ta namen ne sme obdelovati.

3.5.5.4 Obdobje hrambe osebnih podatkov

Splošna uredba prepoveduje, da bi se osebni podatki hranili za nedoločen čas. Upravljavec mora določiti primeren rok hrambe osebnih podatkov še preden se obdelava prične. Podatki se lahko hranijo le toliko časa, kolikor je potrebno za namene, za katere se obdelujejo. Roke hrambe mora redno preverjati (43. člen ZVOP-2), po njihovem izteku pa osebne podatke izbrisati ali anonimizirati.

3.5.5.5 Avtomatizirano sprejemanje odločitev in profiliranje

Avtomatizirano sprejemanje odločitev je s Splošno uredbo omejeno, saj ga spremljajo številna tveganja, ki lahko izvirajo iz nepravilnih, pristranskih ali zgolj nenatančnih podatkov in pomanjkljivosti pri načrtovanju modelov umetne inteligence in njihove netransparentnosti. Avtomatizirano sprejemanje odločitev se lahko na naša tudi samo na del procesa in ni nujno v celoti avtomatizirano[15]. Za človekovo posredovanje se šteje le nadzor nad odločitvijo, ki ima dejansko nek pomen in je izveden s strani nekoga, ki ima avtoriteto in pristojnost, da odločitev tudi spremeni. Pri izključno avtomatiziranem sprejemanju odločitev morajo upravljavci upoštevati dodatne omejitve in izjeme iz 22. člena Splošne uredbe.

Profiliranje je opredeljeno kot vsaka oblika avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, možno pa ga je izvesti tudi brez avtomatiziranega odločanja.

Posameznik, na katerega se nanašajo osebni podatki ima pravico, da zanj ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva.[16]

3.5.5.6 Uresničevanje pravic posameznikov

Upravljavec mora posameznikom omogočiti dostop do informacij o obdelavi njihovih osebnih podatkov in jim omogočiti izvrševanje njihovih pravic skladno s Splošno uredbo.

Kadar sistemi UI vključujejo obdelavo osebnih podatkov, mora upravljavec poskrbeti, da lahko posamezniki uveljavljajo svoje pravice: dostopa (15. člen Splošne uredbe), popravka (16. člen),

---

[15] Glej sodno prakso v zadevi C-634/21: https://infocuria.curia.europa.eu/tabs/affair?sort=AFF_NUM-DESC&searchTerm=%22C-634%2F21%22&publishedId=C-634%2F21.

[16] Smernice Evropskega odbora za varstvo podatkov o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679.

izbrisa (17. člen), omejitve obdelave (18. člen), prenosljivosti (20. člen) in ugovora (21. člen Splošne uredbe). Posamezniki lahko pravice uveljavljajo skozi celoten življenjski cikel sistema UI glede obdelav osebnih podatkov.

3.5.5.7 Zagotavljanje varnosti podatkov

Osebni podatki se morajo obdelovati tako, da je zagotovljen ustrezen nivo varnosti, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo. Upravljavci morajo pri odločitvi, kakšne organizacijske in tehnične ukrepa bodo sprejeli za zagotavljanje ustrezne ravni varnosti upoštevati:

1. najnovejši tehnološki razvoj in stroške izvajanja;
2. naravo, obseg, okoliščine in namen obdelave;
3. tveganja za pravice in svoboščine posameznikov.

Na tem mestu velja posebej izpostaviti ukrepa psevdonimizacije in anonimizacije. Psevdonimizacija osebnih podatkov pomeni, da posameznika ni več mogoče neposredno določiti iz nabora podatkov, temveč ga je mogoče določiti le še z uporabo posebnega ključa, ki omogoča njegovo ponovno identifikacijo. Psevdonimizirani podatki se tako še vedno štejejo za osebne podatke in zanje veljajo vse obveznosti Splošne uredbe. Po drugi strani pa anonimizacija pomeni, da posameznika sploh ni več mogoče določiti z uporabo razumnih tehničnih sredstev. Anonimizirani podatki se ne štejejo več za osebne podatke, kar pomeni, da se zanje ne uporabljajo določbe Splošne uredbe o varstvu podatkov. Pri tem velja poudariti, da brisanje “najbolj očitnih” podatkov (kot npr. ime, priimek, naslov, EMŠO) še ne pomeni anonimizacije posameznika.[17] Upravljavci so dolžni voditi tudi dnevnik obdelav, kadar se v avtomatiziranih sistemih obdelave osebnih podatkov izvaja redno in sistematično spremljanje posameznikov oz. kadar se izvajajo obsežne obdelave posebnih vrst osebnih podatkov. Posebno pozornost pa morajo upravljavci posvetiti posebnim obdelavam podatkov, ki na podlagi 23. člena ZVOP-2 štejejo med bolj tvegane obdelave (npr. obdelave osebnih podatkov s področja upravno notranjih zadev, finančne uprave, zdravstvenega varstva in drugih), kjer se glede ukrepov za obvladovanje tveganj smiselno uporabljajo določbe ZInfV-1, ki se nanašajo na bistvene subjekte. Poleg tega takšnih zbirk osebnih podatkov ni dovoljeno hraniti izven ozemlja Republike Slovenije.

3.5.5.8 Ocena učinka v zvezi z varstvom podatkov

Ocena učinka v zvezi z varstvom podatkov je opredeljena v 35. členu Splošne uredbe o varstvu podatkov in je obvezna v primerih, ko je verjetno, da bi obdelava lahko povzročila veliko tveganje

[17] Ustrezne metode in tehnike za anonimizacijo so primeroma pojasnjene v smernicah EDPB in mnenju glede modelov UI: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en.

za pravice in svoboščine posameznikov, ne glede na to ali gre za obdelavo so pomočjo sistemov UI ali katere druge tehnologije.

Informacijski pooblaščenec je pripravil seznam obdelav, za katere je ocena učinkov obvezna in smernice za njihovo izvedbo[18]. Glede na kriterije, ki sprožijo obveznost priprave ocene učinka, na primer masovno zbiranje podatkov, kombiniranje podatkov iz različnih podatkovnih zbirk, analitika na podlagi masovnih podatkov, inovativna raba novih tehnologij, bo priprava ocene učinka potrebna vsaj pri obdelavi osebnih podatkov tekom razvoja sistema UI.

Tudi če v skladu s kriteriji iz Splošne uredbe ocena učinka ni obvezna, vseeno predstavlja dobro prakso, sledenje kateri Informacijski pooblaščenec priporoča pri implementaciji vseh obsežnejših in kompleksnejših postopkov obdelav osebnih podatkov, kamor gotovo sodijo sistemi UI. Poleg tega lahko ocena učinka v zvezi z varstvom podatkov predstavlja izhodišče za pripravo ocene učinka na temeljne pravice *(angl. Fundamental Rights impact Assessment - FRIA)*, ki jo bodo morali izvesti uvajalci določenih visoko tveganih sistemov UI na podlagi 27. člena Akta o UI.

3.5.6 Tajni podatki po ZTP

Organ javne uprave mora ves čas zagotavljati ustrezno varstvo tajnih podatkov.

3.5.7 Davčna tajnost podatkov

Organ javne uprave mora ves čas zagotavljati ustrezno varstvo podatkov, če zanje veljajo predpisi o davčni tajnosti podatkov.

3.5.8 Avtorske in sorodne pravice

Izvede se presoja zakonitosti obdelave podatkov, ki se nahajajo v sistemu UI z vidika varstva avtorske in sorodnih pravic, prav tako pa tudi presoja obveznosti, iz izhajajo iz relevantne zakonodaje ob morebitni uporabi pridobljenih rezultatov.

3.5.9 Ocena po Zakonu o informacijski varnosti

Organ javne uprave mora ves čas zagotavljati ustrezno varstvo varovanih podatkov in informacijsko varnost. Opredelitev storitve, ki bo delovala s pomočjo UI, je ključnega pomena za sistemski pristop k informacijski varnosti. Za vsako storitev je treba določiti odgovornega skrbnika, ki pozna procesni del storitve in tehničnega skrbnika, ki pozna tehnične zahteve za delovanje storitve.

---

[18] Ključne informacije o ocenah učinka, vključno s smernicami in priporočili so na voljo na: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/ocena-u%C4%8Dinka-v-zvezi-z-varstvom-podatkov/

Skladno z ZInfV-1 je treba pripraviti tudi varnostno dokumentacijo. Organ javne uprave mora zagotavljati visoko raven informacijske in kibernetske varnosti ter odpornosti svojih omrežnih in informacijskih sistemov. V okviru tega mora organ javne uprave vzpostaviti in vzdrževati dokumentirani sistem upravljanja varovanja informacij in sistem upravljanja neprekinjenega poslovanja, ki temeljita na pristopu upoštevanja vseh nevarnosti in tveganj. Varnostna dokumentacija mora obsegati najmanj:

1. politiko ali področne politike o varnosti omrežnih in informacijskih sistemov,
2. natančen in posodobljen popis informacijskih in drugih sredstev in podatkov, potrebnih za nemoteno delovanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev, ter njihove upravljavce;
3. analizo obvladovanja tveganj, vključno z določitvijo sprejemljive ravni tveganja in opisom uporabljene metodologije;
4. politiko in načrt neprekinjenega poslovanja, vključno z oceno vpliva na poslovanje, navedbo postopkov zagotavljanja neprekinjenega poslovanja, določitvijo minimalne ravni poslovanja, upravljanjem varnostnih kopij ter določitvijo vlog in odgovornosti;
5. načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov, ki jih potrebujejo za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja;
6. načrt odzivanja na incidente s protokolom obveščanja pristojne skupine za odzivanje na incidente na področju računalniške varnosti, vključno z opisom sistema za zaznavo in odziv na incidente ter opisom vlog in odgovornosti za odzivanje na incidente;
7. načrt varnostnih ukrepov za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za informacijsko in kibernetsko varnost, pri čemer ta načrt upošteva tveganja in področne posebnosti bistvenega ali pomembnega subjekta in
8. politiko s postopki za presojo učinkovitosti varnostnih ukrepov za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov.

Organ javne uprave določi obseg sistema upravljanja in varovanja informacij ter neprekinjenega poslovanja ob upoštevanju rezultatov analize vpliva na poslovanje, pri čemer mora ta sistem obsegati najmanj tista informacijska, komunikacijska in druga sredstva, podatke in procese, ki so potrebni za njihovo delovanje ali opravljanje storitev.

3.5.10 Poslovna skrivnost in varovani podatki

Organ javne uprave mora pred začetkom izvajanja obravnave podatkov ali dokumentov, ki bi lahko bili poslovne skrivnosti ali varovani podatki, izvesti vse ukrepe, ki so potrebni za zagotavljanje njihovega varstva.

4 UPORABA ORODIJ GENERATIVNE UI, DOSTOPNIH NA SPLETU

Javni uslužbenci za potrebe priprave besedil, povzetkov daljših besedil, prevodov v različne jezike že uporabljajo različna orodja UI, ki so javno dostopna na svetovnem spletu (kot je na primer Microsoft 365 Copilot v okviru oblačne storitve Azure, ChatGPT, Gemini, IBM Watson, Amazon Alexa, Apple Siri, Claude, ipd.). Pri tem je nujno, da spoštujejo varnostne zahteve in priporočila glede vpisovanja varovanih podatkov v javno dostopna orodja UI na spletu, ki so vsebovana v Zavezah za uporabo orodij generativne umetne inteligence, dostopnih na spletu[19], kot tudi v Priporočilih za uporabo javno dostopnih orodij generativne umetne inteligence, ki so priloga teh smernic. Pomembno je zavedanje, da se vsi modeli učijo na vsebinah javne uprave, torej so podatki, ki se jih posreduje javno dostopna orodja UI, posledično v oblačne storitve in splet, lahko tako ali drugače uporabljeni in dostopni tretjim osebam. Prednostno se naj uporablja orodja, ki delujejo v informacijskih okoljih SI in EU.

Predstojnik organa javne uprave mora zagotoviti, da je vsak zaposleni seznanjen s Priporočili za uporabo javno dostopnih orodij generativne umetne inteligence, dostopnih na spletu, ki se nahajajo v Prilogi 2 teh smernic.

Javni uslužbenci se morajo zavedati vrste podatkov, ki jih pri svojem delu obdelujejo. Tako morajo vedeti, ali gre pri obdelavi za varovane podatke (kot so ti opredeljeni v 21. točki 6. člena UUP) kar vključuje zdravstvene in biometrične podatke, podatke, ki se nanašajo na obrambo, javno varnost in informacijsko varnost, ipd. in tudi dokumente, ki so klasificirani s stopnjo tajnosti po Zakonu o tajnih podatkih. Šele ob zavedanju, da ne gre za varovane podatke, se lahko odločajo, ali bodo podatke ali dokumente vnašali v orodja UI, dostopna na spletu.

Javni uslužbenci se morajo namreč zavedati, da uporaba UI orodij, dostopnih na spletu, ne izpolnjuje že osnovnih zahtev varstva podatkov. Osnovno vodilo uporabniku za uporabo tovrstnih orodij naj torej bo, da v orodja UI, dostopna na spletu, uporabniki lahko vnašajo le dokumente in informacije, ki bi jih lahko kadarkoli objavili tudi na svetovnem spletu.

---

19 https://nio.gov.si/products/priporocila%2Bjavnim%2Busluzbencem%2Bpri%2Buporabi%2Borodij%2Bgenerativne%2Bumetne%2Binteligence%2Bdostopnih%2Bna%2Bspletu?release=2.0

5 NAČIN UVEDBE ORODIJ GENERATIVNE UMETNE INTELIGENCE

V tem poglavju so opisane osnovne tehnične značilnosti različnih sistemov generativne UI in opis različnih možnosti njihove postavitve.

V primeru uporabe informacijskih rešitev, ki jih zagotavljajo ponudniki, je treba zagotoviti izhodno strategijo. Še posebej je pomembna v primeru uporabe oblačnih storitev – predlog izvedbenih korakov je opredeljen v prilogi 1 teh smernic.

OPOMBA: Ne glede na namen uporabe in način uvedbe mora vsak upravljavec zagotoviti zakonsko skladno obdelavo podatkov, vključno z njihovo uporabo ter varnost varovanih podatkov.

5.1 Namenska orodja generativne umetne inteligence v nadzorovanih okoljih

V delovnih procesih državnih organov se obdelujejo tudi varovani podatki, potrebe pa narekujejo, da se bodo tudi ti podatki obdelovali z orodji UI. Predpisi pa določajo, da mora zagotavljati, da se bodo podatki obdelovali le na ozemlju varnih držav (kot jih določi Splošna uredba o varstvu podatkov), oziroma v primeru določenih obdelav le na ozemlju Republike Slovenije[20].

5.1.1 Lokalna postavitev z RAG sistemom

Lokalna postavitev z RAG sistemom na infrastrukturi v izključnem upravljanju države omogoča popoln nadzor nad infrastrukturo in podatki, vendar to samo po sebi še ne zagotavlja skladnosti z relevantno zakonodajo. Sistem temelji na odprtokodnih tehnologijah in standardnih komponentah, kar omogoča visoko prilagodljivost. Omogočen je tehničen nadzor nad podatki in naslavljanje zahteve ZVOP-2 za obdelavo osebnih podatkov na območju Republike Slovenije, višja varnost občutljivih podatkov, varnost osebnih podatkov na področju posebnih obdelav, pri katerih se podatki lahko obdelujejo izključno na ozemlju Republike Slovenije, torej na infrastrukturi v upravljanju države, možnost prilagajanja modelov specifičnim potrebam ter neodvisnost od zunanjih ponudnikov.

Takšna postavitev zmogljivosti UI je lahko primerna tako za obdelavo tajnih podatkov po Zakonu o tajnih podatkih kot tudi za obdelavo osebnih podatkov, določenih v zakonih, ki urejajo področja upravnih notranjih zadev, finančne uprave, državljanstva, Slovenske obveščevalno-varnostne agencije, obrambe, zdravstvenega varstva, obveznega zdravstvenega zavarovanja, uveljavljanja pravic iz javnih sredstev ter kazenskih in prekrškovnih evidenc, za katere zakon določa, da jih ni dovoljeno obdelovati (hraniti) izven ozemlja Republike Slovenije.

[20] Na primer: Prva točka prvega odstavka 23. člena ZVOP-2 ali pa peti odstavek 12. člena ZInfV ali tretja alineja prvega odstavka 44. člena UVDAG.

Prav tako pa je takšna postavitev primerna za upoštevanje zahtev petega odstavka 24. člena ZInfV-1, ki zahteva, da izvajalci bistvenih storitev za namen obvladovanja in preprečevanja incidentov zagotavljajo ohranjanje dnevniških zapisov na ozemlju Republike Slovenije (razen za področja digitalne infrastrukture, bančništva in infrastrukture finančnega trga, glede katerih se lahko zagotavlja na ozemlju EU) ter zahtev tretje alineje prvega odstavka 44. člena UVDAG, ki zahteva, da javnopravne osebe v primeru hrambe dokumentarnega in arhivskega gradiva v računalniškem oblaku to gradivo hranijo samo v zasebnem oblaku, kjer je fizična lokacija hrambe tega gradiva znana v vseh fazah hrambe ter obdelave dokumentarnega in arhivskega gradiva in ne sme biti zunaj meja Republike Slovenije.

Lokalna postavitev lahko uporabi tudi t. i. storitev domenski anonimizator. Anonimizacija z UI[21] v lokalnem okolju lahko, če je zagotovljen popoln nadzor nad podatki, omogoči uporabo anonimiziranih podatkov / dokumentov, v nadaljevanju pa tudi omogoči obdelavo z orodji UI v rešitvah s hibridno postavitvijo oz. v okolju z zaprto rešitvijo v javnem oblaku.

5.1.2 Hibridna postavitev z dostopom do javnooblačne storitve

Hibridna postavitev z dostopom do javnooblačne storitve (tj. postavitev, ki za delovanje uporablja strojno opremo, ki je v popolnem nadzoru organov državne uprave, in istočasno tudi strojno opremo, ki jo nudijo različni ponudniki) omogoča kombinacijo lokalnih sistemov z zmogljivimi API storitvami, kar omogoča fleksibilnost pri razvoju informacijskih rešitev in optimizacijo stroškov. Z uporabo lokalne postavitve za nekatere dele obdelave podatkov je omogočen nadzor nad podatki in skladnost z zahtevo ZVOP-2 po obdelavi osebnih podatkov na območju Republike Slovenije. Uporaba javnooblačnih storitev pa omogoča uporabo večjih zmogljivosti obstoječih sistemov.

Hibridna postavitev z dostopom do javnooblačne storitve se na primer lahko uporabi, če se bo uporabljala javno oblačna storitev UI, vendar je zaradi možnosti obdelave varovanih podatkov potrebna predhodna obdelava na infrastrukturi, ki je v upravljanju države (npr. predhodna anonimizacija / psevdonimizacija). Ob uporabi javnooblačnih storitev se uporabi pogodbeno urejena zaprta rešitev.

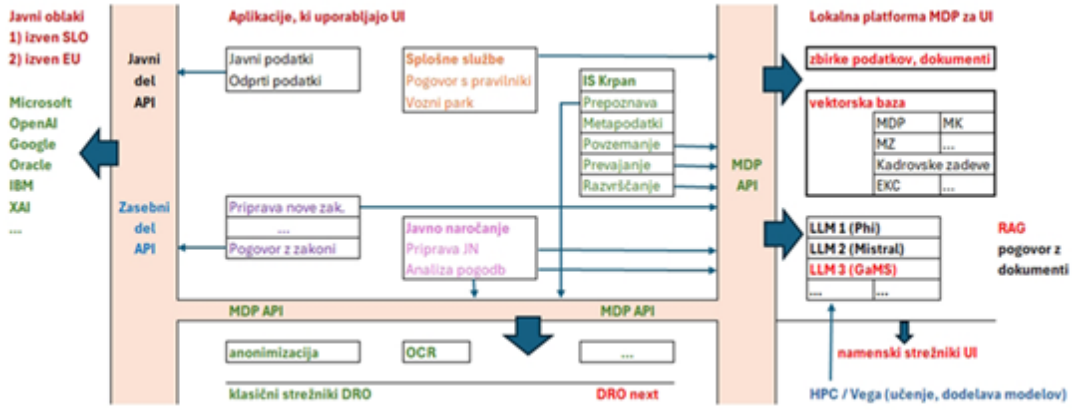
Pri izbiri arhitekture ali ponudnika oblačnih storitev naj organi poleg pravne skladnosti, informacijske varnosti in stroškov upoštevajo tudi podnebne in okoljske kriterije, kot so energetska učinkovitost podatkovnih centrov, delež energije iz obnovljivih virov, učinkovitost hlajenja ter lokacija infrastrukture z vidika ogljičnega odtisa. Prednost naj imajo rešitve, ki pomembno

[21] Anonimizacija mora biti izvedena v skladu z ustreznimi metodami in tehnikami za anonimizacijo, kot so primeroma pojasnjene v smernicah EDPB in mnenju glede modelov UI:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en.

zmanjšujejo okoljski odtis digitalnih storitev javne uprave in so skladne z nacionalnimi cilji blaženja in prilagajanja podnebnim spremembam.

5.2 Ponazoritev arhitekture ter toka podatkov



5.3 Opredelitev načina izmenjave podatkov (vrsta, obseg, kategorije, ipd.)

Način izmenjave podatkov bo opredeljen po vzpostavitvi pilotne postavitve za zagotavljanje UI v državnem računalniškem oblaku (v nadaljnjem besedilu: DRO).

6 KRATICE

AI ang. Artificial intelligence in označuje umetno inteligenco

API ang. Application Programming Interface in označuje programski vmesnik

CSIRT ang. Computer Security Incident Response Team in označuje specializirano ekipo znotraj organizacije ali zunanjo skupino strokovnjakov, katerih glavni cilj je obravnava kibernetskih incidentov

DPIA ang. Data protection impact assessment in označuje oceno učinka v zvezi z varstvom osebnih podatkov

DRO Državni računalniški oblak

EKC Enotni kontaktni center

EU Evropska unija

GDPR ang. General Data Protection Regulation in označuje Splošno uredbo EU o varstvu podatkov

HIPAA ang. Health Insurance Portability and Accountability Act in označuje nabor standardov za upravljanje, prenos in shranjevanje zaščitenih zdravstvenih podatkov

FRIA ang. Fundamental Rights Impact Assessment in označuje Oceno učinka na temeljne pravice po Aktu o umetni inteligenci

LLM ang. Large language model in označuje Velike jezikovne modele

MDP Ministrstvo za digitalno preobrazbo

MZ Ministrstvo za zdravje

RAG ang. Retrieval-augmented generation in označuje Generacijo z razširjenim iskanjem, postopkom, ki se uporablja pri velikih jezikovnih modelih, da bi bili njihovi izhodi bolj relevantni v določenih kontekstih

UI Umetna inteligenca