SIR IUS 5/23
SLOVENSKI INŠTITUT za REVIZIJO
Revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij

Kazalo

Iz prakse za prakso

Novosti in obvestila

Dr. Marjan Odar

Uvodnik

Editorial

Človek naj bi bil najvišje razvito bitje in gospodar sveta. Tako vsaj pravijo. Pa je res tako? Nedavno neurje, poplave, plazovi in druge nesreče ponujajo drugačen razmislek. Narava je pokazala svojo moč. Pa ne le to. Pokazala nam je, da je vsemogočni človek slab gospodar in da z nepremišljenimi dejanji večkrat izziva usodo in moč ter bes naravnih sil. Kot da se hoče narava maščevati za človekovo prevzetnost. V športnem jeziku bi rekli, da smo prejeli rumeni karton. Naslednji je rdeči, sledi izključitev. Ali nas bo to kaj izučilo ali pa bomo še kar nadaljevali po starem? Nekateri bodo prav gotovo še nerazumno vztrajali pri svojem prav. Težko je razumljivo, da kljub večkratnim poplavam v razmeroma kratkem obdobju nekateri kar nočejo priznati, da so gradili na območjih, na katerih naši predniki zagotovo ne bi postavili poslopja. Seveda smo po bitki vsi generali, pa vendar se moramo zavedati, da so se klimatske razmere zelo spremenile in da nič več ne bo tako, kot je bilo. To nas mora predramiti iz lagodja in nas spodbuditi k drugačnemu ravnanju. Prav gotovo bo kamenček v mozaiku prilagoditev in sprememb tudi sprejetje Evropskih standardov o trajnostnem poročanju. Ni prav, da bi nanje gledali kot na dodatne naloge in obveznosti, ampak jih moramo sprejeti kot pomoč pri popravljanju naših napak. Prav gotovo bi nam bilo bolje in ne bi imeli milijardne škode, če bi že prej bolj spoštovali naravne zakonitosti in živeli z naravo ter nam hlastanje za dobički ne bi bilo edino vodilo. Seveda bodo uredbe, direktive in standardi le črke na papirju, če jih bomo razumeli kot dodatno obremenitev, ki so si jo izmislili salonski uradniki, in ne bomo vsi dejavno in brez fige v žepu zares spremenili svojega odnosa do okolja. Tako kot smo izkazali visoko stopnjo solidarnosti pri zadnjih naravnih katastrofah, tako bi morali tudi vsi složno in solidarno stopiti skupaj in vsak prispevati svoj delež pri ohranjanju narave. Prav nič nam ne morejo pomagati trenutni dobički, če nam potem

narava praktično čez noč lahko povzroči z mnogokratniki povečano škodo. Najprej pa se mora vsak zase s seboj pogovoriti in se vprašati, kaj je smisel in kakovost življenja. Pravijo, da je denar sveta vladar, vendar pa praviloma ne prinaša sreče in zadovoljstva. Človek je samo del narave. Upam, da smo blizu spoznanju, da moramo naravo in njene zakonitosti spoštovati ter v njej in z njo uglašeno živeti. To naj bi bil tudi pravi pomen trajnostnosti, kajne?

Mag. Maja Hmelak*

Umetna inteligenca – kje smo v letu 2023

Artificial inteligence – state of things in 2023

POVZETEK ● *Razvoj področja umetne inteligence v letih 2022 in 2023 je vrtoglavo hiter. Ker je na 31. konferenci o revidiranju in kontroli informacijskih sistemov vrsta z umetno inteligenco povezanih tem, smo v uvodni del konference vključili kratek povzetek ključnih trendov, ki so zaznamovali leto 2023. V pričujočem prispevku predstavimo: tehnologije, ki so omogočile razvoj najbolj razširjenih modelov umetne inteligence; glavne igralce na trgu storitev umetne inteligence in njihove ključne izdelke; storitve, ki jih omogočajo najbolj razširjeni modeli umetne inteligence; delovanje platform za razvoj in delovanje umetne inteligence; napovedi sprememb, ki jih uporaba teh storitev pomeni za gospodarstvo in širšo družbo; ter nekatere napovedi sprememb, ki jih bodo modeli umetne inteligence prinesli na področje revidiranja. Prispevek je namenjen predvsem seznanjanju udeležencev konference s ključnimi novostmi, ki jim bodo pomagale razumeti kontekst*

kompleksnejših nadaljnjih predavanj.
Ključne besede ● *umetna inteligenca, naravno procesiranje jezika, generativni transformerji*
SUMMARY ● *The development of the field of artificial intelligence in 2022 and 2023 was dizzyingly fast. As a range of topics related to artificial intelligence will be presented at the 31st International Conference on Information Systems Audit and Control, the introductory part of the conference includes a short summary of the key trends that marked the year 2023. The article covers technologies that enabled the development of the most widespread models of artificial intelligence; the main players in the market of artificial intelligence services and their key products; services provided by the most widespread models of artificial intelligence; operation of AI platforms; the forecast changes that these services will bring to the economy and to the wider society and some predictions of changes that artificial intelligence models will bring to the field of auditing. The article aims at familiarizing conference participants with key innovations that will help them understand the context of the more complex lectures that follow.*
Key words ● *artificial intelligence (AI), natural language processing, generative pre-trained transformer, diffusion model, large language model*

JEL: K 24

Umetna inteligenca (angl. *Artificial Intelligence*, kratica AI[1]) je področje računalništva in informatike, ki proučuje inteligentno vedenje v umetnih sistemih (Islovar, 2023). Sistemi in tehnologije, ki posnemajo človeško inteligenco, omogočajo strojem, da se učijo, razumejo, sklepajo, rešujejo probleme in opravljajo naloge, ki zahtevajo inteligentno vedenje.

Sisteme umetne inteligence delimo na:

- ozko umetno inteligenco (angl. *Narrow Artificial Inteligence*), ki je osredotočena na eno samo ozko usmerjeno nalogo (Islovar, 2023), vendar to nalogo praviloma opravlja bolje kot človeški strokovnjaki; in

- splošno umetno inteligenco (angl. *General Artificial Inteligence*), ki naj bi sistemu umetne inteligence omogočala, da razume ali se nauči katero koli intelektualno nalogo, ki jo lahko opravijo ljudje (Islovar, 2023).

Leta 2023 so prevladujoči modeli umetne inteligence ozki sistemi. Od splošne umetne inteligence, ki bo prevzela svet in zasužnjila človeštvo, pa smo po mnenju strokovnjakov oddaljeni še nekaj let (Bove, 2023).

Čeprav deluje, kot da smo za orodja umetne inteligence slišali šele v 2023, že vrsto let krojijo in usmerjajo naše življenje. Sistemi umetne inteligence na področju **računalniškega vida**, ki strojni opremi omogočajo interpretacijo in razumevanje vizualnih informacij iz realnega sveta, se uporabljajo za prepoznavanja obraza, branje besedila iz tiskanih dokumentov, analizo medicinskih posnetkov in celo samodejno vožnjo vozil. Na orodjih umetne inteligence temelječi **roboti** so široko razširjeni v proizvodnji, pri izvajanju nevarnih opravil in celo na področju gospodinjskih aparatov. Veliki **iskalniki** uporabljajo modele in orodja umetne inteligence za indeksiranje vseh objavljenih spletnih strani in razumevanje njihove vsebine, za interpretacijo iskalnih poizvedb, usklajevanje poizvedb z najbolj natančnimi in kakovostnimi rezultati, za algoritemsko razvrščanje iskalnih rezultatov, procesiranje naravnega jezika (angl. *Natural Language Processing*, kratica NLP), kar omogoča razumevanje iskalnih poizvedb, za analizo slik, izboljšanje ciljanja in kakovosti oglasov ter uporabo zaznavanja vzorcev za prepoznavanje neželene pošte, prevar in podvojenih vsebin. **Družbena omrežja** uporabljajo sisteme umetne inteligence za moderiranje vsebin, personalizacijo uporabniške izkušnje, ciljno oglaševanje in preprodajo uporabniških podatkov. Tudi organizacije pospešeno uporabljajo orodja umetne inteligence, na primer nekatera orodja Microsoft in druga orodja za povečanje produktivnosti.

Izjemen porast zanimanja za področje umetne inteligence v letu 2023 pa je povzročila razširitev uporabe posebnega tipa orodja, ki spada v skupino **generativne umetne inteligence**. Gre za modele in orodja umetne inteligence, ki omogočajo generiranje novih podatkov, podobnih danemu naboru podatkov. Vsebine, ki jih

lahko ustvarijo ta orodja, vključujejo zvok, video, besedilo in slike. Ker je na tem področju v letu 2023 veliko novosti, se v prispevku posvetimo predvsem uporabi sistemov generativne umetne inteligence.

Številni generativni modeli umetne inteligence, ki se uporabljajo v letu 2023, temeljijo na arhitekturi, imenovani **generativni prednaučeni transformerji** (angl. *Generative Pre-trained Transformers*, kratica GPT). Ti modeli podpirajo najrazličnejše naloge, najpogosteje pa se uporabljajo za naloge, povezane z generiranjem besedil. V porastu je tudi uporaba **difuzijskih modelov** (angl. *Diffusion Models*),[2] ki se prav tako učijo iz velikih količin podatkov, vendar se razlikujejo v načinu obdelave konteksta. Ti modeli so lahko zelo uporabni pri nalogah, povezanih z generiranjem slik in celo videa. Kljub temu da obstajajo številni drugi generativni modeli umetne inteligence, je povečanje zanimanja za modele umetne inteligence nastalo predvsem zaradi razširitve uporabe GPT-ja in difuzijskih modelov umetne inteligence v splošno uporabo, zato oba modela v nadaljevanju predstavimo podrobneje.

1. GPT MODELI UMETNE INTELIGENCE

GPT modeli uporabljajo transformersko arhitekturo za generiranje človeku podobnega besedila in so predhodno usposobljeni na velikih količinah podatkov. Prilagodi se jih lahko za specifične naloge, kot so prevajanje jezika, povzemanje besedila in dopolnjevanje besedila. Glavna inovacija, ki jo predstavljajo transformerski modeli, je uporaba samopozornih mehanizmov, ki modelu omogočajo, da se osredotoči na pomembne dele vhodnih podatkov in ustrezno izrazi odvisnosti med njimi (Islovar, b. l.), ter **veliki jezikovni modeli** (angl. *Large Language Models*, kratica LLM), ki so sestavljeni iz nevronske mreže s številnimi parametri in se učijo na velikih količinah neoznačenega besedila z uporabo samonadzorovanega učenja (Islovar, 2023). LLM modeli ocenjujejo verjetnost zaporedja besed v jeziku in napovejo nadaljnje besede glede na prejšnje v vrstici ali stavku.

V letu 2023 je bilo objavljenih veliko novih LLM-jev ter številna na njih temelječa orodja. Večina teh modelov pa ni nastala v

obliki samostojnih modelov, temveč se je razvila iz manjšega števila velikih oziroma **temeljnih LLM-jev** (angl. *Foundational Models*). Ti temeljni LLM-ji se uporabljajo za izgradnjo manjših in ožje usmerjenih LLM-jev in orodij.

V nadaljevanju so na kratko opisani temeljni LLM-ji, ki so bili pogosto omenjeni sredi leta 2023.

Velikost LMM-ja se običajno ocenjuje glede na število parametrov, ki jih ima, pri čemer se parameter nanaša na spremenljivko ali vrednost, ki vpliva na delovanje modela ali na rezultate njegovega predvidevanja. Parametri so nastavljeni med usposabljanjem modela in se uporabljajo za nadzor različnih vidikov modela, kot so število plasti, velikost besedilnega okna in podobno. Parametri vplivajo na zmogljivost modela, njegovo hitrost izvajanja in sposobnost učenja iz podatkov. Vendar pa več parametrov pomeni tudi, da model potrebuje več računalniških virov in podatkov za učinkovito usposabljanje. LLM-ji z več parametri niso nujno tudi zmogljivejši, poleg tega pa so modeli z manj parametri lahko potencialno zelo učinkoviti pri uporabi v manjših okoljih in rešitvah. Poleg tega se LLM-jem dnevno pridružujejo novi modeli, vključno s temeljnimi modeli.

Zaradi omejenih možnosti za primerjavo LLM-jev ter velike dinamike objave LLM-jev v prvi polovici leta 2023 izdelava seznama največjih ali najpomembnejših LLM-jev ni mogoča. Temeljni LLM-ji v nadaljevanju poglavja so vključeni po presoji avtorice.

1.1. GPT-3.5 in 4

GPT-3.5 in 4 sta zaprtokodna temeljna LLM-ja, ki ju je razvilo podjetje OpenAI. Modela delujeta od leta 2020 in sta na voljo prek platforme OpenAI, ta pa za delovanje uporablja infrastrukturo Microsoft Azure. GPT-3.5 naj bi obsegal 175 milijard parametrov (OpenGenus, b.l.), obseg GPT-4 pa sredi leta 2023 še ni bil javno znan.

GPT-4 lahko sledi kompleksnim navodilom v naravnem jeziku in

natančno rešuje zahtevne probleme, zlasti probleme, ki temeljijo na analizi in generiranju naravnega jezika. Omogoča tudi vnose nekaterih slikovnih gradiv, zaradi česar presega »navadne« jezikovne modele (Kazi, 2023). Na temeljnih modelih GPT-ja deluje več različnih izpeljanih modelov in orodij, na primer:

- model, zasnovan kot pogovorno orodje za odgovarjanje na vprašanja, tvorjenje besedil, povzemanje besedil in prevajanje ChatGPT; ChatGTP omogoča nadgradnje z različnimi vtičniki, med drugim za prepoznavanje govora, obrazov, predmetov in besedila (Kovič, 2023);
- serija modelov, ki so optimizirani za krajša navodila ali vgradnje v različne modele InstructGPT;
- aplikacijski programski vmesnik (angl. *Application Programming Interface*, kratica API)[3] GPT API, ki razvijalcem omogoča, da vključijo velik močan jezikovni model v lastne informacijske rešitve, tako da je možno generiranje odzivov s človeku podobnim besedilom v pogovorih v realnem času; to omogoča na primer:
- razvoj sposobnih interaktivnih klepetalnikov, ki vodijo naravno zveneče pogovore s strankami in drugimi uporabniki,
- avtomatizirano generiranje vsebine, na primer čivkov, blogov in celo elektronskih sporočil,
- prevajanje besedila na spletnih straneh in celo v realnem času,
- igranje različnih vlog,
- prilagoditev vsebin slabovidnim osebam,
- pripravo avtomatiziranih povzetkov na podlagi vsebin, ki jih v model posredujejo uporabniki, na primer povzemanje velikega števila elektronskih sporočil, in številne druge funkcionalnosti.

Uporaba ChatGPT-ja je praviloma brezplačna, cena uporabe drugih orodij in storitev OpenAI pa je vezana na obseg uporabe.

1.2. LaMDA

LLM jezikovni model za pogovorne rešitve (angl. *Language Model for Dialogue Applications*, kratica LaMDA) je temeljni zaprtokodni LLM, ki ga je razvilo podjetje Google, obsegal naj bi 137 milijard parametrov (Chang, 2022) in naj bi bil posebej

prilagojen komunikaciji v obliki pogovora. Sredi 2023 ga je Google izbranim uporabnikom poskusno dal na voljo v obliki pogovornega orodja Bard[4].

1.3. LLaMA

LLM veliki jezikovni model Meta AI (angl. *Large Language Model Meta AI*, kratica LLaMA) je temeljni odprtokodni LLM, ki ga je razvilo in objavilo podjetje Meta. Na voljo je v več velikostih, od 7 do 65 milijard parametrov, ter brezplačno na voljo raziskovalcem, znanstvenikom in drugim nekomercialnim uporabnikom. Cilj Mete pri tem je raziskovanje potencialnih uporab LLM-jev in razumevanje njihovih zmogljivosti ter omejitev (Facebook AI, 2023). Sredi leta 2023 sta bila najbolj znana modela oziroma orodji, ki sta nastali na podlagi LLM-ja, demonstracijsko orodje LLaMA za sledenje navodilo Alpaca[5] s 7 milijardami parametrov, ki so ga razvili raziskovalci univerze Stanford (Taori, 2023), in pogovorno orodje Vicuna[6] s 13 milijardami parametrov, ki so ga razvili raziskovalci univerz UC Bearkly, Mohamed bin Zayed University of Artificial Intelligence in Stanford (Parthasarathy, 2023).

1.4. Falcon

LLM Falcon[7] je temeljni odprtokodni LLM, ki ga je razvil in objavil Tehnološki inovacijski inštitut v Abu Dabiju. Na voljo je v velikostih od 7 do 40 milijard parametrov. Model je na voljo brezplačno tudi za komercialno uporabo. Po navedbah avtorjev naj bi bil zelo varčen z računalniškimi viri (spletna stran Tehnološkoinovacijskega inštituta, 2023), po funkcionalnostih pa se želi predvsem približati GPT modelom (Arya, 2023).

2. DIFUZIJSKI MODELI UMETNE INTELIGENCE

Difuzijski modeli uporabljajo podatke, na podlagi katerih se učijo tako, da jih uničijo z dodajanjem šuma, nato pa se naučijo obnoviti podatke tako, da obrnejo ta proces šuma. Tako lahko iz šuma

ustvarijo koherentne izdelke, zaradi česar se uporabljajo zlasti za generiranje raznih multimedijskih vsebin. Podprejo lahko tudi nekatere funkcionalnosti strojnega vida, urejanje slik, semantično in besedilno vodeno ustvarjanje slik, segmentacijo slik. Uporabljajo se za generiranje in dopolnjevanje 3D oblik, odstranjevanje šuma na slikah, popravljanje slik, generiranje videoposnetkov in celo grafično oblikovanje molekul. Nekateri difuzijski modeli lahko prav tako podprejo ustvarjanje drugih multimedijskih vsebin, na primer glasbe. Uporabe difuzijskih modelov so obsežne in se še razvijajo.

2.1. DALL-E 2

Model DALL-E 2[8] za generiranje slik je razvilo podjetje OpenAI. Gre za zaprtokodni difuzijski model, katerega število parametrov sicer ni javno znano, je pa več kot 13 milijard (toliko parametrov je imel predhodni model DALL-E). Namenjen je generiranju realističnih digitalnih slik iz opisov naravnega jezika, na voljo je prek spletnega brskalnika in kot API, ki razvijalcem omogoča integracijo modela v njihove informacijske rešitve. Dostop prek spletnega brskalnika se plačuje po uporabi.

Model DALL-E 2 je že vgrajen v številne informacijske rešitve tretjih strank, med drugim tudi v Microsoftovo rešitev Designer in orodje Image Creator, ki je vključen v iskalnik Bing in brskalnik Microsoft Edge (Rath, 2023). Obe orodji sta v osnovni različici brezplačni.

2.2. Midjourney

Model za generiranje slik Midjourney[9] je razvilo podjetje Midjourney inc. Tudi ta umetnointeligenčni model je zaprtokoden, dostopen pa le na spletu, natančneje na enem izmed kanalov pogovorne informacijske rešitve Discord[10]. Model je izjemno dober pri ustvarjanju visokokakovostnih slik, ki so v nekaterih primerih preslepile celo strokovnjake (Wankhede, 2023). Uporaba modela Midjourney se plačuje po uporabi.

2.3. Stable Diffusion

Model za generiranje slik Stable Diffusion[11] so razvila podjetja CompVis, Stability AI in LAION. Model je odprtokoden in na voljo tudi tretjim osebam, ki bi ga želele uporabiti za razvoj lastnih modelov, omogoča pa tudi uporabo po API-ju.

3. SISTEMI IN ORODJA UMETNE INTELIGENCE V ORGANIZACIJAH

V nadaljevanju predstavljamo nekatere skupine orodij, ki jih v naslednjih letih kot revizorji informacijskih sistemov lahko pričakujemo v organizacijah.

3.1. Orodja za povečanje produktivnosti

Med na modelih umetne inteligence temelječimi orodji, ki jih že uporabljajo številne organizacije, pa tudi posamezniki, lahko štejemo različne virtualne asistente, kot so Siri,[12] Alexa[13] in Google Assistant[14]. Ti asistenti posebej dobro delujejo v angleškem jeziku, pomagajo pa lahko posameznikom predvsem pri načrtovanju, opomnikih in drugih administrativnih nalogah. Orodja, kot je sestankovalno orodje Zoom, že vključujejo nove na modelih umetne inteligence temelječe funkcionalnosti Zoom IQ Meeting Summary,[15] ki omogočajo pripravo povzetka sestankov. Na umetni inteligenci temelječa orodja Power Automate[16] omogočajo pametno upravljanje elektronske pošte in drugih sporočilnih sistemov, upravljanje koledarjev in določanje prednostnih nalog ter tako pomembno izboljšajo odzivni čas.

3.2. Orodja za izboljšanje komuniciranja

Orodja, ki temeljijo na umetni inteligenci, že pomembno izboljšujejo področje komunikacije, tako komuniciranje znotraj organizacij kot tudi z zunanjimi deležniki. Napredek je bil sredi

leta 2023 viden predvsem v komuniciranju v velikih svetovnih jezikih, a je ob trenutni stopnji napredka zelo verjetno, da bodo vsaj nekatera orodja zadovoljivo delovala tudi v jezikih z manj govorci. Možnost obdelave naravnega jezika namreč omogoča napredno prepoznavanje govora in prevajanje, kar bi dolgoročno lahko pomembno olajšalo komunikacijo izza jezikovnih ovir. Na modelih umetne inteligence temelječa orodja in posebej usposobljena orodja, zlasti klepetalniki in virtualni pomočniki, bodo lahko bolj neposredno komunicirala s strankami, s čimer bodo zmanjšala breme na zaposlene. Če bo Evropska unija dovolila t. i. orodja za analizo razpoloženja, torej orodja, ki prepoznavajo čustva naravnih govorcev, bi ta orodja lahko celo izboljšala odnose s strankami. Ne nazadnje orodja, ki temeljijo na modelih umetne inteligence, že zdaj omogočajo odlično organizacijo pisarniškega poslovanja, zlasti boljšo organizacijo elektronske pošte in drugih uradnih sporočilnih sistemov.

3.3. Orodja za zaznavanje prevar

Orodja, ki temeljijo na umetni inteligenci, lahko učinkovito zaznavajo potencialne prevare s pomočjo analize vzorcev in anomalij v velikih količinah podatkov. Ta orodja na podlagi določitve parametrov in treninga na vzorčnih primerih lahko izjemno natančno prepoznajo sumljive transakcije in celo neobičajno vedenje posameznikov. Z avtomatizacijo zaznavanja suma prevar lahko podjetja prihranijo čas in vire ter hkrati zmanjšujejo finančna tveganja in se ščitijo pred goljufivimi dejavnostmi.

3.4. Priporočilni sistemi

V organizacijah, ki se zanašajo na spletno trgovanje, lahko orodja umetne inteligence analizirajo preference in vedenje strank ter jim predlagajo ustrezne izdelke, storitve ali vsebine. Široko je uveljavljena tudi sporna praksa kupovanja navidezno psevdonimiziranih podatkov o vedenju strank na družbenih omrežjih in drugih neodvisnih spletnih straneh ter uporaba orodij

umetne inteligence za integracijo teh podatkov v priporočilne sisteme.

3.5. Prepoznavanje slik in videoposnetkov

Sistemi za prepoznavanje slik in videoposnetkov, ki temeljijo na umetnointeligenčnih modelih in orodjih, analizirajo vizualno vsebino za razvrščanje in selekcijo predmetov, zaznavanje obrazov in prepoznavo vzorcev. Te informacijske rešitve se uporabljajo na področjih, kot so usmerjanje proizvodnje, zagotavljanje kakovosti, varnostni nadzor in avtonomna vozila.

4. VZPOSTAVITEV IN OPERATIVNO DELOVANJE UMETNOINTELIGENČNIH SISTEMOV V POSLOVNEM OKOLJU

Številne organizacije so že ali nameravajo v bližnji prihodnosti na različne načine vzpostaviti lastna umetnointeligenčna orodja za podporo poslovanju.

Nekatera orodja bodo organizacije pridobile v obliki programske opreme kot storitve (angl. *Software as a Service*, kratica SaaS), torej tako, da bodo najele na modelih umetne inteligence temelječa orodja za izvajanje raznih poslovnih funkcij.

Nekatera orodja umetne inteligence bodo vzpostavila v okviru velikih poslovnih informacijskih rešitev, na primer Microsoft 386, SAP in NetSuite. Vsa velika orodja za podporo poslovanju ponujajo številna že vgrajena umetnointeligenčna orodja, ki jih je mogoče nastaviti tako, da ustrezajo zahtevam strank.

Ne nazadnje bodo nekatere napredne organizacije na podlagi razpoložljivih modelov umetne inteligence same vzpostavile svoje modele in orodja, ki bodo posebej prilagojeni njihovim zahtevam in potrebam. Sisteme umetne inteligence je načeloma mogoče vzpostaviti na lastni infrastrukturi, s samostojnimi orodji in knjižnicami za obdelavo podatkov in strojno učenje. Univerza Stanford je svoj model za sledenje navodilom Alpaca na primer razvila tako, da je deloval na računalniških virih v skupni vrednosti 600 USD (Taori, 2023). Manjši različici

umetnointeligenčnih modelov LLaMA in Falcon se lahko izvajata celo na zmogljivih prenosnikih. Vendar pa so za izvajanje večine modelov umetne inteligence potrebni izjemno veliki računski viri. Ustrezno zmogljivost strojne opreme, na kateri se izvajajo umetnointeligenčni sistemi, so omogočili zlasti visokozmogljivi **grafični procesorji** podjetja NVIDIA (angl. *Grafic Processing Units*, kratica GPU). NVIDIA za svoje GPU-je zagotavlja vrsto orodij in gonilnikov, ki programerjem in raziskovalcem omogočajo prilagajanje delovanja GPU-jev za njihove specifične potrebe. To vključuje nastavitve in konfiguracije za optimizacijo izvajanja algoritmov, upravljanje pomnilnika GPU-ja ter prilagajanje parametrov zmogljivosti in porabe energije. Tako prilagojeni procesorji omogočajo hkratno izvajanje velikega števila nalog. Boljši modeli teh procesorjev so zelo dragi in primerni zlasti za uporabo v velikih računalniških centrih, kjer so v veliki meri nadomestili klasične centralne procesorje (angl. *Central Processing Units*, kratica CPU).

Praviloma organizacije svoje umetnointeligenčne sisteme vzpostavljajo na **platformah umetne inteligence**, zmogljivi tehnološki infrastrukturi, namenjeni obdelavi velikih količin podatkov in izvajanju zahtevnih umetnointeligenčnih algoritmov**.**

Platforme umetne inteligence so infrastrukturno okolje, ki omogoča razvoj, upravljanje in izvajanje umetnointeligenčnih sistemov. Take platforme združujejo različne komponente in orodja, ki omogočajo raziskovanje, razvoj, testiranje in vzpostavitev različnih umetnointeligenčnih sistemov in informacijskih rešitev (Portal Predictive Analytics Today Research, 2023).

Platforme umetne inteligence poleg tehnološke infrastrukture omogočajo **razvojna orodja** za modele umetne inteligence, na primer:

- **knjižnice umetne inteligence** – zbirke predhodno napisane kode, ki jih razvijalci lahko uporabijo za izvajanje različnih nalog, kot so obdelava podatkov, usposabljanje modelov in ocenjevanje;
- okvire za **strojno učenje**, ki modelom umetne inteligence omogočajo učiti se in izboljševati delovanje na podlagi

podatkov ali izkušenj preteklega izvajanja (Islovar, 2023); algoritmi strojnega učenja se uporabljajo za razvoj modelov, ki napovedujejo, razvrščajo ali razumejo podatke, kar je osnova delovanja sistemov umetne inteligence.

Platforme umetne inteligence omogočajo tudi **shranjevanje, upravljanje in dostop do podatkovnih virov**, ki se uporabljajo za učenje in napajanje. Podatkovni viri za napajanje sistemov umetne inteligence so lahko med drugim:

- strukturirani podatki, kot so tabelarne podatkovne zbirke in drugi strukturirani zapisi;
- nestrukturirani podatki v obliki besedila, slike, zvoka ali videa;
- senzorski podatki, ki jih zbirajo različni senzorji, kot so temperaturni senzorji, merilniki hitrosti, naprave, s katerim lahko kjer koli določimo lokacijo z geografsko širino in dolžino,[17] merilniki srčnega utripa in podobno;
- podatki iz družbenih medijev;
- podatki s spleta – spletnih strani, pa tudi forumov, blogov in podobno.

Orodja umetnointeligenčnih platform za delo s podatki vključujejo še funkcionalnosti za čiščenje, transformacijo in pripravo podatkov za analizo (Abhishek, 2022).

- Platforme umetne inteligence omogočajo **učenje modelov** z uporabo različnih tehnik, kot so:
- **nadzorovano učenje** (angl. *Supervised Learning*) na učni množici primerov s posebej označeno ciljno lastnostjo, kjer je rezultat učenja napovedni model za napovedovanje te lastnosti (Islovar, 2023);
- **nenadzorovano učenje** (angl. *unsupervised learning*), strojno učenje na učni množici primerov brez posebej označene ciljne lastnosti, kjer je rezultat učenja vzorec;
- **samonadzorovano učenje** (angl. *Self-supervised Learning*, kratica SSL), ki zajema metode za obdelavo in označevanje neoznačenih podatkov za pridobitev uporabnih predstavitev, ki lahko pomagajo pri nadaljnjih nalogah učenja (iSlovar, 2023) in
- **spodbujevalno učenje** (angl. *Reinforcement learning*, kratica RL), kjer se modeli učijo v interakciji s svojim okoljem tako, da

za vsako izvedeno akcijo prejmejo povratno informacijo v obliki nagrade ali kazni s ciljem dolgoročnega maksimiranja skupne nagrade (Wikipedia, 2023).

Platforme umetne inteligence ponujajo tudi funkcionalnosti za ocenjevanje in optimizacijo modelov.

- Platforme umetne inteligence navsezadnje podpirajo **upravljanje modelov umetne inteligence**, **njihovo distribucijo** v produkcijsko okolje in **izvajanje umetne inteligence,** vključno s spremljanjem, sledenjem uspešnosti modelov, verzioniranjem, skaliranjem in avtomatiziranim prenosom v produkcijsko delovanje.
- Platforme umetne inteligence pogosto omogočajo, da jih uporabniki z API-jem povežejo v različne lastne informacijske rešitve, kar lahko pomembno nadgradi njihove funkcionalnosti.

Platforme umetne inteligence lahko vključujejo še tudi druge funkcionalnosti, kot so vizualizacija podatkov, orodja za sodelovalno delo, upravljanje virov, varnostni mehanizmi ter podpora za nadzor in interpretacijo modelov. Platforme umetne inteligence so ključne pri razvoju in uporabi umetne inteligence, saj olajšajo kompleksnost in omogočajo hitro iteracijo v razvoju umetnointeligenčnih sistemov ter njihovo učinkovito upravljanje v produkcijskem okolju.

V nadaljevanju predstavljamo nekaj platform umetne inteligence, ki se široko uporabljajo na področju poslovanja.

4.1. Google AI

Google AI[18] je platforma za umetno inteligenco, ki jo je razvil Google. Vzpostavljena je bila leta 2015 in je namenjena razvijalcem in podjetjem, ki želijo uporabiti umetno inteligenco v svojih izdelkih in storitvah. Primer izdelka, ki ga je razvilo tretje podjetje na platformi Google AI, je Grammarly[19] – pomočnik pri pisanju, ki uporabnikom pomaga izboljšati njihovo pisanje s prepoznavanjem slovničnih in pravopisnih napak ter ponuja predloge za izboljšanje sloga in tona. Primer izdelka v široki

uporabi, ki deluje na platformi Google AI, je tudi Google Photos, ki umetno inteligenco uporablja za organizacijo fotografij in videoposnetkov, in sicer uporablja algoritme strojnega učenja za prepoznavanje obrazov in predmetov ter omogoča iskanje po ključnih besedah in kategorijah.

4.2. Microsoft Azure Machine Learning

Microsoft Azure Machine Learning[20] je platforma za strojno učenje, ki je bila vzpostavljena leta 2014. Lastnik platforme je podjetje Microsoft. Azure Machine Learning je namenjen izvajanju nalog strojnega učenja, vključno s prepoznavanjem vzorcev, razvrščanjem, regresijo, segmentacijo podatkov, predvidevanjem in optimizacijo. Platforma omogoča visoko stopnjo integracije z drugimi storitvami Azure, tudi s skupnim obračunavanjem. V partnerstvu z organizacijo OpenAI na tehnološki infrastrukturi Azure deluje tudi orodje ChatGPT[21].

4.3. Amazon Web Services AWS AI

Amazon Web Services AWS AI[22] je platforma umetne inteligence, ki jo je že leta 2005 vzpostavilo podjetje Amazon in je bila skoraj desetletje vodilna platforma za področje umetne inteligence. Platforma ponuja širok nabor storitev in orodij za obdelavo podatkov ter izvajanje umetnointeligenčnih nalog, kot so strojno učenje, globoko učenje, obdelava naravnega jezika, računalniški vid in avtomatizacija inteligentnih sistemov. Na platformi AWS AI teče med drugim glasovni pomočnik Amazon Alexa, ki je na voljo v različnih napravah, kot so pametni zvočniki, pametni telefoni in tablice, ter omogoča glasovno upravljanje naprav in opravlja druge naloge. Alexa uporablja umetno inteligenco in strojno učenje za razumevanje naravnega jezika in odgovarjanje na uporabnikova vprašanja.

4.4. Salesforce AI

Platforma AI Salesforce[23] je bila vzpostavljena leta 2016. Njen lastnik je podjetje Salesforce, vodilno podjetje na področju upravljanja odnosov s strankami. Platforma je namenjena predvsem rešitvam za izboljšanje uporabniške izkušnje, avtomatizacijo procesov in napovedovanje s pomočjo naprednih algoritmov in analitike. Omogoča močno integracijo z obstoječimi Salesforcevimi rešitvami, napredno podporo odločanju in optimizacijo poslovnih procesov. Najširše uporabljano orodje, ki deluje na platformi Salesforce AI, je Einstein[24] – orodje umetne inteligence, integrirano v različne dele celotnega informacijskega sistema Salesforce.

5. ZAKLJUČEK

Prispevek je zelo kratek in ne povsem strukturiran povzetek nekaterih ključnih znanj, ki bodo v prihodnjih letih ključna za pooblaščene revizorje informacijskih sistemov, pa tudi za notranje revizorje in vse druge, ki podpirajo poslovanje sodobnih organizacij. Modeli in orodja umetne inteligence bodo v poslovanju vse pomembnejši, ker bodo omogočili avtomatizacijo rutinskih nalog, izboljšanje odločanja in vpogled v vedenje strank. Vendar pa uporaba teh modelov in orodij predstavlja tudi možna tveganja, na primer tveganje izgube podatkov, prevar in groženj kibernetske varnosti. V prihodnjih letih bo pomembno, da organizacije uvedejo robustne kontrole in varovala za ublažitev teh tveganj ter zagotovijo odgovorno uporabo modelov in orodij umetne inteligence. Pravilno upravljanje podatkov, redni pregledi in usposabljanje zaposlenih lahko pomagajo preprečiti izgubo podatkov in prevare. Poleg tega bi morale organizacije vlagati v ukrepe kibernetske varnosti, da bi se zaščitile pred zunanjimi grožnjami. Čeprav modeli umetnointeligenčnih orodij predstavljajo številne priložnosti, je pomembno skrbno upravljati povezana tveganja in zagotoviti njihovo odgovorno uporabo.

6. LITERATURA IN VIRI

1. Abhishek, K. (2022). Introduction to artificial intelligence. *Portal Redgate Hub*. Najdeno 13. junija 2023 **na spletnem naslovu**.

2. Anirudh, V. K. (2023). Top 21 Artificial Intelligence Software, Tools, and Platforms. *Spiceworks*. Najdeno 11. junija 2023 **na spletnem naslovu**.
3. Aplikacijski programski vmesnik. *ISlovar*. (b. l.) Najdeno 11. junija 2023 **na spletnem naslovu**.
4. Arya, N. (2023). *KDNuggets*. Falcon LLM: The new king of LLMs. Najdeno 13. junija 2023 **na spletnem naslovu**.
5. Bove, T. (2023). *Fortune*. Google DeepMind CEO: AGI is the 'Holy Grail' of artificial intelligence. Najdeno 11. junija 2023 **na spletnem naslovu**.
6. Carv. (2023). AI tools for businesses in 2023. *Carv Blog*. Najdeno 1. julija 2023 **na spletnem naslovu**.
7. Cheng, H.-T., Thoppilan, R. (2022, 21. januar). LaMDA: Towards Safe, Grounded, and High-Quality Dialog Models for Everything. *Google AI Blog*. Najdeno 11. junija 2023 **na spletnem naslovu**.
8. Facebook AI. (2023). Introducing LLAMA, a large language model that can learn from anyone, anywhere. ***Facebook AI Blog***. Najdeno 13. junija 2023 **na spletnem naslovu**.
9. Generativni prednaučeni transformerji. (2023). *Islovar*. Najdeno 11. junija 2023 **na spletnem naslovu**.
10. Globoko učenje. (b. l.). *Islovar*. Najdeno 11. junija 2023 **na spletnem naslovu**.
11. Kazi, S., Elmahdy, A. (2023, 28. marec). Top Large Language Models (LLMs): GPT-4, LLaMA, FLAN UL2, BLOOM, and More. *Vectara*. Najdeno 11. junija 2023 **na spletnem naslovu**.
12. Kovič, K. (2023). ChatGPT s 45 novimi vtičnik. *Spletna stran Marketing Magazine*. Najdeno 14. junija 2023 **na spletnem naslovu**.
13. Nadzorovano učenje. (b. l). *Islovar*. Najdeno 11. junija 2023 **na spletnem naslovu**.
14. Nenadzorovano učenje. (b. l.) *Islovar*. Najdeno 11. junija 2023 **na spletnem naslovu**.
15. OpenGenus IQ. (b. l.). GPT-3.5 model architecture. *OpenGenus IQ*. Najdeno 11. junija 2023 **na spletnem naslovu**.
16. Ozka umetna inteligenca. (b. l). *Islovar*. Najdeno 11. junija 2023 **na spletnem naslovu**.
17. Parthasarathy, S. (2023). The Significance of Vicuna, an Open-Source Large Language Model for Chatbots. *Medium*. Najdeno 17. junija 2023 **na spletnem naslovu**.

18. Rath, S. (2023). Top 10 AI Art Generation Tools using Diffusion Models. *LearnOpenCV*. Najdeno 1. julija 2023 **na spletnem naslovu**.
19. Reinforcement learning. (b. l.). *Wikipedia*. Najdeno 1. aprila 2023 **na spletnem naslovu**.
20. Splošna umetna inteligenca. (b. l). *Islovar*. Najdeno 11. junija 2023 **na spletnem naslovu**.
21. Strojno učenje. (b. l.). *Islovar*. Najdeno 11. junija 2023 **na spletnem naslovu**.
22. Taori, R., et al. (2023). Alpaca. *Stanford University*. Najdeno 11. junija 2023 **na spletnem naslovu**.
23. Tehnološkoinovacijski inštitut Abu Dhabi. (b. l.). Falcon LLM. Najdeno 17. junija 2023 **na spletnem naslovu**.
24. Top 18 Artificial Intelligence Platforms. (2023). *Predictive Analytics Today Research*. Najdeno 12. junija 2023 **na spletnem naslovu**.
25. Umetna inteligenca. (b. l.). *Islovar*. Najdeno 11. junija 2023 **na spletnem naslovu**.
26. Veliki jezikovni model. (b. l). *Islovar*. Najdeno 11. junija 2023 **na spletnem naslovu**.
27. Wankhede, C. (2023). What is Midjourney? Everything you need to know about the AI art tool. *Android Authority*. Najdeno 1. julija 2023 **na spletnem naslovu**.

Opombe

* Maja Hmelak, mag. znanosti, CISA, CIA, PRIS, svetovalka za revizijsko statistiko, Računsko sodišče Republike Slovenije, hmelak.maja@gmail.com.

1. Zaradi izjemno hitrega razvoja področja umetne inteligence, ki je značilen za leto 2023, smo v članek vključili bolj znane angleške izraze, poleg tega pa uporabljamo kratice iz angleških izrazov.
2. Drugo ime za difuzijske modele je verjetnostni difuzijski modeli.
3. Islovar (2023) API opredeljuje kot vmesnik, ki zagotavlja, da ima računalniški program na razpolago funkcije operacijskega sistema ali drugega računalniškega programa.
4. **Spletni naslov**
5. **Spletni naslov**
6. **Spletni naslov**
7. **Spletni naslov**
8. **Spletni naslov**

9. **Spletni naslov**
10. **Spletni naslov**
11. **Spletni naslov**
12. **Spletni naslov**
13. **Spletni naslov**
14. **Spletni naslov**
15. **Spletni naslov**
16. **Spletni naslov**
17. Angl. *Global Positioning System*, kratica GPS.
18. **Spletni naslov**
19. **Spletni naslov**
20. **Spletni naslov**
21. **Spletni naslov**
22. **Spletni naslov**
23. **Spletni naslov**
24. **Spletni naslov**

Jaka Kosmač*

Novosti v EU-ju na področju kibernetske varnosti: od NIS 2 do kibernetske solidarnosti

EU Cyber Security Update: From NIS 2 to Cyber Solidarity

POVZETEK ● *Direktiva NIS je bila prvi akt, ki je področje kibernetske varnosti urejal na ravni EU-ja. Šest let kasneje je bila sprejeta nova direktiva – NIS 2, s katero želi EU dodatno izboljšati kibernetsko odpornost in odzivnost javnega in zasebnega sektorja ter Unije kot celote. Z direktivo NIS 2 je tudi uradno vzpostavljena Evropska organizacijska mreža za povezovanje v kibernetski krizi (EU-CyCLONe), ki podpira usklajeno upravljanje velikih kibernetskih incidentov. Direktiva razširja seznam zavezancev, deli jih na bistvene in pomembne subjekte, ki bodo dolžni v 24 urah poročati o varnostnih incidentih ter v enem mesecu o incidentu in vzroku ter vpeljanih in načrtovanih ukrepih za odpravljanje tveganj. Podobno kot Splošna uredba o varstvu podatkov – GDPR tudi direktiva NIS 2 predvideva visoke globe za kršitev določil. Poleg direktive NIS 2 sta bili decembra 2022 na sektorskem področju sprejeti še Direktiva o odpornosti kritičnih subjektov (direktiva CER) in Uredba o digitalni operativni odpornosti za finančni sektor. Aktivnosti EU-ja na področju zagotavljanja varnega in odpornega kibernetskega prostora se nadaljujejo tudi v letu 2023. Evropska komisija je aprila sprejela predlog Akta EU o kibernetski solidarnosti, da bi se okrepila zmogljivost v EU-ju za odkrivanje pomembnih in obsežnih kibernetskih groženj in napadov ter odzivanje nanje.*
Ključne besede ● *kibernetska varnost, NIS 2, EU, EU-CyCLONe, Akt EU o kibernetski solidarnosti*
SUMMARY ● *The NIS Directive was the first legislative act that regulated the field of cyber security at the EU level. Six years later EU adopted the new NIS 2 directive, with which it aims to further improve the cyber resilience and responsiveness of the public and private sectors and the EU as a whole. The NIS 2 directive established the European cyber crisis liaison organisation network (EU-CyCLONe), which supports the coordinated management of major cyber incidents. The directive also expands the list of the obligated and divides them into essential and important entities, which will be obliged to report security incidents within 24 hours and within one month to report the incident and the cause, as well as their implemented and planned measures to eliminate the risks. Similar to the General Data Protection Regulation - GDPR, the NIS 2 directive also foresees high fines for violation of its*

provisions. In addition to the NIS 2 directive, the Directive on the Resilience of Critical Entities (CER Directive) and the Regulation on Digital Operational Resilience for the Financial Sector were also adopted in the sector in December 2022. Activities in the field of ensuring a safe and resilient cyber space continue in 2023, namely in April the European Commission adopted a proposal for an EU Cyber Solidarity Act with the aim of strengthening the EU's capacity to detect and respond to significant and large-scale cyber threats and attacks.
Key words ● *cyber security, NIS 2 Directive, EU-CyCLONe, EU Cyber Solidarity Act*

JEL: H 83, K 24

1. UVOD

Direktiva o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (v nadaljevanju: direktiva NIS 2),[1] sprejeta decembra 2022, je zagotovo največji normativni napredek na področju urejanja kibernetske varnosti v EU-ju zadnje obdobje. Gre za ambiciozen dokument, ki nadomešča Direktivo o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (v nadaljevanju: direktivo NIS)[2] – ta je veljala za prvi zakonodajni akt o kibernetski varnosti na ravni EU-ja in je bila hkrati tudi glavni steber strategije EU-ja za kibernetsko varnost. Direktiva NIS je bila tako kot kasneje direktiva NIS 2 sprejeta na podlagi 114. člena Pogodbe o delovanju EU,[3] katerega cilj je vzpostavitev in delovanje notranjega trga z okrepitvijo ukrepov za približevanje nacionalnih pravil. Večja harmonizacija med nacionalnimi pravili je tudi eden izmed razlogov za potrebo po spremembah in sprejemu direktive NIS 2. Kot izhaja iz preambule direktive NIS 2, se zahteve glede kibernetske varnosti, ki jih morajo izpolnjevati subjekti, ki opravljajo storitve ali izvajajo gospodarsko pomembne dejavnosti, med državami članicami močno razlikujejo. Te razlike lahko povzročajo dodatne stroške, pa tudi tveganja in s tem ustvarjajo težave predvsem za tiste subjekte, ki poslujejo v več državah članicah. Ob pregledu izvajanja direktive NIS so se

pokazale velike razlike med državami članicami. Razlike so bile tudi na področju uporabe direktive NIS, saj je bila razmejitev področja uporabe v precejšnji meri prepuščena presoji držav članic, ki so določila direktive NIS v svojo zakonodajo prenesle zelo različno. Pravila na področju kibernetske varnosti so tako omogočala številne rešitve, ki so se med državami članicami razlikovale ali bile celo v nasprotju med seboj. Zelo široko polje proste presoje je direktiva NIS državam članicam prepustila tudi v zvezi z obveznostmi glede varnosti in poročanja o incidentih, ki so se kasneje v praksi na nacionalni ravni izvajale zelo različno. Podobne razlike so nastale pri izvajanju določb o nadzoru in izvrševanju.[4]

Direktiva NIS 2 je kot odgovor na pomanjkljivosti direktive NIS na področju kibernetske varnosti v EU-ju prinesla številne novosti, da bi bila uspešneje zagotavljena visoka skupna raven kibernetske varnosti v EU-ju. Bistveno je razširila nabor sektorjev, med katerimi bodo zdaj tudi subjekti, ki pod direktivo NIS niso bili predmet regulacije, na primer proizvajalci in distributerji kemikalij in medicinskih pripomočkov, predelovalci hrane, proizvajalci avtomobilov, ponudniki družbenih omrežij, ponudniki poštnih in kurirskih storitev ter številni drugi. Direktiva NIS 2 zavezancev ne deli na izvajalce bistvenih storitev[5] in ponudnike digitalnih storitev,[6] ampak subjekte deli le na bistvene in na pomembne subjekte, za katere veljajo enake vsebinske obveznosti, le da so bistveni subjekti podvrženi strožjim obveznostim glede nadzora in izvrševanja, prav tako so za prekrške bistvenih subjektov predpisane visoke globe. Direktiva NIS 2 bistvenim in pomembnim subjektom nalaga nove obveznosti za obvladovanje tveganj kibernetske varnosti, poročanje o kibernetskih incidentih in izmenjavo informacij. Pomembna novost direktive NIS 2 je uvedba odgovornosti vodstvenih organov bistvenih in pomembnih subjektov, ki so odgovorni za odobritev ukrepov za obvladovanje tveganj za kibernetsko varnost in nadzor nad njihovim izvajanjem ter za kršitve navedenih obveznosti. Države članice morajo direktivo NIS 2 v nacionalno zakonodajo prenesti do 17. oktobra 2024. Poleg direktive NIS 2 je bila decembra 2022 sprejeta tudi Direktiva o odpornosti kritičnih subjektov (v nadaljevanju: direktiva CER).[7] Konec decembra pa je bila sprejeta Uredba o

digitalni operativni odpornosti za finančni sektor (v nadaljevanju: DORA).[8] Direktiva NIS 2 je bila z omenjenima predpisoma, ki sta del sektorske zakonodaje, usklajena, s čimer sta zagotovljeni pravna jasnost in skladnost določb vseh treh predpisov.

Aktivnosti in pripravljenost Evropske komisije, da izboljša kibernetsko varnost v EU-ju, se s tem niso končale. Nadaljevala jih je tudi v letu 2023, ko je aprila sprejela predlog Akta EU o kibernetski solidarnosti,[9] s katerim želi doseči izboljšanje pripravljenosti, odkrivanja in odzivanja na kibernetske incidente v EU-ju.

Pričujoči prispevek je sestavljen iz več delov. V uvodu je kratek pregled aktivnosti EU-ja na področju kibernetske varnosti. V druge in tretjem poglavju so podrobneje opisane rešitve direktive NIS 2 in Akta EU o kibernetski solidarnosti. Zaključek pa povzema ugotovitve, možne vplive in možnosti za nadaljnje raziskave ter omejitve.

2. DIREKTIVA NIS 2

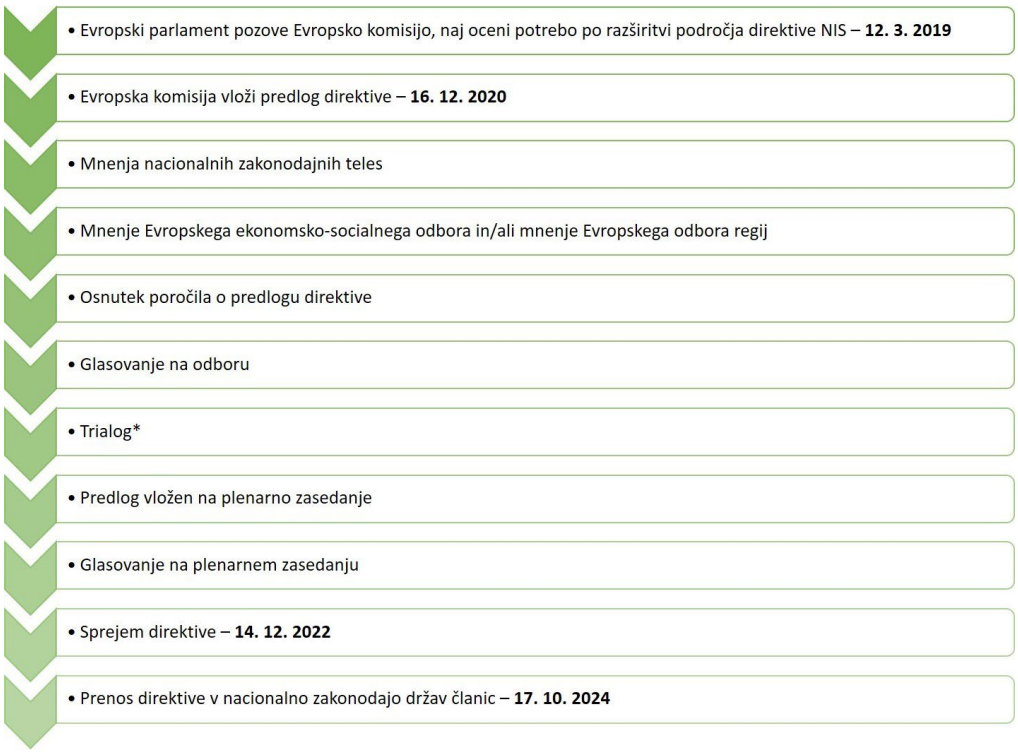
2.1. (Dolga) pot do nove zakonodaje in razlogi za spremembe

Januarja 2023 je začela veljati direktiva NIS 2, ki predstavlja novo, doslej najambicioznejše poglavje EU-ja na področju kibernetske varnosti. Vendarle ne smemo pozabiti, da je pot do implementacije določil nove direktive še dolga. Države članice imajo 21 mesecev časa za prenos direktive NIS 2 v nacionalno zakonodajo, kar pomeni, da bodo nova določila v praksi začela veljati šele v drugi polovici oktobra 2024, marsikatere obveznosti, ki jih predvideva direktiva NIS 2, pa bodo zavezanci uvedli oziroma dolžni izpolniti šele v letu 2025.[10] Pot do nove zakonodaje v EU-ju je dolga (Slika 1: Postopek sprejema direktive), saj je po predložitvi predloga potrebnih veliko usklajevanj in potrjevanj. Od vložitve predloga direktive NIS 2, s katerim se je 16. decembra 2020 začel zakonodajni postopek, do njenega končnega sprejema 14. decembra 2022 sta pretekli dve

leti. Pri tem je pomembno poudariti, da je bilo treba že pred tem pripraviti predlog direktive. Sprejemanje zakonodaje je dolgotrajen postopek ne glede na področje, ki ga ta ureja. Kibernetska varnost pa je področje, ki se zaradi hitrega razvoja tehnologije razvija in spreminja najhitreje oziroma med najhitrejšimi, zato je še toliko pomembneje, da je ob pripravi sprememb opravljen temeljit razmislek o novih pravilih, saj bo sicer novosprejeta zakonodaja ob uveljavitvi oziroma prenosu v nacionalne zakonodaje že zaostala za prakso, številni izzivi pa bodo ostali. Glede na to, da je Evropska komisija predlog vložila že 16. decembra 2020, kar je le dobri dve leti po tem, ko so morale države članice v svojo zakonodajo prenesti določila direktive NIS, bi lahko ocenili, da je hitro zaznala potrebo po spremembah na tem področju in sprožila postopke, da bi se čim prej spremenilo obravnavanje kibernetske varnosti v EU-ju in državah članicah. Še posebno glede na to, da je v direktivi NIS predvideno,[11] da Evropska komisija redno pregleduje delovanje direktive NIS ter o tem poroča Evropskemu parlamentu in Svetu, in sicer prvo poročilo predloži do 9. maja 2021. Kljub siceršnjim uspehom direktive NIS so bile pri pregledu njenega izvajanja ugotovljene pomanjkljivosti, zaradi katerih ni bilo mogoče učinkovito obravnavati aktualnih in prihodnjih izzivov na področju kibernetske varnosti.[12] Med razlogi in potrebami za sprejem nove direktive so bile predvsem razlike med državami članicami pri implementaciji določil direktive NIS. Te povzročajo razdrobljenost notranjega trga ter negativno vplivajo na čezmejno poslovanje in raven kibernetske odpornosti. Poleg tega je pregled izvajanja direktive pokazal naslednje težave: a) nizko stopnjo kibernetske odpornosti podjetij, ki delujejo v EU-ju; b) nedosledno odpornost v državah članicah in sektorjih; c) nizko stopnjo skupnega zavedanja stanja in pomanjkanje skupnega kriznega odzivanja. V praksi je to pomenilo, da na primer nekatere večje bolnišnice v državah članicah niso spadale na področje uporabe direktive NIS, zato niso bile zavezane k izvajanju varnostnih ukrepov, ki jih je ta nalagala. Po drugi strani pa so bili v drugi državi članici skoraj vsi posamezni izvajalci v zdravstvenem sektorju zavezani k spoštovanju pravil direktive NIS. Potrebo po nenehnem izboljševanju kibernetske varnosti in odpornosti EU-ja ter odziva na kibernetske incidente, zlasti v

kritičnih sektorjih, kot so zdravstvo, bančništvo in pravni sistemi, je potrdila tudi pandemija covida 19 (Giannakoulias, 2023). Pandemija je okrepila digitalno transformacijo družbe in razširila število groženj, ki zahtevajo prilagojene in inovativne odzive. Vsaka motnja, tudi tista, ki je sprva omejena na en subjekt ali en sektor, ima lahko kaskadne učinke v širšem smislu, kar povzroči daljnosežne in dolgotrajne negativne učinke pri zagotavljanju storitev na celotnem notranjem trgu (Evropska komisija, 2020). Cilj direktive NIS 2 je bil z določitvijo pravil za delovanje usklajenega regulativnega okvira, z določitvijo mehanizmov za učinkovito sodelovanje med pristojnimi organi držav članic, s posodobitvijo oziroma dopolnitvijo seznama sektorjev, za katere velja direktiva NIS 2, ter z določitvijo učinkovitih pravnih sredstev in izvršilnih ukrepov odpraviti pomembne razlike med državami članicami.[13]

Slika 1: *Postopek sprejemanja direktive*



* Trialog – V okviru rednega zakonodajnega postopka Evropske unije je trialog neformalno medinstitucionalno pogajanje, na katerem sodelujejo predstavniki Evropskega parlamenta, Sveta Evropske unije in Evropske komisije. Cilj trialoga je doseči začasen sporazum o zakonodajnem predlogu, ki je sprejemljiv za Parlament in tudi za Svet, ki sta sozakonodajalca.

Ta začasni sporazum je nato treba sprejeti po formalnih postopkih vsake od teh institucij.

Vir: *Evropski parlament.*

2.2. Ključne novosti in rešitve v direktivi NIS 2

Novosti in rešitve direktive NIS 2 v primerjavi z direktivo NIS v pričujočem prispevku razvrstimo v šest skupin:

- področje uporabe oziroma povečanje števila sektorjev in drugačna delitev,
- ukrepi za zagotavljanje kibernetske varnosti,
- odgovornost upravljalnih organov,
- obveznosti poročanja,
- uvedba upravnih glob in
- izboljšanje sodelovanja na ravni EU-ja in skupne sposobnosti za pripravo in odzivanje ter vzpostavitev mreže EU-CyCLONe.

2.2.1. Področje uporabe / Povečanje števila sektorjev in drugačna delitev

Direktiva NIS 2 je razširila področje uporabe in povečala število sektorjev, katerih subjekti bodo zavezani spoštovati pravila direktive, da bi zagotovila celovito pokritost sektorjev in storitev, ki so bistvenega pomena za ključne družbene in gospodarske dejavnosti na notranjem trgu EU-ja. Cilj direktive NIS 2 pri tem je bil odpraviti pomanjkljivosti razlikovanja med izvajalci bistvenih storitev in ponudniki digitalnih storitev, saj se je to izkazalo za zastarelo in ni odražalo pomena sektorjev ali storitev za družbene in gospodarske dejavnosti na notranjem trgu EU-ja.[14] Seznam sektorjev, ki bodo podvrženi novim pravilom, se je tako v primerjavi z direktivo NIS bistveno razširil. Prav tako je v direktivi NIS 2 podrobneje opredeljeno, kateri subjekti bodo zavezanci, za katere bodo veljale nove zahteve na področju kibernetske varnosti. Direktiva NIS je obsegala naslednje sektorje: energija (elektrika, nafta, plin), transport (letalski, železniški,

vodni, cestni), bančništvo (kreditne institucije), infrastruktura finančnega trga (mesta trgovanja, centralne nasprotne stranke), zdravstveni sektor (zdravstvene ustanove), oskrba s pitno vodo in njena distribucija (dobava in distribucija pitne vode) in digitalna infrastruktura (internetne izmenjevalne točke, ponudniki sistema imenskih domen (v nadaljevanju: DNS),[15] registri vrhnjih domenskih imen (v nadaljevanju: TLD).[16] Subjekti iz teh sektorjev so se šteli za izvajalce bistvenih storitev, ki so morali sprejeti ukrepe za izboljšanje kibernetske varnosti in poročanje o incidentih. Direktiva NIS 2 ta nabor razširja z dodajanjem novih sektorjev, kot so poštne in kurirske storitve, vesolje, javna uprava in drugi. Na podlagi direktive NIS so bile države članice odgovorne za določitev meril, na podlagi katerih so se šteli subjekti za izvajalce bistvenih storitev. Pri tem so med državami članicami nastale velike razlike, zato direktiva NIS 2 za odpravo teh razlik in zagotovitev pravne varnosti v zvezi z ukrepi kibernetske varnosti za obvladovanje tveganja in obveznosti poročanja za vse ustrezne subjekte določa nova enotna merila, na podlagi katerih bodo subjekti določeni kot bistveni ali pomembni in kot taki zavezani k uporabi pravil direktive NIS 2.[17] Pravila iz direktive NIS 2 bodo obvezna za vse subjekte z več kot 250 zaposlenimi in letnim prometom, ki presega 50 milijonov evrov, ali z letno bilanco stanja, ki presega 43 milijonov evrov, ali obojim. V posebnih okoliščinah in za posebej ogrožene sektorje morajo subjekti spoštovati direktivo NIS 2 ne glede na velikost podjetja, kar med drugim velja za ponudnike javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev ali kadar bi motnje storitve lahko imele pomembne posledice na področju javnega zdravja. Direktiva NIS 2 subjekte razvršča v dve kategoriji – med bistvene in med pomembne subjekte.[18]

Med bistvene subjekte direktiva NIS 2 šteje vse subjekte iz Priloge I, ki presegajo zgornjo mejo za srednja podjetja;[19] ponudnike kvalificiranih storitev zaupanja in registri vrhnjih domenskih imen ter ponudniki storitev DNS, ne glede na njihovo velikost; ponudnike javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ki se štejejo za srednja podjetja; subjekte javne uprave na osrednji

državni ravni, kot jih opredeli država članica v skladu z nacionalnim pravom, ali na regionalni ravni, kot jih opredeli država članica v skladu z nacionalnim pravom, in ki po oceni tveganja opravljajo storitve, katerih motnje bi lahko pomembno vplivale na ključne družbene ali gospodarske dejavnosti; vse druge subjekte vrste iz Priloge I ali II, ki jih država članica prepoznava kot bistvene subjekte. Prav tako se med bistvene subjekte uvrščajo subjekti, ki so v skladu z direktivo CER kritični subjekti in, če se država članica tako odloči, tudi vsi subjekti, ki jih je pred 16. januarjem 2023 določila kot izvajalce bistvenih storitev v skladu z direktivo NIS in nacionalnim pravom. Med pomembne subjekte direktiva NIS 2 uvršča vse druge subjekte iz Prilog I in II, ki se ne štejejo za bistvene subjekte. To so srednje veliki in veliki subjekti, pri katerih potencialna motnja storitev ne bi imela resnih družbenih ali gospodarskih posledic. Čeprav morata obe skupini izpolnjevati enake obveznosti, bodo bistveni subjekti pod strožjim nadzorom in s predvidenimi višjimi sankcijami. Prav tako bodo lahko predmet nadzora *ex ante* in *ex post*, pomembni pa samo *ex post*.

Direktiva NIS 2 se ne bo uporabljala za subjekte, ki izvajajo dejavnosti na področjih obrambe, nacionalne varnosti, javne varnosti in kazenskega pregona. Prav tako so iz področja uporabe izključeni sodstvo, parlamenti in centralne banke. Direktiva NIS 2 se ne bo uporabljala niti za subjekte javne uprave, ki so ustanovljeni skupaj s tretjo državo v skladu z mednarodnim sporazumom, ter diplomatska in konzularna predstavništva držav članic v tretjih državah ali za njihove omrežne in informacijske sisteme, če so ti sistemi v prostorih predstavništva ali če delujejo za uporabnike v tretji državi.[20]

V preglednici (Preglednica 1: Primerjava sektorjev po direktivi NIS in NIS 2) je predstavljena primerjava sektorjev, iz katerih so izhajali zavezanci po direktivi NIS in iz katerih izhajajo zavezanci po direktivi NIS 2, ki je število sektorjev bistveno razširila.

Preglednica 1: *Primerjava sektorjev po direktivi NIS in NIS 2*

Direktiva NIS in direktiva NIS 2	Dodatno direktiva NIS 2
• energija • transport • bančništvo • infrastruktura finančnega trga • zdravstveni sektor • oskrba s pitno vodo in njena distribucija • digitalna infrastruktura	• odpadna voda • upravljanje storitev IKT (med podjetji) • javna uprava • vesolje • poštne in kurirske storitve • ravnanje z odpadki • izdelava, proizvodnja in distribucija kemikalij • pridelava, predelava in distribucija živil • proizvodnja • digitalni ponudniki • raziskave

Vir: *direktiva NIS in direktiva NIS 2.*

V Preglednici 2 (Sektorji, iz katerih izhajajo bistveni in pomembni subjekti po direktivi NIS 2) je prikazana razvrstitev sektorjev na tiste, v katere se uvrščajo bistveni, in tiste, v katere se uvrščajo pomembni subjekti, po direktivi NIS 2.

Preglednica 2: *Sektorji, iz katerih izhajajo bistveni in pomembni subjekti po direktivi NIS 2*

Bistveni subjekti	Pomembni subjekti
• energija • transport • bančništvo • infrastruktura finančnega trga • zdravstveni sektor • oskrba s pitno vodo in njena	• poštne in kurirske storitve • ravnanje z odpadki • izdelava, proizvodnja in distribucija kemikalij • pridelava, predelava in distribucija živil

distribucija • odpadna voda • digitalna infrastruktura • upravljanje storitev IKT (med podjetji) • javna uprava • vesolje	proizvodnja • digitalni ponudniki • raziskave

Vir: *direktiva NIS 2.*

2.2.2. Ukrepi za zagotavljanje kibernetske varnosti

Direktiva NIS 2 uvaja nabor obveznih ukrepov,[21] ki jih bodo morali bistveni in pomembni subjekti sprejeti za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev ter za preprečevanje ali zmanjšanje vpliva incidentov na prejemnike svojih storitev in druge storitve. Ukrepi bodo morali zagotavljati raven varnosti omrežnih in informacijskih sistemov, ki ustreza obstoječim tveganjem, pri čemer bo treba pri ocenjevanju njihove sorazmernosti ustrezno upoštevati več dejavnikov – med drugim stopnjo izpostavljenosti subjekta tveganjem, velikost subjekta, verjetnost pojava incidentov in njihovo resnost, vključno z družbenim in gospodarskim vplivom. Poleg tega bodo morali ukrepi temeljiti na upoštevanju vseh nevarnosti, tako da se zaščitijo omrežni in informacijski sistemi ter njihovo fizično okolje pred incidenti, in vključevati vsaj naslednje:[22]

- politike o analizi tveganja in varnosti informacijskih sistemov;
- obvladovanje incidentov;
- neprekinjeno poslovanje, kot je upravljanje varnostnih kopij in vnovična vzpostavitev delovanja po nepredvidljivih dogodkih, ter obvladovanje kriz;
- varnost dobavne verige, vključno z vidiki, povezanimi z varnostjo, ki se nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev;

- varnost pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov, vključno z obravnavanjem in razkrivanjem ranljivosti;
- politike in postopke za oceno učinkovitosti ukrepov za obvladovanje tveganj za kibernetsko varnost;
- osnovne prakse kibernetske higiene in usposabljanje na področju kibernetske varnosti;
- politike in postopke v zvezi z uporabo kriptografije in po potrebi šifriranjem;
- varnost človeških virov, politike nadzora dostopa in upravljanje sredstev;
- uporabo večfaktorske avtentikacije ali rešitev neprekinjene avtentikacije, varovanih glasovnih, video in besedilnih komunikacij ter varnih sistemov za komuniciranje v sili znotraj subjekta, kadar je to primerno.

Med naštetimi ukrepi je bil več pozornosti deležen nov ukrep varnosti dobavne verige, ki ga predhodnica, direktiva NIS, ni posebej obravnavala. Glede na to, da se je v zadnjih letih število napadov z izsiljevalskim programjem v EU-ju eksponentno povečalo, prav tako se je povečalo število napadov na dobavne verige,[23] so tarča napadov na dobavne verige predvsem mala in srednja podjetja, in sicer zaradi manj strogih ukrepov za obvladovanje tveganj na področju kibernetske varnosti in obvladovanja incidentov ter omejenih sredstev za kibernetsko varnost. Pri tem je treba poudariti, da imajo tovrstni napadi na dobavne verige lahko tudi kaskadne učinke za večje napade na subjekte, katerim mala in srednja podjetja dobavljajo blago, in tako napad ne vpliva zgolj nanje.[24] Podobno tudi ENISA ocenjuje, da se bodo napadi na dobavne verige bistveno povečali – v svojem poročilu o grožnjah v EU-ju iz oktobra 2021 je ocenila, da se bodo v letu 2021 napadi na dobavne verige povečali za kar štirikrat v primerjavi z letom 2020 (ENISA, 2021). Direktiva NIS 2 je zaradi krepitve varnosti dobavne verige kot eno izmed nalog skupine za sodelovanje določila izvajanje usklajenih ocen tveganja za varnost kritične dobavne verige, ki jih izvaja v sodelovanju z Evropsko komisijo in agencijo ENISA.[25]

Novost direktive NIS 2, ki se nanaša na ukrepe za zagotavljanje

kibernetske varnosti, je tudi napotilo na uporabo vseh inovativnih tehnologij, vključno z umetno inteligenco, ki bi lahko pripomogle k izboljšanju odkrivanja in preprečevanja kibernetskih napadov. S tem bi dosegli učinkovitejšo in uspešnejšo razporeditev virov za boj proti tem grožnjam. Kot izhaja iz preambule, bi morale države članice spodbujati dejavnosti na področju raziskav in razvoja, ki bi olajšale uporabo inovativnih tehnologij, ki se nanašajo na avtomatizirana ali polavtomatizirana orodja za kibernetsko varnost, že v svojih nacionalnih strategijah za kibernetsko varnost. Direktiva NIS 2 uporabo umetne inteligence priporoči tudi bistvenim in pomembnim subjektom, ki bi morali sprejeti širok nabor osnovnih praks računalniške higiene (načelo popolnega nezaupanja, posodabljanje programske opreme, konfiguracija naprav, segmentacija omrežja, upravljanje identitete in dostopa ter ozaveščanje uporabnikov, organiziranje usposabljanj in ozaveščanja svojega osebja v zvezi s kibernetskimi grožnjami podjetjem, lažnim predstavljanjem in tehnikami socialnega inženiringa) in si po oceni lastnih zmogljivosti na področju kibernetske varnosti prizadevati tudi za uporabo umetne inteligence ali sistemov strojnega učenja za krepitev svojih zmogljivosti ter večjo varnost omrežnih in informacijskih sistemov.[27]

2.2.3. Odgovornost upravljalnih organov

Pomembna novost direktive NIS 2 je vzpostavitev odgovornosti upravljalnih organov. Že prej je stroka poudarjala potrebo po večjem zavedanju pomena kibernetske varnosti pri vodilnih kadrih, a je bil v praksi poseben poudarek in upoštevanje kibernetske varnosti pri načrtovanju poslovanja veliko bolj izjema kot pravilo. Države članice bodo morale pri prenosu direktive NIS 2 zagotoviti, da bodo upravljalni organi bistvenih in pomembnih subjektov: a) odobrili ukrepe za obvladovanje tveganj za kibernetsko varnost, ki jih sprejmejo ti subjekti, b) nadzorovali njihovo izvajanje in c) odgovarjali za kršitve določil v zvezi z ukrepi za obvladovanje kibernetske varnosti.[28] Člani upravljalnega organa bistvenih in pomembnih subjektov se bodo morali usposabljati na področju kibernetske varnosti. Prav tako naj bistveni in pomembni subjekti podobno usposabljanje redno

ponujajo svojim zaposlenim in jih s tem usposobijo za prepoznavanje in ocenjevanje tveganj kibernetske varnosti ter njihovega vpliva na storitve, ki jih opravlja subjekt, pri katerem so zaposleni.[29] V zvezi s temi usposabljanji ni jasno, kakšna bi morala biti vsebina, niti kako bodo subjekti dokazali, da so bila taka usposabljanja izvedena. Vendar obstajajo številni načini za izobraževanje zaposlenih na vseh ravneh o obvladovanju tveganj kibernetske varnosti, pa tudi o najbolj temeljnih dobrih praksah kibernetske higiene. Praktična posledica te zahteve je, da so posamezniki v teh upravnih organih bistvenih in pomembnih subjektov, ki spadajo v področje uporabe direktive NIS 2, lahko osebno odgovorni in predmet prisilnih ukrepov, če ti subjekti kršijo svoje obveznosti v skladu z NIS 2. S prenašanjem odgovornosti za obvladovanje tveganja kibernetske varnosti na vodstveno raven teh subjektov se kaže težnja po zagotavljanju, da je upravljanje tveganja kibernetske varnosti odgovornost višjega vodstva. Čeprav besedilo direktive NIS 2 ne opredeljuje, kdo je upravljalni organ, naj bi te funkcije predstavljale vse osebe, ki opravljajo poslovodne naloge na ravni glavnega izvršnega direktorja ali pravnega zastopnika. Ta vidik bo sčasoma natančneje opredeljen s prenosom določil direktive NIS 2 v nacionalno zakonodajo držav članic (Giannakoulias, 2023).

2.2.4. Obveznosti poročanja

Direktiva NIS 2 uvaja dvostopenjski pristop k poročanju o incidentih.[30] Prizadeti subjekti bodo morali o varnostnih incidentih v 24 urah ter enem mesecu poročati o incidentu in vzroku ter vpeljanih in načrtovanih ukrepih za odpravljanje tveganj. V 24 urah po seznanitvi z incidentom bodo skupini CSIRT ali pristojnemu organu predložili zgodnje opozorilo, iz katerega bo razvidno, ali je bil pomemben incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem ali pa bi lahko imel čezmejni vpliv. V 72 urah po seznanitvi s pomembnim incidentom sledi njegova priglasitev, s katero se posodobijo priglašene informacije ter navede začetna ocena pomembnega incidenta, vključno z njegovo resnostjo in vplivom ter morebitnimi kazalniki ogroženosti.

Končno poročilo bo moral prizadeti subjekt predložiti najkasneje v enem mesecu po predložitvi priglasitve incidenta. Končno poročilo mora vsebovati:

- podroben opis incidenta, vključno z njegovo resnostjo in vplivom;
- vrsto grožnje ali temeljnega vzroka, ki je verjetno sprožil incident;
- izvedene blažilne ukrepe in ukrepe v teku;
- po potrebi čezmejni vpliv incidenta.

Pri incidentu, ki je ob predložitvi končnega poročila še vedno v teku, naj bi prizadeti subjekt v enem mesecu predložil poročilo o napredku, končno poročilo pa najpozneje en mesec po razrešitvi incidenta.

Na zahtevo skupine CSIRT ali pristojnega organa mora prizadeti subjekt pripraviti vmesno poročilo.

2.2.5. Uvedba upravnih glob

Države članice so bile v preteklosti na splošno zadržane pri uvajanju sankcij za subjekte, ki niso uvedli varnostnih ukrepov ali prijavljali incidentov. Ker to lahko negativno vpliva na kibernetsko odpornost subjektov, je direktiva NIS 2 podobno kot Splošna uredba o varstvu podatkov za učinkovito izvrševanje njenih določb vzpostavila skladen okvir za sankcije po vsem EU-ju. Direktiva NIS 2 določa minimalni seznam upravnih sankcij za kršitev obveznosti upravljanja tveganj kibernetske varnosti in poročanja. Sankcije vključujejo zavezujoča navodila nalog za izvajanje priporočil varnostne revizije, ukaz za uskladitev varnostnih ukrepov z zahtevami direktive NIS 2 in upravne globe (Evropska komisija, 2023b). Upravne globe se razlikujejo glede na vrsto subjektov, in sicer se za bistvene subjekte zahteva najvišja raven upravnih glob 10.000.000 EUR oziroma 2 odstotka celotnega svetovnega letnega prometa v prejšnjem poslovnem letu (izmed njiju se izbere znesek, ki je višji) ter za pomembne subjekte najvišja raven upravnih glob v višini 7.000.000 EUR oziroma 1,4 odstotka celotnega svetovnega letnega prometa v prejšnjem poslovnem letu (tudi izmed teh dveh se izbere višji

znesek).[31] Ne glede na tako višino upravnih glob je direktiva NIS 2 predvidela še dodatno varovalko za zagotavljanje skladnosti, in sicer državam članicam omogoča, da v skladu s predhodno odločitvijo pristojnega organa določijo pooblastilo za naložitev periodičnih denarnih kazni, da se bistveni ali pomembni subjekt prisili k prenehanju kršitev.[32]

2.2.6. Izboljšanje sodelovanja na ravni EU-ja in skupne sposobnosti za pripravo in odzivanje ter vzpostavitev mreže EU-CyCLONe

Kibernetske grožnje so vse bolj zapletene in izpopolnjene, zato so dobri ukrepi za njihovo odkrivanje in preprečevanje odvisni predvsem od redne izmenjave obveščevalnih podatkov o grožnjah in ranljivosti med subjekti. Hitra in kakovostna izmenjava informacij lahko pripomore k večji ozaveščenosti o kibernetskih grožnjah med subjekti in s tem krepi sposobnost subjektov, da preprečijo, da bi iz groženj nastali incidenti. Izmenjava informacij omogoča, da subjekti bolje omejijo učinke incidentov in si hitreje opomorejo.[33] Direktiva NIS je vzpostavila skupino za sodelovanje[34] in mrežo skupin CSIRT,[35] ki ju je prevzela tudi direktiva NIS 2, poleg tega pa je vzpostavila še novo Evropsko organizacijsko mrežo za povezovanje v kibernetski krizi (v nadaljevanju: mrežo EU-CyCLONe).

Mreža EU-CyCLONe, ki je velika novost direktive NIS 2, je mreža za povezovanje v kibernetski krizi. Njen namen je podpora usklajenemu obvladovanju kibernetskih incidentov velikih razsežnosti in kriz na operativni ravni ter za zagotovitev redne izmenjave relevantnih informacij med državami članicami in institucijami, organi, uradi in agencijami EU-ja. Sestavljajo jo predstavniki organov držav članic za obvladovanje kibernetskih kriz. Če morebitni ali potekajoči kibernetski incidenti velikih razsežnosti pomembno vplivajo ali bi lahko pomembno vplivali na storitve in dejavnosti, ki spadajo na področje uporabe direktive NIS 2, jo sestavljajo tudi predstavniki Evropske komisije. Evropska komisija sicer sodeluje pri aktivnostih mreže EU-CyCLONe zgolj kot opazovalka. Ob kibernetskem incidentu

velikih razsežnosti ali krizi na ravni EU-ja je nujno usklajeno delovanje, s katerim se zagotovi hiter in učinkovit odziv zaradi velike medsebojne odvisnosti sektorjev in držav članic. Mreža EU-CyCLONe naj bi ob kibernetskih incidentih velikih razsežnosti in kriz delovala kot posrednik med strokovno in politično ravnjo, tako da bi pomagala krepiti sodelovanje na operativni ravni in zagotavljati podporo pri sprejemanju odločitev na politični ravni.[36]

3. AKT EU O KIBERNETSKI SOLIDARNOSTI

Kmalu po začetku veljavnosti novosprejete direktive NIS 2 je Evropska komisija nadaljevala aktivnosti na področju kibernetske varnosti in aprila 2023 predlagala Akt EU o kibernetski solidarnosti, s katerim želi doseči izboljšanje pripravljenosti, odkrivanja in odzivanja na kibernetske incidente v EU-ju. Akt EU o kibernetski solidarnosti prinaša tri ključne rešitve, s katerimi želi EU okrepiti zmogljivosti za odkrivanje in odzivanje na pomembne in obsežne kibernetske groženje in napade. Prva rešitev je vzpostavitev **Evropskega ščita kibernetske varnosti**, ki ga bodo sestavljali medsebojno povezani centri za varnostne operacije (Evropska komisija, 2023a). Naloge Evropskega ščita kibernetske varnosti bodo:[30]

združevanje in izmenjava podatkov o kibernetskih grožnjah in incidentih iz različnih virov prek čezmejnih varnostno operativnih centrov;

ustvarjanje visokokakovostnih, uporabnih informacij in obveščevalnih podatkov o kibernetskih grožnjah, ki jih bodo pridobili z najsodobnejšimi orodji, zlasti umetne inteligence in tehnologij za analizo podatkov;

prispevanje k boljši zaščiti in odzivu na kibernetske grožnje;

prispevanje k hitrejšemu odkrivanju kibernetskih groženj in boljšemu razumevanju stanja kibernetske varnosti v EU-ju;

zagotavljanje storitev in dejavnosti za skupnost kibernetske varnosti v EU-ju, vključno s prispevanjem k razvoju napredne

umetne inteligence in orodij za analizo podatkov.

Naslednja rešitev, ki jo Akt EU o kibernetski solidarnosti ureja v 3. poglavju predloga, je **mehanizem za izredne kibernetske grožnje**, ki bo zagotovil izboljšanje pripravljenosti in odzivanja na kibernetske incidente:

- z ukrepi za pripravljenost – vključno z usklajenim testiranjem pripravljenosti subjektov, ki delujejo v zelo kritičnih oziroma ključnih sektorjih po vsem EU-ju, kot so finance, energetika, zdravstvo in drugi sektorji, zaradi katerih bi bili ob pomanjkljivostih lahko bolj izpostavljeni kibernetskim grožnjam; nabor sektorjev, ki jih bo treba testirati, bo temeljil na skupni oceni tveganja na ravni EU-ja;
- z vzpostavitvijo rezerve EU-ja za kibernetsko varnost – v okviru te bi na zahtevo držav članic ali institucij EU-ja potekal odziv in takojšnje okrevanje po pomembnih in obsežnih kibernetskih incidentih; te ukrepe bi zagotovili zaupanja vredni ponudniki, ki sodelujejo v rezervi EU-ja za kibernetsko varnost;
- ukrepi medsebojne pomoči – te vključujejo zagotavljanje pomoči nacionalnih organov ene države članice drugi državi članici v skladu z direktivo NIS 2, ki določa naloge skupin CSIRT, med katere spada tudi sodelovanje v mreži skupin CSIRT, in zagotavljanje medsebojne pomoči v skladu z zmožnostmi in pristojnostmi drugih članic mreže skupin CSIRT na njihovo zahtevo.

Tretja rešitev Akta EU o kibernetski solidarnosti je vzpostavitev **mehanizma za pregled kibernetskih incidentov** za njihovo oceno in pregled. Po tem mehanizmu bo ENISA zadolžena, da bo na zahtevo Evropske komisije ali nacionalnih organov opravila pregled posebno pomembnega ali obsežnega kibernetskega incidenta. Na podlagi pregleda bo pripravila poročilo, v katerem bodo pridobljene izkušnje in morebitna priporočila za izboljšanje kibernetskega odziva EU-ja.

3.1. Financiranje

Evropski ščit kibernetske varnosti in mehanizem za izredne

razmere na področju kibernetske varnosti bosta podprta s financiranjem v okviru strateškega cilja »kibernetska varnost« v programu Digitalna Evropa oziroma DEP,[38] ki je del večletnega finančnega okvira EU 2021–2027, ustanovljenega z Uredbo o vzpostavitvi programa Digitalna Evropa.[39] Proračun vključuje povečanje za 100 milijonov EUR (prerazporeditev iz drugih strateških ciljev programa), kar pomeni, da bo novi skupni znesek, na voljo za ukrepe na področju kibernetske varnosti, 842,8 milijona EUR, skupaj s prispevki držav članic pa bi bil skupni proračun lahko tudi 1,109 milijarde EUR (Evropska komisija, 2023).

4. ZAKLJUČEK

Evropska unija se je v zadnjih letih soočila s številnimi izzivi, ki so pomembno vplivali na obravnavo in razumevanje pomena varnega in odpornega kibernetskega prostora. Če pustimo ob strani stalno naraščajoč trend kibernetskih napadov, ki ga redno potrjuje tudi ENISA v svojih poročilih o grožnjah, so se EU in države članice najprej soočile s pandemijo covida 19 in nato še z invazijo Rusije v Ukrajini, ki sta vsaka na svoj način pomembno pripomogli k zavedanju o kibernetskih nevarnostih ter pomenu kibernetske varnosti in odpornosti EU-ja in držav članic za nemoteno delovanje notranjega trga in družbe. Direktiva NIS 2 je, kot smo že poudarili, zasnovana velikopotezno, saj poskuša pravočasno zajeti in vključiti vse izzive, ki so se v zadnjem obdobju pojavili v EU-ju. Kljub temu se ob tem postavljajo tudi vprašanja, ali in kako bodo države članice na vse te izzive odgovorile, predvsem glede izpeljave ukrepov v praksi. Prenos direktive NIS je imel pomanjkljivost v tem, da so jo države članice prenesle na zelo različne načine, kar je povzročalo nevšečnosti, stroške in z vidika kibernetske varnosti predvsem ranljivosti in nezadostno raven kibernetske varnosti na ravni EU-ja in držav članic. Direktiva NIS 2 je vse te ugotovljene pomanjkljivosti obravnavala, vendar številna vprašanja ostajajo odprta. Najprej se bomo spraševali tri stvari, koliko zavezancev bo prinesla nova direktiva NIS 2, koliko kadrov bo potrebnih za učinkovito načrtovanje, izvajanje in nadziranje vseh ukrepov ter ne nazadnje tudi koliko finančnih sredstev bo potrebnih za

zagotovitev potrebnih virov. V zvezi s francoskim nacionalnim ozemljem je Guillaume Poupard, generalni direktor francoske agencije za kibernetsko varnost – ANSSI,[40] junija 2022 izjavil, da bo direktiva NIS 2 znatno razširila svoje področje uporabe, kar naj bi pomenilo desetkratno povečanje števila deležnikov, razvrščenih kot izvajalcev bistvenih storitev (Nicaise, 2022). Prav tako se je treba zavedati, da institucije na ravni EU-ja, države članice, podjetja in drugi že leta opozarjajo na pomanjkanje strokovnjakov. Evropsko računsko sodišče je leta 2019 opozorilo, da se ves svet srečuje z vedno večjim primanjkljajem znanj na področju kibernetske varnosti, vrzel v delovni sili pa se je od leta 2015 povečala za 20 odstotkov. Ob tem poudarja, da tradicionalni načini zaposlovanja ne dohajajo povpraševanja, vključno z vodstvenimi in interdisciplinarnimi položaji, na univerzah pa je na netehničnih programih premalo predmetov, povezanih s kibernetsko varnostjo (Evropsko računsko sodišče, 2019). Vrzel v delovni sili se je tudi v kasnejših letih le še povečevala, saj navsezadnje strokovnjaki kibernetske varnosti izhajajo iz istega bazena kadrov kot drugi strokovnjaki na področju informacijske tehnologije, ki jih v svetu prav tako primanjkuje. Dodatne zahteve in potrebe po zagotavljanju kibernetske varnosti so z vidika kibernetske odpornosti seveda dobrodošle, vendarle pa se postavlja vprašanje, kje bodo subjekti pridobili vire za uspešno in učinkovito zagotavljanje vseh zahtev.

Ne glede na navedene pomisleke je treba poudariti, da je zrelost EU-ja na področju kibernetske varnosti neprimerno večja kot ob sprejemu prve direktive NIS. V tem obdobju je bila sprejeta nova strategija kibernetske varnosti, agencija ENISA se je preimenovala ter dobila več pristojnosti in sredstev, poleg tega so bili posodobljeni številni drugi akti s širšega področja kibernetske varnosti, predvsem pa je EU zagotovil več sredstev za izvajanje programov in projektov za izboljšanje kibernetske varnosti. Te aktivnosti EU nadaljuje tudi v letu 2023, ko je aprila Evropska komisija predlagala Akt EU o kibernetski solidarnosti. Glede na to, da gre za področje, ki se hitro spreminja, bomo uspešnost novih pravil za zagotavljanje kibernetske varnosti na ravni EU-ja in držav članic glede na roke za prenos določb direktive NIS 2 v nacionalno zakonodajo v celoti in objektivneje lahko ocenili šele čez nekaj let.

5. LITERATURA IN VIRI

1. Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji. *Uradni list Evropske unije* L 194/1.
2. Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2). *Uradni list Evropske unije* L 333/80.
3. Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES. *Uradni list Evropske unije* L 333/164.
4. ENISA. (2021). *ENISA Threat Landscape*. Najdeno 5. junija 2023 **na spletnem naslovu**.
5. Evropska komisija. (2020). *Proposal for directive on measures for high common level of cybersecurity across the Union*. Najdeno 5. junija 2023 na spletnem naslovu: **Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future (europa.eu)**.
6. Evropska komisija. (2023a). *Akt EU o kibernetski solidarnosti*. Najdeno 5. maja 2023 **na spletnem naslovu**.
7. Evropska komisija. (2023b). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Najdeno 5. junija 2023 **na spletnem naslovu**.
8. Evropska komisija. (2020). *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*. Najdeno 5. junija 2023 **na spletnem naslovu**.
9. Evropska komisija. (2023). *Proposal for a Regulation of the European parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents*. Strasbourg, 18. 4. 2023 COM(2023) 209 final.

10. Evropski parlament. (2023). *The NIS2 Directive - A high common level of cybersecurity in the EU. EPRS – European Parliament Research Service*. Najdeno 5. junija 2023 **na spletnem naslovu**.
11. Evropsko računsko sodišče. (2019). *Izzivi za uspešno politiko EU za kibernetsko varnost*. Informativni dokument. Marec 2019.
12. Giannakoulias, A. (2023). *NIS 2 Directive: implications for system and infrastructure security* (Master's thesis, Πανεπιστήμιο Πειραιώς).
13. Nicaise, V. (2022). *EU NIS2 Directive: what's changing?* Najdeno 5. junija 2023 **na spletnem naslovu**.
14. Uredba (EU) 2021/694 Evropskega parlamenta in Sveta z dne 29. aprila 2021 o vzpostavitvi programa Digitalna Evropa in razveljavitvi Sklepa (EU) 2015/2240. *Uradni list Evropske unije* L 166/1.
15. Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011. *Uradni list Evropske unije* L 333/1.

Opombe

* Jaka Kosmač, univ. dipl. prav., državni revizor, Računsko sodišče Republike Slovenije, jaka.kosmac@rs-rs.si, jakakosmach@gmail.com.

1. Direktiva (EU) 2022/2555 Evropskega parlamenta in sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148.
2. Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.
3. **Spletni naslov**
4. Preambula NIS 2, točka 4.
5. Izvajalec bistvenih storitev pomeni javni ali zasebni subjekt, ki spada med vrste iz Priloge II direktive NIS (energija, promet, bančništvo, infrastruktura finančnega trga, zdravstveni sektor, oskrba s pitno vodo in njena distribucija, digitalna infrastruktura) in izpolnjuje merila, določena v členu 5(2) direktive NIS (subjekt zagotavlja storitev, ki je bistvena za ohranitev ključnih družbenih in/ali gospodarskih dejavnosti;

zagotavljanje te storitve je odvisno od omrežij in informacijskih sistemov; incident bi imel pomemben negativen vpliv na zagotavljanje te storitve).

6. Ponudnik digitalnih storitev pomeni vsako pravno osebo, ki zagotavlja digitalno storitev.

7. Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES.

8. Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) 909/2014 in (EU) 2016/1011.

9. Proposal for a Regulation of the European Parliament and of the Council laying down the measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. Strasbourg, 18. 4. 2023 COM(2023) 209 final.

10. Države članice morajo na primer v skladu s 3. členom direktive NIS 2 do 17. aprila 2025 oblikovati seznam bistvenih in pomembnih subjektov ter subjektov, ki opravljajo storitve registracije domenskih imen.

11. 23. člen direktive NIS.

12. Preambula direktive NIS 2, točka 2.

13. Preambula direktive NIS 2, točka 5.

14. Preambula direktiva NIS 2, točka 6.

15. Angl. Domain name system – DNS.

16. Angl. *Top-level domain* – TLD.

17. Preambula direktive NIS 2, točka 7.

18. Direktiva NIS 2, člen 3.

19. Zgornja meja za srednja podjetja je določena v členu 2(1) Priloge k Priporočilu 2003/361/ES.

20. Preambula direktiva NIS 2, točka 8.

21. Drugi odstavek 21. člena.

22. Direktiva NIS 2, 21. člen.

23. Preambula direktive NIS 2, točka 54.

24. Preambula direktiva NIS 2, točka 56.

25. Direktiva NIS 2, 22. člen.

26. Preambula direktive NIS 2, točka 51.

27. Preambula direktive NIS 2, točka 89.

28. Direktiva NIS 2, 20. člen.

29. Direktiva NIS 2, 20. člen.

30. Direktiva NIS 2, 23. člen.

31. Direktiva NIS 2, 34. člen.

32. Direktiva NIS 2, 34. člen.

33. Preambula NIS 2, točka 119.

34. Namen skupine za sodelovanje je podpiranje in olajšanje

strateškega sodelovanja ter izmenjave informacij med državami članicami, pa tudi za krepitev zaupanja. Skupino za sodelovanje sestavljajo predstavniki držav članic, Evropske komisije in ENISA. Skupina svoje naloge opravlja na podlagi dveletnih delovnih programov.

35. Namen mreže skupin CSIRT je krepitev zaupanja ter spodbujanje hitrega in učinkovitega operativnega sodelovanja med državami članicami. Sestavljajo jo predstavniki skupin CSIRT in skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije Unije (CERT-EU). Države članice v skladu z 10. členom direktive NIS 2 določijo ali vzpostavijo eno ali več skupin CSIRT, lahko se imenujejo ali ustanovijo tudi znotraj pristojnega organa. Izpolnjevati morajo zahteve iz prvega odstavka 11. člena direktive NIS 2 ter pokrivati vsaj sektorje, podsektorje in vrste subjektov iz prilog I in II. Skupine CSIRT morajo biti tudi pristojne za obvladovanje incidentov v skladu z natančno določenim postopkom.
36. Preambula NIS 2, točka 71.
37. Akt EU o kibernetski solidarnosti – predlog, 3. člen.
38. Angl. Digital Europe Programme.
39. Uredba (EU) 2021/694 Evropskega parlamenta in Sveta z dne 29. aprila 2021 o vzpostavitvi programa Digitalna Evropa in razveljavitvi Sklepa (EU) 2015/2240. *Uradni list EU* L166/1.
40. Fr. *Agence nationale de la sécurité des systèmes d'information*.

Alvar Nõuakas*

EUROSAI IT working group – the power of cooperation

Delovna skupina EUROSAI IT – moč sodelovanja

POVZETEK ● *V prispevku je opisano delo delovne skupine*

za informacijsko tehnologijo pri organizaciji EUROSAI (v nadaljevanju: EUROSAI ITWG) med digitalno revolucijo in z njo povezanimi spremembami. Revizorji informacijskih sistemov se srečujemo z veliki izzivi ter pri svojem delu nenehno razvijamo nova orodja, ki nam omogočajo učinkovito in uspešno izvajanje postavljenih ciljev. V prispevku so povzeti cilji vrhovne revizijske ustanove oziroma nacionalnih revizijskih ustanov – računskih sodišč (v nadaljevanju: NAO), na kratko pa je predstavljeno tudi povezovanje teh ustanov v Evropi in po svetu (INTOSAI). V nadaljevanju so navedeni projekti in izobraževanja EUROSAI ITWG ter delo revizorjev informacijskih sistemov v vrhovni revizijski ustanovi v Estoniji.
Ključne besede ● *revizijske ustanove, EUROSAI, delovna skupina za informacijsko tehnologijo – ITWG, sodelovanje*
SUMMARY ● *The paper describes the work of the working group for information technology at EUROSAI (hereinafter EUROSAI ITWG) during the digital revolution and related changes. As auditors of information systems, we face great challenges, in our work we constantly develop new tools that allow us to effectively and successfully implement the set goals. The paper briefly presents the goals of the supreme audit institution of national audit organizations – audit courts (hereinafter referred to as the NAO), their integration in Europe and the world (INTOSAI). In continuation, EUROSAI ITWG projects and trainings, and the work carried out by IT auditors at NAO in Estonia are presented.*
Key words ● *Supreme Audit Institution, EUROSAI, information technology working group – ITWG, cooperation*

JEL: K 24

1. INTRODUCTION

The Supreme Audit Institution[1] (hereafter: SAI), in some countries titled National Audit Organizations (hereafter: NAO), is an independent institution in almost every country acting in the interests of the country's taxpayers. Its function is to investigate and report how the government has spent the taxpayers' money.

The European SAIs are combined in EUROSAI , which is one of the Regional Organisations of the International Organisation of Supreme Audit Institutions (INTOSAI). EUROSAI was established in 1990 by 30 members (the SAIs of 29 European States and the European Court of Auditors[3]). The current membership amounts to 51. The main objectives of EUTOSAI are to:

- Promote professional cooperation among SAI members,
- Encourage the exchange of information and documentation,
- Advance the study of public sector audit,
- Work towards the harmonisation of terminology in the field of public audit, among others (EUROSAI, w.d.)

The EUROSAI as an European Regional Group organization of INTOSAI, which groups together SAIs of 195 Full Members, 5 Associated Members and 1 affiliate Member, and is listed as a support Organisation of the United Nations. Other Regional Groups within INTOSAI are OLACEFS, AFROSAI, ARABOSAI, ASOSAI, PASAI and CAROSAI.

Within EUROSAI, there are different working groups: WGEA - Working Group on Environmental Auditing, WGAFADC - Working Group on the Audit of Funds Allocated to Disasters and Catastrophes, ITWG Working Group on Information Technologies and task forces, like **EUROSAI Task Force on Municipality Audit**. The EUROSAI ITWG was created at the 5th EUROSAI Congress held in Russia in 2002.

The EUROSAI ITWG focuses on supporting the audit process. The Group's priority is substantive and practical work to support public sector auditors in their daily operations. The Group aims at sharing, synthesizing, and developing common good IT audit and IT-use practices in the EUROSAI community (EUROSAI ITWG, w.d.).

NAO Estonia took over the leading of EUROSAI ITWG from Poland in June 2020, currently there are 43 members of ITWG.

2. THE POWER OF COOPERATION

Out of all public organizations sailing through digital revolution, supreme audit institutions probably find themselves in the most challenging position, attacked by whirlwinds from different angles. Expectation from the client – the citizen – to keep an eye on the misuse of public funds in every sector, clashes with the reality of limited capacity. Inability to limit the number of clients or manage their expectations through clever contracts distinguishes the role of the supreme audit institution from private companies. The scope of management – including whole government – distinguishes them from public sector internal auditors.

Developing and implementing constantly advancing tools for fulfilling their objective is the routine task of every public entity; but exercising the mandate to check other entities in their regularity, efficiency and effectiveness to utilize technology – this is something only supreme audit institutions are facing. And on top of all this – best practice should be shown by their own good example.

The core purpose of a supreme audit institution, as stated in the Lima Declaration, is by the means of an audit to reveal deviations from accepted standards and violations of the principles of legality, economy, efficiency and effectiveness of financial management. Public management has implemented information systems for decades and this has directed supreme audit institutions to develop their inner IT auditing capacity. The use of these systems for different decisions and government processes has broadened significantly, and the velocity of developments has risen considerably. Together with updating standards, this trend has forced supreme audit institutions to adjust their risk assessment, selection and pipeline of deliverables – audits, quick reports, articles, blog posts etc.

Searching for ways to follow the rapidly moving target of technological advancement and focussing only on relevant aspects, supreme audit institutions are gradually elaborating their pre-defined identity, negotiating their mandate and resources, balancing what they have been given and what can be achieved with it.

All this considered, supreme audit institutions do not participate in international cooperation out of courtesy, they need international cooperation – to discuss common problems and the way of addressing them from their own unique perspective. In 2002, 16 EUROSAI members formed an IT working group, “in order to further the institutional sharing of expertise and experiences between the SAIs of the European region, and to encourage the implementation of joint activities in the field of information technology”. Today, the number of members has risen to 43 – thus including most audit institutions in Europe.

2.1. Projects

While the members are very different in terms of their type, mandate, size and capacity, the common values and challenges unite them in search for smart solutions with modern tools. From its establishment back in 2002, much has changed, especially in the field of information technology – naturally, auditing standards and methods have evolved accordingly. Therefore, IT working group has followed the process, and through sequential working plans launched and delivered multiple tools in cooperation with several institutions. Namely, capable field experts have been participating in creating intelligent database for exchanging information about finalized audits and risks (CUBE), online application for planning and implementing IT audits (AITAM) in line with IT audit manual created by INTOSAI IT working group, analysing the maturity of IT and IT audit in the institution based on COBIT standard (ITSA & ITASA).

Although these projects are tailored for supreme audit institutions and have innovative valuable features integrated to use for everyday public sector auditing work, they have the potential to affect the wider public auditing community.

2.2. Education

After Estonia took over the chair in 2020, ITWG has explicitly

focused on enhancing auditor's individual knowledge base and practical skills in auditing IT related topics. Based on focus group discussions between auditors and academia, first interactive training programme consisting of 7 modules is being developed, targeted at teaching non-IT auditors the fundamentals of IT auditing in MOOC format (Research and Training Hub, see training.eurosai-it.org). This programme is a good example of institutional cooperation between EUROSAI members, gradually reaching even beyond its borders. For example, the module to be launched in September 2023 called "Information security, protection of personal data and business continuity" is developed by the supreme audit office of Germany (Bundesrechnungshof) and includes practical audit cases from Australia, Denmark, Lithuania, Malta, USA etc.

Training programme is free for all auditors and possible to cover at any time suitable for the learner. This has enabled about 2000 auditors all over the world to obtain knowledge from the four modules published so far: "IT Audit in a Supreme Audit Institution", "IT Systems, Software and Data", "IT Governance" and "Procurement and Outsourcing".

Training non-IT auditors in basic IT auditing has been selected as pilot initiative under the ITWG Research and Training Hub, because most auditors face IT systems in their work and should verify the confidentiality, integrity and availability of data they are processing in their respective audits in specific domains. The role of auditors is also gradually changing with the pace of technological advancement, as is the case with supreme audit institutions. Enhancing the capacity of their employees is the task of every organisation, but international cooperation between audit institutions enables sharing experience in timely manner utilizing recent development in adult training methodology.

Raising awareness of trends in auditing and impact of utilizing technology in state governance is something the working group is addressing in its meetings. In response to the constant changes in the auditing environment, the tradition of two annual thematic seminars has been established together with more informal experience-sharing sessions between them. The idea behind

holding thematic meetings is not merely to exchange audit experience – although this also receives sufficient attention – but rather to analyse the wider picture that supreme audit institutions are dwelling in, and what is the potential intervention vector. Just an example – in April 2022, a seminar „Water behind the dam – challenges regarding data flow for a SAI“ discussed legal and technical obstacles auditing institutions are facing when connecting to data sources. There are number of issues to consider – implementation of GDPR, mandate and technology for using data in data warehouse, remarkable but frequently unused potential in cooperation with academia etc.

Considering the above, one may call EUROSAI IT working group an “exploration hub”, as it fosters creative and forward-looking vision that potentially has worldwide application despite technological or legal obstacles. Going even further, this platform for cooperation is indirectly helping to re-conceptualize auditing in the changing environment and this is also the motivation of one of the smallest supreme audit institutions – the National Audit Office of Estonia (NAOE) – to lead the working group.

3. THE PERSPECTIVE OF NAO ESTONIA

In Estonia, we are facing complicated and borderline challenges the same way they have emerged on the agenda for other institutions. Being among the top performers according to the E-Government Development Index and open to experimenting with government services, like step-by-step application of proactive services, raises the number of potential risks significantly in Estonia. Some might be easy to predict and mitigate, others emerge unexpectedly during the implementation phase. It is valuable for any auditor to learn from ecosystems, where similar processes have been evolving longer and specific flaws detected. Moreover, in Europe many developments originate from the directives or initiatives launched by the European Union – for example, auditing or monitoring the ongoing process of electronic identification. Addressing the topic in a joint format, for example parallel audit, enables supreme audit institutions to formalize measurable criteria that can be later used for benchmarking and assessing the adherence to the timeframe.

Similarly, as other institutions, the NAOE has experienced confusion among auditees when accessing and processing potentially sensitive data from various sources. It raises the issue of independence of a constitutional audit institution to determine the proportional usage of auditing methods for implementing its work plan. There is the grey area in the relationship between national statistics agency and audit institution regarding the usage of granular data for statistical or scientific purposes. And when an audit institution is considering robotic process automation (RPA) for government data flow and creating ways for continuous auditing, there is also an interpretation on restricted mandate for a single audit. These and other issues are feasible to tackle in a joint format, creating common understanding on legal and technological considerations according to the overall objective of a supreme audit institution.

4. CONCLUSION

To sum up – international cooperation is the way to enhance supreme audit institutions, to harmonize and train their voice and then – to make this voice heard. Unique position in the society with limited resources does not mean an institution is left alone to invent a plan for its intervention. By learning from others, articulating the challenges with others, a supreme audit institution generates more value for the society and at the same time – rewrites its own mandate.

5. REFERENCES

1. EUROSAI, **EUROSAI at a Glance**, retrieved on: August, 21, 2023.
2. EUROSAI ITWG, **EUROSAI IT Working Group**, Activities, retrieved on: August, 21, 2023. **Lima Declaration**.

Opombe

* Alvar Nõuakas, Head of EUROSAI IT Working Group, NAO Estonia – Rigikontroll, Kiriku 2/4 15013 Tallinn, Estonia.

1. Slovenian: Vrhovna revizijska inštitucija oziroma Računsko sodišče.

2. European Organization od Supreme Audit Institutions.
3. **Spletni naslov**.

Alenka Blas in Ruti Rous*

Evropska strategija za podatke: regulativni okvir za upravljanje podatkov

European Data Strategy: Regulatory Framework for Data Governance

POVZETEK ● *Za spodbujanje evropskega gospodarstva je Evropska komisija sprejela strategijo, s katero želi izkoristiti vrednost podatkov, ki so na voljo v evropskem prostoru. Na njeni podlagi se sprejema vrsta aktov, namenjenih povečanju prostega pretoka podatkov, njihovi ponovni uporabi in premišljenemu upravljanju. EU želi s tem vzpostaviti regulativni okvir, ki bi zagotovil usklajeno ravnanje držav članic in okrepil varstvo zasebnosti ter pravice potrošnikov. Z novimi akti si EU prizadeva ohraniti in nadgraditi standarde, ki so bili vzpostavljeni v obstoječih aktih, povezanih z varstvom osebnih podatkov in prostim pretokom neosebnih ter odprtih podatkov javnega sektorja. Akti urejajo široko področje, ki zajema upravljanje podatkov in njihovo interoperabilnost, digitalne storitve in trge ter umetno inteligenco, pri čemer hkrati sledijo tako cilju svobodne izmenjave podatkov in njihove uporabe v pridobitne namene kot tudi cilju krepitve varstva zasebnosti in kibernetske varnosti. Posledično*

zagotavljanje medsebojne usklajenosti aktov in preprečevanje kolizij predstavlja izziv že ob oblikovanju aktov, kakšen bo njihov dejanski učinek, pa se bo izkazalo šele ob uporabi teh aktov.
Ključne besede ● *Evropska strategija za podatke, podatki, upravljanje podatkov, prost pretok, ponovna uporaba, vrednost podatkov*
SUMMARY ● *The European Commission has adopted a strategy with the aim of promoting the European economy by harnessing the value of data available in the European area. Based on this strategy, a series of acts are being adopted to increase the free flow of data, their re-use, and thoughtful management. The EU seeks to establish a regulatory framework that ensures coordinated practices by member states and strengthens the protection of privacy and consumer rights. Through these new acts, the EU aims to maintain and enhance the standards established in existing acts regarding the protection of personal data and the free flow of non-personal and open data of public sector. The acts cover a wide range of areas, including data governance and interoperability, digital services and markets and artificial intelligence. They simultaneously pursue both the free exchange of data and their use for commercial purposes, as well as the strengthening of privacy protection and cybersecurity. As a result, ensuring their mutual consistency and preventing collisions presents a challenge already during their formulation, while their actual impact will only be revealed through their implementation.*
Key words ● *European Data Strategy, data, data governance, free flow, re-use, data value*

JEL: K 24, O 33

1. UVOD

Podatki v današnjem gospodarstvu so osnovno sredstvo večine gospodarskih dejavnosti. S kakovostnimi podatki lahko izboljšujemo in optimiziramo nabavne procese, proizvodnjo, prodajo, razvoj produktov in podobno. Zbiranje in analiza podatkov je za številna podjetja temeljni način zagotavljanja

gospodarske prednosti pred konkurenco. Trgovanje s podatki pa vse pogosteje postaja tudi samostojni poslovni model, ki prinaša visoke donose. To ne velja samo za gospodarstvo, ampak je vrednost podatkov vse pomembnejša v posameznih državah članicah in EU-ju kot celoti. Kakovost zbranih podatkov in njihova souporaba bosta v bližnji prihodnosti ključni za uspešnost EU-ja pri zagotavljanju konkurenčne prednosti pred tujimi trgi, zlasti kitajskim in ameriškim.

Vendar pa ima EU v primerjavi z omenjenimi gospodarstvi pri učinkovitem gospodarjenju s podatki nekoliko več zadržkov zaradi kulturološko in pravno vzpostavljenih višjih standardov pri varstvu zasebnosti, boja proti diskriminaciji in varstva potrošnikov. Iskanje ravnovesja med gospodarskimi ambicijami pri upravljanju podatkov in varstvom drugih temeljnih vrednot EU-ja je zato kompleksen proces, ki se odraža v številnih splošnih in sektorskih aktih, v zadnjih letih sprejetih oziroma predlaganih na ravni EU-ja.

V tem prispevku se seznanimo z vizijo Evropske komisije na tem področju in s temeljnimi akti[1], ki naj bi jo pomagali uresničevati. Pri tem preverimo stanje pred sprejetjem strategije in pregledamo, kateri akti so področje podatkov urejali že pred njo (povezava s točko 2.1), povzamemo idejo strategije (povezava s točko 2.2) in ukrepe, ki jih uvaja (povezava s točko 2.3), predstavimo pa tudi akte, ki so že bili sprejeti na njeni podlagi (povezava s točko 2.4), in nekatere tiste, ki so še v usklajevanju pred sprejetjem (povezava s točko 2.5).

2. EVROPSKA STRATEGIJA ZA PODATKE

Evropska strategija za podatke[2] je obsežen načrt Evropske komisije za vzpostavitev enotnega evropskega podatkovnega prostora, ki naj bi omogočal prosto in varno izmenjavo podatkov ter s tem spodbudil inovacije in gospodarsko rast v EU-ju.

Strategija je bila sprejeta kot odziv na vse večji pomen podatkov za gospodarstvo in družbo. V njej je zapisano, da so podatki osnova za številne nove izdelke in storitve, da spodbujajo produktivnost, učinkovitost rabe virov, boljše zdravstveno varstvo

in številne druge prednosti.

2.1. Stanje pred sprejetjem strategije

V primerjavi z vodilnimi trgi na področju podatkovnega gospodarstva, kot sta ZDA in Kitajska, se je EU pri spodbujanju tovrstnih aktivnosti tako v preteklosti kot tudi danes soočal z nekaterimi dodatnimi ovirami. Te po večini izvirajo iz razdrobljenosti ureditve in pristopov med državami članicami, kar prinaša različne pravne prakse zlasti na področju dojemanja pravic udeležencev na trgu podatkov (tako fizičnih oseb kot javnih in zasebnih pravnih oseb). Države članice se zato težko dogovorijo za enotne pristope pri uporabi podatkov za pregon kaznivih dejanj, znanstvene raziskave in podobno. Hkrati so jezikovne omejitve in razdrobljeno imetništvo podatkov ovire zaradi slabše razpoložljivosti in interoperabilnosti podatkov. Evropska komisija je v strategiji med ovirami za razvoj podatkovnega gospodarstva izpostavila še neravnovesje tržne moči zaradi prisotnosti velikih ponudnikov informacijskih storitev. Za nadaljnji razvoj sektorja bi bilo nujno izboljšati tudi sistem upravljanja podatkov ter povečati vlaganja v podatkovne tehnologije in krepitev sposobnosti, spretnosti in podatkovne pismenosti tako malih in srednjih podjetij kot posameznikov. Ob tem pa je kot nujno izpostavljeno tudi ustrezno obvladovanje tveganj, ki jih razvoj podatkovnega gospodarstva prinaša na področju kibernetske varnosti.

Evropska komisija je že pred Evropsko strategijo za podatke sprejemala številne ukrepe, ki vplivajo na evropski podatkovni prostor. Pri tem so pomembne zlasti Direktiva o zasebnosti in elektronskih komunikacijah[3], Splošna uredba o varstvu osebnih podatkov[4] (v nadaljevanju: GDPR), Direktiva o odprtih podatkih in ponovni uporabi informacij javnega sektorja[5] (v nadaljevanju: Direktiva o odprtih podatkih) in Uredba o okviru za prosti pretok neosebnih podatkov v EU[6] (v nadaljevanju: Uredba o prostem pretoku neosebnih podatkov). Poleg tega je bila na nekaterih področjih sprejeta še posebna sektorska[7] zakonodaja. Za razvoj podatkovnega gospodarstva v EU-ju so bili pomembni tudi akti s področja zagotavljanja informacijske varnosti[8] in varstva

potrošnikov pri dostopu do digitalnih storitev[9]. Temeljne akte, ki so oblikovali pravni okvir do sprejetja strategije, predstavljamo v nadaljevanju.

2.1.1. Direktiva o zasebnosti in elektronskih komunikacijah

Direktiva o zasebnosti in elektronskih komunikacijah je začela veljati leta 2009, v obliki dopolnitve direktive 2002/58/ES. Obravnava nekatera vprašanja glede obdelave osebnih podatkov in zaščite zasebnosti v sektorju elektronskih komunikacij. Po vsebini zajema zlasti področje obdelave podatkov in vključuje določbe o zagotavljanju varnosti omrežij in storitev, zaupnosti komunikacij, dostopu do shranjenih podatkov ter obdelavi prometa in lokacije podatkov. Med pomembnimi spremembami, ki jih je prinesla ta direktiva, je bila uvedba obveznega obvestila o vdoru v osebne podatke ter zagotavljanje nadzora nad metapodatki.

Evropska komisija je leta 2017 pripravila predlog posodobitve direktive, da bi se uskladila z GDPR-jem in vključila problematiko spletnega sledenja, vendar je predlog v letu 2019 zavrnil Evropski svet.

2.1.2. GDPR

GDPR, sprejet leta 2016, se je začel uporabljati maja 2018 in predstavlja temeljni akt o varstvu osebnih podatkov v EU-ju. V njem so določene pravice posameznikov v zvezi z varstvom osebnih podatkov, pravne podlage za zbiranje osebnih podatkov s strani upravljavcev zbirk osebnih podatkov, odgovornosti upravljavcev zbirk osebnih podatkov ter pogoji za njihovo obdelavo in podobdelavo. V GDPR-ju je opredeljen sistem nadzora nad izvrševanjem določb.

Uredba je namenjena predvsem zagotavljanju varstva osebnih podatkov, vendar pa je imela pomemben učinek na digitalno zaupanje in s tem tudi na razvoj podatkovnega gospodarstva v EU-ju. Čeprav je bila namenjena le osebnim podatkom, je *de facto* vplivala tudi na obdelavo neosebnih podatkov, kadar so bili

vključeni v mešane podatkovne zbirke. Ker v poslovnem svetu zbirke podatkov pogosto vsebujejo tako osebne kot anonimne in neosebne podatke, je njihovo strogo razvrščanje lahko tehnično in ekonomsko neučinkovito ter jih je bolje v celoti obravnavati v okviru GDPR-ja. Evropska komisija je pripravila tudi standardna pogodbena določila za prenos osebnih podatkov,[10] s katerimi je želela olajšati zagotavljanje skladnosti z GDPR-jem pri prenosu podatkov v tretje države.

GDPR je tako vzpostavil osnovne mehanizme upravljanja podatkov, pokazal pa je tudi na diskrepanco na področju upravljanja podatkov med državami članicami in vzpostavil prakse sodelovanja, ki so oziroma bodo uporabne tudi v zvezi z neosebnimi podatki.

2.1.3. Direktiva o odprtih podatkih

Direktiva o odprtih podatkih je bila sprejeta leta 2019, da se spodbudi uporaba nevarovanih podatkov javnega sektorja za razvoj novih ali izboljšanih proizvodov in storitev. Gre za spodbujanje ponovne uporabe podatkov iz obstoječih dokumentov, ki jih javni sektor ustvari v povezavi z izpolnjevanjem javnih nalog oziroma zagotavljanjem storitev v splošnem interesu, ter podatkov, ki se ustvarijo pri znanstvenem raziskovanju.

Direktiva o odprtih podatkih napotuje, da se za organe javnega sektorja in javna podjetja določi obveznost zagotavljanja odprtih podatkov, to je podatkov v odprtem formatu, ki omogočajo vsakomur, da jih uporablja in deli brez pravnih, finančnih in tehničnih omejitev. To pomeni, da so podatki zagotovljeni:

- v razpoložljivem formatu (elektronsko, po priznanih odprtih standardih, v strojno berljivi obliki, če je mogoče, skupaj z metapodatki, ažurno, prek aplikacijskih programskih vmesnikov in z možnostjo masovnega prenosa);
- brezplačno (oziroma z minimalnim plačilom za povrnitev stroškov morebitne anonimizacije podatkov in njihove reprodukcije);
- na pregleden način (z vnaprejšnjim obveščanjem o morebitno

potrebnih plačilih in razpoložljivih pravnih sredstvih);
- brezpogojno in
- na praktičen način (podatki so dejansko razpoložljivi in omogočeno je enostavno iskanje dokumentov prek enotne točke dostopa).

Posebno pozornost Direktiva o odprtih podatkih namenja naborom podatkov velike vrednosti (angl. *High Value Datasets* ali *HDVs)*. Gre za podatke, ki ustvarjajo pomembne družbeno-gospodarske in okoljske koristi za veliko uporabnikov, pomagajo ustvarjati prihodke in se enostavno povezujejo z drugimi nabori podatkov, torej imajo velik potencial za ustvarjanje dodane vrednosti. Po tematskih področjih zajemajo:

- geoprostorske podatke (npr. poštne številke, zemljevidi);
- podatke v zvezi z opazovanjem Zemlje in okolja (npr. satelitski posnetki, poraba energije);
- meteorološke podatke;
- statistične podatke (npr. demografski in gospodarski kazalniki);
- podatke o družbah in lastništvu družb (npr. poslovni registri) in
- podatke o mobilnosti (npr. cestni promet, plovba).

Konec decembra 2022 je Evropska komisija sprejela še izvedbeno uredbo,[11] ki določa seznam naborov podatkov velike vrednosti po tematskih področjih ter tudi način ureditve teh podatkov za objavo in ponovno uporabo v obliki minimalnih zahtev glede odprtega dostopa do podatkov, njihove strojne berljivosti, dostopnosti prek aplikativnih programskih vmesnikov in njihove ažurnosti. Ta uredba bo v državah članicah neposredno uporabljiva od 9. junija 2024 dalje.

2.1.4. Uredba o prostem pretoku neosebnih podatkov

Uredba o prostem pretoku neosebnih podatkov je bila sprejeta leta 2018 z namenom omogočiti prost pretok tistih podatkov, za katere tega ne zagotavlja že GDPR. Gre torej za neosebne podatke kot elektronske informacije, ki jih ni mogoče povezati z določenim ali določljivim posameznikom.

Analiziranje takih podatkov ter njihovo združevanje in povezovanje s posameznimi storitvami in proizvodi ima pomemben potencial za ustvarjanje dodane vrednosti v gospodarstvu, vendar pa je bilo to preprečeno zaradi nacionalnih zahtev držav članic po lokalizaciji podatkov in prakse, ki je poslovne uporabnike omejevala pri menjavi ponudnika obdelave podatkov.[12] To je povzročilo odsotnost konkurence med ponudniki storitev v oblaku, podjetjem za raziskave pa otežilo sodelovanje z drugimi organizacijami znotraj EU-ja in s tem zaviralo inovacije. Tako je bilo preprečeno doseganje enotnega digitalnega trga in onemogočena racionalizacija stroškov shranjevanja podatkov, s tem pa omejena konkurenčnost EU-ja.

Uredba o prostem pretoku neosebnih podatkov velja tako za osebe javnega kot zasebnega prava in:

- prepoveduje lokalizacijo podatkov, to je omejevanje prostega pretoka podatkov znotraj EU-ja;
- prepoveduje omejevanje prenosa podatkov ob menjavi ponudnika obdelave podatkov;
- zahteva omogočanje primerjave storitev;
- zahteva sodelovanje pristojnih organov držav članic med njimi in
- zahteva, da posamezna država članica pred uveljavitvijo novega pravila o lokalizaciji podatkov pridobi odobritev Evropske komisije.

Določila Uredbe o prostem pretoku neosebnih podatkov so v korist predvsem izvajalcem digitalnih storitev (npr. izvajalcem storitev računalništva v oblaku), saj jim omogočajo obdelavo neosebnih podatkov s celotnega območja EU-ja, hkrati pa tudi uporabnikom njihovih storitev, saj prosti pretok spodbuja konkurenco. Vsekakor ne gre zanemariti širšega učinka, ki ga bo predvidoma imela predmetna uredba na evropsko gospodarstvo, saj bo to razpolagalo z večjim obsegom podatkov ter njihovo hitrejšo in boljšo dostopnostjo.

2.2. Ideja strategije

Kljub pomembni že obstoječi regulaciji upravljanja podatkov se je Evropska komisija zavedala, da ne bo zadoščala za uresničitev cilja evropske digitalne neodvisnosti do leta 2030. Še vedno namreč ni na voljo dovolj podatkov za zagon gospodarstva z inovacijami, saj ima zasebni sektor zaradi skrbi pred izgubo konkurenčne prednosti na trgu zadržke pri deljenju podatkov, hkrati pa podatki javnega sektorja niso v celoti izkoriščeni, kljub temu da so ustvarjeni z javnimi sredstvi in bi zato morali biti na voljo vsem. Zato je vizija strategije, da se ustvari spodbudno okolje za podatkovno gospodarstvo, izkoristi njegov potencial ter da se omogoči tako javnemu kot zasebnemu sektorju boljše, s podatki podprto sprejemanje odločitev ob hkratnem spoštovanju evropskih vrednot in temeljnih človekovih pravic. Strategija naj bi pripomogla k nastanku skupnega evropskega podatkovnega prostora, ki bi omogočal pretok podatkov po vsem EU-ju in med vsemi sektorji, zagotavljal spoštovanje varstva osebnih podatkov, potrošnika in konkurenčnega prava ter pravična, praktična in jasna pravila o dostopu do podatkov in njihovi uporabi.

Pri doseganju tega se EU spopada z več izzivi, povezanimi zlasti z razdrobljenostjo evropskega podatkovnega prostora. Strategija ugotavlja, da je razpoložljivost podatkov, ki so v EU-ju na voljo za ponovno uporabo in razvoj umetne inteligence, nizka; težave se pri tem pojavljajo tako pri podatkih javnega kot zasebnega sektorja. Na razvoj podatkovnega gospodarstva pomembno negativno vpliva neravnovesje tržne moči, saj velike spletne platforme kopičijo ogromne količine podatkov, ki jim zagotavljajo bistveno konkurenčno prednost. Za učinkovito podatkovno gospodarstvo bo EU moral zagotoviti tudi ustrezno kakovost in operabilnost podatkov ter uvesti ustrezne organizacijske pristope upravljanja podatkov. Dotakniti se bo treba tudi vprašanja odvisnosti od ponudnikov izven EU-ja in urediti razmerje do pravnih norm, ki jih za te ponudnike določajo tretje države. Med ključnimi izzivi strategija navaja vprašanje usposobljenosti posameznikov na področju digitalne pismenosti in uveljavljanja njihovih pravic ter zagotavljanje kibernetske varnosti.

2.3. Ukrepi, ki jih uvaja strategija

Ukrepi strategije temeljijo na štirih stebrih, ki naj bi povzeli temeljne izzive, kot jih je izpostavila Evropska komisija.

Prvi steber ukrepov Evropske strategije za podatke predstavlja *Medsektorski okvir upravljanja za dostop do podatkov in njihovo uporabo*. Gre zlasti za sprejetje splošnih pravnih aktov, ki bodo veljali za vse sektorje in bodo omogočili upravljanje skupnih evropskih podatkovnih prostorov. Predvideno je, da bo v teh aktih določeno, kateri podatki se lahko uporabljajo v katerih okoliščinah, da bo olajšana njihova čezmejna uporaba ter zagotovljeni standardi glede njihove interoperabilnosti. Z njimi naj bi bili vzpostavljeni mehanizmi, ki bi olajšali soglašanje z uporabo podatkov za posameznike, ki to želijo (t. i. podatkovni altruizem). Evropska komisija si je ob tem zadala, da bo preučila tudi, kateri zakonodajni ukrepi so potrebni za ureditev odnosov med akterji v podatkovnem gospodarstvu in kateri za vzpostavitev zbirk podatkov za namene podatkovne analize in strojnega učenja. Med dodatnimi nalogami, ki si jih je v strategiji zadala Evropska komisija, je še obravnava vprašanja tržnih koncentracij in izkrivljanja konkurence ter zagotavljanje teritorialne veljave evropskih norm za vse akterje, ki ponujajo storitve na trgu EU-ja.

Drugi steber ukrepov predstavljajo *Omogočitveni dejavniki: naložbe v podatke in krepitev evropske zmogljivosti in infrastrukture za gostovanje, obdelavo in uporabo podatkov, interoperabilnost*. Evropska komisija je v strategiji napovedala, da bo uporabila programe financiranja EU-ja, da okrepi tehnološko suverenost. Napovedala je vlaganja v projekte z velikim učinkom v zvezi z evropskimi podatkovnimi prostori in skupno infrastrukturo oblaka. Projekt naj bi med drugim financiral infrastrukturo, orodja za souporabo podatkov, arhitekture in mehanizme upravljanja za uspešno souporabo podatkov ter ekosisteme umetne inteligence. Evropska komisija je napovedala tudi vzpostavitev evropske tržnice storitev v oblaku in pripravo oblakovnega pravilnika za EU.

Tretji steber ukrepov so *Kompetence: opolnomočenje posameznikov, vlaganje v znanje in spretnosti ter v mala in srednja podjetja*. Ta sklop ukrepov po eni strani predvideva pravno opolnomočenje posameznikov za odločanje o tem, kako se

ravna z njihovimi podatki v smislu okrepitve pravic iz GDPR-ja. Po drugi strani pa predvideva tudi finančne naložbe v znanje in spretnosti, tako za digitalne strokovnjake, med drugim na področju velepodatkov (angl. *big data*) in analitike, kot tudi za splošno podatkovno pismenost prebivalstva ter znanja, ki jih potrebujejo mala in srednja podjetja za sodelovanje v podatkovnem gospodarstvu.

Četrti steber so *Skupni evropski podatkovni prostori v strateških sektorjih in na področju javnega interesa*. Ukrepi zajemajo podporo Evropske komisije za vzpostavitev skupnih evropskih podatkovnih prostorov za devet področij, in sicer: industrija, zeleni dogovor, mobilnost, zdravstvo, finance, energija, kmetijstvo, javna uprava ter znanje in spretnosti. Podpora Evropske komisije pri vzpostavitvi teh skupnih podatkovnih prostorov naj bi zajemala ukrepe tako pravne kot organizacijske in investicijske narave.

V tem prispevku se osredotočamo na prvi steber, ki zagotavlja pravni okvir za razvoj podatkovnega gospodarstva v EU-ju.

2.4. Akti, sprejeti za uresničevanje strategije

Evropska komisija je v okviru uresničevanja Evropske strategije za podatke pripravila vrsto predlogov novih predpisov. Pri tem ločnica, kateri akti pomenijo neposredno uresničevanje strategije in kateri ne, ni povsem jasna. Zagotovo pri nobenem ni mogoče zanikati vsaj posrednega vpliva na ureditev področja podatkov. Ta prispevek se poskuša osredotočiti na temeljne akte, ki so neposredno povezani z Evropsko strategijo za podatke, omeni pa tudi nekatere, ki smo jih kljub posrednemu vplivu prepoznali kot ključne. Področje podatkov ureja še vrsta sektorskih in drugih aktov, zato izbora v tem prispevku ne gre razumeti kot vseobsegajočega seznama.

V nadaljevanju predstavljamo akte, ki sta jih Evropski parlament in Evropski svet na predlog Evropske komisije že sprejela: Uredbo o evropskem upravljanju podatkov[13] (v nadaljevanju: Akt o

upravljanju podatkov), Uredbo o tekmovalnih in pravičnih trgih v digitalnem sektorju[14] (v nadaljevanju: Akt o digitalnih trgih) in Uredbo o enotnem trgu digitalnih storitev[15] (v nadaljevanju: Akt o digitalnih storitvah), v delu, ki se nanaša neposredno na podatke, pa povzamemo tudi Direktivo o ukrepih za visoko skupno raven kibernetske varnosti v Uniji[16] (v nadaljevanju: NIS 2).

2.4.1. Akt o upravljanju podatkov

Akt o upravljanju podatkov je bil prvi izmed aktov, sprejetih neposredno s ciljem uresničevanja Evropske strategije za podatke. Osnovna ideja akta je bila ustvariti ustrezne pogoje, ki bodo omogočali tistim, ki želijo podatke deliti, da to lahko storijo na način, ki mu lahko zaupajo. Akt naj bi vzpostavil alternativni model deljenja informacij, ki bi bil neodvisen od velikih tehnoloških podjetij, ter tako upošteval tudi probleme, kot so visoki transakcijski stroški in nezadostna količina podatkov, ki so na voljo za ponovno uporabo. Akt je bil sprejet kot uredba s ciljem poenotenja regulativne razpršenosti med državami članicami in uvaja ukrepe, razdeljene na štiri stebre.

Prvi steber ukrepov se osredotoča na vzpostavitev pogojev za ponovno uporabo občutljivih podatkov, ki jih posedujejo organizacije javnega sektorja. Nanaša se na podatke, katerih ponovna uporaba je otežena, saj so varovani z različnimi pravicami in upravičenji, med drugim iz naslova intelektualne lastnine in poslovnih skrivnosti. Akt naj bi zagotovil zadostno raven zaščite za deljenje teh podatkov. Uredba je glede tega komplementarna Direktivi o odprtih podatkih. Vsaka država članica naj bi ustanovila vsaj eno enotno kontaktno točko, ki bo povezovala subjekte, zainteresirane za ponovno uporabo podatkov, z organizacijo javnega sektorja, ki te podatke poseduje. Pri tem pa organov javnega sektorja ne obvezuje, da dovolijo ponovno uporabo podatkov.

Drugi steber ukrepov se nanaša na vzpostavitev okvira za nove subjekte na trgu podatkov, t. i. **posrednike podatkov**, ki naj bi kot zaupanja vredni subjekti zagotavljali osnovno infrastrukturo za deljenje podatkov. Tako naj bi se spodbudilo prostovoljno deljenje

podatkov ob sočasnem zagotovilu, da bodo podjetja in posamezniki, na katere se podatki nanašajo, ohranili nadzor nad podatki. Subjekti, ki bi želeli zagotavljati storitev posredovanja podatkov, bodo morali priglasiti svojo dejavnost organu javnega sektorja ter ob tem zagotoviti ustrezno zaščito občutljivih podatkov in izkazati, da na trgu nastopajo kot nevtralne tretje osebe. Posredniki morajo biti ustanovljeni v EU-ju ali imeti v EU-ju svoje pravne predstavnike.

Tretji steber ukrepov naj bi pripomogel k vzpostaviti t. i. podatkovnega altruizma. Gre za idejo, v skladu s katero naj bi posamezniki in podjetja prostovoljno in brezplačno dovolili obdelavo svojih podatkov z namenom, da se s tem pripomore k uresničevanju javne koristi, na primer znanstvenim raziskavam, preprečevanju oziroma boju proti epidemijam, učinkovitejšemu javnemu sektorju in podobno. Organizacije, ki bodo zagotovile skladnost z zahtevami po transparentnosti in ustreznem varstvu pravic oseb, na katere se nanašajo podatki, pa bodo lahko pridobile status **zaupanja vredne organizacija podatkovnega altruizma** in bodo vključene v evropski register teh organizacij.

Četrti steber ukrepov naj bi okrepil koordinacijo in interoperabilnost na evropski ravni z vzpostavitvijo Evropskega odbora za podatkovne inovacije. Odbor naj bi pomagal Evropski komisiji pri načrtovanju razvoja področja ter pospeševal sodelovanje nacionalnih organov zlasti z izmenjavo nacionalnih praks in politik. Svetoval naj bi tudi o prioritizaciji standardov interoperabilnosti za medsektorsko in čezmejno ponovno uporabo podatkov.

Akt o upravljanju podatkov je po svoji pravni naravi uredba, kar pomeni, da se uporablja neposredno, ne da bi ga morale države članice prenesti v svojo zakonodajo. Sprejet je bil 30. maja 2022, začne pa se uporabljati 24. septembra 2023. Akt sam zase določa subsidiarno uporabo glede na akte in pravila, ki urejajo varstvo podatkov, ter nekatere druge akte.

2.4.2. Akt o digitalnih trgih

Akt o digitalnih trgih se uporablja za t .i. jedrne platformne

storitve,[17] ki jih poslovnim uporabnikom s sedežem v EU-ju ali končnim uporabnikom, ki imajo sedež ali so v EU-ju, zagotavljajo podjetja, ki se v skladu z Aktom o digitalnih trgih imenujejo za t. i. vratarja (angl. *gatekeeper*).

Podjetje se imenuje za vratarja, če ima znaten vpliv na notranji trg,[18] če zagotavlja jedrno platformno storitev, ki je pomembna vstopna točka,[19] ter ima pri izvajanju svojih dejavnosti utrjen in trajen položaj ali se predvideva, da bo tak položaj imelo v bližnji prihodnosti. Za podjetje, ki dosega mejne vrednosti, se pričakuje, da bo samo prijavilo svoj položaj Evropski komisiji, ta pa podjetje poimenuje za vratarja bodisi na prejeto prijavo bodisi po uradni dolžnosti. Akt podrobneje opredeljuje postopek imenovanja vratarjev in na Evropsko komisijo delegira pristojnost za sprejemanje natančnejših kriterijev in postopkov.

Akt nadalje določa seznam prepovedanih in seznam obveznih praks, ki naj bi jih vratarji upoštevali. Akt za vratarja uvaja omejitve v zvezi z varstvom osebnih podatkov, med drugim tako, da ne sme obdelovati osebnih podatkov, ki jih pridobijo njegovi uporabniki, združevati osebnih podatkov, uporabljati osebnih podatkov pri drugih storitvah, ki jih vratar zagotavlja ločeno, ter vpisovati končnih uporabnikov v druge storitve vratarja, da bi združil osebne podatke, razen kadar je dal uporabnik privolitev v skladu z GDPR-jem. Nadalje uvaja omejitve na področju varstva konkurence. Pri tem omejuje več ravnanj vratarja, ki so usmerjena v zagotavljanje prednosti pred konkurenčnimi platformami.[20] Vratar med drugim pri konkuriranju poslovnim uporabnikom ne sme uporabljati podatkov, ki niso javno dostopni in jih pridobi prek svojih jedrnih platform, ne sme dajati prednosti svojim aplikacijam v smislu pogojevanja njihove uporabe ali onemogočanja prenosa na konkurenčne rešitve, ne sme ugodneje obravnavati lastnih storitev in produktov v brskalnikih in podobno. Vratar ima tudi obveznosti glede zagotavljanja interoperabilnosti medosebnih komunikacijskih storitev. Akt pri tem pooblašča Evropsko komisijo tako za posamezne preiskovalne ukrepe kot za sankcioniranje vratarjev.

Akt o digitalnih trgih v primerjavi z drugimi akti, s katerimi naj bi se uresničevala Evropska strategija za podatke, ne določa podlage

ali postopkov za deljenje podatkov, temveč se usmerja predvsem na zagotavljanje konkurence in omejevanje vratarjev pri nepoštenih praksah. Tako naj bi Akt o digitalnih trgih zagotavljal lažji vstop na trg za manjša podjetja in zagonska podjetja, zmanjšal odvisnost uporabnikov od velikih spletnih platform, omogočal lažji prehod potrošnikov med posameznimi platformami in tako zagotovil boljšo potrošniško izkušnjo tako glede cen kot tudi pogojev uporabe platform.

Akt o digitalnih trgih se uporablja od maja 2023, vendar se bodo nekateri člani v celoti lahko uporabljali šele kasneje.

2.4.3. Akt o digitalnih storitvah

Akt o digitalnih storitvah je bil sprejet kot posodobitev Direktive o elektronskem poslovanju[21] iz leta 2000 in bo neposredno uporabljiv od 17. februarja 2024. Njegov cilj je omejiti razširjanje nezakonite vsebine na spletu ter s sprejemom pravil za digitalne storitve zagotoviti varno, zaupanja vredno in predvidljivo spletno okolje ter zaščititi potrošnike in njihove temeljne pravice. Njegov namen je torej predvsem zamejiti sovražni govor, širjenje terorističnih vsebin, spletno prodajo oziroma posredovanje nevarnih in prepovedanih proizvodov, storitev in vsebin ter v povezavi s tem še posebej ščititi interese mladoletnih.

Pravila se nanašajo na posredniške storitve, storitve spletnega gostovanja in na storitve spletnih platform, kar v praksi med drugim zajema spletne tržnice, družbena omrežja, platforme za deljenje vsebine, platforme za posredovanje potovanj in nastanitev ter spletno gostovanje. Pri tem določbe Akta o digitalnih storitvah veljajo:

- za vse posredniške storitve ponudnika posredniških storitev, ne glede na to, kje ima sedež, če gre za posredovanje prejemniku storitve, ki ima svoj sedež ali je v EU-ju; in
- za izključni prenos, predpomnjenje in gostovanje, torej tako glede prenosa informacij, ki jih zagotovi prejemnik storitve, kot tudi glede njihovega (samodejnega, vmesnega, začasnega ali dolgoročnega) shranjevanja.

Akt o digitalnih storitvah uvaja nove obveznosti za ponudnike posredniških storitev, ki vključujejo poročanje o preglednosti (o moderiranju vsebin, prejetih odločbah, prijavah in pritožbah glede nezakonitih vsebin in sprejetih ukrepih), razkrivanje algoritemskih sistemov spletnih platform, sprejem postopkov za hitro odstranitev nezakonite vsebine, uvedbo pritožbenih in mediacijskih mehanizmov, uvaja pa se tudi odgovornost ponudnikov storitev spletnih platform za takojšnje ukrepanje glede škodljive in nezakonite vsebine na njihovih spletnih platformah.

Za uporabnike digitalnih storitev Akt o digitalnih storitvah uvaja pravico do informiranosti in možnost zahtevati, da spletna platforma odstrani neresnično oziroma škodljivo vsebino, poleg tega se uvajajo mehanizmi, ki uporabniku zagotavljajo boljšo preveritev informacij o prodajalcu proizvodov in preglednejše splošne pogoje poslovanja. Pregon kršitev Akta o digitalnih storitvah je naložen državam članicam, ki so dolžne določiti koordinatorje digitalnih storitev kot organe nadzora na nacionalni ravni.

2.4.4. NIS 2

Evropska strategija za podatke kot pomemben del digitalne preobrazbe v EU-ju vpliva tudi na vsebino in izvajanje aktov, ki jih EU vzporedno sprejema v okviru digitalne strategije. Eden izmed takšnih je NIS 2, v zvezi s katerim morajo države članice sprejeti uskladitvene predpise do 17. oktobra 2024. Zagotavljanje visoke ravni kibernetske varnosti v EU-ju je povezano tako z osebnimi kot neosebnimi podatki, ki jih ustvarjajo, prenašajo in obdelujejo posamezniki ter subjekti javnega in zasebnega sektorja. Enega izmed izzivov implementacije NIS 2 predstavlja vzporedno zagotavljanje ustrezne ravni varstva osebnih podatkov in s tem povezane skladnosti z GDPR-jem. Kot potencialno problematično velja izpostaviti utemeljenost pravnega interesa za obdelavo osebnih podatkov z namenom zagotavljanja varnosti informacijskih sistemov, postopke za priglasitev incidentov, ki vključujejo osebne podatke, in razmejitev pristojnosti med organi, odgovornimi za NIS 2 oziroma GDPR, kadar so vključeni osebni podatki.

2.5. Akti v sprejemanju

Kljub temu da se Evropska strategija za podatke deloma že uresničuje, pa vsi akti, predvideni za celostno ureditev področja podatkovne strategije, še niso sprejeti. Akti, ki so trenutno v obliki predloga Evropske komisije in v fazi medinstitucionalnega usklajevanja, so: Predlog Uredbe o harmoniziranih pravilih za pravičen dostop do podatkov in njihovo uporabo[22] (v nadaljevanju: Predlog Akta o podatkih), Predlog Uredbe o določitvi ukrepov za visoko raven interoperabilnosti javnega sektorja v Uniji[23] (v nadaljevanju: Predlog Akta o interoperabilni Evropi), Predlog Uredbe o določitvi harmoniziranih pravil o umetni inteligenci[24] (v nadaljevanju: Predlog Akta o umetni inteligenci) in Predlog Uredbe o evropskem zdravstvenem podatkovnem prostoru[25] (v nadaljevanju: Predlog Akta o evropskem zdravstvenem podatkovnem prostoru).

2.5.1. Predlog Akta o podatkih

Predlog Akta o podatkih predstavlja nadgradnjo Uredbe o prostem pretoku neosebnih podatkov, ki je odpravila ovire za mednarodno izmenjavo podatkov. Predlog Akta o podatkih želi doseči povečanje obsega neosebnih podatkov v prostem pretoku ter s tem povečanje ponovne uporabe podatkov in z njo konkurenčnosti evropskega gospodarstva.

Predmet urejanja so predvsem podatki, ustvarjeni z napravami interneta stvari (angl. *Internet of Things – IoT*), ki jih imajo subjekti v uporabi (podatki povezanih naprav)[26] in ki so primarno namenjeni za uporabo v pridobitne namene v zasebnem sektorju. Predvideno je, da se bodo podatki lahko uporabljali v kateri koli zakonit namen, pri čemer mora biti ta dogovorjen s subjektom, ki jih je dal na voljo (uporabnik povezane naprave). Predlog Akta o podatkih želi določiti pravila, kdo lahko te podatke uporablja in pod katerimi pogoji. Obravnava tri vrste posredovanja podatkov:

- *Business-to-Consumers* (B2C) – poslovanje s strankami:

uporabniki povezanih naprav bodo imeli pravico dostopati in posredovati podatke, ki nastanejo z njihovo uporabo povezane naprave, pri čemer bo proizvajalec naprave odgovoren to privzeto zagotavljati;
- *Business-to-Business* (B2B) – medpodjetniško elektronsko poslovanje: vzpostavljena bodo pravila, ki bodo z enakovrednim dostopom do podatkov zagotavljala razpršitev podatkovne vrednosti med manjša in velika podjetja na trgu;
- *Business-to-Government* (B2G) – elektronsko poslovanje z javno upravo: subjekti javnega sektorja bodo ob izjemni potrebi (splošna nevarnost in druge izjemne razmere) lahko zahtevali dostop do podatkov.

Poleg tega Predlog Akta o podatkih želi določiti interoperabilnostni okvir za vzpostavitev skupnih evropskih podatkovnih prostorov, ki bo zavezoval upravljavce podatkovnih prostorov in ponudnike storitev obdelave podatkov, da uporabnikom omogočijo lažje prehajanje med različnimi ponudniki storitev. Dodatno je predvideno preprečevanje mednarodnega dostopa in prenosa neosebnih podatkov, ki se hranijo v EU-ju, kar bo od ponudnikov storitev v oblaku zahtevalo sprejemanje nekaterih tehničnih in organizacijskih ukrepov.

2.5.2. Predlog Akta o interoperabilni Evropi

Predlog Akta o interoperabilni Evropi je eden izmed ukrepov Evropske komisije za pospešitev digitalizacije evropskega javnega sektorja, ki je osredotočen na čezmejne digitalne javne storitve. Interoperabilnost se razume kot vzajemno sodelovanje evropskega javnega sektorja pri doseganju vzajemno koristnih ciljev, in sicer z izmenjavo informacij in znanja ter podatkov med njegovimi omrežnimi in informacijskimi sistemi. To se namerava doseči z vzpostavitvijo treh stebrov interoperabilnosti:

- z uvedbo interoperabilnostnih rešitev,
- s podpornimi ukrepi in
- z ustreznim okvirom upravljanja.

Med interoperabilnostnimi rešitvami je predvidena določitev tehnične specifikacije, ki jo mora izpolnjevati omrežni in

informacijski sistem, da se poveča čezmejna interoperabilnost. To pomeni, da bi rešitve zagotavljale pravno, organizacijsko, semantično in tehnično interoperabilnost, torej pravne podlage za nemoteno zagotavljanje javnih storitev med državami članicami, učinkovito usklajevanje med organi javnega sektorja, zagotavljanje ohranitve oblike in razumevanja izmenjanih podatkov ter tehnično kompatibilnost omrežnih in informacijskih sistemov.

Predvideno je, da bodo podporni ukrepi zagotavljali projekte za podporo organom javnega sektorja za zagotavljanje interoperabilnosti, kar vključuje izboljšanje obstoječih interoperabilnostnih rešitev ali razvoj novih, usposabljanja in vzpostavitev regulativnih peskovnikov. Slednji so mišljeni kot okolje za preizkušanje interoperabilnostnih rešitev, ki bi omogočalo razvoj in preizkušanje inovativnih rešitev, preden se taki sistemi vključijo v omrežne in informacijske sisteme javnega sektorja. Njihov namen je spodbuditi inovacije ter olajšati razvoj in uvajanje novih rešitev.

Za zagotavljanje ustreznega okvira upravljanja je predvidena ustanovitev Odbora za interoperabilno Evropo, ki bi ga sestavljali predstavniki držav članic in relevantnih evropskih organizacij, ter oblikovanje Skupnosti interoperabilne Evrope, ki bi jo sestavljal širši krog strokovne javnosti.

Kot enotna vstopna točka za informacije v zvezi z interoperabilnostjo omrežnih in informacijskih sistemov bo uveden Portal interoperabilne Evrope, ki bo namenjen spodbujanju izmenjave informacij med organi javnega sektorja glede implementiranih informacijskih rešitev, kar bi spodbudilo deljenje in ponovno uporabo preizkušenih orodij kot hiter in stroškovno učinkovit pristop k oblikovanju digitalnih javnih storitev.

Predvideno je, da bodo interoperabilnostni ukrepi veljali za organe javnega sektorja v državah članicah in za organizacije EU-ja, ki zagotavljajo ali upravljajo omrežne ali informacijske sisteme, ki omogočajo elektronsko izvajanje in upravljanje javnih storitev. Največji učinki izvajanja teh ukrepov se pričakujejo na področju pravosodja, notranjih zadev, davkov, carine, prometa, zdravja,

kmetijstva in industrije.

2.5.3. Predlog Akta o umetni inteligenci

Predlog Akta o umetni inteligenci je Evropska komisija podala s ciljem zagotoviti, da so umetnointeligenčni sistemi varni ter spoštujejo temeljne pravice in vrednote EU-ja; zagotoviti pravno varnost za olajšanje naložb in inovacij; izboljšati izvrševanje obstoječe zakonodaje o temeljnih pravicah in varnostnih zahtevah ter olajšati razvoj enotnega trga za zakonito, varno in zaupanja vredno uporabo umetne inteligence.

Predlog Akta o umetni inteligenci temelji na k tveganjem usmerjenem pristopu in razlikuje med uporabami umetne inteligence, ki ustvarjajo: a) nesprejemljivo tveganje, (b) veliko tveganje in (c) majhno ali minimalno tveganje. Pojem **velikega tveganja** pri tem ni natančno določen, saj si je Evropska komisija v želji zagotavljanja aktualnosti akta pridržala pristojnost naknadnega določanja pojma, upoštevajoč dana merila in usmeritve. Predlog Akta o umetni inteligenci določa štiri vrste prepovedanih praks umetne inteligence, ki so v nasprotju z vrednotami EU-ja. Prepovedi zajemajo prakse, ki imajo znaten potencial za manipulacijo oseb s subliminalnimi tehnikami, ki presegajo njihovo zavest, ali za izkoriščanje šibkih točk posebno ranljivih skupin, kot so otroci ali invalidi, da bi materialno izkrivili njihovo vedenje, tako da bi se njim ali drugi osebi lahko povzročila psihična ali fizična škoda. Predlog prepoveduje tudi družbeno točkovanje na podlagi umetne inteligence za splošne namene, ki jih izvajajo javni organi. Nazadnje je prepovedana tudi uporaba sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, razen v posebej opredeljenih izjemah.

Predlog natančneje določa tudi previdnostne ukrepe za visokotvegane umetnointeligenčne sisteme, ki se morajo izvrševati, tako preden se da sistem na trg kot tudi med samim delovanjem sistema. Predlog poleg tega določa obveznosti ponudnikov in uporabnikov umetnointeligenčnih sistemov in

drugih strank, na primer uvoznikov in distributerjev. Države članice morajo vzpostaviti t. i. priglasitvene organe, ki ugotavljajo skladnost in spremljanje teh sistemov.

Sankcioniranje naj bi bilo v skladu s predlogom prepuščeno državam članicam, ki morajo ustanoviti ali določiti tudi organ za nadzor. Na ravni EU-ja pa naj bi bil ustanovljen Evropski odbor za umetno inteligenco, ki bo koordiniral sodelovanje in skrbel za izmenjavo praks med državami članicami.

2.5.4. Predlog Akta o evropskem zdravstvenem podatkovnem prostoru

Evropska strategija za podatke kot enega izmed ukrepov predvideva ustanovitev t. i. skupnih evropskih podatkovnih prostorov. Ti naj bi omogočali nizkocenovno zaupanja vredno izmenjavo podatkov in s tem povečali razvoj s podatki povezanih produktov in storitev. Maja 2022 je bil kot eden prvih izvedbenih aktov za vzpostavitev skupnih evropskih podatkovnih prostorov predlagan Akt o Evropskem zdravstvenem podatkovnem prostoru, ki naj bi predvsem opolnomočil posameznike, da imajo več nadzora nad svojimi elektronskimi zdravstvenimi podatki. Hkrati naj bi zdravstvenim delavcem omogočil boljši dostop do relevantnih zdravstvenih podatkov ter pomagal oblikovalcem politike in raziskovalcem dostopati do pomembnih zdravstvenih podatkov v anonimizirani obliki. Nanaša se na podatke v elektronskih zdravstvenih kartotekah, aplikacijah, medicinskih napravah in zdravstvenih registrih. V skladu z aktom naj bi vsaka država članica vzpostavila nacionalni organ za digitalno zdravje, po katerem bi se uresničevale pravice posameznikov in izvrševale izmenjave podatkov. Komisija pa naj bi vzpostavila osrednjo platformo za digitalno zdravje, ki naj bi podpirala in olajševala izmenjavo elektronskih zdravstvenih podatkov med državami članicami.

Akt določa še nekatere obveznosti subjektov v zvezi z vodenjem, trženjem in skladnostjo elektronskih zdravstvenih zapisov, registracijo teh zapisov in sistemom nadzora. Poleg tega določa pravila v zvezi s ponovno uporabo elektronskih zdravstvenih

podatkov, pri čemer opredeljuje kategorije podatkov, dovoljene in prepovedane namene ponovne uporabe podatkov, organizacijske ukrepe za izvajanje ponovne uporabe, zlasti pristojnosti organov za dostop do zdravstvenih podatkov, dolžnosti imetnikov podatkov, vprašanje dovoljenj in zahtev za ponovno uporabo zdravstvenih podatkov ter čezmejni dostop do njih. Akt vključuje še nekatere druge ukrepe, vključno z ustanovitvijo Odbora za evropski zdravstveni podatkovni prostor.

3. ZAKLJUČEK

Evropska komisija je v uvodu Evropske strategije za podatke zapisala, da »današnji zmagovalci ne bodo nujno v ospredju tudi v prihodnosti« (angl. *the winners of today will not necessarilly be the winners of tomorrow*)[27]. S tem je poudarila, da se zaveda pomembnosti, ki jo imajo podatki za napredek v evropskem prostoru, ter hkrati napovedala odločne in celovite ukrepe EU-ja za prevzem vodstva pri izkoriščanju vrednosti podatkov v svetovnem merilu.

Z osnovno idejo, da se poveča prost pretok osebnih in neosebnih podatkov znotraj meja EU-ja, hkrati pa omeji in prepreči mednarodni dostop in iznos teh podatkov izven njenih meja, EU sledi cilju, da vrednost, ki jo prinašajo dostop, ponovna uporaba in obdelava podatkov, koristi evropskemu gospodarstvu. Zato je bil na ravni EU-ja predlagan obsežen sveženj aktov za zagon evropskega podatkovnega gospodarstva.

Pri sprejemanju Evropske strategije za podatke je moral EU graditi na nekaterih že sprejetih aktih s tega področja, ki so vzpostavili temelje za varstvo osebnih in neosebnih podatkov. S strategijo je EU podatke začel obravnavati v luči digitalizacije, zaradi česar se je področje urejanja nekoliko razširilo v smer digitalnih trgov in storitev, umetne inteligence in kibernetske varnosti. Posledica razširitve je tako številčna kot vsebinska obsežnost sprejetih predpisov, s tem pa tudi občutek razdrobljenosti urejanja področja. Pričakovati bi bilo, da bi obširna prizadevanja EU-ja zagotovila vseobsežno ureditev, vendar pa sta uporaba že sprejetih predpisov in medsektorsko usklajevanje predpisov, ki so še v fazi predloga, že izpostavila še

odprta pomembna vprašanja.

Prvi izziv, s katerim se ga bo moral EU še dodatno ukvarjati, je vprašanje kolizije določb o varstvu podatkov in spodbujanju njihove uporabe v pridobitne namene. Podatki so namreč kot osnovni gradnik prisotni tako na področju spodbujanja gospodarskega napredka kot umetne inteligence, hkrati pa se z vzponom naprednih tehnologij, kot sta umetna inteligenca in internet stvari, povečuje potreba po zaščiti pred zlorabami podatkov, varstvu zasebnosti, kibernetski varnosti ter po zaupanja vrednih in etičnih praksah uporabe podatkov. Kljub že sprejetim evropskim predpisom na področju varstva zasebnosti in kibernetske varnosti bo potrebno stalno spremljanje morebitnih zlorab in nadgrajevanje varnostnih mehanizmov.

Zasebni sektor ob tem opozarja na nepreglednost regulativnega okolja, saj so zaradi velikega števila pravnih aktov stroški zagotavljanja skladnosti v nekaterih sektorjih že sedaj visoki.[28] Med nekaterimi akti za uresničevanje podatkovne strategije je možno tudi prekrivanje obveznosti in pristojnosti. Akti namreč za različne vrste podatkov predvidevajo različne postopke v zvezi z varstvom, obdelavo in ponovno uporabo, za katere so lahko pristojne tudi različne nacionalne in evropske organizacije. Pri tem meje pristojnosti posameznih organov niso v celoti določene. Imetniki podatkov imajo v svojih podatkovnih bazah pogosto zajete tako osebne kot neosebne podatke, zato ni vedno povsem jasno, katera pravila so uporabljiva za posamezen sklop podatkov, hkrati pa so možna tudi nasprotujoča si mnenja posameznih pristojnih organizacij. Ta pravna negotovost lahko negativno vpliva na razvoj poslovnih modelov podatkovnega gospodarstva. Na to negotovost še dodatno vpliva dejstvo, da se je sprejemanje nekaterih aktov, ki bi morali kot komplementarni akti delovati v sinergiji z že sprejetimi, upočasnilo oziroma ustavilo.

Da bi se odpravila razdrobljenost regulativnega okolja, so akti večinoma sprejeti v obliki neposredno uporabljivih uredb, ki pa od držav članic implicitno zahtevajo sprejetje izvedbenih predpisov ter ustanovitev oziroma imenovanje nacionalnih organov za njihovo izvajanje. Akti ob tem niso povsem določni glede posameznih izvedbenih vsebin, kar prinaša tveganje za nadaljnje

neenotne prakse držav članic.

Ob vsem tem je v EU-ju še vedno prisotna določena mera digitalne neenakosti, saj porazdeljenost digitalnih veščin državljanov in gospodarstva v evropskem prostoru ni enakomerna. To povzroča tako ovire prostega pretoka podatkov kot neuravnoteženost koristi. EU se ob tem še vedno sooča tudi z nezadostno tehnološko suverenostjo.

Ideja EU-ja o podatkih kot peti svoboščini (poleg osnovnih štirih: prosti pretok blaga, storitev, oseb in kapitala) je tako dobrodošla, vendar pa glede na to, da so akterji na svetovnem trgu v časovni prednosti in da jim ohlapnejše zahteve po varstvu osebnih podatkov omogočajo večjo svobodo, njeno uresničevanje nekoliko zaostaja.

4. LITERATURA

1. Komisija Evropskih skupnosti (2020, 19. februar). *Evropska strategija za podatke*. COM(2020) 66 final. Sporočilo Evropske komisije Evropskemu parlamentu in Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij. Bruselj: Komisija Evropskih skupnosti, 2020.
2. Direktiva 2009/136/ES Evropskega parlamenta in Sveta o spremembah Direktive 2002/22/ES o univerzalnih storitvah in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov. UL L 337, 25. november 2009.
3. Uredba (EU) 2016/679 Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES. UL L 119, 27. april 2016.
4. Direktiva (EU) 2019/1024 Evropskega parlamenta in Sveta o odprtih podatkih in ponovni uporabi informacij javnega sektorja. UL L 172, 20. junij 2019.
5. Uredba (EU) 2018/1807 Evropskega parlamenta in Sveta o

okviru za prosti pretok neosebnih podatkov v Evropski uniji. UL L 303, 14. november 2018.
6. Direktiva 2009/136/ES Evropskega parlamenta in Sveta o spremembah Direktive 2002/22/ES o univerzalnih storitvah in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov. UL L 337, 25. november 2009.
7. Izvedbeni sklep Evropske komisije (EU) 2021/914 o standardnih pogodbenih določilih za prenos osebnih podatkov v tretje države v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta. UL L 199, 4. junij 2021.
8. Izvedbena uredba Evropske komisije (EU) 2023/138 o določiti seznama posebnih naborov podatkov velike vrednosti ter ureditve za njihovo objavo in ponovno uporabo. UL L 19, 21. december 2022.
9. Uredba (EU) 2022/868 Evropskega parlamenta in Sveta o evropskem upravljanju podatkov in spremembi Uredbe (EU) 2018/1724. UL L 15, 30. maj 2022.
10. Uredba (EU) 2022/1925 Evropskega parlamenta in Sveta o tekmovalnih in pravičnih trgih v digitalnem sektorju in spremembi direktiv (EU) 2019/1937 in (EU) 2020/1828. UL L 265, 14. september 2022.
11. Uredba (EU) 2022/2065 Evropskega parlamenta in Sveta o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES. UL L 277, 19. oktober 2022.
12. Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148. UL L 333, 14. december 2022.
13. Uredba (EU) 2022/1925 Evropskega parlamenta in Sveta o tekmovalnih in pravičnih trgih v digitalnem sektorju in spremembi direktiv (EU) 2019/1937 in (EU) 2020/1828. UL L 265, 14. september 2022.
14. Direktiva 2000/31/ES Evropskega parlamenta in Sveta o nekaterih pravnih vidikih storitev informacijske družbe, zlasti

elektronskega poslovanja na notranjem trgu. UL L 178, 8. junij 2000.
15. Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148. UL L 333, 14. december 2022.
16. Evropska komisija (2022, 23. februar). Predlog Uredbe Evropskega parlamenta in Sveta o harmoniziranih pravilih za pravičen dostop do podatkov in njihovo uporabo. COM(2022) 68 final.
17. Evropska komisija (2022, 18. november). Predlog Uredbe Evropskega parlamenta in Sveta o določitvi ukrepov za visoko raven interoperabilnosti javnega sektorja v Uniji. COM(2022) 720 final.
18. Evropska komisija (2021, 21. april). Predlog Uredbe Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci. COM(2021) 206 final.
19. Evropska komisija (2022, 3. maj). Predlog Uredbe Evropskega parlamenta in Sveta o evropskem zdravstvenem podatkovnem prostoru. COM(2022) 197 final.
20. *Digital Europe: Data Transfers in the Data Strategy: Understanding Myth and Reality*. Najdeno 13. junija 2023 **na spletnem naslovu**.

Opombe

* Alenka Blas, univ. dipl. pravnica, državna revizorka, pomočnica vrhovnega državnega revizorja na Računskem sodišču Republike Slovenije, **alenka.blas@rs-rs.si**. Ruti Rous, univ. dipl. pravnica, državna revizorka, pomočnica vrhovnega državnega revizorja na Računskem sodišču Republike Slovenije, **ruti.rous@rs-rs.si**. Prispevek izraža izključno mnenje in stališče avtoric in ne institucije, pri kateri sta avtorici zaposleni.

1. Zaradi količine in obsega evropske zakonodaje so v prispevku predstavljeni le najpomembnejši horizontalni akti, ki veljajo v vseh sektorjih. Pri tem opozarjamo, da je na evropski ravni še vrsta drugih predpisov, ki vplivajo na področje izvrševanja strategije in so bodisi starejšega datuma bodisi sektorske narave ter v tem prispevku niso predstavljeni.
2. Evropska strategija za podatke je bila sprejeta v obliki Sporočila

Evropske komisije Evropskemu parlamentu in Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij (COM(2020) 66 final, 19. 2. 2020).

3. Direktiva 2009/136/ES.
4. Uredba EU 2016/679.
5. Direktiva EU 2019/1024.
6. Uredba EU 2018/1807.
7. Zlasti v avtomobilskem sektorju (Uredba ES 715/2007, spremenjena z Uredbo ES595/2009), na področju plačilnih storitev (Direktiva EU 2015/2366) in energetike (Direktiva EU 2019/944 za električno energijo in Direktiva 2009/73/ES za plinomere).
8. Na primer Uredba EU 2019/881.
9. Na primer Direktiva EU 2019/770.
10. Izvedbeni sklep Evropske komisije (EU) 2021/914.
11. Izvedbena uredba Evropske komisije (EU) 2023/138.
12. Gre za storitve zbiranja, urejanja, shranjevanja (v oblaku), spreminjanja, uporabe, razširjanja, kombiniranja, obdelave in izbrisa elektronskih podatkov.
13. Uredba EU 2022/868.
14. Uredba EU 2022/1925.
15. Uredba EU 2022/2065.
16. Direktiva EU 2022/2555.
17. Med jedrne platformne storitve po uredbi spadajo: spletne posredniške storitve; spletni iskalniki; spletne storitve družbenega mreženja; storitve platform za izmenjavo videov; medosebne komunikacijske storitve, neodvisne od številke; operacijski sistemi; spletni brskalniki; virtualni pomočniki; storitve računalništva v oblaku; storitve spletnega oglaševanja.
18. Letni promet, ki je enak ali višji od 7,5 milijarde EUR, ali njegova enakovredna pravična tržna vrednost v zadnjem poslovnem letu znaša najmanj 75 milijard EUR.
19. 45 milijonov mesečno aktivnih končnih uporabnikov in vsaj 10.000 letno aktivnih poslovnih uporabnikov s sedežem v Uniji.
20. Vratar na primer ne sme zahtevati, da bi poslovni uporabnik na njegovi platformi izdelke ponujal pod enakimi ali ugodnejšimi pogoji kot na drugih platformah, ne sme jim pogodbeno prepovedati reševanja sporov pred sodišči oziroma organi EU-ja, od uporabnikov ne sme zahtevati, da uporabljajo njegove aplikacije ali da zagotovijo interoperabilnost z njegovimi aplikacijami, in podobno.
21. Direktiva 2000/31/ES.
22. Predlog COM (2022) 68 final.
23. Predlog COM (2022) 720 final.
24. Predlog COM (2021) 206 final.
25. Predlog COM (2022) 197 final.
26. Gre za fizične izdelke (vozila, naprave za dom, medicinske in

zdravstvene pripomočke, kmetijske in industrijske stroje), ki prek svojih komponent pridobivajo, ustvarjajo ali zbirajo podatke v zvezi s svojo uporabo, delovanjem ali okoljem (digitalizacija dejanj in dogodkov uporabnikov) in ki imajo možnost te podatke sporočati po javno dostopni elektronski komunikacijski storitvi (različna omrežja).

27. Evropska strategija za podatke, str. 3.
28. **Spletni naslov**.

Mag. Matjaž Štiglic*

Revidiranje skladnosti hrambe gradiva v digitalni obliki z Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA)

Auditing the compliance of digital document preservation with the Protection of documents and archives and archival institutions act (ZVDAGA)

POVZETEK ● *Revizorji so z rednimi pregledi elektronske*

hrambe zelo pomemben institut zagotavljanja varne in zakonsko skladne elektronske hrambe dokumentov, saj je pri taki hrambi nadvse pomembno, da sta dolgoročno zagotovljeni veljavnost in dokazna vrednost elektronskih dokumentov. V prispevku je na začetku nekaj splošnih informacij o pomenu varstva dokumentarnega gradiva, nato je povzeta osnovna zakonodaja na tem področju, ki vzpostavlja okvir zakonsko skladne elektronske hrambe. V nadaljevanju opredeljujemo vrste revizijskega posla, ki jih revizor lahko opravi pri revidiranju skladnosti z ZVDAGA-jem. Osrednji del prispevka je osredotočen na ustrezno pripravo revizijskega posla, ki mora postaviti dobre temelje tako za razumevanja problemskega področja kot za učinkovito in sistematično izvedbo revizijskega dela.
Ključne besede ● *revizor informacijskih sistemov, revizijski posel, kontrole, ZVDAGA, UVDAGA, PETZ, MoReq*
SUMMARY ● *IT Auditors, through regular audits of digital document preservation, play an exceptionally important institution in ensuring secure and legally compliant electronic document retention. In electronic document storage, it is crucial that their long-term validity and evidentiary value are guaranteed. In the article's introduction, we provide some general information about the importance of protecting documentary materials and briefly summarize the basic legislation in this area that establishes the framework for legally compliant electronic storage. In the continuation of the article, we define the types of audit tasks that an auditor can perform as part of auditing compliance with the Protection of Documents and Archives and Archival Institutions Act (ZVDAGA). The central part of the article focuses on the proper preparation of the audit work, which must lay a solid foundation for understanding the problem area and enable the auditor to conduct the audit work effectively and systematically.*
Key words ● *Information systems auditor, IS audit, controls, Protection of Documents and Archives and Archival institutions Act (ZVDAGA), Decree on the Protection of Documentary and Archive Material (UVDAGA), Rules on Uniform Technological Requirements for Capture and Storage of Materials in Digital Form (PETZ), MoReq*

JEL: K 24, M 42

1. UVOD

Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA) pomeni pravno ureditev celotnega področja elektronske hrambe, ki je z leti čedalje pomembnejše. Vse več organizacij želi hraniti svoje dokumente elektronsko, kar omogoča prihranek virov pri obvladovanju papirne dokumentacije, hkrati pa organizacije pričakujejo pravno veljavnost svojih elektronsko shranjenih dokumentov med hrambo. Revizorji so z rednimi pregledi elektronske hrambe zelo pomemben institut zagotavljanja varne in zakonsko skladne elektronske hrambe.

2. O VARSTVU DOKUMENTARNEGA GRADIVA

Varstvo gradiva je pomembno področje, ki se nanaša na zaščito in ohranjanje različnih vrst dokumentarnega gradiva; mednje se štejejo tudi pisni oziroma tiskani dokumenti, fotografije, filmi, avdio- in videoposnetki ter spletne strani. Cilj varstva gradiva je zagotoviti, da so dokumenti varni, ohranjeni in dostopni tako za sedanje kot tudi prihodnje generacije. Ena od ključnih dejavnosti na področju varstva gradiva je ustrezno shranjevanje in upravljanje gradiva. Dokumenti morajo biti hranjeni varno in primerno, tako da je zagotovljena njihova ohranjenost. Pomembno je, da so dokumenti ustrezno označeni in organizirani, da jih je mogoče enostavno najti in uporabiti. Drugo pomembno področje varstva gradiva je zagotavljanje dostopa do dokumentov za različne namene, kot so poslovi nameni, raziskovanje, izobraževanje, administrativni in pravni postopki ter drugo. Pri tem je pomembno upoštevati zakonske omejitve dostopa do nekaterih vrst dokumentov, kot so na primer osebni podatki in zaupne informacije.

Organizacijam lahko elektronska hramba gradiva prinese številne prednosti, kot so prihranek prostora, lažje iskanje in uporaba dokumentov, večja varnost in trajnost dokumentov ter možnost enostavnega varnostnega kopiranja, po drugi strani pa se pri

hranjenju gradiva v elektronski obliki pojavljajo številni izzivi in vprašanja. Naj naštejemo nekaj pomembnejših:

- ena od ključnih težav je zagotavljanje dolgoročne ohranjenosti in dostopnosti dokumentov; elektronski mediji imajo omejen rok trajanja, zato je pomembno zagotoviti ustrezno varnostno kopiranje in obnovo podatkov ob okvari ali izgubi podatkov v primarni elektronski hrambi;
- druga pomembna težava je zagotavljanje zakonske skladnosti; pri elektronski hrambi je pomembno upoštevati zakonske zahteve za varstvo podatkov, dostopnost, hrambo, arhiviranje in obdelavo;
- organizacije morajo upoštevati tudi zahteve za ohranjanje različnih vrst dokumentov z različnimi zakonskimi roki hrambe, kot so na primer davčni dokumenti, pogodbe, osebni podatki in drugi;
- nadalje je pri hranjenju gradiva v elektronski obliki pomembno zagotavljanje ustrezne organiziranosti in označevanja dokumentov; dokumenti morajo biti ustrezno shranjeni in razvrščeni, da jih je mogoče enostavno najti in uporabiti;
- pomembno je tudi zagotoviti ustrezne varnostne ukrepe, kot so gesla, šifriranje in druge, ki zagotavljajo varnost in zaupnost podatkov.

3. PRAVNA PODLAGA UREDITVE ELEKTRONSKE HRAMBE

Na področju hranjenja gradiva v elektronski obliki obstaja več standardov in smernic, ki pomagajo pri oblikovanju praks in politik za upravljanje gradiva. Med njimi so na primer standardi ISO 15489, ki določajo smernice za upravljanje gradiva, družina standardov ISO /IEC 27000, ki določa smernice za upravljanje informacijske varnosti, v Republiki Sloveniji pa je še posebej priljubljena specifikacija MoReq, na kateri temeljijo tudi slovenska zakonodaja ter zahteve glede organizacije in upravljanja elektronske hrambe dokumentov.

Dokazna vrednost in pravna veljava e-dokumentov je bila v Republiki Sloveniji deloma urejena že v Zakonu o elektronskem poslovanju in elektronskem podpisu[1] (ZEPEP, 2004), vendar pa sta bila tako ta zakon kot tudi Zakon o arhivskem gradivu in

arhivih[2] (ZAGA,1997) pomanjkljiva z vidika urejanja postopkov in pogojev hrambe elektronskih dokumentov. Danes so osnovna pravna podlaga e-hrambe v Sloveniji:

- Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih[3] (ZVDAGA, 2006) ter Zakon o spremembah in dopolnitvah Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih[4] (ZVDAGA-A, 2014) – zakon določa pravila in obveznosti za ravnanje z gradivom, ki nastaja pri delu organov javne uprave, sodišč, državnih tožilstev, državnih organov, organov lokalnih skupnosti in drugih organizacij javnega in zasebnega sektorja, ter za ravnanje z arhivskim gradivom, ki ima trajno vrednost in se ga ne sme uničiti; v zakonu so določene obveznosti in odgovornosti organov in organizacij, ki so zadolžene za varstvo in upravljanje tega gradiva, ter zagotovljena pravica do dostopa do arhivskega gradiva;
- Uredba o varstvu dokumentarnega in arhivskega gradiva[5] (UVDAGA, 2017), v kateri je opredeljena podrobnejša ureditev elektronske hrambe na podlagi notranjih pravil;
- Pravilnik o enotnih tehnoloških zahtevah za zajem in hrambo gradiva v digitalni obliki[6] (PETZ, 2020), v katerem so navedene podrobne organizacijske in tehnološke zahteve za elektronsko hrambo.

4. REVIDIRANJE PO ZVDAGA-JU

Zaradi zagotavljanja dolgoročne uporabnosti, dostopnosti in varnosti dokumentarnega gradiva je treba redno preverjati postopke, kontrole in seveda celotno infrastrukturo, na kateri temelji elektronska hramba gradiva. Pri poslih revidiranja skladnosti z ZVDAGA-jem gre lahko za dve različni vrsti revizijskega posla:

- revidiranje skladnosti programske opreme, ki se uporablja za zajem in elektronsko hrambo gradiva;
- revidiranje skladnosti storitve zajema in hrambe gradiva v digitalni obliki, ki temelji na sprejetih notranjih pravilih.

Prva je manj pogosta in se običajno izvaja pri ponudnikih

programske opreme, ki se uporablja za elektronsko hrambo. Revidiranje zajema in elektronske hrambe gradiva pa je pogostejše, saj bi bilo vsaj teoretično nujno za vsako organizacijo, ki svoje gradivo hrani elektronsko, in dolgoročno pričakuje pravno veljavnost in dokazno vrednost tako hranjenega gradiva.

Priprava in izvedba revizijskega posla je zelo zahtevna in pomembna naloga, saj mora revizijski posel poleg odgovorov o zanesljivosti, učinkovitosti in varnosti elektronsko hranjenega gradiva podati tudi mnenje o zakonski skladnosti hranjenja zaradi zagotavljanja dolgoročne verodostojnosti in veljavnosti gradiva.

Načrtovanje revizijskega posla je ključna faza v celotnem postopku revidiranja, ki strokovnjaku revidiranja informacijskih sistemov, v nadaljevanju ga bomo kratko poimenovali revizor, omogoča učinkovito in sistematično izvajanje revizijskega dela. Tako pri izvedbi kot tudi pri načrtovanju revizijskega posla mora revizor najprej upoštevati *Hierarhijo pravil revidiranja informacijskih sistemov*, ki od njega zahteva, da poleg zakonskih podlag pri svojem delu upošteva še standarde, smernice ter orodja in tehnike za strokovnjake revidiranja kontrol in dajanja zagotovil na področju informacijske tehnologije.

Načrtovanje revizijskega posla zagotavlja strukturiran pristop k prepoznavanju ciljev revizije, določanju obsega, ocenjevanju tveganj ter izbiri ustrezne metodologije in pristopa za dosego teh ciljev. Splošni elementi, ki jih mora revizor opredeliti pri pripravi revizorskega posla, so predpisani v *Okviru strokovnega ravnanja za dajanje zagotovil in revidiranja informacijskih sistemov*[7] ITAF™ (angl. A Professional Practices Framework for IS Audit/Assurance). Sledi nekaj osnovnih korakov oziroma področij, ki jih mora revizor skrbno načrtovati in uskladiti z naročnikom pred izvedbo samega revizijskega posla:

- **Osnovne informacije**: Pridobimo osnovne informacije o organizaciji (naročniku posla) ter programski opremi, ki se uporablja za elektronsko hrambo.
- **Cilji:** Jasno opredelimo cilje revizije, kot je ocena učinkovitosti, varnosti in skladnosti elektronske hrambe z zakonodajo. Pri reviziji skladnosti z ZVDAGA-jem je v

ospredju skladnost hrambe in/ali programske opreme s predpisi na področju hrambe dokumentarnega in arhivskega gradiva v elektronski obliki, pri čemer je največji poudarek na zagotavljanju varnosti hranjenega gradiva.

- **Obseg:** Revizor naj določi meje revizije, vključno z moduli, komponentami in postopki, ki bodo pregledani. Opredeliti je treba morebitne izključitve ali omejitve v obsegu revizije.
- **Vrsta revizijskega posla:** Jasno je treba opredeliti obliko revizijskega posla, pri čemer izbiramo med pregledom in revizijo. Izvedba posla se pri obeh vrstah izvaja podobno, vendar revizija zagotavlja višjo raven zagotovila o učinkovitosti kontrolnih postopkov, seveda pa zahteva tudi več virov za izvedbo.
- **Sodila:** Sodila, ki so revizorjeva večna dilema pri odločanju o učinkovitosti delovanja kontrol, so v našem primeru jasna. Ker gre za revizijske posle preverjanja skladnosti z ZVDAGA-jem, so običajno sodila zakonski predpisi s področja varne hrambe dokumentarnega in arhivskega gradiva, dopolnjena s standardi in okviri dobrih praks na področju informacijske varnosti.
- **Metodologija revizije:** Revizor naj opredeli pristop k revizijskemu poslu, ki lahko vključuje kombinacijo intervjujev, pregledov dokumentacije, ogledov sistema in preizkušanja, pripravi način zbiranja dokazov in način ocenjevanja dokazov glede na določene kriterije.
- **Revizijski tim:** Revizor določi člane tima za revizijski posel in njihove vloge (na primer vodja revizije, tehnični strokovnjak, strokovnjak za skladnost). Pri tem poskrbimo, da ima tim ustrezno znanje in veščine za učinkovito ocenjevanje področja revizije.
- **Urnik revizije:** Revizor izdela časovnico za pripravo in izvedbo revizijskega posla, vključno s planiranjem, terenskim delom, analizo in poročanjem. Pri tem je pomembno, da dodeli dovolj časa za vsako fazo glede na vrsto revizijskega posla ter ga uskladi z revidirancem.
- **Postopki revizije:** Podrobno opišemo specifične korake in postopke, ki jih bo treba upoštevati med revizijo, na primer:
- pregled dokumentacije, politik in postopkov v zvezi z elektronsko hrambo;
- izvedba intervjujev z odgovornimi osebami;
- ocena arhitekture sistema elektronske hrambe, preverba

upravljanja nadzora dostopa in drugih varnostnih mehanizmov;
- izvedba preizkusa sistema, da se preverijo implementirana funkcionalnost in varnostni ukrepi;
- analiza skladnosti z ustreznimi predpisi in standardi;
- prepoznava morebitnih tveganj in ranljivosti v upravljanju elektronske hrambe;
- preverba postopkov varnostnega kopiranja podatkov in obnovitve ob nesreči.
- **Zbiranje in analiza podatkov:** Opišemo, kako se bodo podatki zbirali, organizirali in analizirali med izvajanjem revizijskega posla. Pripravimo morebitna orodja in tehnike, ki se bodo uporabljale za analizo podatkov.
- **Ocenjevanje tveganj:** Revizor mora prepoznati in oceniti morebitna tveganja na področju revizijskega posla, npr. kršitve varnosti, izguba podatkov ali neskladnost. Tveganja razvrstimo glede na njihov potencialni vpliv na varnost gradiva in verjetnost pojavitve.
- **Ugotovitve in priporočila:** Opišemo postopek dokumentiranja ugotovitev, vključno z odstopanji od kriterijev revizijskega posla, pozitivnimi opažanji in navedbo področij za izboljšave. Naročniku pripravimo in predstavimo okvir za oblikovanje praktičnih in izvedljivih priporočil.
- **Poročanje:** Pojasnimo, kako bodo rezultati zaključenega revizijskega posla združeni v celovito poročilo. Določimo strukturo, vsebino in obliko poročila. Navedemo ciljno občinstvo poročila.
- **Spremljanje in korektivni ukrepi**: Opišemo postopek za spremljanje izvajanja priporočil v organizaciji ter določimo časovni okvir in odgovornosti za korektivne ukrepe.
- **Zaključek:** Povzamemo ključne točke načrta revizijskega posla. Poudarimo pomembnost preglednosti v timu, ki bo izvedel revizijski posel, in sodelovanja z naročnikom.
- **Odobritev in komunikacija:** Opisati je treba korake ustreznih deležnikov za pridobitev odobritve načrta revizijskega posla. Pojasnimo, kako se bo načrt posredoval vodstvu organizacije in ustreznim osebam. Načrt je treba prilagoditi glede na posebne značilnosti in potrebe sistema za upravljanje dokumentov ter naročnika.

5. ZAKLJUČEK

V zadnjem času se čedalje več organizacij odloča za elektronsko hrambo gradiva, saj to omogoča prihranek virov pri obvladovanju papirne dokumentacije in pohitritev postopkov hrambe in iskanja gradiva. Eden ključnih problemom elektronske hrambe gradiva je varnost gradiva in dolgoročno ohranjena pravna in dokazna vrednost gradiva.

Republika Slovenija je zakonodajno uredila področje elektronske hrambe gradiva, in sicer z učinkovitim okvirom zahtev, ki ob njihovem izpolnjevanju zagotavlja dolgoročno varno in zakonsko skladno elektronsko hrambo gradiva.

Revizorji smo z rednimi pregledi elektronske hrambe že danes pomemben deležnik v celotnem sistemu elektronskega poslovanja in seveda tudi elektronske hrambe gradiva. Želimo pa si, da bi našo vlogo prepoznale vse organizacije, ki hranijo svoje dokumente v elektronski obliki. Glede na pomen revidiranja elektronske hrambe in seveda tudi glede na pomen mnenja o njeni skladnosti z zakonodajo je treba vsak revizijski posel na tem področju še pred izvedbo skrbno pretehtati in ustrezno načrtovati. Revizor se mora zavedati svoje odgovornosti pri opredeljevanju glede skladnosti elektronske hrambe z veljavno zakonodajo.

6. LITERATURA IN VIRI

1. Hajtnik, T. (2016). *Celovit pristop k pretvorbi elektronskih dokumentov v obliko za dolgoročno hrambo*. Doktorska disertacija. Maribor: Univerza v Mariboru, Fakulteta za elektrotehniko računalništvo in informatiko.
2. Hierarhija pravil revidiranja informacijskih sistemov. *Uradni list RS*, št. 40/2011.
3. ISACA. (2014). *Okvir strokovnega ravnanja za dajanje zagotovil revidiranje IS – ITAF™*, 3. izdaja. Slovenski prevod. Ljubljana: Slovenski odsek ISACA.
4. Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih. *Uradni list RS*, št. 30/06 in 51/14.
5. Uredba o varstvu dokumentarnega in arhivskega gradiva. *Uradni list RS*, št. 42/17.
6. Pravilnik o enotnih tehnoloških zahtevah za zajem in hrambo

gradiva v digitalni obliki. *Uradni list RS*, št. 118/20.

Opombe

* Matjaž Štiglic, magister znanosti, preizkušeni revizor informacijskih sistemov, Informis, d. o. o, matjaz.stiglic@informis.si.

1. Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT, 46/14, 121/21 – ZEISZ in 130/22 – ZN-H.
2. Uradni list RS, št. 20/97, 32/97 – popr., 24/03 – ZDIJZ in 30/06 – ZVDAGA.
3. Uradni list RS, št. **30/06**.
4. Uradni list RS, št. **51/14**.
5. Uradni list RS, št. 42/17.
6. Uradni list RS, št. **118/20**.
7. **Spletna stran**.

Mitja Trampuž*

Artificial Intelligence and Projects in Slovenia

Umetna inteligenca in projekti v Sloveniji

POVZETEK ● *Umetna inteligenca (UI) lahko preoblikuje poslovanje v Sloveniji. Lahko se uporablja za izboljšanje učinkovitosti, storilnosti, storitev za stranke in upravljanje tveganj. Slovenija ima številne priložnosti za uporabo umetne inteligence v svojo korist, na primer pri analizi podatkov, odkrivanju goljufivega poslovanja in upravljanju oskrbnih verig. Organizacije v Sloveniji morajo biti pripravljene sprejeti UI, da bi ostale konkurenčne. Pri uvajanju UI se podjetja*

soočajo z izzivi, kot so potreba po novih veščinah in virih, nevarnost pristranskosti in pomanjkanje regulative. Poleg tega morajo organizacije upoštevati še varnostne izzive umetne inteligence ter sprejeti ustrezne ukrepe za zaščito svojih podatkov in sistemov. Slovenske organizacije, ki želijo uspešno uvesti UI, morajo te izzive obravnavati z vlaganjem v usposabljanje zaposlenih, zbiranje in čiščenje podatkov, ustrezno varovanje podatkov in sistemov umetne inteligence ter razvijanje etičnih praks UI. Na področju uvajanja umetne inteligence je zaradi dostopa do financiranja in virov iz EU-ja veliko priložnosti za slovenske organizacije. S sestavljanjem pravih veščin, tehnologij in virov si slovenska podjetja lahko pridobijo položaj za uspešno uvedbo umetne inteligence v redno poslovanje.
Ključne besede ● *umetna inteligenca, revizijske institucije, EUROSAI, učinkovitost, storilnost, odločanie, delovna skupina za informacijsko tehnologijo – ITWG, sodelovanje*
SUMMARY ● *Artificial intelligence (AI) can potentially transform Slovenia's business landscape. AI can improve efficiency, productivity, customer service, and risk management. Slovenia has several opportunities to use AI to its advantage, such as in data analysis, fraud detection, and supply chain management. Businesses in Slovenia need to be prepared to adopt AI to remain competitive. The adoption of AI in Slovenia is facing challenges, such as the need for new skills and resources, the potential for bias, and the lack of regulation. In addition, businesses need to be aware of the cybersecurity risks that AI can pose and take steps to protect their data and systems. Slovenian organizations that want to adopt AI must address these challenges by investing in training, collecting and cleaning data, securing data and AI systems, and developing ethical AI practices. There are also opportunities for Slovenian organizations aiming to adopt AI, such as access to funding and resources from the EU. By assembling the right skills, technologies, and resources, Slovenian organizations can position themselves to adopt AI successfully*
Key words ● *artificial intelligence, audit institutions, EUROSAI, efficiency, productivity, decision-making, information technology working group (ITWG), cooperation*

JEL: K 24

1. INTRODUCTION

Artificial intelligence (AI) is a rapidly evolving technology that profoundly impacts many industries, including small businesses. AI can be used to improve efficiency, increase productivity, reduce costs, and gain a competitive advantage.

The adoption of AI in Slovenia has been slow due to several challenges, including:

- Lack of understanding of AI
- Lack of skills and resources
- Concerns about the impact of AI on jobs

However, Slovenian organizations also have several opportunities to use AI to their advantage. These opportunities include:

- Improving efficiency: AI can be used to automate tasks, identify patterns, and make predictions, all of which can help to improve efficiency.
- Increasing productivity: AI can free up human workers to focus on more creative and strategic tasks, leading to increased productivity.
- Reducing costs: AI can reduce costs by automating tasks, optimizing processes, and improving decision-making.
- Gaining competitive advantage: AI can help Slovenian companies to differentiate themselves from their competitors by offering more personalized products and services, improving customer service, and developing new products and services.
- Mitigation of risks: AI can be used to analyse large amounts of data to identify patterns and trends that may indicate risks. AI can also be used to make predictions about the likelihood of risks occurring and the impact they may have. This information can be used to take steps to mitigate risks, such as implementing controls or developing contingency plans.

2. ESSENTIAL PILLARS OF AI ADOPTION

Four key pillars are essential for the successful adoption of AI in business:

1. Organization culture: An organization culture that embraces change and innovation is essential for successfully adopting AI. Employees must be open to new ideas and willing to learn new skills. This means creating a culture where employees feel comfortable asking questions, taking risks, and making mistakes. It also means providing employees with the resources to learn about AI and how to use it.
2. Human resources: Adequate skills and resources are needed to develop and deploy AI solutions. Organizations need to invest in training their employees on AI and ensure they have the right tools and infrastructure. This includes investing in AI software, hardware, and data storage. It also means investing in training programs that will teach employees how to use AI tools and techniques.
3. Data: High-quality data is essential for the success of AI-powered businesses. Organizations need to collect and clean their data to be used to train AI models. This means ensuring that the data is accurate, complete, and up-to-date. It also means removing any bias or noise from the data.
4. Infrastructure: The proper infrastructure, including hardware, software, and networking, is needed to support AI-powered businesses. Organizations must have the appropriate infrastructure to store and process large amounts of data. They also need to ensure they have the proper security measures to protect their data.

In addition to these four pillars, a few other factors can contribute to the successful adoption of AI in business. These include:

- Leadership support: Executive leadership must support AI adoption and provide the resources needed to make it happen.
- A clear vision: Organizations need to have a clear vision for how they plan to use AI to achieve their business goals.
- A phased approach: AI adoption should start with small pilot projects and scale up as the company gains experience.
- Continuous learning: Organizations must be committed to continuously learning about AI and how to use it effectively.

Businesses can increase their chances of successful AI adoption by addressing these factors.

3. CREATING A "CONTRACT" BETWEEN THE PROPONENT OF THE IMPLEMENTATION OF AN AI SOLUTION AND MANAGEMENT

A business case is a document that outlines why an organization should invest in a particular project or initiative. A good business case will clearly articulate the benefits of the investment, as well as the costs. Therefore, it is a "contract" between the proponent of implementing an AI solution and management and a guide in developing and deploying the solution.

In the case of AI, the business case should identify the specific benefits AI can deliver to the organization. These benefits can include:

- Increased efficiency: AI can automate tasks currently done manually, freeing up employees to focus on more strategic work. This can lead to increased efficiency and productivity.
- Improved accuracy: AI can improve decision-making accuracy by analysing large amounts of data and identifying patterns that humans might miss. This can lead to reduced errors and improved outcomes.
- Reduced risk: AI can identify and mitigate risks like fraud or cyberattacks. This can help to protect the organization's assets and reputation.
- New revenue opportunities: AI can be used to develop new products and services or to improve existing ones. This can lead to new revenue opportunities for the organization.

In addition to identifying the benefits of AI, the business case should also identify the costs of implementing and maintaining AI solutions. These costs can include (1) the cost of acquiring AI software and hardware, (2) the cost of training employees on AI, (3) the cost of data collection and cleaning, and (4) the cost of ongoing maintenance and support. By carefully considering the benefits and costs of AI, businesses can create a robust business case that justifies the investment.

Some additional tips for creating a robust business case for AI:

- Be specific about the benefits that AI can deliver. Don't just say that AI will "improve efficiency." Instead, say how much time and money AI can save the company.
- Quantify the benefits of AI whenever possible. This will make the business case more persuasive.
- Use real-world examples to illustrate the benefits of AI. This will help to make the business case more credible.
- Get input from stakeholders throughout the process. This will help to ensure that the business case is comprehensive and well-considered.

By following these tips, businesses can create a robust business case to help them make informed decisions about AI adoption.

4. SELECTING THE RIGHT USE CASES

When selecting suitable AI use cases, it is essential to consider the following factors:

- The organization's goals: What are the organization's short-term and long-term goals? How can AI help the organization achieve those goals?
- The organization's resources: What resources does the organization have available? This includes financial resources, human resources, and data.
- The organization's culture: Is the organization open to change and innovation? Is there a culture of learning and experimentation?
- The maturity of the AI technology: How mature is the AI technology that is being considered? Is it ready for use in a production environment?
- The risks and benefits: What are the risks and benefits of using AI in this use case?
- Once these factors have been considered, the organization can start to identify potential AI use cases. Some possible use cases for AI in Slovenian companies include:
    - Data analysis: AI can analyse large amounts of data to identify patterns and trends. This can help businesses to

make better decisions, improve customer service, and develop new products and services. For example, an insurance organization could use AI to analyse claims data to identify fraud patterns.
- Fraud detection: AI can be used to detect fraudulent transactions. This can help businesses to protect themselves from financial losses. For example, a bank could use AI to detect fraudulent credit card transactions.
- Risk assessment: AI can be used to assess risk, such as the risk of a customer defaulting on a loan. This can help businesses to make better lending decisions. For example, a mortgage lender could use AI to assess the risk of a borrower defaulting on a mortgage.
- Customer service: AI can provide customer service by answering questions and resolving problems. This can help businesses to improve customer satisfaction. For example, a customer service chatbot could answer customer questions about products or services.
- Supply chain management: AI can be used to optimize supply chains, such as by identifying inefficiencies and reducing costs. For example, a logistics company could use AI to optimize the routing of deliveries.

These are just a few examples of potential AI use cases for Slovenian organizations. The specific use cases that are most appropriate will vary depending on the individual organization's goals, resources, and culture.

It is also important to note that AI is a rapidly evolving technology. As AI technology develops, new and innovative use cases will emerge. Businesses should be open to exploring new AI use cases as they become available.

5. THE FUTURE OF AI IN SLOVENIA

Artificial intelligence (AI) can potentially transform Slovenia's business landscape. By embracing AI, Slovenian organizations can improve their products and services, enter new markets, and gain a competitive advantage.

Here are some of the ways that AI can be used to improve businesses in Slovenia:

- Productivity: AI can automate tasks currently done manually, freeing employees to focus on more strategic work. This can lead to increased efficiency and productivity.
- Innovation: AI can be used to develop new products and services, or to improve existing ones. This can help businesses to stay ahead of the competition.
- Customer service: AI can provide customer service by answering questions and resolving problems. This can help businesses to improve customer satisfaction and loyalty.
- Risk management: AI can identify and mitigate risks like fraud or cyberattacks. This can help companies to protect their assets and reputation.
- Decision-making: AI can make better decisions by analysing large amounts of data and identifying patterns humans might miss. This can lead to improved outcomes for businesses.
- However, there are also some challenges to the adoption of AI in Slovenia, such as:
    - The need for new skills and resources: AI requires new skills and resources, which can challenge small businesses.
    - The potential for bias: AI models can be biased, leading to unfair or discriminatory outcomes.
    - The lack of regulation: Slovenia currently has no clear regulatory framework for AI. This could make it difficult for businesses to adopt AI safely and responsibly.

Slovenian organizations that want to adopt AI successfully need to address these challenges. They need to invest in training their employees on AI, ensure they have the correct data and infrastructure, and develop ethical AI practices.

Here are some of the things that Slovenian organizations can do to address these challenges:

- Invest in training: Businesses need to train their employees in AI. This will help employees understand how AI works and can be used to improve the business.
- Collect and clean data: Businesses must collect and clean data to train AI models. This data needs to be accurate, complete,

and up-to-date.
- Develop ethical AI practices: Businesses need to develop ethical AI practices to ensure that AI is used safely and responsibly. This includes addressing the potential for bias and ensuring that AI is not used to discriminate against individuals or groups.

By addressing these challenges, Slovenian organizations can position themselves to successfully adopt AI and reap the benefits that it has to offer.

In addition to the challenges mentioned above, some opportunities for Slovenian organizations in AI exist. For example, Slovenia has a strong academic community in AI. This means that there is a pool of skilled talent that businesses can tap into. Additionally, Slovenia is a member of the European Union, meaning organizations can access funding and resources from the EU to support their AI initiatives.

Overall, the future of AI in Slovenia is bright. By embracing AI, Slovenian organizations can improve their products and services, enter new markets, and gain a competitive advantage.

6. BUSINESSES SHOULD PROTECT THEMSELVES FROM AI-POWERED CYBERATTACKS

In the previous chapter, we mentioned that AI can help companies defend against cyberattacks. However, attackers can also use AI technologies and carry out cyberattacks with the help of AI.

As AI becomes more widespread, so does the risk of cybersecurity attacks. AI-powered systems are often complex and challenging to secure, making them attractive targets for hackers. In addition, AI can automate cyberattacks, making them more efficient and effective.

Businesses can take several steps to mitigate the risk of AI-powered cyberattacks. These include:

- Educating employees about cybersecurity risks: Employees should know the latest cybersecurity threats and how to protect

themselves and the company's data.
- Enforcing strong cybersecurity policies: Businesses should have strong cybersecurity policies like password requirements and data encryption.
- Investing in cybersecurity solutions: Businesses should invest in cybersecurity solutions like firewalls and intrusion detection systems.
- Staying up-to-date on security patches: Businesses should apply security patches to their software as soon as they are available.

By taking these steps, businesses can help to protect themselves from AI-powered cyberattacks.

7. ASSEMBLING THE RIGHT SKILLS, TECHNOLOGIES, AND RESOURCES

The organization must identify the right skills and technologies for AI adoption:

- Skills: The organization needs to identify the skills needed to implement and use AI. This includes technical skills, such as programming and data science, and soft skills, such as problem solving and communication. The organization can find these skills through various means, such as hiring new employees, upskilling or reskilling existing employees, or partnering with a third-party vendor.
- Technologies: The company must also identify the right technologies to implement and use AI. This includes hardware, servers, GPUs (Graphics Processing Unit), and software, such as machine learning frameworks. The company can find these technologies through various means, such as purchasing them from vendors or developing them in-house.
- Resources: The organization needs to allocate the necessary resources to support AI adoption. This includes time, money, and people. The organization must ensure they have the resources to implement and use AI successfully.

There are many resources available to help Slovenian organizations get started with AI. One such resource is the AI4SI initiative. AI4SI is an European Union initiative that aims to help businesses in Slovenia to adopt AI. The AI4SI initiative provides

various resources, such as training, funding, and networking opportunities.

By assembling the right skills, technologies, and resources, Slovenian organizations can position themselves to adopt AI successfully.

Here are some specific examples of resources that Slovenian organizations can use to assemble the right skills, technologies, and resources for AI adoption:

- Training: There are many training courses available for AI skills. These courses can be found at the universities, online, or through private organizations.
- Funding: Several government programs provide funding for AI projects. These programs can be found at the national, regional, and local levels.
- Networking opportunities: Many networking events and conferences focus on AI. These events can be a great way to learn about AI and meet others working in the field.

By taking advantage of these resources, Slovenian organizations can build the skills, technologies, and resources they need to adopt AI successfully.

8. CONCLUSION

Artificial intelligence (AI) is a powerful technology that has the potential to help Slovenian organizations succeed. However, there are challenges to using AI in business. Organizations that want to adopt AI successfully need to address these challenges.

Here are some of the challenges of using AI in business:

- The need for new skills and resources: AI requires new skills and resources, which can challenge small businesses.
- The potential for bias: AI models can be biased, leading to unfair or discriminatory outcomes.
- The lack of regulation: Slovenia currently has no clear regulatory framework for AI. This could make it difficult for businesses to adopt AI safely and responsibly.

- The ethical implications: AI raises several ethical concerns, such as the right to privacy and the potential for job displacement.

Despite these challenges, there are many reasons why Slovenian organizations should consider adopting AI. Here are some of the benefits of AI for businesses:

- Increased productivity: AI can automate tasks currently done manually, freeing up employees to focus on more strategic work. This can lead to increased efficiency and productivity.
- Improved decision-making: AI can make better decisions by analysing large amounts of data and identifying patterns humans might miss. This can lead to improved outcomes for businesses.
- New product development: AI can develop new products and services or improve existing ones. This can help businesses to stay ahead of the competition.
- Improved customer service: AI can provide customer service by answering questions and resolving problems. This can help businesses to improve customer satisfaction and loyalty.
- Risk mitigation: AI can identify and mitigate risks like fraud or cyberattacks. This can help companies to protect their assets and reputation.

By addressing the challenges of AI and leveraging its benefits, Slovenian organizations can position themselves to succeed in the digital age.

Here are some specific tips for Slovenian organizations that want to adopt AI successfully:

- Start small: Do not try to do too much too soon. Start with a small project that you can use to learn about AI and its potential benefits.
- Partner with experts: Many organizations specialize in AI. Partnering with an expert can help you avoid making mistakes and get the most out of AI.
- Be patient: AI is a complex technology. It takes time to develop and implement AI solutions. Be patient, and do not expect to see results overnight.

- Be ethical: AI raises several ethical concerns. Be sure to address these concerns as you develop and implement AI solutions.

Slovenian organizations can increase their chances of successfully adopting AI by following these tips.

9. REFERENCES

1. Jain, R. (April 2, 2023). *The Impact of Artificial Intelligence on Business: Opportunities and Challenges*. Available at SSRN: **URL** or **alternate URL**.
2. Trampuž, M., Bračun, F., Čebela, T., Fuart, F., Lampe, A., Pucihar Baebler, M. (2023). *Vodič uvajanja umetne inteligence v mala in srednja podjetja v Sloveniji – Zagotovite, da bo vaše podjetje pripravljeno za 21. stoletje*.
3. Davenport, Thomas H., Mittal, N. (2023). *All-in On AI: How Smart Companies Win Big with Artificial Intelligence*. Harvard Business Review Press.
4. Enholm, Ida Merete, Papagiannidis, E., Mikalef, P., Krogstie, J. (2022). Artificial Intelligence and Business Value: a Literature Review. *Inf Syst Front* 2022, 24, p. 1709–1734.
5. Mikalef, P., Gupta, M. (2021). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. *Information & Management*, 2021, 58 (3), Article 103434.

Opombe

* Avtorju
1. Opomba

IZ PRAKSE ZA PRAKSO

Kombiniranje primerjalnih meril za določanje pomembnosti pri reviziji računovodskih izkazov

IZ PRAKSE ZA PRAKSO (PR-REV 5-5/23)

Revizijski svet Slovenskega inštituta za revizijo je v sodelovanju z Agencijo za javni nadzor nad revidiranjem v septembru 2023 obravnaval način določanja pomembnosti za namene revidiranja računovodskih izkazov s kombiniranjem različnih primerjalnih meril in o tem pripravil strokovno razlago.

IZHODIŠČE

Namen revizije je zvišati stopnjo zaupanja predvidenih uporabnikov v računovodske izkaze. To se doseže z izraženim mnenjem revizorja o tem, ali so računovodski izkazi v vseh pomembnih pogledih sestavljeni v skladu s primernim okvirom računovodskega poročanja.[1] Iz namena revidiranja torej izhajata dve za revizorja ključni vprašanji:

1. Kdo so predvideni uporabniki računovodskih izkazov?
2. Kje je meja med pomembnimi in nepomembnimi napakami?

Predvideni uporabniki so posamezniki ali organizacije ali njihove

skupine, za katere revizor pričakuje, da bodo uporabljali revizorjevo poročilo. V nekaterih primerih se predvideni uporabniki razlikujejo od tistih, na katere je naslovljeno revizorjevo poročilo.[2]

Napačne navedbe, vključno z opustitvami, se štejejo za pomembne, če bi lahko upravičeno pričakovali, da posamič ali skupaj vplivajo na gospodarske odločitve uporabnikov, sprejete na podlagi računovodskih izkazov.[3]

Kot izhodiščna točka pri določanju pomembnosti za celoto računovodskih izkazov se pogosto uporablja določen odstotek od izbranega primerjalnega merila. Dejavniki, ki lahko vplivajo na opredelitev primernega primerjalnega merila, so med drugim:[4[

- sestavine računovodskih izkazov (na primer sredstva, obveznosti, kapital, prihodki, odhodki);
- ali obstajajo postavke, na katere je pretežno osredotočena pozornost uporabnikov računovodskih izkazov določene organizacije (za vrednotenje finančnih učinkov utegnejo uporabniki na primer usmeriti pozornost pretežno na dobiček, prihodke ali neto sredstva);
- vrsta organizacije in kje je organizacija v svojem razvojnem ciklu, pa tudi panoga in gospodarsko okolje, v katerem organizacija deluje;
- lastniška struktura organizacije in način, kako je financirana (na primer, če se organizacija financira izključno z dolgovi namesto s kapitalom, utegnejo uporabniki posvetiti več pozornosti sredstvom in terjatvam v zvezi z njimi kot pa dobičku organizacije), in
- sorazmerna nestanovitnost primerjalnega merila.

O pomembnosti se presoja glede na okoliščine, na presojo pa vplivata revizorjevo zaznavanje potreb uporabnikov računovodskih izkazov po računovodskih informacijah in velikost ali vrsta napačne navedbe ali kombinacija obeh.[5]

Revizijski svet Slovenskega inštituta za revizijo je v letu 2014 sprejel metodološko gradivo,[6] ki revizijskim družbam in pooblaščenim revizorjem daje podrobnejše usmeritve v zvezi z

določanjem zneska pomembnosti pri revidiranju računovodskih izkazov. Gradivo po vrstah pravnega subjekta predlaga ustrezna primerjalna merila in njihove odstotke, ki naj bi odražali zaznavanje pomembnosti predvidenih uporabnikov njihovih računovodskih izkazov.

Za določitev pomembnosti na ravni računovodskih izkazov ali po vrstah poslov, saldov na kontih ali razkritij je torej najpomembnejša revizorjeva presoja o učinkih možnih napak na gospodarske odločitve predvidenih uporabnikov računovodskih izkazov oziroma ali se uporabniki osredotočajo na določene postavke v računovodskih izkazih. Ustrezno izbrano primerjalno merilo bi zato moralo biti povezano s tem, čemur uporabniki v računovodskih izkazih namenjajo največ pozornosti.

V praksi so možne tudi okoliščine, v katerih revizor ugotovi več različnih skupin predvidenih uporabnikov računovodskih izkazov z različnimi vidiki pomembnosti oziroma z osredotočenostjo na različne postavke v računovodskih izkazih, ki bi lahko predstavljale primerjalna merila. Posledica tega so pristopi revizorjev, ko za potrebe določitve pomembnosti presojajo več primerjalnih meril ter na tej podlagi določijo pomembnost bodisi na način, da izberejo eno izmed njih, bodisi pa na njihovi podlagi računajo povprečja. Omenjeni pristopi zahtevajo od revizorjev dodatno presojo in razmislek. Kot je mogoče razumeti določbe pravil revidiranja, predvsem MSR 320, revizorja napotujejo na določitev enega primerjalnega merila za določitev pomembnosti, ki najbolje odraža interese predvidenih uporabnikov računovodskih izkazov. Resda pa uporaba več primerjalnih meril ni izrecno prepovedana.

Na podlagi predstavljenega izhodišča je bila sprejeta strokovna razlaga.

STROKOVNA RAZLAGA

Revizijski svet Slovenskega inštituta za revizijo revizijske družbe in pooblaščene revizorje opozarja:

a) Kadar revizor zazna eno pomembno skupino predvidenih

uporabnikov revidiranih računovodskih izkazov, poišče ključno postavko računovodskih izkazov, na katero je najbolj usmerjena njihova pozornost. Strokovno ni upravičeno, da v teh primerih revizor uporabi za svojo presojo različna primerjalna merila za določanje pomembnosti, ki niso ključna, niti da pomembnost izračuna na podlagi njihovih povprečij.
b) Kadar je več skupin predvidenih uporabnikov revidiranih računovodskih izkazov, se presoja, ali obstajajo različne postavke računovodskih izkazov, na katere je usmerjena njihova pozornost in ki bi bile lahko primerjalna merila za določanje pomembnosti vsake izmed njih. Če je tako, revizijski svet meni, da:

- *zneska pomembnosti za namene revizije računovodskih izkazov ni primerno določati kot povprečje različnih pomembnosti na podlagi različnih primerjalnih meril, saj je tako določena pomembnost neprimerno velika vsaj za eno skupino predvidenih uporabnikov računovodskih izkazov;*
- *se s povprečenjem iz procesa določanja pomembnosti izloči revizorjeva strokovna presoja;*
- *mora revizor presoditi, ali ne bi bilo primerneje pomembnost določiti na ravni primerjalnega merila, ki pomembnost določa na najnižji ravni od možnih, oziroma ali ni primerneje uporabiti drugo primerjalno merilo, ki bi ustrezalo prepoznanim skupinam predvidenih uporabnikov.*

c) Strokovno presojo, ki je vodila do končne določitve pomembnosti, je treba ustrezno dokumentirati.

Opombe

1. MSR 200, odstavek 3.
2. Razlagalni slovar.
3. MSR 320, odstavek 2.
4. MSR 320, odstavek A4.
5. MSR 200, odstavek 6.
6. Metodološko gradivo Slovenskega inštituta za revizijo – Pomembnost pri izvajanju in načrtovanju revizije.

Primernost uporabe modelov AVM pri ocenjevanju vrednosti nepremičnin

IZ PRAKSE ZA PRAKSO (PR-OCV 5-5/23)

Na Odbor sekcije pooblaščenih ocenjevalcev vrednosti je bilo naslovljeno vprašanje, ali je pri vrednosti nepremičnin (pravic na nepremičninah) dovoljena uporaba modelov AVM in ali so tovrstne ocene usklajene z zahtevami MSOV-jev. Problematiko ocenjevanja vrednosti uporabe modelov AVM pri ocenjevanju vrednosti nepremičnin (pravic na nepremičninah) je obravnaval Odbor sekcije pooblaščenih ocenjevalcev vrednosti in o tem pripravil strokovno razlago.

IZHODIŠČE

Odbor pooblaščenih ocenjevalcev vrednosti spremlja področje ocenjevanja vrednosti po avtomatiziranih modelih (angl. *Automated Valuation Model*, v nadaljevanju: AVM) že od leta 2019. Modeli AVM so opredeljeni kot sistemi, ki uporabniku podajo oceno vrednosti določenega sredstva na določen datum z avtomatiziranimi tehnikami izračunavanja. O uporabi modelov AVM je odbor v preteklosti organiziral strokovno srečanje in na to temo izdal nekaj strokovnih mnenj. Oktobra 2020 je OMSOV[1] objavil prispevek *Agenda Consultation 2020*, v katerem je najavil, da je tehnični odbor OMSOV problematiko uporabe modelov

AVM zaznal, obravnaval in odprl javno razpravo, da se do te problematike strokovno opredeli. Konec leta 2022 je OMSOV objavil *Perspectives Paper*[2] z naslovom *Automated Valuation Models and Residential Valuations* kot prvega v nizu prispevkov, namenjenih razpravi o primernosti in omejitvah uporabe modelov AVM pri ocenjevanju vrednosti stanovanjskih objektov z namenom zavarovanega posojanja. Po oblikovanju stališč o navedeni problematiki bo OMSOV obravnavo nadaljeval še za področju nestanovanjskih nepremičnin. Ker področje uporabe modelov AVM pri ocenjevanju nepremičnin ne bo vključeno v novo različico MSOV-jev, ki začnejo veljati v letu 2024, se je odbor zaradi pereče problematike, povezane z uporabo modelov AVM v slovenski praksi, odločil, da izoblikuje strokovno stališče. Odbor ugotavlja:

- da se v Sloveniji povečuje uporaba modelov AVM, kar samo po sebi ni sporno;
- da se v poročilih o ocenah vrednosti, narejenih po modelih AVM, v katerih je navedeno, da so ocene vrednosti narejene v skladu z MSOV-ji, pojavljajo posamezni segmenti, preneseni neposredno iz modelov AVM, ne da bi se ocenjevalci vrednosti kritično opredelili do njihove vsebine in predpostavk ter jih ustrezno analitično obdelali; to vodi do pavšalnih, vsebinsko neustreznih in napačnih ugotovitev in ocen;
- da ocenjevalci vrednosti z modeli AVM ne zagotovijo ustrezne sledljivosti in ponovljivosti izvedenih ocen vrednosti. Podatki, na katerih temeljijo modeli AVM, so pogosto časovno nekonsistentni. Z osveževanjem baz podatkov, iz katerih modeli črpajo podatke, se izhodiščni podatki ocenjevanja spreminjajo tudi za nazaj. To ima za posledico, da uporaba modelov AVM pogosto ne izpolnjuje zahtev po ponovljivosti in sledljivosti, kar povzroča, da so ocene vrednosti istega predmeta ocenjevanja na isti datum ocenjevanja, izvedene v različnih časovnih obdobjih, različne.

STROKOVNA RAZLAGA

Odbor se je na podlagi stališč OMSOV-ja in zaznane problematike, povezane z uporabo AVM-jev v Sloveniji, odločil, da oblikuje strokovno mnenje glede:

1. *primernosti uporabe modelov AVM,*
2. *omejitev v zvezi z njihovo uporabo in*
3. *usklajenosti ocen vrednosti, izvedenih z modeli AVM, z MSOV-ji.*

Ocena vrednosti, ki jo izvede pooblaščeni ocenjevalec vrednosti (v nadaljevanju: ocenjevalec), je mnenje o vrednosti, ki izhaja iz procesa ocenjevanja vrednosti, usklajenega z zahtevami MSOV-jev. Pri tem ocenjevalec lahko uporabi različna orodja, velja pa, da uporaba teh orodij ne more in ne sme nadomestiti ocenjevalčeve osebne strokovne presoje glede končne ocene vrednosti.

Primernost uporabe modelov AVM

V poglavju MSOV-ja 105 – Načini in metode ocenjevanja vrednosti *so opredeljeni modeli ocenjevanja vrednosti:*

»90.1 Model ocenjevanja vrednosti je skupen izraz za kvantitativne metode, sisteme, tehnike in kakovostne presoje, ki se uporabljajo za ocenjevanje in dokumentiranje vrednosti.

90.2 Pri uporabi in ustvarjanju modela ocenjevanja vrednosti mora ocenjevalec vrednosti:
a) voditi ustrezne evidence v podporo izbire ali stvaritve modela,
b) razumeti in zagotoviti izid modela ocenjevanja vrednosti, da so pomembne predpostavke in omejevalne okoliščine skladne s podlago in obsegom ocenjevanja vrednosti, in
c) upoštevati ključna tveganja, povezana s postavljenimi predpostavkami v modelu ocenjevanja vrednosti.

90.3 Ne glede na vrsto modela ocenjevanja vrednosti mora ocenjevalec vrednosti, da je model skladen z MSOV-ji, zagotoviti, da je ocenjevanje vrednosti skladno z vsemi drugimi zahtevami, ki so vsebovane v njih.«

Vidimo, da MSOV-ji pri uporabi modelov AVM za ocenjevanje vrednosti ocenjevalcem postavljajo zahteve in omejitve.

Razumevanje in obvladovanje delovanja modelov AVM

Modeli AVM, ki jih pri svojem delu uporabljajo slovenski ocenjevalci, se razlikujejo po kompleksnosti. Njihov nabor je širok. Med njimi so tako napredne klasične Excelove preglednice, katerih avtorji so ocenjevalci sami, kot tudi sofisticirani modeli AVM, temelječi na strojnem učenju in umetni inteligenci. Modeli AVM od ocenjevalca zahtevajo različne stopnje strokovnega vložka. Modeli, ki jih za ocenjevanje sestavijo ocenjevalci sami, so najpogosteje modeli, ki jih ocenjevalci razumejo in obvladujejo predpostavke, ki so vanje vgrajene. Bolj dovršeni modeli, ki jih sestavljajo in ponujajo zunanji ponudniki, pa so pogosto tako kompleksni, da ocenjevalci ne razumejo v celoti predpostavk, ki so v te modele vgrajene, načina njihovega delovanja, načina zajema podatkov in omejitev, ki jih imajo ti modeli vgrajene implicitno. Nerazumevanje modela ocenjevanja ocenjevalca ne odvezuje odgovornosti pri oceni končne vrednosti premoženja.

Razumevanje in obvladovanje vhodnih podatkov

Ocenjevalec se ne more in ne sme slepo zanašati na model ocenjevanja, ki ga uporablja pri svojem delu. V skladu z zahtevo 90.3 iz MSOV-jev mora ocenjevalec zagotoviti, da je uporabljeni model skladen z MSOV-ji, pa tudi, da je ocenjena vrednost skladna z vsemi drugimi zahtevami iz standardov. V skladu z zahtevo MSOV-ja 102 – Raziskave in skladnost*, točka 20.2, je ocenjevalec, kadar naloga ocenjevanja »vključuje sklicevanje na informacije, ki jih dostavi kdo drug in ne ocenjevalec vrednosti,« dolžan »proučiti, ali je informacija verodostojna in ali se je nanjo sicer mogoče zanesti, ne da bi to škodljivo vplivalo na verodostojnost mnenja o oceni vrednosti«. Prav tako je dolžan, da »prouči pomembne vhodne podatke, jih razišče in/ali zanje dobiti potrditev, kadar za verodostojnost ali zanesljivost dobljenih informacij ni mogoče dobiti dokazne podpore«. Hkrati je dolžan »razmisliti, ali/oziroma kako se take informacije uporabijo pri ocenjevanju vrednosti«.*

Modeli AVM sami po sebi teh zahtev ne izpolnjujejo, zato ocene, izpeljane iz teh modelov, brez hkratnega izpolnjevanja vseh drugih zahtev MSOV-jev niso usklajene z MSOV-ji.

PREPOZNAVANJE INDIVIDUALNIH LASTNOSTI PREMOŽENJA

Modeli AVM večinoma delujejo tako, da ni dopuščeno prepoznavanje posebnosti ocenjevanega premoženja. Zato je mogoče, da vrednost premoženja odstopa od tržnih norm in povprečij. Modeli AVM sami po sebi niso zmožni zagotoviti tovrstne presoje. Zato jo lahko izvede samo ocenjevalec vrednosti z ustreznim strokovnim znanjem in izkušnjami.

PODLAGE VREDNOSTI, OCENJEVANJE ZA NAMEN ZAVAROVANEGA POSOJANJA IN NAJGOSPODARNEJŠA UPORABA

Ocene vrednosti za namen zavarovanega posojanja praviloma temeljijo na tržni vrednosti. Tržna vrednost je podlaga vrednosti, ki mora odražati najgospodarnejšo uporabo nepremičnine. Podlaga vrednosti opisuje temeljne premise, na katerih temeljijo poročane vrednosti. V MSOV-ju 104 – Podlage vrednosti *je v točki 10.1 navedeno, da mora»podlaga (ali podlage) vrednosti ustrezati pogojem in namenu ocenjevanja vrednosti, ker podlaga vrednosti lahko vpliva na izbiro ali celo narekuje ocenjevalčevo izbiro metod, vhodnih podatkov in predpostavk ter s tem vpliva tudi na končno mnenje o vrednosti«.Tržna vrednost sredstva odraža njegovo najgospodarnejšo uporabo. Najgospodarnejša uporaba sredstva je tista, ki maksimira potencial ocenjevanega sredstva, ki je mogoča, zakonito dopustna in finančno izvedljiva. Najgospodarnejša uporaba se lahko nanaša na nadaljevanje sedanje uporabe sredstva ali na drugo vrsto uporabe. To je določeno glede na uporabo, ki jo tržni udeleženec za sredstvo predvideva, kadar oblikuje ceno, ki bi jo bil pripravljen ponuditi. Modeli AVM ne glede na raven sofisticiranosti niso zmožni oblikovati ustrezno zanesljivega in strokovno utemeljenega mnenja o najgospodarnejši rabi nepremičnine. Strokovno*

utemeljeno mnenje o najgospodarnejši rabi lahko oblikuje samo ocenjevalec vrednosti z ustreznim strokovnim znanjem in izkušnjami.

PRILAGODITVE

V MSOV-jih se zahteva, da morata biti vrsta in vir vhodnih podatkov za ocenjevanje skladna s podlago vrednosti, ta pa mora upoštevati namen ocenjevanja vrednosti. Mnenje o vrednosti se lahko pridobi na različne načine in po raznih metodah. Pri načinu tržnih primerjav se praviloma uporabijo podatki, ki izhajajo s trga. Za določitev tržne vrednosti naj bi uporabili na donosu zasnovani način ter vhodne podatke in predpostavke, ki bi jih sprejeli tržni udeleženci. Za določitev tržne vrednosti po nabavnovrednostnem načinu je nabavna cena sredstva enaka njegovi koristnosti, ustrezno amortizacijo pa bi bilo treba določiti z analizo cen in amortizacije na tržni podlagi. V MSOV-ju 105 – Načini in metode ocenjevanja vrednosti *se v točki 20.5 zahteva, da mora ocenjevalec, »kadar se primerljiva tržna informacija ne nanaša na točno ali v bistvu enako sredstvo, opraviti primerjalno analizo podobnosti in razlik po kakovosti in količini med primerljivimi sredstvi in ocenjevanim sredstvom. Na podlagi primerjalne analize bo pogosto treba opraviti prilagoditve. Take prilagoditve morajo biti utemeljene in ocenjevalec vrednosti mora dokumentirati razloge za prilagoditve in kako jih je količinsko določil«.Zahtevane vsebinsko ustrezne primerjalne analize tržnih informacij, še posebej kadar je nabor primerljivih sredstev heterogen, modeli AVM niso zmožni zagotoviti. Heterogenost populacije v analizo vključenih primerljivih sredstev lahko povzroči, da se ta sredstva pomembno razlikujejo od ocenjevanega sredstva ter da pridobljeni in uporabljeni podatki niso primerni za oceno predmeta ocenjevanja.V MSOV-ju 105 –* Načini in metode ocenjevanja vrednosti *je v točki 30.7 še navedeno, da naj bi»ocenjevalec vrednosti izbral primerljive posle v naslednjem miselnem okviru:*

a) dokazi več poslov so na splošno boljši od enega samega posla ali dogodka;
b) dokazi iz poslov z zelo podobnimi sredstvi (idealno bi bilo z

enakimi) dajejo boljši kazalnik vrednosti kot sredstva, za katere je treba cene teh poslov pomembno prilagajati;
c) posli, ki so se zgodili bliže datumu ocenjevanja vrednosti, so bolj reprezentativni za trg na ta datum, kot so po datumu starejši posli, zlasti na nestanovitnih trgih;
d) za večino podlag vrednosti naj bi bili to posli, sklenjeni po tržnih načelih med nepovezanimi strankami;
e) na voljo naj bi bilo dovolj informacij o poslu, da se ocenjevalec vrednosti lahko dovolj dobro seznani s primerljivim sredstvom in da lahko oceni metriko ocenjevanja vrednosti
ziroma primerljive dokaze;
f) informacije o primerljivih poslih naj bi prišle iz zanesljivega in zaupanja vrednega vira;
g) dejansko izpeljani posli dajejo boljše dokaze o ocenjevanju vrednosti kot samo nameravani posli.«

Tovrstno presojo lahko izvede samo ocenjevalec vrednosti z ustreznim strokovnim znanjem in izkušnjami. Pri ocenjevanju mora ocenjevalec izvesti potrebne prilagoditve za vse pomembne razlike med primerljivimi posli in ocenjevanim sredstvom.

Za trg nepremičnin v Sloveniji je značilno, da je število tržnih transakcij sorazmerno omejeno, razpoložljivi podatki o transakcijah pa pomanjkljivi in nezanesljivi. Modeli AVM teh pomanjkljivosti niso zmožni zaznati in sami po sebi izvesti potrebnih prilagoditev, saj je že sam izbor primerljivih transakcij/podatkov deloma ali v celoti posledica predpostavk, ki so jih v modele vgradili njihovi avtorji. Tovrstne predpostavke so ocenjevalcu vrednosti lahko deloma ali v celoti nepoznane, kar vodi do napačnih sklepov in napačnih mnenj o ocenjenih vrednostih. Vsebinsko presojo ustreznosti tržnih podatkov lahko izvede samo ocenjevalec vrednosti z ustreznim znanjem in izkušnjami.

Podobno velja za izbor metod ocenjevanja vrednosti. V MSOV-ju 105 – Načini in metode ocenjevanja vrednosti *v točki 10.4 piše:»Od ocenjevalca vrednosti se ne zahteva uporaba več kot ene metode za ocenjevanje vrednosti enega sredstva, zlasti kadar ocenjevalec vrednosti zelo zaupa v natančnost in zanesljivost posamezne metode glede na dejstva in okoliščine posla*

ocenjevanja vrednosti. Vendar pa naj bi ocenjevalec vrednosti razmislil o uporabi več načinov in metod in proučil več kot en sam način ali eno samo metodo, ki bi jih lahko uporabil za določitev vrednosti. To bi prišlo v poštev, zlasti kadar nima dovolj stvarnih ali opazovanih vhodnih podatkov, ki bi omogočali, da bi že z eno samo metodo lahko prišel do zanesljive sklepne ugotovitve o ocenjeni vrednosti. Kadar se uporabi več kot en sam način ali metoda ali celo več metod v okviru enega samega načina, naj bi bil sklep o vrednosti na podlagi teh več načinov in/ali metod utemeljen, celoten postopek analiziranja in usklajevanja različnih vrednosti v eno samo sklepno ugotovitev brez povprečenja pa naj bi ocenjevalec vrednosti opisal v poročilu.« Modeli AVM v okoliščinah, ki od ocenjevalca zahtevajo uporabo več metod, ne morejo biti primarni ali edini način ocenjevanja vrednosti. Izbor ustrezne metode ali metod ocenjevanja lahko izvede samo ocenjevalec z ustreznim znanjem in izkušnjami.

POROČANJE

V modele AVM so pogosto vključeni moduli, ki omogočajo izdelavo standardiziranih poročil o oceni vrednosti. Malo verjetno je, da modeli AVM sami po sebi v okviru standardiziranega načina poročanja vsebinsko zadostijo v MSOV-jih postavljenim zahtevam po razkritju obsega, namena, predpostavk, posebnih predpostavk pomembnih negotovosti in omejitvenih pogojih, vključenih v oceno vrednosti. V MSOV-ju 103 – Poročanje *so zahteve, ki jim mora poročilo o oceni vrednosti zadostiti, da bi bila ocena vrednosti skladna z MSOV-ji. V točki 10.2 tega standarda je navedeno: »Za zagotovitev koristnih informacij mora poročilo vsebovati jasen in natančen opis obsega naloge, njen namen in nameravano uporabo (vključno z vsemi omejitvami te uporabe) ter razkritje vseh predpostavk, posebnih predpostavk (odstavek 200.4 MSOV-ja 104 – Podlage vrednosti), pomembne negotovosti ali omejitvene pogoje, ki neposredno vplivajo na ocenjevanje vrednosti.«*

Omenjene zahteve moramo razumeti vsebinsko, ne zgolj formalno. Da bi bila ocenjena vrednost skladna z zahtevami MSOV-jev, se mora ocenjevalec o obsegu, namenu, predpostavkah, posebnih

predpostavkah, pomembnih negotovostih in omejitvenih pogojih v poročilu o oceni vrednosti vsebinsko in argumentirano opredeliti. Tega modeli AVM sami po sebi ne zagotavljajo.

USKLAJENOST OCEN VREDNOSTI, IZVEDENIH Z MODELI AVM, Z MSOV-ji

Z MSOV-ji usklajeno ocenjevanje vrednosti je proces, v katerem mora ocenjevalec določiti namen ocenjevanja vrednosti, izvesti potrebne raziskave in presoje, določiti podlage vrednosti, izbrati ustrezne pristope, tehnike in metode ocenjevanja ter o rezultatih ocenjevanja poročati v skladu z zahtevami MSOV-jev. Vse to so pogoji, ki jim mora ocenjevalec zadostiti, da bi bila končna ocena vrednosti usklajena z MSOV-ji. Ocene vrednosti, izvedene z modeli AVM, tudi če ocenjevalec poda končno presojo ocenjene vrednosti, niso usklajene z MSOV-ji, če ocenjevalec ne izvede vseh postopkov in ne zadosti vsem zahtevam MSOV-jev, vključno z zahtevano obliko poročanja. Velja, da ocenjevalec vrednosti pri svojem delu modele AVM sicer lahko uporablja kot pripomoček, a mora, da bi bila končna ocenjena vrednost usklajena z zahtevami MSOV-jev, pri tem izvesti vse zahtevane in predpisane postopke ter jih ustrezno razkriti v končnem poročilu o oceni vrednosti. Če tega ne izvede, tudi če se opredeli do samodejno izračunane ocene vrednosti, tovrstne ocene niso usklajene z MSOV-ji. Modeli AVM so torej lahko zgolj pripomoček za ocenjevanje vrednosti, vendar pa brez predpisanega in zahtevanega strokovnega vložka ocenjevalca vrednosti, brez izvedenega zahtevanega načina poročanja, brez ustreznih razkritij in brez ocenjevalčevega razumevanja, kako modeli AVM delujejo in kakšne so njihove omejitve, ocena vrednosti ne more biti usklajena z MSOV-ji. MSOV-ji ocenjevanje vrednosti opredeljujejo kot dejanje ali proces določanja mnenja ali sklepa o vrednosti sredstva na podlagi vrednosti na datum, ki je določen v skladu z zahtevami standardov. V procesu ocenjevanja morajo biti spoštovana vsa temeljna načela standardov ocenjevanja vrednosti:[3]

1. ***Etika:*** *Ocenjevalci vrednosti morajo slediti etičnim načelom*

neoporečnosti, objektivnosti, nepristranskosti, zaupnosti, usposobljenosti in strokovnosti, da spodbujajo in ohranjajo zaupanje javnosti.

2. ***Strokovna usposobljenost:*** *V času ocenjevanja vrednosti morajo imeti ocenjevalci vrednost potrebne strokovne veščine in znanje za ustrezno dokončanje naloge ocenjevanja vrednosti.*
3. ***Skladnost:*** *Ocenjevalci vrednosti morajo razkriti ali sporočiti objavljene standarde ocenjevanja vrednosti, ki jih uporabljajo pri svoji nalogi, in ravnati v skladu z njimi.*
4. ***Podlaga (tj. vrsta standarda) vrednosti:*** *Ocenjevalci vrednosti morajo izbrati podlago (ali podlage) vrednosti, ki je primerna za nalogo, in slediti vsem ustreznim zahtevam. Podlaga (ali podlage) vrednosti mora biti opredeljena ali navedena.*
5. ***Datum vrednosti (tj. datum veljavnosti/datum ocenitve vrednosti):*** *Ocenjevalci vrednosti morajo razkriti ali sporočiti datum ocene vrednosti, ki je podlaga njihovih analiz, mnenj ali sklepov. Ocenjevalci vrednosti morajo navesti tudi datum, na katerega razkrijejo ali sporočijo svojo oceno vrednosti.*
6. ***Predpostavke in pogoji:*** *Ocenjevalci vrednosti morajo razkriti pomembne predpostavke in pogoje, ki so značilni za nalogo in lahko vplivajo na njen izid.*
7. ***Predvidena uporaba:*** *Ocenjevalci vrednosti morajo razkriti ali sporočiti jasen in natančen opis predvidene uporabe ocene vrednosti.*
8. ***Predvideni uporabnik(i):*** *Ocenjevalci vrednosti morajo razkriti ali sporočiti jasen in natančen opis predvidenega uporabnika oz. predvidenih uporabnikov ocene vrednosti.*
9. ***Obseg dela:*** *Ocenjevalci vrednosti morajo določiti, izvesti ter razkriti ali sporočiti obseg dela, ki je za nalogo primeren, tako da bo vodil do verodostojne ocene vrednosti.*
10. ***Opredelitev predmeta ocenjevanja vrednosti:*** *Ocenjevalci vrednosti morajo jasno opredeliti predmet ocenjevanja vrednosti.*
11. ***Podatki:*** *Ocenjevalci vrednosti morajo uporabiti primerne informacije in vhodne podatke na jasen in pregleden način, tako da zagotovijo verodostojno ocenjevanje vrednosti.*
12. ***Metodologija ocenjevanja vrednosti:*** *Ocenjevalci vrednosti morajo pravilno uporabiti primerno metodologijo ali metodologije ocenjevanja vrednosti, da izvedejo verodostojno ocenjevanje vrednosti.*

13. ***Obveščanje o ocenjevanju vrednosti****: Ocenjevalci vrednosti morajo predvidene uporabnike jasno obveščati o analizah, mnenjih in sklepih ocenjevanja vrednosti.*
14. ***Evidentiranje:*** *Ocenjevalci vrednosti morajo po dokončanju naloge določen čas hraniti en izvod ocene vrednosti in zapis/evidenco o opravljenem delu pri ocenjevanju vrednosti.*

Modeli AVM, ki jih v Sloveniji trenutno ponujajo zunanji ponudniki, teh pogojev brez ustreznih ocenjevalčevih dodatnih postopkov in strokovnih vložkov ne izpolnjujejo.

Odbor ugotavlja, da:

- ***ocene vrednosti, izvedene po modelih AVM, vendar pa brez v MSOV-jih zahtevanih postopkov ocenjevanja in poročanja ocenjevalca ter izpolnjenih vseh zahtev MSOV-jev, niso z MSOV-ji usklajene ocene vrednosti;***
- ***nerazumevanje delovanja modelov AVM ocenjevalca ne odvezuje odgovornosti za končno oceno vrednosti premoženja;***
- ***modeli AVM zaradi navedenih pomanjkljivosti in ne da bi ocenjevalec izvedel vse zahtevane postopke ocenjevanja in poročanja ter izpolnil vse zahteve MSOV-jev, ne morejo biti primerno orodje za ocenjevanje za namen zavarovanega posojanja;***
- ***so modeli AVM za ocenjevalce vrednosti lahko zgolj pripomoček v procesu ocenjevanja vrednosti. Pri tem veljata pogoj, da njihova uporaba ni omejujoča in zavajajoča, ter pogoj, da ocenjevalec pozna in razume ključne predpostavke in delovanje uporabljenega modela;***
- ***mora ocenjevalec, če je pri ocenjevanju vrednosti uporabljal model AVM zunanjega ponudnika, ki ustreza definiciji modela AVM, to v poročilu tudi ustrezno razkriti.***

LITERATURA

1. Mednarodni standardi ocenjevanja vrednosti (MSOV). 2022.
2. Automated Valuation Models and Residential Valuations. Persective paper. IVSC, 2022.

Opombe

1. Odbor za Mednarodne standarde ocenjevanja vrednosti (*International Valuation Standards Council* – IVSC).
2. OMSOV izdaja *Prospective Papers* z namenom raziskovanja stališč trga glede pomembnih tem, ki se nanašajo na področje ocenjevanja vrednosti, ali pa je to raziskovalni dokument, kadar je OMSOV v začetni fazi preučevanja vprašanj, ki so pomembna z vidika standardov IVS. *Perspectives Papers* dopolnjujejo standarde IVS in ne nadomeščajo ali izpodrivajo standardov. Pooblaščeni ocenjevalci vrednosti so pri izvajanju ocenjevanja vrednosti dolžni upoštevati standarde.
3. Uvod v MSOV, 2021.

Računovodenje zalog, ki jih kupec ne prevzame, stroški vračila pa presegajo čisto iztržljivo vrednost ali stroške uničenja

IZ PRAKSE ZA PRAKSO (PR-RAC 6-5/23)

Računovodenje zalog, ki jih kupec ne prevzame, stroški vračila pa presegajo čisto iztržljivo vrednost ali stroške uničenja, je obravnaval Odbor sekcije preizkušenih računovodij in o tem pripravil strokovno razlago.

IZHODIŠČE

Občasno se zgodi, da kupec iz različnih razlogov ne prevzame naročenega blaga[1]. Lahko gre za blago neustrezne kakovosti, s prekratkim rokom uporabe ali katerih drugih značilnosti, ki kupcu ne ustrezajo, tako da zavrne prevzem blaga. Lahko se zgodi, da bi bili stroški vračila takega blaga v izhodiščno skladišče višji, kot je čista iztržljiva vrednost takega blaga, ali pa stroški uničenja ali zavrženja takega blaga v kraju, kjer je shranjeno, organizacija pa nima namena, da bi tako blago obdržala iz drugih razlogov.

V takem primeru se zastavlja vprašanje, kako naj organizacija računovodi tak dogodek.

Po SRS-ju 4.4 (2016) zaloga, namenjena prodaji, zajema dokončane proizvode in trgovsko blago v skladišču ter količine na poti do kupca, dokler jih ne prevzame v obvladovanje.

V SRS-ju 4.7 (2016) je določeno, da se stvar v knjigovodskih razvidih in bilanci stanja pripozna, če: a) jo organizacija obvladuje in ji omogoča doseganje gospodarskih koristi iz njih in b) je mogoče njeno nabavno oziroma stroškovno vrednost ali pošteno vrednost (kadar gre za zaloge iz bioloških sredstev oziroma kmetijskih pridelkov) zanesljivo izmeriti.

Nadalje je v SRS-ju 4.17 (2016) določeno, da se zaloge vrednotijo po izvirni vrednosti ali čisti iztržljivi vrednosti, in sicer po manjši izmed njiju.

Na podlagi predstavljenega izhodišča je bila sprejeta strokovna razlaga.

STROKOVNA RAZLAGA

Kadar se zgodi, da kupec ne prevzame naročenega blaga in ga torej še ne obvladuje, stroški vračila takega blaga v skladišče organizacije pa bi bili višji, kot je čista iztržljiva vrednost takega

blaga, ali pa stroški uničenja ali zavrženja takega blaga v kraju, kjer je, je za organizacijo ekonomsko morda bolj smiselno, da tako blago uniči ali zavrže v kraju, kjer je blago.

Vsebinsko gledano je v takem primeru čista iztržljiva vrednost negativna. Taka zaloga ne izpolnjuje več pogoja doseganja gospodarskih koristi. Tako zmanjšanje vrednosti zalog obremenjuje prevrednotovalne poslovne odhodke.

Organizacija mora z vidika zagotavljanja verodostojnih podlag za evidentiranje poslovnih dogodkov zagotoviti dokaze o tem, da gre res za tak primer.

Opombe

1. Pod pojmom blago je v tem kontekstu mišljeno bodisi trgovsko blago bodisi proizvod.

Status davčnega zavezanca pri presoji kraja obdavčitve storitev

IZ PRAKSE ZA PRAKSO (PR-DAV 5-5/23)

Vprašanje dokazovanja statusa davčnega zavezanca pri presoji kraja obdavčitve storitev je obravnaval Odbor sekcije preizkušenih davčnikov in o tem pripravil strokovno razlago.

IZHODIŠČE

Po 25. členu Zakona o davku na dodano vrednost (v nadaljevanju: ZDDV-1) je kraj opravljanja storitev, ki jih prejme davčni zavezanec, ki deluje kot tak, kraj, kjer ima ta davčni zavezanec sedež svoje dejavnosti. Če so te storitve opravljene za stalno poslovno enoto davčnega zavezanca, ki ni v kraju, kjer ima sedež svoje dejavnosti, je kraj opravljanja teh storitev kraj, kjer ima ta davčni zavezanec stalno poslovno enoto. Če takega sedeža ali take stalne poslovne enote ni, je kraj opravljanja storitev kraj, kjer ima davčni zavezanec, ki prejme te storitve, stalno oziroma običajno prebivališče. Če storitve prejme oseba, ki ni davčni zavezanec, pa kraj, kjer ima izvajalec storitev sedež svoje dejavnosti. Če so te storitve opravljene iz stalne poslovne enote izvajalca, ki ni v kraju, kjer ima izvajalec sedež svoje dejavnosti, je kraj opravljanja teh storitev kraj, kjer ima izvajalec storitev stalno poslovno enoto. Če takega sedeža ali take stalne poslovne enote ni, je kraj opravljanja storitev kraj, kjer ima izvajalec storitev stalno oziroma običajno prebivališče.

Po tem splošnem pravilu in nekaterih posebnih pravilih, ki kraj obdavčitve tudi opredeljujejo različno za osebe, ki so davčni zavezanci, in osebe, ki niso davčni zavezanci, je torej pomembna opredelitev statusa davčnega zavezanca, da bi se lahko pravilno določil kraj obdavčitve opravljenih storitev. Če osebo opredelimo kot davčnega zavezanca, pa je treba imeti v zvezi s tem tudi ustrezna dokazila. Postavlja se vprašanje, kako naj slovenski dobavitelji preverijo status kupcev, še posebej tistih, ki imajo sedež izven EU-ja, saj tega ni mogoče preveriti na podlagi EU ID številke za DDV.

Splošna opredelitev davčnega zavezanca je v 5. členu ZDDV-1. Davčni zavezanec je vsaka oseba, ki kjer koli neodvisno opravlja katero koli gospodarsko dejavnost, ne glede na namen opravljanja dejavnosti.

Za uporabo pravil o kraju opravljanja storitev je v 24. členu ZDDV-1 podana dodatna opredelitev davčnega zavezanca, da se za davčnega zavezanca šteje tudi:

- davčni zavezanec, ki opravlja tudi dejavnosti ali transakcije, ki v skladu s prvim odstavkom 3. člena ZDDV-1 niso opredeljene kot obdavčljive dobave blaga ali storitev, in sicer za vse storitve, ki so mu bile opravljene;
- pravna oseba, ki ni davčni zavezanec, je pa identificirana za namene DDV-ja.

Kako preveriti status prejemnika storitve, je podrobneje določeno v Izvedbeni uredbi Sveta EU št. 282/2011 v členih od 17 do 19. Tam med drugim piše, da lahko izvajalec storitev, če nima nasprotnih informacij, šteje, da ima prejemnik s sedežem v Uniji status davčnega zavezanca, če:

a) mu je prejemnik sporočil svojo ID za DDV in izvajalec to številko preveri v sistemu;
b) prejemnik še nima ID za DDV, vendar je seznanil izvajalca, da je zanjo zaprosil, in izvajalec pridobi katero koli drugo dokazilo, iz katerega se lahko razbere, da je davčni zavezanec ali pravna oseba, ki ni davčni zavezanec, ki je lahko identificiran/-a za DDV, in če z običajnimi poslovnimi varnostnimi ukrepi, kot so ukrepi v zvezi s preverjanjem identitete ali plačil, v razumni meri preveri točnost informacij, ki mu jih je poslal prejemnik.

Za zavezance, ki imajo sedež zunaj Unije, lahko skladno z določbami izvedbene uredbe davčni zavezanec šteje, da imajo status davčnega zavezanca, če:

a) od prejemnika pridobi potrdilo pristojnih davčnih organov prejemnika o vključenosti prejemnika v gospodarske dejavnosti, kar mu omogoča, da zahteva vračilo DDV-ja v skladu z Direktivo Sveta 86/560/EGS);
b) prejemnik nima potrdila, dobavitelj pa ima DDV številko ali podobno številko, ki jo je prejemniku dodelila država sedeža in se uporablja za identifikacijo dejavnosti, ali katero koli drugo dokazilo, iz katerega se lahko razbere, da je prejemnik davčni zavezanec, ter če dobavitelj z običajnimi poslovnimi varnostnimi ukrepi, kot so ukrepi v zvezi s preverjanjem identitete ali plačil, v razumni meri preveri točnost informacij, ki mu jih je poslal prejemnik.

Dokazovanje na podlagi uredbe ni edino možno oziroma pravilno.

Davčni zavezanec lahko status prejemnika storitve dokaže tudi kako drugače, vendar si davčni zavezanci z dokazovanjem statusa skladno z uredbo lahko zagotovijo pravno varnost v davčnem nadzoru. Če zavezanec želi dokazovati status z drugimi dokazili, pa obstaja večje tveganje individualne presoje davčnega organa.

Na podlagi predstavljenega izhodišča je bila sprejeta strokovna razlaga.

STROKOVNA RAZLAGA

Slovenski davčni zavezanec, ki dobavi storitve, ki so v skladu z ZDDV-1 obdavčene po sedežu naročnika, oziroma storitve, pri katerih je za določitev kraja obdavčitve pomemben status prejemnika kot davčnega zavezanca, je dolžan preveriti status prejemnika.

Če so prejemniki storitev zavezanci s sedežem v EU-ju in izvajalcu sporočijo svojo ID za DDV, se lahko to preveri z vpogledom v bazo VIES ali se pridobi drugo uradno dokazilo o obstoju ID za DDV, ki jo je priporočljivo shraniti. Če prejemnik ID za DDV nima, je potrebno drugo dokazilo, s katerim se dokaže, da je prejemnik storitev zaprosil za ID za DDV v drugi državi članici in bi glede na dokazila o njegovi dejavnosti in pravilih, določenih za davčne zavezance v Direktivi 2006/112/EU in izvedbeni uredbi, moral zaprositi za oziroma lahko pridobil ID za DDV.

Za prejemnike storitev, ki nimajo sedeža v EU-ju, lahko izvajalec storitve šteje, da imajo status davčnega zavezanca, če od njih prejme dokazilo o opravljanju gospodarske dejavnosti ali katero koli drugo potrdilo, izvajalec pa z ustrezno mero skrbnosti preveri, da prejemnik dejansko opravlja gospodarsko dejavnost.

IT kontrole in MSR 315

IZ PRAKSE ZA PRAKSO (PR-RIS 3-5/23)

Problematiko pregledov področij, ki so ključna za revizije računovodskih izkazov po Mednarodnem standardu revidiranja 315 (v nadaljevanju: MSR 315), sta obravnavala Odbor sekcije preizkušenih revizorjev informacijskih sistemov in Revizijski svet ter o tem pripravila strokovno razlago.

IZHODIŠČE

Leta 2022 je začel veljati prenovljeni MSR 315. Naziv standarda je *Prepoznavanje in ocenjevanje tveganj pomembno napačne navedbe*. Gre za enega ključnih standardov, ki jim mora revizor računovodskih izkazov upoštevati pri načrtovanju revizije. Ključni namen tega standarda je prepoznava in ocena tveganj pomembno napačnih navedb v računovodskih izkazih. Je temelj za pripravo revizijskega načrta, na podlagi katerega revizor računovodskih izkazov izvede ustrezna in zadostna preizkušanja z namenom pridobitve zadostnih in ustreznih revizijskih dokazov za izdajo mnenja. Danes vse organizacije za spremljanje poslovanja in pripravo računovodskih izkazov uporabljajo eno ali več informacijskih rešitev. Te delujejo v različnih okoljih, ki so izpostavljena različnim tveganjem. Iz vsega tega je razvidno, da je za revizorja računovodskih izkazov ključno, da se seznani s tveganji v teh okoljih in oceni njihov vpliv na računovodske izkaze. Pri tem mora razumeti vrste tveganj, ki izhajajo iz informacijskega okolja ter so ključne za spremljanje poslovanja in pripravo računovodskih izkazov. V MSR-ju 315 so ta področja opredeljena. V standardu so navedene tudi konkretne informacijske rešitve, ki naj bi bile predmet pregleda.

Tveganja, ki izhajajo iz informacijskih sistemov revidirancev pri revizijah računovodskih izkazov, vplivajo na dva segmenta:

- zaupanje podatkom in informacijam, ki izhajajo iz teh sistemov in so predmet revidiranja;
- preizkušanje aplikativnih kontrol, ki so lahko del preizkušanja.

Na podlagi predstavljenih izhodišč je bila sprejeta strokovna razlaga.

STROKOVNA RAZLAGA

Pri reviziji računovodskih izkazov delimo kontrole informacijske tehnologije na dve področji:

- *splošne kontrole informacijske tehnologije (v nadaljevanju: splošne IT kontrole) in*
- *aplikativne kontrole.*

Prve so predmet MSR-ja 315 – njihovo poznavanje ter ocena zasnove in delovanja so ključni za prepoznavanje in oceno tveganj pri revidiranju ter posledično za načrt izvajanja revizijskih postopkov preizkušanja.

Aplikativne kontrole so avtomatske notranje kontrole, vgrajene v posamezne procese, ki zagotavljajo točnost, popolnost in obstoj podatkov. Te kontrole v osnovi niso predmet prepoznavanja in ocene tveganj po MSR-ju 315. Gre za preizkušanja.

V MSR-ju 315 se zahteva, da se prepoznavanje in ocena tveganj opravi v informacijskih sistemih, znotraj katerih delujejo informacijske rešitve, ki so ključne za spremljanje poslovanja in pripravo računovodskih izkazov. Revizor informacijskih sistemov mora torej najprej popisati te informacijske rešitve. To običajno naredi:

- *s poizvedovanjem pri stranki,*
- *v sodelovanju z revizorjem računovodskih izkazov.*

Posebna previdnost je potrebna pri popolnosti zajetih informacijskih rešitev: če revidiranec uporablja več različnih informacijskih rešitev, podatki med njimi pa prehajajo samodejno prek vmesnikov, so tudi ti vmesniki predmet pregleda splošnih IT

kontrol.

Za vse tako prepoznane informacijske rešitve mora revizor preveriti zasnovo in delovanje splošnih IT kontrol. Te namreč lahko, ali pa tudi ne, zagotavljajo ustrezno podlago za zaupanje v podatke, ki jih revizor računovodskih izkazov dobi od revidiranca, in za način preizkušanja aplikativnih kontrol, če nas k temu napoti revizijski načrt. Iz MSR-ja 315 lahko splošne IT kontrole združimo v sklope:

- *upravljanje pooblastil,*
- *upravljanje sprememb,*
- *zagotavljanje neprekinjenosti poslovanja.*

Ustrezno upravljanje *pooblastil je ključno zaradi zagotavljanja ustrezne razmejitve dolžnosti. Pomembno je, da revizor računovodskih izkazov ve, ali so podatke v preteklem letu lahko vnašale in spreminjale le za to pooblaščene osebe.*

Ustrezno upravljanje sprememb *je ključno, da revizor računovodskih izkazov lahko oceni skladnost procesov in kontrol v sistemih celotno obdobje revidiranja (običajno eno leto).*

Zagotavljanje neprekinjenosti poslovanja *je ključno predvsem zato, da revizor računovodskih izkazov razume, ali so bili v revidiranem letu kakšni incidenti, ki bi kakor koli vplivali na točnost in popolnost računovodskih podatkov. Ta del je pomemben, da razumemo, ali bi bil možen kakšen vpliv v zvezi s predpostavko delujočega podjetja, ki je ena od ključnih predpostavk pri pripravi računovodskih izkazov z vsemi splošno sprejetimi okviri računovodskega poročanja v Sloveniji.*

Pri pregledih navedenih področij revizor upošteva dobre prakse zagotavljanja ustrezne informacijske varnosti, kot so npr. ISO/IEC Standardi, Cobit, GTAG ipd. Ključno je, da se seznanitev s procesi in kontrolami na navedenih področjih opravi za celotno obdobje revidiranja (običajno eno leto). Za isto obdobje je treba opraviti tudi pregled delovanja ugotovljenih kontrol.

Če revizor računovodskih izkazov izda mnenje o računovodskih izkazih, mora opraviti revizijo računovodskih izkazov skladno z

vsemi standardi revidiranja, torej tudi skladno z MSR-jem 315. Revizija računovodskih izkazov brez seznanitve z informacijskimi rešitvami, ki so ključne pri pripravi računovodskih izkazov in ocene morebitnih tveganj v okoljih, v katerih te informacijske rešitve delujejo, torej ni opravljena skladno z Mednarodnimi standardi revidiranja. V takem primeru revizor računovodskih izkazov v mnenju ne more trditi, da je bila revizija opravljena skladno z Mednarodnimi standardi revidiranja. Ključno je torej, da revizor računovodskih izkazov skladno z MSR-jem 315:

- *prepozna vse informacijske rešitve, ki so ključne za spremljanje poslovanja in pripravo računovodskih izkazov;*
- *prepozna in oceni tveganja, ki lahko vplivajo na postopke revidiranja iz tega naslova;*
- *načrtuje postopke, ki zajemajo preizkušanje notranjih kontrol, podatkov ali analitične postopke.*

NOVOSTI IN OBVESTILA

Kandidati, ki so uspešno zaključili izobraževanje pri inštitutu

Po uspešni izdelavi in zagovoru zaključnega dela je Slovenski

inštitut za revizijo izdal potrdilo (certifikat) za strokovni naziv preizkušena notranja revizorka:

- **Nini Majcen.**

Čestitkam se v imenu vseh imetnikov nazivov, vpisanih v registre pri Slovenskem inštitutu za revizijo, pridružuje tudi inštitut sam.