Gospodarska zbornica Slovenije

Vodstvo
Dimičeva 13, 1504 Ljubljana, 01 5898 413, www.gzs.si, kabinet@gzs.si

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSTVO, TURIZEM IN ŠPORT
Ad Hoc delovna skupina za poenostavitve zakonodaje z namenom krepitve konkurenčnosti gospodarstva
predsedujoči mag. Dejan Židan, državni sekretar
Kotnikova 5
1000 Ljubljana

Datum: 12. december 2025

ZADEVA: Stališče Gospodarske zbornice Slovenije o Digitalnem omnibusu

Gospodarska zbornica Slovenije (v nadaljevanju: GZS) podaja naslednje stališče in pripombe k Digitalnemu omnibusu (v nadaljevanju tudi: Omnibus), ki so usklajene s stališči, ki jih GZS na ravni EU zastopa preko evropskih gospodarskih združenj v katerih aktivno sodeluje.

Digitalni omnibus je pomembna priložnost za poenostavitev zapletenega regulativnega okvira EU na področju digitalne tehnologije, katere namen mora biti spodbujanje bolj inovativnega, konkurenčnega in usklajenega enotnega digitalnega trga. Digitalni omnibus je ključnega pomena za evropsko gospodarstvo, saj danes zapletena in prekrivajoča se digitalna pravila pogosto prinašajo dodatne stroške in administrativne obremenitve za podjetja, zlasti tista, ki želijo rasti, inovirati ali poslovati čez meje.

GZS se zavzema za jasnejša, enostavnejša in bolj usklajena digitalna pravila, ki zmanjšujejo nepotrebne administrativne obremenitve, podpirajo digitalne naložbe in omogočajo nove priložnosti za podjetja. To je bistveno za ohranjanje konkurenčnosti Evrope in okrepitev enotnega trga, ki mora delovati v praksi, ne le v teoriji.

I. Pripombe k spremembam Direktive NIS 2 (2022/2555) - Uvedba enotne vstopne točke, odprava podvajanj poročanja

Pri GZS pozdravljamo uvedbo enotne vstopne točke, vendar opominjamo, da se Digitalni omnibus osredotoča samo na to, kako podjetja poročajo o incidentih, ne pa tudi na to, kaj in kdaj morajo poročati.
Ključni problem predstavlja zasnova časovnih okvirov. V zadnjih letih je zahteva GDPR o obveščanju v roku 72 ur postala dejanska referenčna točka za poročanje o incidentih. NIS2, CER, CRA in DORA so temu dodali še vrsto zgodnjih opozoril v 24 urah (ali celo 4 urah v primeru DORA), ki jim sledijo vmesna in končna poročila. Omnibus prinaša tveganje, da se bo takšen večstopenjski model dokončno utrdil.
Čeprav podpiramo spodbujanje hitrega odzivanja na kibernetske incidente, se podjetja v praksi soočajo z odvečno administracijo: sredstva se preusmerjajo iz preiskovanja in obvladovanja incidentov na pripravo številnih obveznih posodobitev. Menimo, da bi bil boljši pristop dogovor o prožnem 72-urnem roku kot standardu, ki bi podjetjem omogočal, da poročajo prej, kadar je to

mogoče in kadar jim to prinaša dodano vrednost. Tako se lahko podjetja in organi osredotočijo na odpravo incidentov namesto na poročanje.

Trenutni seznam predpisov, po katerih je predvideno poročanje preko enotne vstopne točke, ni popoln. Vključevati bi moral tudi Akt o UI, saj bodo incidenti, ki vključujejo sisteme umetne inteligence, nedvomno imeli varnostno razsežnost. Hkrati ima ENISA že mandat za vzpostavitev enotne platforme CRA za prijavo resnih incidentov in ranljivosti. Zato menimo, da mora Digitalni omnibus jasno zavezati k uporabi te platforme kot enotne vstopne točke.

Omnibus bi moral določiti enotno osnovno predlogo za poročanje o incidentih, dopolnjeno le z omejenimi sektorskimi dodatki. Tako bi se izognili množici nekoliko različnih predlog. Osnovna predloga bi morala vključevati opis incidenta, vpliv, ukrepe za omilitev ter nadaljnje ukrepanje, z možnostjo dodatnih polj za zahteve specifične za posamezne sektorje.

Omnibus ne posega v obstoječe zapletene obveznosti CRA glede področja uporabe, bistvenih zahtev in postopkov ugotavljanja skladnosti. To pomeni, da deli kibernetskega pravnega okvira, ki najmočneje vplivajo na poslovne modele in varnostne procese, ostajajo nespremenjeni. Vsled navedenega pri GZS menimo, da bi morali biti v Omnibus vključeni dodatni ukrepi, ki so nujni za resnično poenostavitev.

II. Pripombe k spremembam Uredbe (EU) 2024/1689 (Akt o umetni inteligenci)

GZS podpira predloge Evropske komisije v okviru UI omnibusa za odlog rokov ter nujno poenostavitev izvajanja Akta o umetni inteligenci, saj trenutne časovnice ob odsotnosti harmoniziranih standardov in nepopolne pripravljenosti držav članic ne omogočajo realne skladnosti podjetij in organov. Ključna prioriteta mora biti hitro, ločeno sprejetje zamika rokov (člena 111 in 113), s čimer se prepreči regulativni prepad in zagotovi predvidljivost za podjetja. GZS prav tako podpira ohranitev obveznosti UI pismenosti iz člena 4, ob jasni opredelitvi, da gre za obveznost zagotavljanja usposabljanja in ne doseganja določenega rezultata, ter uskladitev novega člena 4a z GDPR, da podjetja dobijo enotno in jasno pravno podlago za uporabo posebnih vrst osebnih podatkov pri odpravljanju pristranskosti. Nadalje GZS poudarja potrebo po praktičnih smernicah za uporabo člena 6, ki določa klasifikacijo visokorizičnih sistemov, da se zagotovi proporcionalna obravnava in prepreči prekomerna regulacija, zlasti za MSP. Celovito GZS podpira omnibus kot priložnost za poenostavitve, večjo pravno predvidljivost ter učinkovito, varno in konkurenčno uvajanje umetne inteligence v Sloveniji in EU.

- **Pripombe k členu 113 Akta o UI (Začetek veljavnosti in uporaba)**

Akt o UI vstopa v fazo, ko naj bi podjetja začela izpolnjevati obsežne obveznosti, vendar ključni pogoji za to še niso zagotovljeni: standardi, ki so temeljno orodje za praktično skladnost, zamujajo za več kot leto, številne države članice pa še niso vzpostavile pristojnih organov. Ker bodo podjetja, posebej manjša, brez teh standardov in smernic težko izpolnila zahteve za visokorizične sisteme iz Priloge III in še zahtevnejše obveznosti iz Priloge I, GZS podpira zamik rokov za obe omenjeni prilogi, da se prepreči nerealna obremenitev gospodarstva ter omogoči varna in kakovostna implementacija zakonodaje.

Da bi bili ti nujni zamiki sprejeti pravočasno, GZS predlaga, da se časovne prilagoditve izločijo iz preostalega dela UI omnibusa in obravnavajo v ločenem, hitrejšem zakonodajnem postopku. To bi EU institucijam omogočilo, da pravočasno zagotovijo stabilno in predvidljivo časovnico, medtem ko bi se druge, vsebinsko zahtevnejše spremembe lahko obravnavale po redni poti. Tak pristop bi podjetjem zagotovil jasno okolje, zmanjšal tveganje regulativnega kaosa in omogočil uvajanje umetne inteligence na način, ki podpira inovacije in konkurenčnost evropskega gospodarstva.

- **Pripombe k členu 4 Akta o UI (Pismenost na področju UI)**

GZS podpira ohranitev določb o UI pismenosti, saj je usposabljanje zaposlenih, uporabnikov in drugih deležnikov ključno za varno, odgovorno in učinkovito uvajanje umetne inteligence. Mnoga podjetja so obveznosti iz člena 4 začela izvajati že letos, vključila izobraževanja v svoje UI strategije ter razvila praktične programe pismenosti. Zato ne vidimo potrebe po večjih spremembah člena, razen jasnejše opredelitve, da gre za obveznost zagotavljanja izobraževanja, ne določenega končnega nivoja znanja. Pojem »zadostne ravni UI pismenosti« je potrebno obrazložiti v recitalu z dodatnimi pojasnili, da se doseže pravna jasnost.

Komisijo pozivamo, naj nadgradi obstoječe smernice in primere dobrih praks ter pripravi praktična navodila za izvajanje UI pismenosti, ki bodo podjetjem pomagali pri razvoju ustreznih programov.

- **Pripombe k novemu členu 4a Akta o UI**

GZS podpira namen EU, da se podjetjem in javnim institucijam omogoči uporaba tudi posebnih vrst osebnih podatkov za odkrivanje in odpravljanje pristranskosti v UI sistemih, vendar opozarja, da mora biti to urejeno usklajeno med Aktom o UI in GDPR. Predlagani novi člen 4a Akta o UI je strožji in manj jasen kot hkrati predlagani novi člen 88c GDPR, ki za te namene uporablja podlago zakonitega interesa. Za slovenska podjetja to pomeni, da bi različna pravila v dveh predpisih ustvarila pravno negotovost in jih odvračala od uporabe podatkov za testiranje in izboljšanje nepristranskosti njihovih UI rešitev. GZS zato zagovarja, da se novi člen 4a Akta o UI prilagodi in uskladi z rešitvijo v GDPR, saj bo le enotna in jasna pravna podlaga omogočila, da slovenska podjetja varno, odgovorno in učinkovito izboljšujejo svoje sisteme umetne inteligence.

III. Pripombe k spremembam Uredbe (EU) 2016/679 (GDPR)

GDPR velja že od njene uveljavitve za eno najbolj zapletenih uredb, ki zahteva visoko raven pravnega znanja. Od podjetij zahteva celovito vzpostavljen sistem notranjih pravil, vodenje evidenc obdelave podatkov, ocene tveganj, jasno določene postopke v primerih kršitev varstva osebnih podatkov in uresničevanje pravic posameznikov. Dodatne izzive povzročajo nepopolno opredeljeni pravni pojmi (npr. obseg »znanstvene raziskave«, kriteriji »nujnosti« itd.) zaradi česar so podjetja izpostavljena različnim interpretacijam in neenotni praksi nadzornih organov. Predvsem MSP-ji pogosto nimajo zadostnih virov in strokovnega znanja za učinkovito upravljanje zapletenega regulativnega okolja, zato se znajdejo ujeta med pretiranim birokratskim pristopom in negotovostjo glede skladnosti.
Pri GZS predlagane spremembe GDPR v Digitalnem omnibusu podpiramo kot korak k sodobnejšemu, jasnejšemu in bolj sorazmernemu regulativnemu okviru, in menimo, da bodo spremembe prispevale k bolj uravnoteženemu in izvedljivemu varstvu podatkov, ki še vedno ohranja temeljne pravice posameznikov, hkrati pa podjetjem omogoča učinkovitejše delovanje, hitrejše uvajanje inovacij in manj birokratskih ovir. Še posebej pomembna je uvedba nove pravne podlage za obdelavo osebnih podatkov v okviru razvoja in delovanja sistemov UI.

Pri GZS želimo opozoriti še na dodatne vzroke administrativnih obremenitev za podjetja in predlagati naslednje izboljšave:

- **Pripombe k členu 6(1) (Zakonitost obdelave)**

Podjetja se še vedno soočajo z pravno negotovostjo glede ustrezne pravne podlage za obdelavo osebnih podatkov, zlasti glede obdelave, ki je potrebna za izvajanje pogodbe in obdelave na podlagi zakonitega interesa. Zaradi te negotovosti se pogosto pretirano uporablja pravna podlaga privolitev, četudi bi bile druge pravne podlage primernejše. Regulatorji to še zaostrujejo z

omejevanjem možnosti, pri čemer spregledajo »utrujenost« posameznikov od nenehnih zahtev za privolitev in zanemarjajo na tveganju temelječo odgovornost.
Regulatorji bi morali zagotoviti jasna in praktična navodila glede uporabe pravnih podlag, zlasti izvajanje pogodbe in zakoniti interes, da bi zmanjšali negotovost in preprečili pretirano zanašanje na privolitev kot privzeto rešitev.
Komisija bi morala spodbujati informacijske pooblaščence, da prepoznajo, podprejo in okrepijo uporabo pravne podlage zakonitega interesa in izvajanje pogodbe, kjer je to ustrezno, pri čemer naj se upošteva model odgovornosti na podlagi tveganja in ne pristopa osredotočenega na privolitev.

- **Pripombe k členu 15 (Pravica dostopa posameznika, na katerega se nanašajo osebni podatki)**

Zaradi povečane ozaveščenosti o GDPR in širjenja podatkovne ekonomije podjetja vse več sredstev namenjajo obravnavanju zahtev posameznikov za dostop do podatkov (Data Subject Access Request - DSAR). Mapiranje in konsolidacija podatkov iz različnih sistemov in virov je izredno draga in zamudna, zlasti pri psevdonimiziranih ali nestrukturiranih podatkih. Obseg in zapletenost zahtevanih razkritij, kot so pravne podlage, obdobja hrambe ali obširna pojasnila o pravicah, so pogosto nesorazmerni z dejanskim tveganjem in interesom stranke.
Celovite praktične smernice, podobni tistim, ki jih je EDPB zagotovil za videonadzor leta 2019 (Smernice 3/2019 o obdelavi osebnih podatkov z video napravami), bi podjetjem pomagale poenostaviti skladnost s pravico do dostopa v okviru povečane uporabe zapletenih algoritmov ali sistemov umetne inteligence.

- **Pripombe k členu 22 (Avtomatizirano sprejemanje posameznih odločitev, vključno z oblikovanjem profilov)**

Glede na najnovejšo sodno prakso Sodišča Evropske unije (zadeva C-634/21 SCHUFA Holding (Scoring)) in postopno uveljavljanje Akta o UI podjetja potrebujejo več smernic za uporabo pravil v zvezi z avtomatiziranim individualnim odločanjem. Sedanje Smernice o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov so bile revidirane 6. februarja 2018.
Jasna in praktična navodila, vključno s konkretnimi primeri, bi bila zelo koristna. Na primer, koristno bi bilo ponazoriti najboljše prakse za učinkovit človeški nadzor pri uporabi orodij UI za obdelavo osebnih podatkov, s čimer bi se zagotovila skladnost in odgovorno posredovanje skozi celoten proces.

- **Pripombe k členu 24 (Odgovornost upravljavca)**

Člen 24 od upravljavcev zahteva, da izvedejo ustrezne tehnične in organizacijske ukrepe, pri čemer upoštevajo vrsto, obseg, okoliščine in namene obdelave ter tveganja različne verjetnosti in resnosti za pravice in svoboščine fizičnih oseb.
Pri GZS poudarjamo pomembnost doslednega upoštevanja pristopa GDPR, ki temelji na principu tveganja in načelu sorazmernosti. V praksi se pogosto preveč osredotoča na samo možnost škode, pri čemer se premalo pozornosti posveča verjetnosti in resnosti tveganj ter temu, kako se ta razlikujejo med sektorji in poslovnimi dejavnostmi.

- **Pripombe k členu 25 (Vgrajeno in privzeto varstvo podatkov)**

Obveznosti, določene v tem členu, zahtevajo enako strogo izvajanje ne glede na velikost podjetja in občutljivost podatkov. Zato menimo, da bi bilo potrebno člen 25 revidirati tako, da bi zahteval eksplicitno razvrščanje tveganj glede na občutljivost podatkov, obseg obdelave in zmogljivosti podjetij. Poleg tega bi morala Evropska komisija uvesti za MSP prilagojene tehnične standarde za ključne zaščitne ukrepe, vključno s tehnikami anonimizacije, kontrolami dostopa in sistemi za zaznavanje kršitev, s čimer bi se zagotovilo, da so ukrepi skladnosti hkrati učinkoviti in sorazmerni s tveganji.
Vzpostaviti bi bilo potrebno trden mehanizem spremljanja, ki bi nacionalne organe pristojne za varstvo podatkov zavezal k poročanju (na primer vsaki dve leti) o stroških skladnosti za MSP ter o učinkovitosti teh poenostavljenih ukrepov, s čimer bi zagotovili stalno izboljševanje in odgovornost pri podpori prizadevanjem MSP na področju varstva podatkov.

- **Pripombe k členu 30 (Evidenca dejavnosti obdelave)**

Predlagana razširitev izjem iz člena 30(5) GDPR, ki jo predvideva že Omnibus IV predstavlja pozitiven korak k razbremenitvi podjetij določenih obveznosti iz naslova skladnosti z GDPR. Pri GZS pozdravljamo te spremembe, da bodo SMC izvzeta iz obveznosti vodenja evidenc, zlasti pa, da je ta izjema postala dostopnejša za MSP. Vendar poudarjamo, da bodo druge obveznosti iz GDPR, kot sta odgovornost in preglednost, ostale v celoti veljavne, zato bi lahko predlagana sprememba člena 30(5) imela le zelo omejen praktičen učinek.
Da bi na primer upoštevali načelo preglednosti, morajo upravljavci posameznikom, na katere se nanašajo osebni podatki, zagotoviti ažurne politike zasebnosti. Kako lahko upravljavec zagotovi ažurne politike zasebnosti, če nima ažurnega popisa svojih dejavnosti obdelave podatkov? Takšen popis pa predstavlja evidenco dejavnosti obdelave.
Zato bi morali upravljavci, tudi če bi bili izvzeti iz obveznosti vodenja evidence o dejavnostih obdelave, evidence še vedno imeti, da bi lahko pripravili in posodobili svoje politike zasebnosti ter tako obvestili posameznike, na katere se nanašajo osebni podatki. Enako velja za načelo odgovornosti. Kako lahko upravljavec podatkov spoštuje načelo odgovornosti, če ne more dokazati, da se zaveda dejavnosti obdelave, ki jih izvaja? Zato bi moral imeti dokaze ali vsaj popis obdelav osebnih podatkov, ki jih izvaja.
Zmanjšanje obveznosti vodenja evidenc za MSP mora nujno spremljati poenostavitev obveznosti MSP na področju obveščanja, odgovornosti in preglednosti, sicer bi poenostavitev člena 30(5) imela zelo omejen praktični učinek.
Vse te prilagoditve morajo biti usmerjene v večjo pozornost pristopu, ki temelji na tveganju, ter odpravi obstoječih pravnih negotovosti. Recital 13 GDPR, ki priznava poseben položaj MSP doslej v praksi ni imel skoraj nobene vloge.

- **Pripombe k členu 40 (Kodeksi ravnanja) in 42 (Potrjevanje)**

Kodeksi ravnanja in potrjevanje so bili zasnovani kot orodja za odgovornost za določene sektorje in dejavnosti obdelave. Kljub svojim prednostim, kot so spodbujanje doslednih pristopov k varstvu podatkov, omogočanje skladnosti in zmanjšanje delovne obremenitve organov za varstvo podatkov, pa se jih premalo uporablja.

Nujno je potrebno, da organi za varstvo podatkov ponovno preučijo svoje zelo stroge zahteve glede takšnih kodeksov ravnanja ter sodelujejo z deležniki prek poenostavljenih postopkov odobritve, da bi ustrezno naslovili sektorske izzive, tveganja in dobre prakse.

- **Pripombe k členu 44 in naslednjim (Prenos osebnih podatkov v tretje države ali mednarodne organizacije)**

Po sodbi Sodišča EU v zadevi Schrems II in po sprejetju okvira za varstvo podatkov med EU in ZDA (EU-US Data Privacy Framework) so Evropska komisija in regulativni organi zavzeli strogo stališče glede mednarodnega prenosa podatkov v države, s katerimi EU nima sklenjenih ustreznih sporazumov. Kljub dragim ocenam vpliva prenosa (Transfer Impact Assessments) morajo podjetja še vedno odpraviti vsa tveganja nepooblaščenega dostopa do evropskih osebnih podatkov ne glede na naravo podatkov, verjetnost dostopa tujih organov ali resnost morebitne škode. Takšen strog pristop podjetja zavezuje k uvedbi dodatnih ukrepov. To predstavlja izziv, zlasti za manjša podjetja, ki pozivajo k bolj uravnoteženemu, na tveganju temelječemu pristopu.
Evropska komisija bi morala razviti mednarodne standarde in zagotoviti jasna navodila o ravni varstva podatkov v tretjih državah. Ocene vpliva prenosa (TIA) morajo temeljiti na tveganju, pri čemer je treba razlikovati med podatki z nizkim tveganjem, kot so neobčutljivi poslovni kontaktni podatki, in podatki z visokim tveganjem, tako, da se stroge zaščitne ukrepe uporablja le, kadar je to resnično potrebno. Za podporo podjetij, zlasti MSP, bi moral Evropski odbor za varstvo podatkov (EDPB) vzdrževati standardizirane, sektorsko prilagojene predloge in kontrolne sezname za TIA, kar bi proces ocenjevanja naredilo bolj praktičen in enoten po celotni EU.

- **Pripombe k členu 82 (Pravica do odškodnine in odgovornost)**

Glede pravice do odškodnine obstajajo velike negotovosti. Čeprav je Sodišče EU pojasnilo posamezna vprašanja, v praksi še vedno ni jasno, pod kakšnimi pogoji in v kakšnem obsegu se lahko zahteva odškodnina za kršitve GDPR. To vodi do nepredvidljivih tveganj, ki obremenjujejo in zavirajo gospodarstvo (ovira za naložbe).

IV. Pripombe k spremembam Direktive ePrivacy

Pri GZS velik problem vidimo v delni integraciji pravil direktive ePrivacy. Direktiva ePrivacy ureja vso obdelavo podatkov terminalne opreme, ne le piškotkov in spletnega oglaševanja, ampak tudi vsako branje ali pisanje na napravo in zbiranje informacij z nje. Politična razprava je to pogosto omejila na pasice in sledenje, vendar je pravni obseg bistveno širši. Zavzemamo se za vključitev obdelave podatkov iz terminalne opreme v okvir GDPR, da se upravljavci lahko zanašajo na GDPR in celoten niz pravnih podlag. To vključuje predvsem zakoniti interes za namene, kot so varnost, izboljšanje storitev in raziskave. To je bistveno ne le za potrošniške storitve, ampak tudi za industrijska okolja, kjer se ePrivacy trenutno uporablja za podatke iz naprav in strojev, ki so ključni za konkurenčnost evropskih industrijskih sektorjev.

Omnibus ohranja ločen, na soglasju temelječ režim in poskuša rešiti problem z razširitvijo izjem od soglasja – za prenos, zagotavljanje osnovnih storitev, določene varnostne in merilne funkcije itd. Tak pristop ne more zajeti celotnega spektra legitimnih načinov uporabe podatkov naprav, ki jih podjetja nujno potrebujejo.

Omnibus nadalje ustvarja neprimerno asimetrijo. Medtem ko osebne podatke iz terminalne opreme vključuje v GDPR, anonimne podatke iz terminalne opreme pušča v okviru pravil ePrivacy. To pomeni, da je manj invazivna obdelava podatkov, ki ne identificira posameznikov, podvržena strožjim zahtevam kot obdelava osebnih podatkov. Takšna ureditev je nelogična in bo upravljavce spodbujala, da podatkov ne anonimizirajo.

Predlagani nov člen 88b GDPR, ki uvaja obvezne strojno berljive signale privolitve in tehnične ukrepe na ravni naprav ali programske opreme, ponovno odpira še eno nerešeno razpravo iz neuspelih pogajanj o uredbi ePrivacy. Za takšen sistem ni skupne tehnične podlage in ni jasne povezave z obstoječimi standardi. Poleg tega bi ta sistem soglasje naredil za edini dejanski mehanizem za obdelavo podatkov iz terminalne opreme: programska oprema bi postala vratar, ki bi blokiral vsako operacijo, za katero ni bil dan signal. To bi upravljavcem preprečilo obdelavo podatkov naprav, tudi če je to dovoljeno na podlagi druge pravne podlage.

Menimo, da je edina primerna rešitev ta, da se vsa obdelava podatkov terminalne opreme v celoti vključi v pravne podlage GDPR in da se postopno opusti vzporedni režim ePrivacy za dostop do naprav. Vsaka delna rešitev bo še naprej odvračala od odgovorne rabe podatkov terminalne opreme.

V. Pripombe k spremembam Uredbe (EU) 2023/2854 (Data Act)

GZS podpira prizadevanja Evropske komisije za večjo usklajenost evropskega podatkovnega okvira ter pozdravlja konsolidacijo obstoječih predpisov v enoten Data Act, saj to prinaša preglednejšo ureditev in bolj jasne postopke za javne uprave. Kljub temu predlagane spremembe ne naslovijo bistvenih vprašanj, ki za slovenska podjetja določajo možnosti ustvarjanja dodane vrednosti iz podatkov, zaščito poslovno občutljivih informacij ter razvoj naprednih digitalnih storitev. Posebej izstopa težava obveznega, horizontalnega deljenja podatkov, ki ne upošteva

dejanskih poslovnih modelov v industriji, energetiki, zdravstvu in napredni proizvodnji ter lahko oslabi konkurenčnost podjetij in ovira vlaganja v digitalne rešitve.

GZS zato zagovarja, da se pristop k deljenju podatkov uravnoteži in temelji na prostovoljnem sodelovanju, ki se je kot najučinkovitejši model že izkazal v praksi. Industrijsko oblikovani panožni kodeksi ravnanja lahko ustrezno opredelijo dostop, zaščitijo občutljive informacije, zagotovijo interoperabilnost in jasno razdelijo odgovornosti v vrednostni verigi. GZS predlaga, da omnibus omogoči Komisiji formalno priznanje takšnih kodeksov, kar bi podjetjem ponudilo stabilen in zaupanja vreden okvir, v katerem izmenjava podatkov dejansko podpira inovacije, varnost in konkurenčnost, hkrati pa se izognemo negativnim učinkom prisilnega odpiranja podatkov v sektorjih, ki temeljijo na dolgoročnih vlaganjih v digitalne tehnologije in industrijsko znanje.

VI. Harmonizacija implementacije med državami članicami

Čeprav je digitalna regulacija v EU zasnovana enotno, se v praksi pri njenem prenosu in izvajanju med državami članicami še vedno pojavljajo razhajanja.
Ena od osrednjih težav je t. i. gold plating, države članice pri implementaciji prava EU (zlasti direktiv) sprejemajo nacionalne določbe, ki presegajo minimalne zahteve oziroma standarde, določene v aktih EU, ter s tem nalagajo dodatne ali strožje materialne in/ali postopkovne obveznosti. Tako države članice pogosto ustvarjajo ovire in pripomorejo k večji razdrobitvi enotnega trga zaradi nepravilnega in nepotrebno različnega ali obremenjujočega izvajanja prava EU. To podjetjem, ki poslujejo čezmejno povečuje stroške skladnosti, saj so podjetja prisiljena slediti različnim nacionalnim zakonodajam. Takšna razdrobljenost nesorazmerno bremeni MSP-je ter zmanjšuje učinkovitost in predvidljivost regulativnega okolja v EU.

Menimo, da je nujno potrebno, da Komisija pripravi ukrepe, ki bi omejili možnost nacionalnega razširjanja obveznosti. Ter, da Slovenija pri prenosu in izvajanju aktov EU s področja digitalne regulacije spoštuje načelo minimalne implementacije ter se vzdrži kakršnih koli dodatnih zahtev, ki jih pravo EU ne predpisuje in niso objektivno potrebne za zagotovitev skladnosti z obveznostmi iz prava EU.

VII. »one-stop-shop« za digitalno skladnost

Slovenska podjetja se pri izpolnjevanju obveznosti digitalne zakonodaje pogosto soočajo z nepreglednostjo in razpršenostjo informacij. Posledično težko ugotovijo, kateri predpisi se uporabljajo za njihov konkreten primer, katere obrazce morajo uporabiti, kateri je pristojni organ za poročanje ter katera dokumentacija je obvezna. Takšna razdrobljenost informacij povzroča znatne časovne in administrativne obremenitve, povečuje tveganje napačnih ravnanj ter povečuje odvisnost od zunanjih svetovalcev za vprašanja, ki bi jih bilo mogoče učinkovito razrešiti prek enotne kontaktne točke (»one-stop-shop«).

Vsled zgoraj navedenemu GZS predlaga vzpostavitev kompetenčnega centra za digitalno skladnost, ki bi deloval kot enotna kontaktna točka (»one-stop-shop«) in ki bi podjetjem omogočal

jasno navigacijo po digitalni zakonodaji, pomoč pri zagotavljanju skladnosti in dostop do standardiziranih dokumentov. Menimo, da bi vzpostavitev takšnega centra bistveno zmanjšala administrativne obremenitve, okrepila pravno varnost podjetij ter pospešila njihovo prilagajanje hitro razvijajočemu se evropskemu digitalnemu regulativnemu okviru. Prepričani smo, da bi na podlagi podeljenega javnega pooblastila takšna enotna kontaktna točka lahko bila vzpostavljena pod okriljem GZS.

****

Predlagamo, da pristojno ministrstvo zgoraj podane usmeritve oziroma predloge GZS vsebinsko povzame in jih smiselno zagovarja kot stališče Republike Slovenije na EU ravni. Za dodatna pojasnila smo vam na voljo.

S spoštovanjem,

Pripravila:
Marko Štefančič
Nataša Tomažin

mag. Marko Djinović, l.r.
Izvršni direktor