					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P37S					Naziv dokumenta: **Politika pravne i regulatorne usklađenosti**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrola 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
GDPR EU	Članci 5, 6, 32, 33	
Direktiva EU NIS2	Članci 21(2)(a), 21(2)(f), 23	
Uredba EU DORA	Članci 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Svrha

1.1 Ova politika definira pristup organizacije utvrđivanju, ispunjavanju i dokazivanju usklađenosti s pravnim, regulatornim i ugovornim obvezama.

1.2 Njome se utvrđuju jasne odgovornosti i praktični koraci kako bi organizacija ispunila svoje obveze usklađenosti, uključujući propise o zaštiti podataka, okvire kibernetičke sigurnosti, ugovore s klijentima i certifikacijske standarde.

1.3 Njome se osigurava da organizacija, i bez namjenskog tima za usklađenost, može održavati pravno usklađeno poslovanje, primjereno odgovoriti na incidente i zadržati spremnost za reviziju.

1.4 Ova je politika ključna za omogućavanje certifikacije prema ISO/IEC 27001:2022 i ispunjavanje vanjskih očekivanja klijenata, regulatora i partnera.

2. Područje primjene

2.1 Ova se politika primjenjuje na:

2.1.1 sve zaposlenike, ugovorne izvođače, freelancere i dobavljače trećih strana

2.1.2 sve usluge, operacije, sustave i aktivnosti obrade podataka u kojima organizacija mora ispunjavati pravne ili ugovorne zahtjeve

2.1.3 sve lokacije i uređaje koji se koriste za obradu poslovnih informacija, bilo u uredima, pri radu na daljinu ili u sustavima smještenima u oblaku

2.2 Ova politika obuhvaća:

2.2.1 propise o zaštiti podataka kao što je GDPR

2.2.2 propise o kibernetičkoj sigurnosti kao što je Direktiva EU NIS2

2.2.3 sektorski specifične obveze, ako su primjenjive

2.2.4 ugovore s klijentima, ugovore o povjerljivosti i revizijske klauzule

2.2.5 dobrovoljne certifikacije (npr. ISO/IEC 27001) i interne politike koje se moraju provoditi radi usklađenosti

3. Ciljevi

3.1 Uspostaviti odgovornost: dodijeliti jasnu odgovornost za praćenje, ažuriranje i provedbu pravnih, regulatornih i ugovornih obveza.

3.2 Zaštititi organizaciju: smanjiti rizik od kršenja propisa, novčanih kazni, povreda podataka i reputacijske štete.

3.3 Osigurati spremnost za reviziju: održavati dokazive zapise koji pokazuju kako organizacija ispunjava svoje obveze usklađenosti.

3.4 Podržati integraciju politika: osigurati dosljednu provedbu pravnih i regulatornih obveza u svim politikama i procesima.

3.5 Transparentno upravljati iznimkama: osigurati da se svaka iznimka od zahtjeva usklađenosti dokumentira, obrazloži i odobri kako bi se izbjegla odgovornost.

4. Uloge i odgovornosti

4.1 Glavni direktor (GM)

4.1.1 snosi ukupnu odgovornost za pravnu i regulatornu usklađenost organizacije

4.1.2 vodi Registar usklađenosti i osigurava njegovu ažurnost

4.1.3 pregledava ugovore s klijentima i osigurava da se specifične obveze prate i provode

4.1.4 odobrava iznimke od obveza usklađenosti samo kada su pravno opravdane i uz primjenu kompenzacijskih kontrola

4.2 Vanjski savjetnici (npr. pravni, IT ili savjetnici za usklađenost)

4.2.1 pružaju podršku GM-u u utvrđivanju primjenjivih propisa, certifikacija i obveza (npr. GDPR, NIS2, ISO/IEC 27001)

4.2.2 daju smjernice za tumačenje novih propisa ili izmjena postojećih zakona

4.2.3 prema potrebi mogu pomagati pri ažuriranju politika, revizijama ili odgovoru na povrede kada postoji pravna izloženost

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Planirani godišnji pregled

9.1.1 Ovu politiku GM mora pregledati svakih 12 mjeseci.

9.1.2 Pregled mora potvrditi:

9.1.2.1 relevantnost za aktualni pravni i ugovorni kontekst

9.1.2.2 odgovarajući odraz ugovora s klijentima i obveza pružanja usluga

9.1.2.3 usklađenost s Registrom usklađenosti i drugim politikama

9.2 Ažuriranja potaknuta događajem

9.2.1 Neposredan pregled obvezan je ako:

9.2.1.1 novi zakon ili propis postane primjenjiv (npr. novo pravilo zaštite podataka)

9.2.1.2 klijent u svoj ugovor doda složene zahtjeve usklađenosti

9.2.1.3 dođe do povrede ili incidenta neusklađenosti

9.2.1.4 organizacija proširi poslovanje na regulirano tržište ili sektor

9.3 Odobravanje ažuriranja i upravljanje verzijama

9.3.1 Sva ažuriranja moraju biti dokumentirana, verzionirana i odobrena od strane GM-a.

9.3.2 Povijesne verzije moraju se čuvati za potrebe revizije i pravne potrebe.

9.4 Komunikacija promjena

9.4.1 Zaposlenici i ugovorni izvođači moraju biti obaviješteni o promjenama politike u roku od 5 radnih dana od odobrenja.

9.4.2 Svi dobavljači na koje promjene utječu također moraju potvrditi prihvaćanje ažuriranih uvjeta prije nastavka pružanja usluge.

10. Povezane politike i poveznice

10.1 Ova se politika podržava i provodi kroz sljedeće SME politike:

10.1.1 P3S – Politika prihvatljivog korištenja (AUP): sprječava ponašanja koja mogu dovesti do kršenja pravnih ili ugovornih uvjeta (npr. neovlašteno dijeljenje datoteka)

10.1.2 P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: educira osoblje o obvezama usklađenosti i načinima izbjegavanja kršenja

10.1.3 P14S – Politika zadržavanja i zbrinjavanja podataka: osigurava zakonite prakse postupanja s podacima tijekom cijelog životnog ciklusa podataka

10.1.4 P17S – Politika zaštite podataka i privatnosti: ispunjava zahtjeve GDPR-a i zahtjeve klijenata u vezi s postupanjem s podacima

10.1.5 P30S – Politika odgovora na incidente: utvrđuje način odgovora na povrede podataka ili neuspjehe usklađenosti, uključujući rokove za obavješćivanje

10.1.6 P36S – Politika društvenih mreža i vanjske komunikacije: osigurava da javna komunikacija ne krši pravne ili regulatorne obveze

10.2 Svaka povezana politika provodi dio okvira pravne usklađenosti i mora se primjenjivati usklađeno s ostalima.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 6.1 – Radnje za postupanje s rizicima i prilikama: uključuje rizike usklađenosti

11.1.2 Točka 8.1 – Operativno planiranje i upravljanje: zahtijeva provedbu procesa koji ispunjavaju pravne i ugovorne zahtjeve

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.36 – usmjerava organizaciju u vođenju evidencije o obvezama i osiguravanju odgovarajućeg odgovora na pravne i regulatorne zahtjeve

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politika i postupci: zahtijeva formalne politike usklađenosti

11.3.2 PM-1 – Plan programa informacijske sigurnosti: zahtijeva integraciju pravne usklađenosti u planiranje sigurnosti

11.3.3 CA-1 – Procjena, autorizacija i praćenje

11.3.4 AU-1 – Politika revizije: zahtijeva održavanje dokaza o usklađenosti

11.4 GDPR EU

11.4.1 Članak 5 – načela obrade podataka, uključujući odgovornost

11.4.2 Članak 6 – pravna osnova za obradu

11.4.3 Članak 32 – sigurnost obrade

11.4.4 Članak 33 – prijava povrede u roku od 72 sata

11.5 Direktiva EU NIS2

11.5.1 Članak 21(2)(a) i (f) – interne politike za upravljanje rizikom i regulatorni nadzor

11.5.2 Članak 23 – provedba i sankcije za neusklađenost

11.6 Uredba EU DORA

11.6.1 Članak 5(2) – nadzor nad upravljanjem IKT rizicima

11.6.2 Članak 9(1) – interno upravljanje usklađenošću

11.6.3 Članak 17 – ugovorni aranžmani s pružateljima IKT usluga

11.7 COBIT 2019

11.7.1 APO12 – Upravljani rizik: osigurava da se rizici usklađenosti prate i obrađuju

11.7.2 APO13 – Upravljana sigurnost: obuhvaća provedbu regulatorne i ugovorne usklađenosti utemeljene na riziku

11.7.3 DSS01 – Upravljane operacije: zahtijeva operativnu spremnost za ispunjavanje pravnih obveza