					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P37					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**

1. Svrha

1.1 Ova politika uspostavlja obvezni okvir za utvrđivanje, upravljanje i osiguravanje usklađenosti sa svim pravnim, regulatornim i ugovornim obvezama relevantnima za informacijsku sigurnost, zaštitu privatnosti podataka i operativne funkcije organizacije.

1.2 Cilj je spriječiti neusklađenost koja može dovesti do novčanih kazni, pravne odgovornosti, poremećaja poslovanja, narušavanja ugleda ili regulatornog postupanja.

1.3 Ova politika podupire integraciju zahtjeva usklađenosti u upravljanje, upravljanje rizicima, operativne procese, životne cikluse projekata i projektiranje sustava.

1.4 Njome se osigurava da su sve relevantne obveze — u različitim jurisdikcijama, industrijskim sektorima i regulatornim okvirima — jasno dokumentirane, procijenjene, praćene i provedene unutar organizacije.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve odjele, funkcije, poslovne jedinice i osobe koje djeluju u ime organizacije, uključujući:

2.1.1 zaposlenike na neodređeno i određeno vrijeme

2.1.2 ugovorne izvođače, savjetnike i vježbenike

2.1.3 dobavljače, izvršitelje obrade ili partnere koji postupaju s podacima, sustavima ili regulatornim obvezama organizacije

2.1.4 svaki poslovni proces, projekt ili inicijativu koji podliježu pravnim ili regulatornim zahtjevima

2.2 Područja usklađenosti uređena ovom politikom uključuju, ali nisu ograničena na:

2.2.1 obveze informacijske i kibernetičke sigurnosti (npr. ISO/IEC 27001, NIS2, DORA)

2.2.2 zakonodavstvo o zaštiti podataka i privatnosti (npr. GDPR, sektorski propisi o privatnosti)

2.2.3 sektorske propise (npr. financijski, medicinski, automobilski, obrambeni sektor)

2.2.4 ugovorne obveze koje proizlaze iz ugovora o povjerljivosti, ugovora o razini usluge (SLA) ili ugovora o obradi podataka

2.2.5 pravne zahtjeve povezane s prijavom incidenata, postupanjem prema tijelima kaznenog progona i međunarodnim prijenosom podataka

3. Ciljevi

3.1 Osigurati da se svi primjenjivi zakoni, propisi, standardi i ugovorne obveze utvrde, dokumentiraju, protumače i provedu u cijeloj organizaciji.

3.2 Integrirati pravne i regulatorne zahtjeve u sustav upravljanja informacijskom sigurnošću (ISMS), procese upravljanja rizicima, ugovore s dobavljačima te projektiranje proizvoda i usluga.

3.3 Uspostaviti mehanizam za proaktivno praćenje regulatornih promjena te odgovarajuće ažuriranje kontrola i dokumentacije.

3.4 Definirati jasnu odgovornost za nadzor usklađenosti, eskalaciju kršenja, postupanje s iznimkama i vanjsko izvješćivanje.

3.5 Osigurati mogućnost revizije i dokazivanja pravnog i regulatornog profila organizacije tijekom inspekcija, istraga ili certifikacijskih pregleda.

4. Uloge i odgovornosti

4.1 Izvršno rukovodstvo

4.1.1 Snosi stratešku odgovornost za usklađenost s pravnim i regulatornim zahtjevima na razini cijele organizacije.

4.1.2 Pregledava i odobrava odluke o usklađenosti visokog rizika, uključujući prihvaćanje rizika i pravne sporove.

4.2 Službenik za usklađenost / pravni savjetnik / voditelj pravnih poslova

4.2.1 Održava Registar obveza usklađenosti, koji sadrži sve primjenjive zakone, standarde, certifikate i ugovorne odredbe.

4.2.2 Provodi procjene pravnog učinka za nove usluge, tržišta ili tokove podataka.

4.2.3 Daje mjerodavna tumačenja zakona i standarda.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Godišnji pregled politike

9.1.1 Ova politika mora se pregledati najmanje jednom u kalendarskoj godini radi:

9.1.1.1 osiguravanja trajne usklađenosti s ažuriranim zakonima, industrijskim standardima i regulatornim okvirima

9.1.1.2 potvrde operativne djelotvornosti na temelju revizijskih nalaza i povijesti incidenata

9.1.1.3 odražavanja organizacijskih promjena (npr. nove jurisdikcije, sustavi ili poslovne linije)

9.2 Pregledi potaknuti događajem

9.2.1 Izvanredni pregledi moraju se pokrenuti kada:

9.2.2 se donese ili ažurira novi pravni ili regulatorni zahtjev

9.2.3 incident usklađenosti ili revizija otkrije nedostatke politike

9.2.4 organizacija uđe na novo tržište ili u novu uslužnu djelatnost uređenu posebnim okvirima usklađenosti

9.2.5 trendovi regulatornog postupanja ili smjernice regulatora upućuju na promjenu profila rizika

9.3 Vlasništvo i odobrenje

9.3.1 Pravna služba i službenik za usklađenost zajednički su odgovorni za koordinaciju postupka pregleda.

9.3.2 Konačne izmjene politike mora odobriti izvršno rukovodstvo te ih treba evidentirati u registru promjena politike, uz povezane reference upravljanja promjenama i planove komunikacije.

9.4 Upravljanje verzijama i komunikacija

9.4.1 Svaka ažurirana verzija ove politike mora:

9.4.1.1 sadržavati sažetak ključnih promjena

9.4.1.2 biti ponovno distribuirana službenim kanalima (npr. portal za politike, LMS, interni bilteni)

9.4.1.3 zahtijevati potvrdu upoznatosti od pogođenog osoblja, osobito onoga u pravnim, operativnim, sigurnosnim i ulogama upravljanja dobavljačima

10. Povezane politike i upućivanja

10.1 Ova politika primjenjuje se zajedno sa sljedećim politikama unutar ISMS-a organizacije i dodatno ih podupire:

10.1.1 P1 – Politika informacijske sigurnosti: utvrđuje temeljna načela upravljanja kojima se osigurava da su sve politike informacijske sigurnosti — uključujući usklađenost — usklađene sa strateškim poslovnim i regulatornim zahtjevima.

10.1.2 P2 – Politika uloga i odgovornosti u upravljanju: definira ovlasti odlučivanja, uključujući pravne uloge i uloge usklađenosti odgovorne za regulatorni nadzor i odgovornost.

10.1.3 P6 – Politika upravljanja rizicima: podupire vrednovanje, vlasništvo i ublažavanje rizika pravne i regulatorne usklađenosti na razini cijele organizacije.

10.1.4 P8 – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: osigurava da je svo osoblje upoznato s odgovornostima u području usklađenosti te da prima osposobljavanje primjereno svojoj ulozi.

10.1.5 P12 – Politika upravljanja imovinom: dodatno učvršćuje pravne obveze upravljanja i zaštite regulirane ili ugovorne imovine, uključujući imovinu koja sadrži osobne podatke i elemente kritične infrastrukture.

10.1.6 P30 – Politika odgovora na incidente: uređuje obvezne pravne prijave (npr. članak 33. GDPR-a) i postupke eskalacije u slučaju povrede usklađenosti ili regulatornog događaja.

10.1.7 P33 – Politika praćenja revizije i usklađenosti: osigurava strukturirane aktivnosti potvrđivanja, uključujući testiranje kontrola i prikupljanje dokaza, potrebne za unutarnju i vanjsku provjeru usklađenosti.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 4.2 – Razumijevanje potreba i očekivanja zainteresiranih strana: zahtijeva utvrđivanje i integraciju pravnih i regulatornih zahtjeva u ISMS.

11.1.2 Točka 5.1 – Vodstvo i opredijeljenost: propisuje izvršnu odgovornost za uspostavu i održavanje pravne usklađenosti u cijeloj organizaciji.

11.1.3 Točka 5.3 – Organizacijske uloge, odgovornosti i ovlasti: osigurava jasnoću uloga za pravni nadzor i regulatornu usklađenost.

11.1.4 Kontrola A.5.36 – Usklađenost s pravnim i ugovornim zahtjevima: uspostavlja obvezu utvrđivanja i ispunjavanja obveza koje proizlaze iz zakona, propisa i ugovora.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.36: daje smjernice za provedbu održavanja registra obveza usklađenosti, provjere regulatornih zahtjeva i osiguravanja strukturiranog čuvanja dokaza.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politika i postupci sigurnosnog planiranja: zahtijeva da se zahtjevi usklađenosti ugrade u strukture upravljanja i dokumentaciju.

11.3.2 PM-1 – Plan programa informacijske sigurnosti: propisuje regulatorne kontrole kao sastavni dio šireg sigurnosnog programa.

11.3.3 CA-7 – Kontinuirano praćenje: podupire nadzor nad djelotvornošću kontrola u ispunjavanju pravnih zahtjeva i zahtjeva politike.

11.3.4 AU-9 – Zaštita revizijskih informacija: osigurava da su revizijski zapisi i dokumentacija usklađenosti zaštićeni i dostupni za pregled.

11.4 GDPR EU (2016/679)

11.4.1 Članak 5 – Načela obrade: zahtijeva zakonitu obradu, transparentnost i odgovornost.

11.4.2 Članak 6 – Zakonitost obrade: propisuje odgovarajuće pravne osnove za sve aktivnosti obrade podataka.

11.4.3 Članak 24 – Odgovornost voditelja obrade: uspostavlja izravnu odgovornost za osiguravanje regulatorne usklađenosti.

11.4.4 Članak 32 – Sigurnost obrade: zahtijeva provedbu odgovarajućih tehničkih i organizacijskih kontrola.

11.4.5 Članak 33 – Prijava povrede: zahtijeva da se povrede osobnih podataka prijave nadležnim tijelima u roku od 72 sata.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članci 20–21: zahtijevaju da ključni i važni subjekti uspostave dokumentirano upravljanje, strategije pravne usklađenosti i kontinuirani pregled pravnih rizika.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 5(2) – Okvir za upravljanje IKT rizicima: zahtijeva integraciju pravne usklađenosti u šire funkcije upravljanja rizicima i nadzora.

11.6.2 Članak 19 – Rizik trećih strana povezan s IKT-om: nameće posebne pravne zahtjeve za upravljanje ugovornim i regulatornim obvezama koje uključuju vanjske dobavljače i platforme.

11.7 COBIT 2019

11.7.1 APO12 – Upravljanje rizicima: uključuje pravnu i regulatornu usklađenost kao ključne sastavnice upravljanja rizicima organizacije.

11.7.2 MEA03 – Praćenje usklađenosti s vanjskim zahtjevima: definira kontinuirano praćenje, postupanje s iznimkama i spremnost za reviziju za sve oblike regulatornih obveza.