					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P37					Naslov dokumenta: **Politika pravne in regulativne skladnosti**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

1. Namen

1.1 Ta politika določa obvezen okvir za identifikacijo, upravljanje in zagotavljanje skladnosti z vsemi pravnimi, regulativnimi in pogodbenimi obveznostmi, ki so pomembne za informacijsko varnost, varstvo podatkov in operativne funkcije organizacije.

1.2 Cilj je preprečiti neskladnost, ki bi lahko povzročila globe, pravno odgovornost, motnje poslovanja, škodo ugledu ali izvršilne ukrepe regulatorjev.

1.3 Ta politika podpira vključevanje zahtev skladnosti v upravljanje, procese obvladovanja tveganj, operativne poteke dela, življenjske cikle projektov in zasnovo sistemov.

1.4 Zagotavlja, da so vse relevantne obveznosti v različnih jurisdikcijah, panožnih sektorjih in regulativnih področjih uporabe jasno dokumentirane, ocenjene, spremljane in uveljavljene znotraj organizacije.

2. Področje uporabe

2.1 Ta politika velja za vse oddelke, funkcije, poslovne enote in posameznike, ki delujejo v imenu organizacije, vključno z:

2.1.1 zaposlenimi za nedoločen ali določen čas

2.1.2 pogodbenimi izvajalci, svetovalci in pripravniki

2.1.3 zunanjimi dobavitelji, obdelovalci osebnih podatkov ali partnerji, ki obdelujejo podatke organizacije, uporabljajo njene sisteme ali izvajajo njene regulativne obveznosti

2.1.4 vsemi poslovnimi procesi, projekti ali pobudami, ki so predmet pravnega ali regulativnega nadzora

2.2 Področja skladnosti, ki jih ureja ta politika, med drugim vključujejo:

2.2.1 obveznosti s področja informacijske in kibernetske varnosti (npr. ISO/IEC 27001, NIS2, DORA)

2.2.2 zakonodajo s področja varstva podatkov in zasebnosti (npr. GDPR, panožni predpisi o zasebnosti)

2.2.3 sektorske predpise (npr. finančni, zdravstveni, avtomobilski, obrambni sektor)

2.2.4 pogodbene obveznosti, ki izhajajo iz pogodb o nerazkrivanju informacij, sporazumov o ravni storitev (SLA) ali pogodb o obdelavi osebnih podatkov s tretjimi osebami

2.2.5 pravne zahteve v zvezi s poročanjem o incidentih, sodelovanjem z organi pregona in mednarodnimi prenosi podatkov

3. Cilji

3.1 Zagotoviti, da so vsi veljavni zakoni, predpisi, standardi in pogodbene obveznosti identificirani, dokumentirani, interpretirani in uveljavljeni na ravni celotne organizacije.

3.2 Vključiti pravne in regulativne zahteve v sistem upravljanja informacijske varnosti (ISMS), procese obvladovanja tveganj, dogovore z dobavitelji ter zasnovo produktov in storitev.

3.3 Vzpostaviti mehanizem za proaktivno spremljanje regulativnih sprememb ter ustrezno posodabljanje kontrol in dokumentacije.

3.4 Določiti jasno odgovornost za nadzor skladnosti, eskalacijo kršitev, obravnavo izjem in zunanje poročanje.

3.5 Zagotoviti preverljivost in pravno vzdržnost pravnega in regulativnega profila organizacije med inšpekcijskimi nadzori, preiskavami ali certifikacijskimi presojami.

4. Vloge in odgovornosti

4.1 Najvišje vodstvo

4.1.1 Nosi strateško odgovornost za skladnost s pravnimi in regulativnimi zahtevami na ravni celotne organizacije.

4.1.2 Pregleduje in odobrava odločitve o skladnosti z visokim tveganjem, vključno s sprejemanjem tveganj in pravnimi spori.

4.2 Pooblaščenec za skladnost / generalni pravni svetovalec / pravni svetovalec

4.2.1 Vzdržuje evidenco obveznosti skladnosti, v kateri so navedeni vsi veljavni zakoni, standardi, certifikati in pogodbene klavzule.

4.2.2 Izvaja presoje pravnih vplivov za nove storitve, trge ali tokove podatkov.

4.2.3 Podaja verodostojno razlago zakonov in standardov.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1 Letni pregled politike

9.1.1 Ta politika mora biti pregledana najmanj enkrat v koledarskem letu, da se:

9.1.1.1 zagotovi trajna skladnost s posodobljenimi zakoni, panožnimi standardi in regulativnimi okviri

9.1.1.2 preveri operativna učinkovitost na podlagi ugotovitev presoj in zgodovine incidentov

9.1.1.3 upoštevajo organizacijske spremembe (npr. nove jurisdikcije, sistemi ali poslovne linije)

9.2 Pregledi na podlagi sprožilcev

9.2.1 Vmesni pregledi se morajo začeti, kadar:

9.2.2 je sprejeta ali posodobljena nova pravna ali regulativna zahteva

9.2.3 incident skladnosti ali presoja razkrije pomanjkljivosti politike

9.2.4 organizacija vstopi na nov trg ali začne novo storitveno dejavnost, za katero veljajo ločeni okviri skladnosti

9.2.5 trendi izvrševanja ali usmeritve regulatorjev kažejo na spremembe profila tveganja

9.3 Lastništvo in odobritev

9.3.1 Pravna služba in pooblaščenec za skladnost sta skupaj odgovorna za usklajevanje postopka pregleda.

9.3.2 Končne spremembe politike mora odobriti najvišje vodstvo in jih evidentirati v registru sprememb politike skupaj s povezanimi sklici na nadzor sprememb in komunikacijskimi načrti.

9.4 Nadzor različic in komuniciranje

9.4.1 Vsaka posodobljena različica te politike mora:

9.4.1.1 vključevati povzetek ključnih sprememb

9.4.1.2 biti ponovno distribuirana prek uradnih kanalov (npr. portal politik, LMS, interni bilteni)

9.4.1.3 zahtevati potrditev prizadetega osebja, zlasti zaposlenih v pravnih, operativnih, varnostnih in vlogah upravljanja dobaviteljev

10. Povezane politike in povezave

10.1 Ta politika se uporablja skupaj z naslednjimi politikami v okviru sistema upravljanja informacijske varnosti (ISMS) organizacije in jih dopolnjuje:

10.1.1 P1 – Politika informacijske varnosti: določa temeljna načela upravljanja, ki zagotavljajo, da so vse politike informacijske varnosti, vključno s skladnostjo, usklajene s strateškimi poslovnimi in regulativnimi zahtevami.

10.1.2 P2 – Politika vlog in odgovornosti upravljanja: določa pristojnosti odločanja, vključno s pravnimi vlogami in vlogami skladnosti, odgovornimi za regulativni nadzor in odgovornost.

10.1.3 P6 – Politika upravljanja tveganj: podpira vrednotenje, lastništvo in zmanjševanje tveganj pravne in regulativne skladnosti na ravni celotne organizacije.

10.1.4 P8 – Politika ozaveščanja in usposabljanja za informacijsko varnost: zagotavlja, da so vsi zaposleni seznanjeni z odgovornostmi glede skladnosti in prejmejo vlogi prilagojeno usposabljanje.

10.1.5 P12 – Politika upravljanja sredstev: utrjuje pravne obveznosti za upravljanje in zaščito reguliranih ali pogodbenih sredstev, vključno s tistimi, ki vključujejo osebne podatke in kritično infrastrukturo.

10.1.6 P30 – Politika odzivanja na incidente: ureja obvezna pravna obvestila (npr. člen 33 GDPR) in postopke eskalacije v primeru kršitve skladnosti ali regulativnega dogodka.

10.1.7 P33 – Politika spremljanja presoj in skladnosti: zagotavlja strukturirane dejavnosti zagotavljanja, vključno s testiranjem kontrol in zbiranjem dokazil, ki so potrebni za notranje in zunanje preverjanje skladnosti.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 4.2 – Razumevanje potreb in pričakovanj zainteresiranih strani: zahteva identifikacijo in vključitev pravnih ter regulativnih zahtev v ISMS.

11.1.2 Klavzula 5.1 – Vodenje in zavezanost: določa odgovornost izvršnega vodstva za vzpostavitev in vzdrževanje pravne skladnosti v organizaciji.

11.1.3 Klavzula 5.3 – Organizacijske vloge, odgovornosti in pooblastila: zagotavlja jasno opredelitev vlog za pravni nadzor in regulativno skladnost.

11.1.4 Priloga A, Kontrola 5.36 – Skladnost s pravnimi in pogodbenimi zahtevami: določa zahtevo za identifikacijo in izpolnjevanje obveznosti, ki izhajajo iz zakonov, predpisov in pogodb.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.36: podrobneje določa smernice za vzdrževanje evidence obveznosti skladnosti, preverjanje regulativnih zahtev in zagotavljanje strukturirane hrambe dokazil.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politika in postopki varnostnega načrtovanja: zahteva, da so zahteve skladnosti vključene v strukture upravljanja in dokumentacijo.

11.3.2 PM-1 – Načrt varnostnega programa: določa, da so regulativne kontrole sestavni del širšega varnostnega programa.

11.3.3 CA-7 – Stalno spremljanje: podpira nadzor nad učinkovitostjo kontrol pri izpolnjevanju pravnih zahtev in zahtev politike.

11.3.4 AU-9 – Zaščita revizijskih informacij: zagotavlja, da so revizijski dnevniki in zapisi o skladnosti zaščiteni ter na voljo za pregled.

11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 5 – Načela v zvezi z obdelavo: zahteva zakonito obdelavo, preglednost in odgovornost.

11.4.2 Člen 6 – Zakonitost obdelave: določa ustrezne pravne podlage za vse dejavnosti obdelave podatkov.

11.4.3 Člen 24 – Odgovornost upravljavca: vzpostavlja neposredno odgovornost za zagotavljanje regulativne skladnosti.

11.4.4 Člen 32 – Varnost obdelave: zahteva uvedbo ustreznih tehničnih in organizacijskih kontrol.

11.4.5 Člen 33 – Obvestilo o kršitvi: zahteva, da se kršitve varnosti osebnih podatkov v 72 urah prijavijo pristojnim organom.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člena 20–21: zahtevata, da bistveni in pomembni subjekti uvedejo dokumentirano upravljanje, strategije pravne skladnosti in stalni pregled pravnih tveganj.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 5(2) – Okvir upravljanja IKT-tveganj: zahteva vključitev pravne skladnosti v širše funkcije upravljanja tveganj in nadzora.

11.6.2 Člen 19 – Tveganje IKT, povezano s tretjimi osebami: določa posebne pravne zahteve za upravljanje pogodbenih in regulativnih obveznosti, ki vključujejo zunanje dobavitelje in platforme.

11.7 COBIT 2019

11.7.1 APO12 – Upravljanje tveganj: vključuje pravno in regulativno skladnost kot kritični sestavini upravljanja tveganj organizacije.

11.7.2 MEA03 – Spremljanje skladnosti z zunanjimi zahtevami: določa stalno spremljanje, obravnavo izjem in pripravljenost na revizijo za vse oblike regulativnih obveznosti.