					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P17					Naziv dokumenta: **Politika zaštite podataka i privatnosti**							
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, 6.1.3, 8.1, 10	Relevantne opće, tehničke i upravljačke kontrole za kontinuirano poboljšanje i zaštitu podataka
ISO/IEC 27002:2022	Kontrole 5.34, 8.10, 8.11, 8.12	Kontrole za postupanje s osobnim podacima (PII), zadržavanje, brisanje, anonimizaciju i prava ispitanika
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Zahtjevi za upravljanje, rizike, upravljanje pristupom, zapisivanje i nadzor, odgovor na povrede i program privatnosti
GDPR EU	Članci 5, 6, 12–23, 25, 28, 30, 32–34; uvodna izjava 78	Temeljna načela privatnosti, odgovornost, prava ispitanika, zahtjevi ispitanika, povrede osobnih podataka te zaštita podataka u fazi projektiranja i prema zadanim postavkama
Direktiva EU NIS2	Članak 21(2)(e), (f)	Sigurnosne kontrole temeljene na riziku za ključne i važne subjekte
Uredba EU DORA	Članci 6(2)(d), 11(1)(c), 15(1), 17	Upravljanje, rizik trećih strana i rokovi za sigurnu obradu
COBIT 2019	APO12, DSS01, DSS05, MEA	Upravljanje rizicima, sigurne operacije i nadzor usklađenosti

1. Svrha

1.1 Ova politika uspostavlja obvezna organizacijska načela i tehničke zahtjeve za zaštitu osobnih podataka i provedbu zaštite podataka u fazi projektiranja u svim okruženjima.

1.2 Njome se formaliziraju odgovornosti organizacije u skladu s međunarodnim standardima i regulatornim okvirima te osigurava da se osobni podaci prikupljaju, obrađuju, čuvaju, dijele i zbrinjavaju zakonito, sigurno i transparentno.

1.3 Ova politika dodatno jača usklađenost s primjenjivim zakonima i okvirima privatnosti, uključujući GDPR EU, Direktivu EU NIS2, Uredbu EU DORA, ISO/IEC 27001:2022 i COBIT 2019.

2. Područje primjene

2.1 Ova se politika primjenjuje na sve organizacijske jedinice, osoblje i sustave uključene u obradu osobnih podataka, uključujući:

2.1.1 Zaposlenike, ugovorne izvođače, konzultante i pružatelje usluga trećih strana.

2.1.2 Podatke prikupljene iz internih i vanjskih izvora u svim poslovnim funkcijama.

2.1.3 Fizičke i digitalne medije, uključujući usluge u oblaku, SaaS platforme, mobilne uređaje i papirnatu dokumentaciju.

2.1.4 Sva okruženja, uključujući produkcijske, razvojne, testne sustave i sustave sigurnosnih kopija u kojima mogu postojati osobni podaci.

2.2 Obuhvaća sve aktivnosti obrade uređene primjenjivim propisima i standardima privatnosti, uključujući, ali ne ograničavajući se na:

2.2.1 Prikupljanje, pohranu, uporabu, prijenos i zbrinjavanje osobnih podataka.

2.2.2 Ostvarivanje prava ispitanika, dokumentiranje pravne osnove i upravljanje privolama.

2.2.3 Prekogranične prijenose, obavješćivanje o povredama i dijeljenje podataka s trećim stranama.

2.2.4 Siguran dizajn i provedbu zaštite podataka prema zadanim postavkama u sustavima i procesima.

3. Ciljevi

3.1 Osigurati zakonitu, transparentnu i odgovornu obradu osobnih podataka u skladu s ISO/IEC 27001:2022 i povezanim pravnim zahtjevima.

3.2 Ugraditi načela zaštite podataka u fazi projektiranja i zaštite podataka prema zadanim postavkama u sve informacijske sustave, usluge i poslovne procese.

3.3 Provoditi tehničke i organizacijske mjere (TOM) koje štite povjerljivost, cjelovitost i dostupnost osobnih podataka tijekom cijelog njihova životnog ciklusa.

3.4 Definirati upravljačke uloge i strukture odgovornosti za zaštitu podataka, uključujući odgovornosti službenika za zaštitu podataka (DPO), informacijske sigurnosti, pravnih poslova i vlasnika podataka.

3.5 Omogućiti punu usklađenost s člancima 5., 6., 25., 30. i 32. GDPR-a, kao i sa zahtjevima za smanjenje rizika i otpornost prema NIS2 i DORA-i.

3.6 Osigurati prava ispitanika, uključujući pristup, ispravak, brisanje, ograničenje obrade, prenosivost, prigovor i zaštitu od automatiziranog donošenja odluka.

3.7 Ublažiti regulatorne, reputacijske, pravne i operativne rizike koji proizlaze iz neovlaštenog pristupa, zlouporabe ili gubitka osobnih podataka.

4. Uloge i odgovornosti

4.1 Izvršno rukovodstvo

4.1.1 Osigurava strateški nadzor i dodjeljuje dostatne resurse za potporu programu privatnosti.

4.1.2 Odobrava ovu politiku i osigurava njezinu provedbu u cijeloj organizaciji.

4.2 Službenik za zaštitu podataka (DPO)

4.2.1 Djeluje neovisno radi nadzora usklađenosti s propisima o zaštiti podataka.

4.2.2 Održava evidenciju aktivnosti obrade (RoPA) u skladu s člankom 30. GDPR-a.

4.2.3 Vodi komunikaciju s regulatornim tijelima, provodi procjene učinka na zaštitu podataka (DPIA) i upravlja postupcima obavješćivanja o povredama.

4.2.4 Pregledava iznimke povezane s privatnošću i vodi Registar iznimaka privatnosti.

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

9. Pregled i ažuriranje zahtjeva

9.1 Ova politika mora se pregledavati najmanje jednom godišnje ili ranije u sljedećim slučajevima:

9.1.1 Značajna pravna ili regulatorna ažuriranja (npr. izmjene GDPR-a, rokovi iz DORA-e)

9.1.2 Novi sustavi ili aktivnosti obrade koje uključuju osobne podatke

9.1.3 Nalazi unutarnje revizije koji upućuju na nedostatke u politici

9.1.4 Značajni incidenti povrede ili povratne informacije nadzornog tijela

9.2 Odgovornosti za pregled

9.2.1 Službenik za zaštitu podataka (DPO) mora pokrenuti pregled politike, u koordinaciji s pravnim poslovima, upravljanjem rizicima, informacijskom sigurnošću i Izvršnim rukovodstvom.

9.2.2 Sva ažuriranja moraju se evidentirati u Registru upravljanja dokumentacijom ISMS-a i distribuirati pogođenim dionicima.

9.3 Kontrola promjena

9.3.1 Svaka izmjena ove politike mora biti formalno odobrena od strane Izvršnog rukovodstva.

9.3.2 Zastarjele verzije moraju se sigurno arhivirati, a ažurirana verzija mora sadržavati dokumentiranu povijest promjena.

10. Povezane politike i poveznice

10.1 P1 – Politika informacijske sigurnosti. Uspostavlja krovna načela upravljanja sigurnošću na kojima se temelji ova politika privatnosti. P1 podupire povjerljivost, cjelovitost i dostupnost osobnih podataka u svim sustavima i uslugama.

10.2 P6 – Politika upravljanja rizicima. Definira metodologiju obrade rizika organizacije, koja je ključna za procjenu rizika privatnosti, DPIA procese i vrednovanje preostalog rizika koje zahtijevaju GDPR i točka 6.1.3 norme ISO/IEC 27001.

10.3 P13 – Politika klasifikacije podataka i označavanja. Uređuje kategorizaciju osobnih i osjetljivih podataka, koja čini osnovu za primjenu odgovarajućih kontrola privatnosti, uključujući provedbu zadržavanja, ograničavanje pristupa i sigurno zbrinjavanje.

10.4 P14 – Politika zadržavanja i zbrinjavanja podataka. Izravno podupire zahtjeve privatnosti iz članka 5. stavka 1. točke (e) i članka 17. GDPR-a te osigurava da se osobni podaci zadržavaju samo onoliko dugo koliko je potrebno i sigurno zbrinjavaju u skladu sa zakonskim obvezama.

10.5 P16 – Politika maskiranja podataka i pseudonimizacije. Uspostavlja kontrole za smanjenje mogućnosti identifikacije osobnih podataka putem tehničkih mjera kao što su tokenizacija, dinamičko maskiranje i pseudonimizacija te time provodi članak 32. GDPR-a i kontrolu 5.34 norme ISO/IEC 27002.

10.6 P30 – Politika odgovora na incidente. Utvrđuje obvezne protokole odgovora na povrede koji su usklađeni s postupanjem u slučaju povreda privatnosti i rokovima obavješćivanja iz članaka 33. i 34. GDPR-a.

10.7 P33 – Politika praćenja revizije i usklađenosti. Uspostavlja planirane procjene djelotvornosti programa privatnosti, primjene politike i praćenja korektivnih radnji u organizacijskim jedinicama i kod izvršitelja obrade trećih strana.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 5.1 – Vodstvo i opredijeljenost: uspostavlja odgovornost na razini rukovodstva za zaštitu osobnih podataka i provedbu načela privatnosti.

11.1.2 Točka 6.1.3 – Obrada rizika informacijske sigurnosti: podupire identifikaciju, procjenu i obradu rizika privatnosti putem DPIA procjena i iznimaka.

11.1.3 Točka 8.1 – Operativno planiranje i kontrola: zahtijeva tehničke i proceduralne zaštitne mjere kako bi se osiguralo da se osobni podaci obrađuju sigurno.

11.1.4 Točka 10.1 – Kontinuirano poboljšanje: nalaže periodično vrednovanje i prilagodbu programa privatnosti.

11.2 ISO/IEC 27002:2022 kontrole 5.34, 8.10, 8.11, 8.12: daju smjernice za postupanje s osobnim podacima (PII), provedbu zadržavanja, brisanja, anonimizacije i transparentnosti u vezi s pravima ispitanika.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: definiraju upravljanje, uloge, odgovornost i obveze osposobljavanja o privatnosti.

11.3.2 PL-2, PL-8: zahtijevaju integraciju kontrola privatnosti u životni ciklus sustava i arhitekturu poduzeća.

11.3.3 AC-2, AC-6: provode načelo najmanjih ovlasti i upravljanje računima radi zaštite osobnih podataka.

11.3.4 AU-2, AU-6, AU-9: nalažu zapisivanje, sljedivost i cjelovitost revizije za pristup osobnim podacima.

11.3.5 IR-4, IR-5, IR-6: definiraju strukturirane procese otkrivanja, analize i prijavljivanja povreda privatnosti.

11.3.6 PM-1, PM-21, PM-23: uspostavljaju sveobuhvatan program privatnosti usklađen sa strateškim ciljevima upravljanja rizicima i podacima.

11.4 GDPR EU (2016/679)

11.4.1 Članci 5., 6., 12.–23., 25., 28., 30., 32.–34.: uređuju zakonitu obradu, ograničenje svrhe, prava ispitanika, odgovornost, zaštitu podataka u fazi projektiranja i prema zadanim postavkama, obveze trećih strana te upravljanje povredama.

11.4.2 Uvodna izjava 78: dodatno potvrđuje načela zaštite podataka u fazi projektiranja.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(e) i (f): zahtijeva provedbu sigurnosnih kontrola temeljenih na riziku i zaštitu osobnih podataka za subjekte obuhvaćene područjem primjene direktive kao ključne i važne subjekte.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 6(2)(d): nalaže unutarnje upravljanje IKT rizikom povezanim s postupanjem s podacima.

11.6.2 Članak 11(1)(c): nalaže nadzor rizika trećih strana za usluge povezane s podacima.

11.6.3 Članci 15(1) i 17: zahtijevaju sigurnu obradu podataka od strane pružatelja usluga i pravodobno regulatorno izvješćivanje nakon incidenata povezanih s IKT-om.

11.7 COBIT 2019

11.7.1 APO12 – Upravljanje rizicima: uključuje rizik privatnosti u širi nadzor korporativnih rizika.

11.7.2 DSS01 – Upravljane operacije i DSS05 – Sigurnosne usluge: osiguravaju sigurne operacije, uključujući kontrolu pristupa, zadržavanje i cjelovitost sustava.

11.7.3 MEA03 – Praćenje usklađenosti: zahtijeva trajni pregled statusa usklađenosti s regulatornim zahtjevima i obvezama privatnosti na temelju politika.