					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P14S					Naziv dokumenta: **Politika zadržavanja i zbrinjavanja podataka**							
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 6.1.3, 8	Obuhvaća obradu rizika, operativne kontrole i zahtjeve za zadržavanje
ISO/IEC 27002:2022	Kontrola 5	Smjernice za razdoblja zadržavanja i metode sigurnog uništavanja
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Zadržavanje revizijskih zapisa, sanitizacija medija te ograničenja i provedba zadržavanja podataka
EU NIS2	Članak 21(2)(a)	Zahtijeva politiku upravljanja životnim ciklusom primjerenu riziku
EU DORA	Članak 5(1)	Upravljanje IKT rizicima: dostupnost i uklanjanje podataka
COBIT 2019	BAI03.04, DSS01	Kontrole životnog ciklusa informacija i sigurno zbrinjavanje
GDPR EU	Članak 5(1)(e), 17	Podaci se ne smiju čuvati dulje nego što je potrebno; pravo na brisanje

1. Svrha

1.1 Svrha ove politike jest utvrditi provediva pravila za zadržavanje i sigurno zbrinjavanje informacija u SME okruženju. Njome se osigurava da se zapisi čuvaju samo onoliko dugo koliko to zahtijevaju zakon, ugovorna obveza ili poslovna potreba te da se nakon toga sigurno uništavaju.

1.2 Ova politika ima za cilj smanjiti informacijski rizik, upravljati pravnom izloženošću i ograničiti pohranu redundantnih ili zastarjelih podataka. Pomaže osigurati usklađenost s normom ISO/IEC 27001 i okvirima privatnosti kao što je GDPR, smanjenjem neovlaštenog zadržavanja osobnih ili osjetljivih informacija.

1.3 Dobro strukturiran okvir za zadržavanje i zbrinjavanje smanjuje operativne troškove, poboljšava performanse sustava i povećava spremnost za reviziju. Za SME organizacije s ograničenim IT kapacitetima pruža praktičan način odgovornog upravljanja digitalnom i fizičkom informacijskom imovinom.

2. Područje primjene

2.1 Ova politika primjenjuje se na:

2.1.1 sve zapise, datoteke, dnevnike, komunikacije i skupove podataka koje organizacija stvara, prikuplja, obrađuje ili pohranjuje

2.1.2 sve zaposlenike, ugovorne izvođače i vanjske pružatelje usluga koji postupaju s podacima organizacije

2.1.3 sve formate podataka (npr. papirnate, elektroničke, slikovne, audio ili dnevničke zapise) i sve medije za pohranu (npr. lokalne diskove, usluge u oblaku, poslužitelje e-pošte, sigurnosne kopije)

2.2 Područje primjene uključuje:

2.2.1 poslovne dokumente (npr. račune, ugovore, projektna izvješća)

2.2.2 operativne zapise (npr. dnevnike, povijest pristupa, snimke sigurnosnih kopija)

2.2.3 osobne podatke (npr. HR datoteke, komunikaciju s klijentima, zapise podrške)

2.2.4 podatke hostirane interno, eksterno ili u hibridnim okruženjima

2.2.5 arhivirane podatke i sigurnosne kopije, bilo da su aktivni ili neaktivni

2.3 Sve faze životnog ciklusa podataka obuhvaćene su ovom politikom, od nastanka do odobrenog zbrinjavanja.

3. Ciljevi

3.1 Utvrditi dosljedna pravila zadržavanja na temelju pravnih, operativnih i regulatornih kriterija.

3.2 Spriječiti prerano brisanje ključnih zapisa i ukloniti nepotrebno gomilanje podataka.

3.3 Osigurati sigurno i nepovratno zbrinjavanje podataka kada zadržavanje više nije potrebno.

3.4 Dodijeliti odgovornost za provedbu odluka o zadržavanju i brisanju uz uvažavanje ograničenja resursa na razini SME organizacije.

3.5 Osigurati dokumentaciju spremnu za reviziju radi dokazivanja dužne pažnje u skladu s ISO 27001, GDPR-om, NIS2 i drugim okvirima.

3.6 Promicati sigurno postupanje s podacima tijekom cijelog životnog ciklusa bez nametanja nepotrebnog tehničkog opterećenja osoblju koje nije specijalizirano za IT ili sigurnost.

4. Uloge i odgovornosti

4.1 Glavni rukovoditelj (GM)

4.1.1 Odobrava ovu politiku i odgovoran je za nju.

4.1.2 Osigurava da se postupci zadržavanja i zbrinjavanja provode na način usklađen s pravnim i poslovnim rizikom.

4.1.3 Odobrava iznimke i pravno zadržavanje kada je to potrebno.

4.1.4 Pokreće preglede politike i odobrava ažuriranja na temelju poslovnih ili regulatornih promjena.

4.2 Imenovani vlasnik podataka

4.2.1 Imenuje se za svaku kategoriju podataka (npr. financijski podaci, HR zapisi, evidencije klijenata).

4.2.2 Klasificira zapise i određuje odgovarajuće razdoblje zadržavanja na temelju politike i pravnih smjernica.

4.2.3 Odobrava brisanje kada su zahtjevi zadržavanja ispunjeni.

4.2.4 Podržava interne revizije pružanjem konteksta o logici zadržavanja i događajima zbrinjavanja.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Ova politika mora se pregledati najmanje jednom godišnje ili nakon:

9.1.1 promjena primjenjivih propisa (npr. o privatnosti podataka, financijskom izvještavanju)

9.1.2 uvođenja novih sustava ili procesa koji utječu na životni ciklus podataka

9.1.3 nalaza revizije ili incidenata koji otkriju nedostatke u praksama zadržavanja

9.2 Pregledi moraju osigurati da Registar zadržavanja ostane potpun i da obuhvaća sve glavne kategorije zapisa.

9.3 Ažuriranja politike mora odobriti GM i o njima se mora obavijestiti obuhvaćeno osoblje. Najnovija verzija mora biti dostupna i pod verzijskom kontrolom.

10. Povezane politike i poveznice

10.1 P2S – Politika uloga i odgovornosti u upravljanju: definira vlasništvo nad politikom i ovlasti za iznimke.

10.2 P13S – Politika klasifikacije i označavanja podataka: određuje kako su pravila zadržavanja usklađena s klasifikacijom podataka.

10.3 P12S – Politika upravljanja imovinom: uređuje medije za pohranu koji sadrže podatke obuhvaćene zadržavanjem i zbrinjavanjem.

10.4 P17S – Politika zaštite podataka i privatnosti: osigurava minimizaciju podataka i podržava zakonitu obradu u skladu s GDPR-om.

10.5 P30S – Politika odgovora na incidente: aktivira se kada propusti u zbrinjavanju ili zadržavanju rezultiraju mogućom izloženošću podataka.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 6.1.3: zahtijeva obradu rizika povezanih s informacijama, uključujući rizike zadržavanja.

11.1.2 Točka 8.1: definira operativne kontrole životnog ciklusa.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.33: daje smjernice za određivanje razdoblja zadržavanja i metoda sigurnog uništavanja.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: zahtijeva zadržavanje revizijskih zapisa.

11.3.2 MP-6: definira postupke sanitizacije medija.

11.3.3 SI-12: uređuje ograničenja zadržavanja podataka i njihovu provedbu.

11.4 GDPR EU

11.4.1 Članak 5(1)(e): podaci se moraju čuvati ne dulje nego što je potrebno.

11.4.2 Članak 17: pravo na brisanje primjenjuje se kada se podaci više ne zadržavaju na zakonitoj osnovi.

11.5 EU NIS

11.5.1 Članak 21(2)(a): zahtijeva organizacijske politike primjerene riziku, uključujući upravljanje životnim ciklusom.

11.6 EU DORA

11.6.1 Članak 5(1): upravljanje IKT rizicima uključuje dostupnost i uklanjanje podataka.

11.7 COBIT 2019

11.7.1 BAI03.04: zahtijeva kontrole životnog ciklusa informacija.

11.7.2 DSS01.06: zahtijeva postupke sigurnog zbrinjavanja kao dio zaštite informacijske imovine.