					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P14					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 regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 6.1.3, 8.1	
ISO/IEC 27002:2022	Kontrole 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
GDPR EU	Članci 5(1)(e), 17, 32	
Direktiva EU NIS2	Članak 21(2)(a-e)	
Uredba EU DORA	Članci 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Svrha

1.1 Svrha ove politike jest definirati organizacijske zahtjeve za zadržavanje podataka i sigurno zbrinjavanje tijekom svih faza životnog ciklusa informacija. Ova politika osigurava usklađenost s primjenjivim zakonskim, regulatornim i ugovornim obvezama te sprječava nepotrebno ili rizično gomilanje podataka.

1.2 Ova politika podupire provedbu norme ISO/IEC 27001:2022 uspostavom kontrola nad razdobljima pohrane podataka i praksama nepovratnog zbrinjavanja. Omogućuje sljedivu evidenciju zapisa, osigurava zadržavanje usklađeno s osjetljivošću klasifikacije te osigurava spremnost za reviziju, regulatorni nadzor i pravno otkrivanje.

1.3 Dodatno, cilj ove politike jest očuvati povjerljivost, cjelovitost i dostupnost podataka uz istodobno smanjenje poslovnog rizika, operativnih neučinkovitosti i izloženosti povredama privatnosti koje proizlaze iz neprimjerenog zadržavanja ili uništavanja podataka.

2. Područje primjene

2.1 Ova politika primjenjuje se na svu fizičku i digitalnu informacijsku imovinu u vlasništvu organizacije, koju organizacija obrađuje ili zadržava, uključujući i onu pod kontrolom trećih strana, povezanih društava ili partnera za izdvojene usluge.

2.2 Područje primjene uključuje, ali nije ograničeno na:

2.2.1 dokumente, datoteke i zapise (u digitalnom i papirnatom obliku)

2.2.2 baze podataka i arhive

2.2.3 e-poštu i zapise trenutačnog dopisivanja

2.2.4 sigurnosne kopije, dnevničke zapise sustava i revizijske tragove

2.2.5 izvorni kod, podatke aplikacija i imovinu hostiranu u oblaku

2.2.6 prijenosne medije i zastarjeli hardver koji sadrži podatke

2.3 Ova politika uređuje i operativne zapise i regulirane skupove podataka (npr. financijske, pravne, kadrovske, podatke povezane s klijentima i sadržaj relevantan za reviziju), neovisno o lokaciji pohrane ili sustavu.

2.4 Primjenjuje se na sve organizacijske odjele te na zaposlenike, ugovorne izvođače i dobavljače koji sudjeluju u izradi, pohrani, upravljanju ili zbrinjavanju podataka.

3. Ciljevi

3.1 Osigurati da se podaci zadržavaju samo onoliko dugo koliko je to zakonski, ugovorno ili operativno potrebno te da se sigurno zbrinu kada više nisu potrebni.

3.2 Spriječiti preuranjeno, neovlašteno ili slučajno brisanje zapisa potrebnih za tekuće poslovanje, usklađenost, sudske postupke ili potrebe revizije.

3.3 Uspostaviti i provoditi dosljedne rokove zadržavanja na temelju klasifikacije informacija, vrste imovine, primjenjivih propisa i izloženosti riziku.

3.4 Zaštititi privatnost i povjerljivost podataka tijekom razdoblja zadržavanja i pri njihovu zbrinjavanju, uključujući ostvarivanje prava ispitanika (npr. brisanje prema članku 17. GDPR-a).

3.5 Osigurati da su sve metode zbrinjavanja podataka nepovratne, odgovarajuće dokumentirane i usklađene s priznatim standardima kao što je NIST SP 800-88.

3.6 Smanjiti operativne neučinkovitosti, dodatne troškove i pravnu izloženost uzrokovanu prekomjernim zadržavanjem ili nesljedivim naslijeđenim podacima.

3.7 Poduprijeti ciljeve kontinuiteta poslovanja i oporavka od katastrofe putem integriranog upravljanja zadržavanjem sigurnosnih kopija i dokazive prakse arhiviranja podataka.

4. Uloge i odgovornosti

4.1 Izvršno vodstvo

4.1.1 Odobrava ovu politiku i osigurava odgovarajuća financijska sredstva, resurse i integraciju u program upravljanja rizicima i usklađenošću na razini organizacije.

4.1.2 Snosi ukupnu odgovornost za zakonsku i regulatornu usklađenost povezanu sa zadržavanjem podataka i sigurnim zbrinjavanjem.

4.2 Glavni direktor za informacijsku sigurnost (CISO)

4.2.1 Vlasnik je ove politike i odgovoran je za definiranje i preispitivanje upravljanja zadržavanjem i zbrinjavanjem u skladu sa sustavom upravljanja informacijskom sigurnošću (ISMS).

4.2.2 Osigurava da se zahtjevi za zadržavanje i zbrinjavanje temeljeni na klasifikaciji provode u poslovnim jedinicama i tehničkim sustavima.

4.2.3 Prati usklađenost s politikom i nalaže korektivne radnje kada je to potrebno.

[... 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 preispitivati najmanje jednom godišnje ili kada nastupi bilo koji od sljedećih uvjeta:

9.1.1 promjene primjenjivih zakona ili propisa koje utječu na zadržavanje podataka (npr. ažuriranja GDPR-a, poreznih propisa, Uredbe EU DORA)

9.1.2 izmjene okvira klasifikacije ili poslovnih procesa koje utječu na faze životnog ciklusa podataka

9.1.3 uvođenje novih IT sustava, platformi za arhiviranje ili tehnologija za zbrinjavanje medija

9.1.4 nalazi unutarnje revizije ili regulatorne preporuke koji ukazuju na nedostatke u praksama zadržavanja ili zbrinjavanja

9.2 Preispitivanje vode CISO i službenik za zaštitu podataka (DPO), uz doprinos pravne službe, funkcije usklađenosti, IT-a i poslovnih jedinica.

9.3 Glavni raspored zadržavanja podataka (MDRS) i Registar zbrinjavanja moraju se preispitivati usporedno kako bi se osiguralo:

9.3.1 da rasporedi ostanu točni i odražavaju operativne, pravne i regulatorne potrebe

9.3.2 da je dokumentacija o zbrinjavanju potpuna i podobna za reviziju

9.3.3 da su zapisi o pravnom zadržavanju provjereni i ukinuti kada je to primjereno

9.4 Svako ažuriranje politike mora:

9.4.1 biti formalno verzionirano i zadržano u repozitoriju dokumenata ISMS-a

9.4.2 uključivati povijest izmjena i obrazloženje promjene

9.4.3 biti odobreno od strane izvršnog vodstva

9.4.4 biti priopćeno relevantnom osoblju uz ažurirane materijale za osposobljavanje ili upute

9.5 Kada dođe do značajnih promjena politike, pogođeni zaposlenici moraju završiti ciljano ponovno osposobljavanje u roku od 30 dana od objave kako bi se osigurala trajna usklađenost.

9.6 Povezane politike i poveznice

10. Povezane politike i poveznice

10.1.1 P4 - Politika kontrole pristupa: Osigurava da samo ovlaštene osobe pristupaju podacima tijekom razdoblja njihova zadržavanja te da su podaci kojima je istekao rok ograničeni do zbrinjavanja.

10.1.2 P12 - Politika upravljanja imovinom: Utvrđuje koja imovina sadrži podatke koji zahtijevaju planirano zbrinjavanje i prati njihov životni ciklus od nabave do uništenja.

10.1.3 P13 - Politika klasifikacije i označavanja podataka: Usmjerava odluke o klasifikaciji koje izravno utječu na trajanje zadržavanja podataka i potrebnu metodu zbrinjavanja.

10.1.4 P15 - Politika sigurnosnih kopija i povrata podataka: Definira razdoblja zadržavanja i postupke zbrinjavanja za medije sigurnosnih kopija i repliciranu podatkovnu imovinu.

10.1.5 P18 - Politika kriptografskih kontrola: Podržava kriptografsko brisanje za potrebe zbrinjavanja i nalaže šifriranje tijekom pohrane podataka do njihova uništenja.

10.1.6 P30 - Politika odgovora na incidente: Aktivira se u slučajevima kada neprimjereno zbrinjavanje dovede do mogućeg gubitka podataka, povrede ili regulatornog kršenja.

10.2 Svaka povezana politika ima ulogu u provedbi koherentnog modela upravljanja podacima kroz klasifikaciju, kontrolu životnog ciklusa, pristup i spremnost za reviziju.

11. Referentni standardi i okviri

11.1 Ova politika usklađena je s globalno priznatim standardima i regulatornim okvirima koji definiraju sigurne, usklađene i učinkovite prakse upravljanja životnim ciklusom podataka.

11.2 ISO/IEC 27001:

11.2.1 Točka 6.1.3 - plan obrade rizika: Podržava ublažavanje rizika povezanih s prekomjernim zadržavanjem, povredama podataka ili neuspjesima zbrinjavanja.

11.2.2 Točka 8.1 - operativno planiranje i kontrola: Uspostavlja kontrole životnog ciklusa koje uređuju pohranu, arhiviranje i uništenje.

11.3 ISO/IEC 27002:2022 - Kontrole 5.10, 5.12, 5.30, 5: Pružaju praktične smjernice o prihvatljivoj uporabi podataka, opravdanosti zadržavanja, kontroliranom brisanju i dokazivom vođenju zapisa u skladu s tolerancijom na rizik organizacije.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - zadržavanje revizijskih zapisa: Osigurava dovoljno dugo zadržavanje revizijskih zapisa i dokaza o usklađenosti.

11.4.2 MP-6 - sanitizacija medija: Zahtijeva sigurne i dokumentirane metode uništenja fizičkih i elektroničkih medija.

11.4.3 SI-12 - postupanje s informacijama: Nalaže primjereno postupanje s podacima usklađeno s kontrolama zadržavanja i zbrinjavanja.

11.4.4 PL-2 - plan sigurnosti i privatnosti sustava: Zahtijeva dokumentaciju po sustavima o postupanju s podacima tijekom životnog ciklusa i odredbama sigurnog zbrinjavanja.

11.5 GDPR EU (2016/679):

11.5.1 Članak 5(1)(e) - minimizacija podataka i ograničenje pohrane: Zahtijeva da se podaci ne zadržavaju dulje nego što je potrebno.

11.5.2 Članak 17. - pravo na brisanje („pravo na zaborav“): Zahtijeva žurno i trajno brisanje osobnih podataka na temelju valjanog zahtjeva.

11.5.3 Članak 32. - sigurnost obrade: Jača zaštitu podataka tijekom zadržavanja i nalaže sigurno uništenje zapisa kojima je istekao rok.

11.6 Direktiva EU NIS2 (2022/2555):

11.6.1 Članak 21(2)(a-e): Zahtijeva da subjekti usvoje politike i tehničke mjere za sigurno postupanje s podacima, uključujući ograničenja pohrane i metode zbrinjavanja.

11.7 Uredba EU DORA (2022/2554):

11.7.1 Članak 5 - upravljanje i kontrola: Nalaže strukturirano upravljanje IKT rizicima, uključujući sigurno postupanje s informacijama tijekom njihova životnog ciklusa.

11.7.2 Članak 9 - okvir za upravljanje IKT rizicima: Zahtijeva politike za zadržavanje podataka, uništavanje i zakonsku/regulatornu usklađenost digitalnih operacija.

11.8 COBIT 2019:

11.8.1 DSS01 - upravljane operacije: Podržava praćenje zadržavanja i dosljednost kroz podatkovne sustave.

11.8.2 DSS05 - upravljane sigurnosne usluge: Osigurava zaštitu pohranjenih i arhiviranih podataka do njihova sigurnog zbrinjavanja.

11.8.3 MEA03 - praćenje, vrednovanje i procjena usklađenosti: Omogućuje reviziju provedbe zadržavanja, postupaka brisanja i ispunjavanja regulatornih zahtjeva.