					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P17S					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**

Usklađenost sa standardima i regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Kontrole 5.34, 8.10–8.12	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
GDPR EU	Članak 5, 6, 12-23, 30, 32-34	
Direktiva EU NIS2	Članak 21(2)(e), 21(2)(f)	
Uredba EU DORA	Članci 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA03	

1. Svrha

1.1. Ova politika definira način na koji organizacija štiti osobne podatke u skladu sa zakonskim obvezama, regulatornim okvirom i međunarodnim sigurnosnim standardima.

1.2. Ova politika osigurava da se osobni podaci kupaca, zaposlenika i partnera prikupljaju, upotrebljavaju, pohranjuju i brišu zakonito, pošteno i sigurno.

1.3. Ova politika također osigurava usklađenost s normom ISO/IEC 27001:2022 i podupire revizijsku spremnost primjenom dosljednog pristupa zaštiti privatnosti utemeljenog na riziku.

1.4. Ovom politikom organizacija iskazuje odgovornost i gradi povjerenje klijenata davanjem prednosti transparentnosti, minimizaciji podataka i učinkovitom upravljanju privatnošću.

2. Područje primjene

2.1. Ova politika primjenjuje se na:

2.1.1. sve zaposlenike, ugovaratelje i pružatelje usluga koji pristupaju osobnim podacima, obrađuju ih ili njima upravljaju

2.1.2. svaki sustav, aplikaciju ili lokaciju na kojoj se osobni podaci pohranjuju ili prenose

2.1.3. sve osobne podatke, neovisno o tome jesu li pohranjeni elektronički, u papirnatom obliku, u sustavima u oblaku ili na mobilnim uređajima

2.2. Ova politika primjenjuje se na podatke koji se odnose na klijente, zaposlenike, dobavljače i sve druge pojedince koji se mogu identificirati.

2.3. Ova politika primjenjuje se neovisno o tome obrađuju li se podaci interno ili ih obrađuju pružatelji usluga trećih strana.

3. Ciljevi

3.1. Osigurati da se osobni podaci obrađuju u skladu s propisima o privatnosti i sigurnosnim standardima, uključujući GDPR, NIS2 i ISO 27001.

3.2. Zaštititi osobne podatke od neovlaštenog pristupa, zlouporabe, izmjene ili gubitka primjenom jasno definiranih tehničkih i organizacijskih kontrola.

3.3. Poštovati prava pojedinaca na privatnost, uključujući pravo na pristup, ispravak i brisanje njihovih podataka.

3.4. Uspostaviti jasne uloge i odgovornosti za zaštitu podataka unutar organizacije.

3.5. Osigurati minimizaciju podataka, sigurno zadržavanje i pravodobno brisanje u svim sustavima i procesima.

3.6. Smanjiti rizik od neusklađenosti, pravnih sankcija, reputacijske štete i gubitka povjerenja klijenata.

4. Uloge i odgovornosti

4.1. glavni direktor (GM)

4.1.1. odobrava ovu politiku i osigurava njezinu provedbu

4.1.2. osigurava potrebne resurse za upravljanje rizicima privatnosti i odgovor na incidente

4.1.3. snosi ukupnu odgovornost za usklađenost s propisima o privatnosti i primjenjivim standardima

4.2. Koordinator za privatnost (interni ili vanjski)

4.2.1. održava evidenciju aktivnosti obrade osobnih podataka

4.2.2. odgovara na zahtjeve pojedinaca povezane s privatnošću i na upite regulatornih tijela

4.2.3. podupire procjene rizika, osposobljavanje i provedbu politike

4.2.4. dokumentira povrede osobnih podataka i obavještava nadležna tijela 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. Planirani pregledi

9.1.1. ovu politiku moraju najmanje jednom u 12 mjeseci preispitati Koordinator za privatnost, a odobriti glavni direktor

9.1.2. pregled mora obuhvatiti relevantnost politike, usklađenost s regulatornim zahtjevima i operativnu učinkovitost

9.2. Pokretači izvanrednog pregleda

9.2.1. ažuriranja politike moraju se pokrenuti i kao odgovor na:

9.2.1.1. nove ili izmijenjene propise o zaštiti podataka (npr. GDPR, DORA)

9.2.1.2. sigurnosne incidente ili povrede privatnosti koje uključuju osobne podatke

9.2.1.3. uvođenje novih sustava, alata ili usluga koji obrađuju osobne podatke

9.2.1.4. značajne revizijske nalaze ili preporuke regulatornih tijela

9.3. Upravljanje promjenama i komunikacija

9.3.1. sve promjene politike moraju se formalno dokumentirati u zapisniku promjena

9.3.2. revidirane verzije moraju se distribuirati svim zaposlenicima i primjenjivim ugovarateljima

9.3.3. arhivirane verzije moraju se čuvati radi osiguravanja revizijskog traga usklađenosti

10. Povezane politike i poveznice

10.1. Ova politika primjenjuje se zajedno s drugim SME politikama kako bi se uspostavio cjelovit i provediv okvir privatnosti:

10.1.1. P13S – Politika klasifikacije podataka i označavanja: osigurava da se osobni podaci klasificiraju na odgovarajući način kako bi se mjere zaštite privatnosti mogle primjenjivati na temelju rizika.

10.1.2. P14S – Politika zadržavanja i zbrinjavanja podataka: propisuje jasna pravila o razdoblju čuvanja osobnih podataka i sigurnim metodama njihova zbrinjavanja nakon isteka roka.

10.1.3. P16S – Politika maskiranja podataka i pseudonimizacije: određuje kako se osobni identifikatori moraju transformirati prije upotrebe podataka u neprodukcijskom okruženju ili njihove vanjske razmjene.

10.1.4. P30S – Politika odgovora na incidente: obuhvaća korake potrebne za odgovor na povrede podataka, uključujući obavještavanje regulatornih tijela i pogođenih pojedinaca u propisanim rokovima.

10.1.5. P2S – Politika uloga i odgovornosti u upravljanju: pojašnjava strukturu odgovornosti i uloge u donošenju odluka koje se primjenjuju na provedbu i nadzor privatnosti.

10.2. Ove povezane politike moraju se pregledavati i primjenjivati zajedno kako bi se osigurala cjelovita zaštita privatnosti u sustavima, među zaposlenicima i kod dobavljača.

11. Referentni standardi i okviri

11.1. ISO/IEC 27001

11.1.1. Točka 5.1 – zahtijeva da najviše rukovodstvo pokaže vodstvo i opredijeljenost za zaštitu osobnih podataka.

11.1.2. Točka 6.1.3 – zahtijeva obradu rizika povezanih s obradom osobnih podataka.

11.1.3. Točka 8.1 – zahtijeva provedbu operativnih kontrola za zaštitu podataka tijekom cijelog njihova životnog ciklusa.

11.2. ISO/IEC 27002

11.2.1. Kontrola 5.34 – daje smjernice za provedbu zaštite privatnosti i sigurnog postupanja s osobnim podacima (PII).

11.2.2. Kontrola 8.10 – uređuje sigurno zbrinjavanje osobnih podataka radi sprječavanja preostalog otkrivanja podataka.

11.2.3. Kontrola 8.11 – podupire primjenu maskiranja i pseudonimizacije radi minimizacije podataka.

11.2.4. Kontrola 8.12 – sprječava neovlašteno curenje podataka primjenom kontrola pristupa podacima i njihove uporabe.

11.3. NIST SP 800-53 Rev.5

11.3.1. AR-2 – dodjeljuje uloge i odgovornosti za upravljanje rizikom privatnosti.

11.3.2. PL-5 – zahtijeva dokumentiranje plana privatnosti koji obuhvaća upotrebu i zaštitu podataka.

11.3.3. AC-6 – zahtijeva primjenu načela najmanjih ovlasti i kontrola pristupa za osobne podatke.

11.3.4. IR-4 – zahtijeva postupke upravljanja incidentima za povrede koje uključuju osobne podatke.

11.4. GDPR EU

11.4.1. Članak 5 – definira temeljna načela zakonite, poštene i transparentne obrade podataka.

11.4.2. Članak 6 – zahtijeva valjanu pravnu osnovu za svaku aktivnost obrade osobnih podataka.

11.4.3. Članci 12–23 – propisuju prava ispitanika, uključujući pristup, ispravak, brisanje i prigovor.

11.4.4. Članak 30 – zahtijeva vođenje evidencije aktivnosti obrade.

11.4.5. Članak 32 – zahtijeva odgovarajuće tehničke i organizacijske sigurnosne mjere.

11.4.6. Članci 33–34 – propisuju obveze prijave povrede nadležnim tijelima i ispitanicima.

11.5. Direktiva EU NIS2

11.5.1. Članak 21(2)(e) – zahtijeva mjere za osiguravanje zaštite podataka usklađene s politikama kibernetičke sigurnosti.

11.5.2. Članak 21(2)(f) – zahtijeva mehanizme za upravljanje sigurnošću osobnih i povjerljivih podataka u IKT sustavima.

11.6. Uredba EU DORA

11.6.1. Članak 6 – zahtijeva interne okvire upravljanja koji obuhvaćaju upravljanje rizikom podataka i njihovom zaštitom.

11.6.2. Članak 15 – obvezuje financijske subjekte da osiguraju da pružatelji usluga trećih strana štite osobne podatke i podupiru usklađenost s regulatornim zahtjevima.

11.6.3. Članak 17 – zahtijeva da organizacije osiguraju da su IKT sustavi koji obrađuju osobne podatke sigurni, otporni i pod nadzorom.

11.7. COBIT 2019

11.7.1. APO12 – Upravljanje rizicima: zahtijeva identifikaciju i obradu rizika privatnosti i zaštite podataka.

11.7.2. DSS05 – Upravljanje sigurnosnim uslugama: zahtijeva zaštitne mjere za sprječavanje neovlaštenog pristupa osobnim podacima.

11.7.3. MEA03 – Praćenje usklađenosti: zahtijeva da organizacije osiguraju trajnu usklađenost s propisima o privatnosti i zaštiti podataka.