					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P17S					Naslov dokumenta: **Politika varstva podatkov in zasebnosti**							
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**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzule 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Kontrole 5.34, 8.10–8	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
Uredba EU GDPR	Členi 5, 6, 12–23, 30, 32–34	
Direktiva EU NIS2	Člen 21(2)(e), 21(2)(f)	
Uredba EU DORA	Členi 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA	

1. Namen

1.1. Ta politika določa, kako organizacija varuje osebne podatke v skladu s pravnimi obveznostmi, regulativnimi okviri in mednarodnimi varnostnimi standardi.

1.2. Zagotavlja, da se osebni podatki strank, zaposlenih in partnerjev zbirajo, uporabljajo, hranijo in brišejo zakonito, pošteno in varno.

1.3. Ta politika podpira tudi skladnost z ISO/IEC 27001:2022 in pripravljenost na revizijo z vzpostavitvijo doslednega pristopa k varstvu zasebnosti, ki temelji na tveganjih.

1.4. S to politiko organizacija izkazuje odgovornost in krepi zaupanje strank s poudarkom na preglednosti, minimizaciji podatkov in učinkovitem upravljanju zasebnosti.

2. Področje uporabe

2.1. Ta politika se uporablja za:

2.1.1. vse zaposlene, pogodbene izvajalce in ponudnike storitev, ki dostopajo do osebnih podatkov oziroma jih obdelujejo ali upravljajo,

2.1.2. vsak sistem, aplikacijo ali lokacijo, kjer se osebni podatki hranijo ali prenašajo,

2.1.3. vse osebne podatke, ne glede na to, ali so shranjeni v elektronski obliki, na papirju, v oblačnih sistemih ali na mobilnih napravah.

2.2. Ta politika se uporablja za podatke, povezane s strankami, zaposlenimi, dobavitelji in drugimi določljivimi posamezniki.

2.3. Ta politika velja ne glede na to, ali se podatki obdelujejo interno ali pri zunanjih ponudnikih storitev.

3. Cilji

3.1. Zagotoviti, da se osebni podatki obdelujejo v skladu z zakonodajo o zasebnosti in varnostnimi standardi, vključno z GDPR, NIS2 in ISO 27001.

3.2. Varovati osebne podatke pred nepooblaščenim dostopom, neustrezno uporabo, spremembo ali izgubo z jasno opredeljenimi tehničnimi in organizacijskimi kontrolami.

3.3. Zagotoviti spoštovanje pravic posameznikov do zasebnosti, vključno s pravico do dostopa, popravka in izbrisa njihovih podatkov.

3.4. Določiti jasne vloge in odgovornosti za varstvo podatkov v organizaciji.

3.5. Zagotoviti minimizacijo podatkov, varno hrambo in pravočasen izbris v vseh sistemih in procesih.

3.6. Zmanjšati tveganje neskladnosti, pravnih sankcij, škode za ugled in izgube zaupanja strank.

4. Vloge in odgovornosti

4.1. generalni direktor (GM)

4.1.1. odobri to politiko in zagotovi njeno izvajanje,

4.1.2. zagotovi potrebne vire za upravljanje tveganj zasebnosti in odzivanje na incidente,

4.1.3. nosi celotno odgovornost za skladnost z zakonodajo in standardi s področja zasebnosti.

4.2. koordinator za zasebnost (interni ali zunanji)

4.2.1. vodi evidence dejavnosti obdelave osebnih podatkov,

4.2.2. obravnava zahteve posameznikov glede zasebnosti in poizvedbe regulatorjev,

4.2.3. podpira ocenjevanje tveganj, usposabljanje in izvajanje te politike,

4.2.4. dokumentira kršitve in, kadar je to zahtevano, obvešča pristojne organe.

[... 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. Redni pregledi

9.1.1. To politiko mora najmanj enkrat na 12 mesecev pregledati koordinator za zasebnost, odobriti pa jo mora generalni direktor.

9.1.2. Pregled mora oceniti ustreznost politike, skladnost s predpisi in operativno učinkovitost.

9.2. Sprožilci za vmesni pregled

9.2.1. Posodobitev politike se mora izvesti tudi kot odziv na:

9.2.1.1. nove ali spremenjene predpise s področja varstva podatkov (npr. GDPR, DORA),

9.2.1.2. varnostne incidente ali kršitve zasebnosti, ki vključujejo osebne podatke,

9.2.1.3. uvedbo novih sistemov, orodij ali storitev, ki obdelujejo osebne podatke,

9.2.1.4. pomembne ugotovitve presoje ali priporočila regulatorjev.

9.3. Nadzor sprememb in obveščanje

9.3.1. Vse spremembe politike morajo biti formalno dokumentirane v evidenci sprememb.

9.3.2. Revidirane različice morajo biti razdeljene vsem zaposlenim in zadevnim pogodbenim izvajalcem.

9.3.3. Arhivirane različice je treba hraniti zaradi revizijske sledi skladnosti.

10. Povezane politike in povezave

10.1. Ta politika se uporablja skupaj z drugimi SME politikami za vzpostavitev celovitega in izvršljivega okvira varstva zasebnosti:

10.1.1. P13S – Politika razvrščanja in označevanja podatkov: zagotavlja, da so osebni podatki ustrezno razvrščeni, tako da se ukrepi varstva zasebnosti uporabljajo glede na tveganje.

10.1.2. P14S – Politika hrambe podatkov in odstranjevanja: določa jasna pravila o tem, kako dolgo je treba osebne podatke hraniti in katere varne metode je treba uporabiti za njihovo odstranitev po izteku roka hrambe.

10.1.3. P16S – Politika maskiranja podatkov in psevdonimizacije: določa, kako je treba osebne identifikatorje preoblikovati, preden se podatki uporabijo v neprodukcijskih okoljih ali delijo zunaj organizacije.

10.1.4. P30S – Politika odzivanja na incidente: določa korake za odzivanje na kršitve varnosti osebnih podatkov, vključno z obveščanjem regulatorjev in prizadetih posameznikov v predpisanih rokih.

10.1.5. P2S – Politika vlog in odgovornosti upravljanja: pojasnjuje strukturo odgovornosti in vloge odločanja, ki se uporabljajo za uveljavljanje in nadzor varstva zasebnosti.

10.2. Te povezane politike je treba pregledovati in uporabljati skupaj, da se zagotovi celovito varstvo zasebnosti v sistemih, pri zaposlenih in dobaviteljih.

11. Referenčni standardi in okviri

11.1. ISO/IEC 27001

11.1.1. Klavzula 5.1 – zahteva, da najvišje vodstvo izkazuje voditeljstvo in zavezanost varstvu osebnih podatkov.

11.1.2. Klavzula 6.1.3 – zahteva obravnavo tveganj, povezanih z obdelavo osebnih podatkov.

11.1.3. Klavzula 8.1 – zahteva uvedbo operativnih kontrol za varovanje podatkov v celotnem njihovem življenjskem ciklu.

11.2. ISO/IEC 27002

11.2.1. Kontrola 5.34 – podaja smernice za izvajanje varstva zasebnosti in varno ravnanje z osebno določljivimi podatki.

11.2.2. Kontrola 8.10 – obravnava varno odstranjevanje osebnih podatkov za preprečevanje preostalega razkritja.

11.2.3. Kontrola 8.11 – podpira uporabo maskiranja in psevdonimizacije za minimizacijo podatkov.

11.2.4. Kontrola 8.12 – preprečuje nepooblaščeno uhajanje podatkov s kontrolami dostopa do podatkov in njihove uporabe.

11.3. NIST SP 800-53 Rev.

11.3.1. AR-2 – določa vloge in odgovornosti za upravljanje tveganj zasebnosti.

11.3.2. PL-5 – zahteva dokumentiran načrt zasebnosti, ki zajema uporabo in varstvo podatkov.

11.3.3. AC-6 – zahteva načelo najmanjših privilegijev in kontrole dostopa za osebne podatke.

11.3.4. IR-4 – zahteva postopke obravnave incidentov za kršitve, ki vključujejo osebne podatke.

11.4. Uredba EU GDPR

11.4.1. Člen 5 – določa temeljna načela zakonite, poštene in pregledne obdelave osebnih podatkov.

11.4.2. Člen 6 – zahteva veljavno pravno podlago za vsako dejavnost obdelave osebnih podatkov.

11.4.3. Členi 12–23 – določajo pravice posameznikov, na katere se podatki nanašajo, vključno z dostopom, popravkom, izbrisom in ugovorom.

11.4.4. Člen 30 – zahteva vodenje evidenc dejavnosti obdelave.

11.4.5. Člen 32 – zahteva ustrezne tehnične in organizacijske varnostne ukrepe.

11.4.6. Členi 33–34 – določajo obveznosti obveščanja o kršitvah pristojnim organom in posameznikom, na katere se podatki nanašajo.

11.5. Direktiva EU NIS2

11.5.1. Člen 21(2)(e) – zahteva ukrepe za zagotavljanje varstva podatkov, usklajene s politikami kibernetske varnosti.

11.5.2. Člen 21(2)(f) – zahteva mehanizme za upravljanje varnosti osebnih in zaupnih podatkov v sistemih IKT.

11.6. Uredba EU DORA

11.6.1. Člen 6 – zahteva notranje okvire upravljanja za obvladovanje tveganj in varstvo podatkov.

11.6.2. Člen 15 – od finančnih subjektov zahteva, da zagotovijo, da zunanji ponudniki varujejo osebne podatke in podpirajo regulatorno skladnost.

11.6.3. Člen 17 – zahteva, da organizacije zagotovijo, da so sistemi IKT, ki obdelujejo osebne podatke, varni, odporni in nadzorovani.

11.7. COBIT 2019

11.7.1. APO12 – upravljanje tveganj: zahteva identifikacijo in obravnavo tveganj zasebnosti ter varstva podatkov.

11.7.2. DSS05 – upravljanje varnostnih storitev: zahteva varnostne ukrepe za preprečevanje nepooblaščenega dostopa do osebnih podatkov.

11.7.3. MEA03 – spremljanje skladnosti: zahteva, da organizacije zagotavljajo stalno skladnost z zakonodajo o zasebnosti in varstvu podatkov.