| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vnesite naziv registrirane pravne osebe | | | | | | | |
| Številka dokumenta:<br>P17 | | | | | Naslov dokumenta:<br>**Politika varstva podatkov in zasebnosti** | | | | | | | |
| Različica:<br>1.0 | | Datum začetka veljavnosti:<br>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, 8.1, 10 | Ustrezne splošne in tehnične kontrole ter kontrole za nenehno izboljševanje in varstvo podatkov |
| ISO/IEC 27002:2022 | Kontrole 5.34, 8.10, 8.11, 8.12 | Kontrole za ravnanje z osebno določljivimi podatki (PII), hrambo, izbris, anonimizacijo in pravice posameznikov, na katere se podatki nanašajo |
| 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 | Zahteve glede upravljanja, tveganj, upravljanja dostopa, beleženja, odzivanja na kršitve in programa zasebnosti |
| Uredba EU GDPR | Členi 5, 6, 12–23, 25, 28, 30, 32–34; uvodna izjava 78 | Vse temeljne zahteve glede zasebnosti, odgovornosti, pravic posameznikov, zahtev posameznikov glede podatkov, kršitev ter načel vgrajenega in privzetega varstva podatkov |
| Direktiva EU NIS2 | Člen 21(2)(e), (f) | Varnostne kontrole na podlagi tveganj za bistvene in pomembne subjekte |
| Uredba EU DORA | Členi 6(2)(d), 11(1)(c), 15(1), 17 | Upravljanje, tveganja tretjih oseb in roki za varno obdelavo |
| COBIT 2019 | APO12, DSS01, DSS05, MEA | Upravljanje tveganj, varne operacije, nadzor skladnosti |

**1. Namen**

1.1 Ta politika določa obvezna organizacijska načela in tehnične zahteve za varstvo osebnih podatkov ter uveljavljanje načel vgrajenega varstva zasebnosti v vseh okoljih.

1.2 Opredeljuje odgovornosti organizacije v skladu z mednarodnimi standardi in regulativnimi okviri ter zagotavlja, da se osebni podatki zbirajo, obdelujejo, hranijo, delijo in odstranjujejo zakonito, varno in pregledno.

1.3 Ta politika dodatno krepi skladnost z veljavnimi predpisi in okviri na področju zasebnosti, vključno z Uredbo EU GDPR, Direktivo EU NIS2, Uredbo EU DORA, ISO/IEC 27001:2022 in COBIT 2019.

**2. Področje uporabe**

**2.1 Ta politika velja za vse organizacijske enote, osebje in sisteme, vključene v obdelavo osebnih podatkov, vključno z:**

2.1.1 zaposlenimi, pogodbenimi izvajalci, svetovalci in ponudniki storitev tretjih oseb.

2.1.2 podatki, zbranimi iz notranjih in zunanjih virov v vseh poslovnih funkcijah.

2.1.3 fizičnimi in digitalnimi mediji, vključno s storitvami v oblaku, platformami SaaS, mobilnimi napravami in papirno dokumentacijo.

2.1.4 vsemi okolji, vključno s produkcijskimi, razvojnimi, testnimi sistemi in sistemi za varnostne kopije, v katerih so lahko prisotni osebni podatki.

**2.2 Zajema vse dejavnosti obdelave, ki jih urejajo veljavni predpisi in standardi s področja zasebnosti, vključno, vendar ne omejeno na:**

2.2.1 zbiranje, hrambo, uporabo, prenos in odstranjevanje osebnih podatkov.

2.2.2 uveljavljanje pravic posameznikov, na katere se podatki nanašajo, dokumentiranje pravnih podlag in upravljanje privolitev.

2.2.3 čezmejne prenose, obveščanje o kršitvah in deljenje podatkov s tretjimi osebami.

2.2.4 varno načrtovanje ter privzeto uveljavljanje varstva zasebnosti v sistemih in procesih.

**3. Cilji**

3.1 Zagotoviti zakonito, pregledno in odgovorno obdelavo osebnih podatkov v skladu z ISO/IEC 27001:2022 in povezanimi pravnimi zahtevami.

3.2 Vključiti načeli vgrajenega in privzetega varstva zasebnosti v vse informacijske sisteme, storitve in poslovne procese.

3.3 Uveljaviti tehnične in organizacijske ukrepe (TOM), ki v celotnem življenjskem ciklu osebnih podatkov varujejo zaupnost, celovitost in razpoložljivost (CIA).

3.4 Opredeliti upravljavske vloge in strukture odgovornosti za varstvo podatkov, vključno z odgovornostmi pooblaščene osebe za varstvo podatkov (DPO), informacijske varnosti, pravne službe in lastnikov podatkov.

3.5 Omogočiti popolno skladnost s členi 5, 6, 25, 30 in 32 Uredbe EU GDPR ter z zahtevami glede zmanjševanja tveganj in odpornosti po NIS2 in DORA.

3.6 Zagotavljati pravice posameznikov, na katere se podatki nanašajo, vključno s pravico do dostopa, popravka, izbrisa, omejitve obdelave, prenosljivosti, ugovora in varstva pred avtomatiziranim odločanjem.

3.7 Zmanjševati regulativna, ugledna, pravna in operativna tveganja, ki izhajajo iz nepooblaščenega dostopa, neustrezne uporabe ali izgube osebnih podatkov.

**4. Vloge in odgovornosti**

**4.1 Najvišje vodstvo**

4.1.1 Zagotavlja strateški nadzor in dodeljuje zadostne vire za podporo programu zasebnosti.

4.1.2 Odobri to politiko in zagotavlja njeno izvajanje v celotni organizaciji.

**4.2 Pooblaščena oseba za varstvo podatkov (DPO)**

4.2.1 Deluje neodvisno pri nadzoru skladnosti s predpisi o varstvu podatkov.

4.2.2 Vzdržuje evidenco dejavnosti obdelave (RoPA) v skladu s členom 30 Uredbe EU GDPR.

4.2.3 Vodi komunikacijo z regulatorji, izvaja ocene učinka v zvezi z varstvom podatkov (DPIA) in upravlja postopke obveščanja o kršitvah.

4.2.4 Pregleduje izjeme na področju zasebnosti in vzdržuje register izjem zasebnosti.

[ ... 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 Ta politika se mora pregledati najmanj enkrat letno ali prej v naslednjih primerih:**

9.1.1 pomembne pravne ali regulatorne posodobitve (npr. spremembe Uredbe EU GDPR, roki po DORA)

9.1.2 novi sistemi ali dejavnosti obdelave, ki vključujejo osebne podatke

9.1.3 ugotovitve notranje revizije, ki kažejo na vrzeli v politiki

9.1.4 pomembni incidenti kršitev ali povratne informacije nadzornih organov

**9.2 Odgovornosti za pregled**

9.2.1 DPO mora začeti pregled politike in pri tem usklajevati aktivnosti s pravno službo, upravljanjem tveganj, informacijsko varnostjo in najvišjim vodstvom.

9.2.2 Vse posodobitve morajo biti zabeležene v registru nadzora dokumentov ISMS in posredovane zadevnim zainteresiranim stranem.

**9.3 Nadzor sprememb**

9.3.1 Vsako spremembo te politike mora formalno odobriti najvišje vodstvo.

9.3.2 Zastarele različice morajo biti varno arhivirane, posodobljena različica pa mora vključevati dokumentirano evidenco sprememb.

**10. Povezane politike in povezave**

10.1 P1 – Politika informacijske varnosti. Določa krovna načela upravljanja informacijske varnosti, na katerih temelji ta politika zasebnosti. P1 podpira zaupnost, celovitost in razpoložljivost (CIA) osebnih podatkov v vseh sistemih in storitvah.

10.2 P6 – Politika upravljanja tveganj. Opredeljuje metodologijo obravnave tveganj v organizaciji, ki je bistvena za presojo tveganj zasebnosti, postopke DPIA in ocene preostalega tveganja, zahtevane po GDPR in klavzuli 6.1.3 standarda ISO/IEC 27001.

10.3 P13 – Politika razvrščanja in označevanja podatkov. Usmerja kategorizacijo osebnih in občutljivih podatkov ter predstavlja podlago za uporabo ustreznih kontrol zasebnosti, vključno z uveljavljanjem hrambe, omejevanjem dostopa in varnim odstranjevanjem.

10.4 P14 – Politika hrambe podatkov. Neposredno podpira zahteve zasebnosti po členu 5(1)(e) in 17 Uredbe EU GDPR ter zagotavlja, da se osebni podatki hranijo le toliko časa, kot je potrebno, in se varno odstranijo v skladu s pravnimi obveznostmi.

10.5 P16 – Politika maskiranja podatkov in psevdonimizacije. Določa kontrole za zmanjšanje prepoznavnosti osebnih podatkov s tehničnimi ukrepi, kot so tokenizacija, dinamično maskiranje in psevdonimizacija, s čimer uveljavlja člen 32 Uredbe EU GDPR in kontrolo 5.34 standarda ISO/IEC 27002.

10.6 P30 – Politika odzivanja na incidente. Opredeljuje obvezne protokole odzivanja na kršitve, ki se povezujejo z obravnavo kršitev zasebnosti in roki za obveščanje po členih 33 in 34 Uredbe EU GDPR.

10.7 P33 – Politika spremljanja presoj in skladnosti. Uveljavlja načrtovane presoje učinkovitosti programa zasebnosti, izvajanja politike in spremljanja korektivnih ukrepov po organizacijskih enotah in pri obdelovalcih tretjih oseb.

**11. Referenčni standardi in okviri**

**11.1 ISO/IEC 27001**

11.1.1 Klavzula 5.1 – Vodenje in zavezanost: določa odgovornost izvršnega vodstva za varstvo osebnih podatkov in uveljavljanje načel zasebnosti.

11.1.2 Klavzula 6.1.3 – Obravnava tveganj informacijske varnosti: podpira identifikacijo, presojo in obravnavo tveganj zasebnosti prek DPIA in izjem.

11.1.3 Klavzula 8.1 – Operativno načrtovanje in nadzor: zahteva tehnične in postopkovne varovalne ukrepe za varno obdelavo osebnih podatkov.

11.1.4 Klavzula 10.1 – Nenehno izboljševanje: zahteva periodično vrednotenje in prilagajanje programa zasebnosti.

11.2 ISO/IEC 27002:2022 Kontrole 5.34, 8.10, 8.11, 8.12: podajajo usmeritve za ravnanje z osebno določljivimi podatki (PII), uveljavljanje hrambe, izbrisa, anonimizacije in preglednosti glede pravic posameznikov.

**11.3 NIST SP 800-53 Rev.5**

11.3.1 AR-1, AR-2, AR-4, AR-5: opredeljujejo upravljanje, vloge, odgovornost in obveznosti glede usposabljanja za zasebnost.

11.3.2 PL-2, PL-8: zahtevata vključitev kontrol zasebnosti v življenjski cikel sistemov in korporativno arhitekturo.

11.3.3 AC-2, AC-6: uveljavljata načelo najmanjših privilegijev in upravljanje računov za varstvo osebnih podatkov.

11.3.4 AU-2, AU-6, AU-9: zahtevajo beleženje, sledljivost in celovitost revizijske sledi za dostop do osebnih podatkov.

11.3.5 IR-4, IR-5, IR-6: opredeljujejo strukturirane procese zaznavanja, analize in poročanja o kršitvah zasebnosti.

11.3.6 PM-1, PM-21, PM-23: vzpostavljajo celovit program zasebnosti, usklajen s strateškimi cilji tveganj in upravljanja podatkov.

**11.4 Uredba EU GDPR (2016/679)**

11.4.1 Členi 5, 6, 12–23, 25, 28, 30, 32–34: urejajo zakonito obdelavo, omejitev namena, pravice posameznikov, odgovornost, varstvo podatkov že pri načrtovanju in privzeto, obveznosti tretjih oseb ter upravljanje kršitev.

11.4.2 Uvodna izjava 78: dodatno potrjuje načela vgrajenega varstva zasebnosti.

**11.5 Direktiva EU NIS2 (2022/2555)**

11.5.1 Člen 21(2)(e) in (f): zahteva uvedbo varnostnih kontrol na podlagi tveganj in varstvo osebnih podatkov za bistvene in pomembne subjekte.

**11.6 Uredba EU DORA (2022/2554)**

11.6.1 Člen 6(2)(d): zahteva notranje upravljanje tveganj IKT, povezanih z ravnanjem s podatki.

11.6.2 Člen 11(1)(c): zahteva nadzor nad tveganji tretjih oseb pri storitvah, povezanih s podatki.

11.6.3 Člena 15(1) in 17: zahtevata varno obdelavo podatkov pri ponudnikih storitev in pravočasna obvestila nadzornim organom po incidentih, povezanih z IKT.

**11.7 COBIT 2019**

11.7.1 APO12 – Upravljanje tveganj: vključuje tveganja zasebnosti v širši nadzor nad tveganji organizacije.

11.7.2 DSS01 – Upravljane operacije in DSS05 – Zaščita pred zlonamerno programsko opremo: zagotavljata varne operacije, vključno z nadzorom dostopa, hrambo in celovitostjo sistemov.

11.7.3 MEA03 – Spremljanje skladnosti: zahteva stalni pregled stanja skladnosti glede na regulativne in s politiko določene obveznosti zasebnosti.