



POLITIKA SKLADNOSTI Z GDPR

cyber-sec.si in academy.cyber-sec.si

Verzija: 1.1

Zadnja posodobitev: 7. september 2025

Kazalo vsebine

Izvršni povzetek.....	3
Izjava o uporabnosti	3
1. Politika zasebnosti	4
Upravljavec.....	4
Nameni in pravne podlage	4
Kategorije osebnih podatkov	4
Prejemniki / kategorije prejemnikov	5
Hramba	5
Profiliranje in avtomatizirano odločanje.....	5
2. Politika piškotkov.....	5
Načela in pravna podlaga.....	6
Kategorije	6
3. Načrt hrambe podatkov	6
5. Tehnični in organizacijski ukrepi (TOM)	7
6. Postopek za uveljavljanje pravic posameznikov (DSR)	7
Kako vložiti zahtevo:	7
Preverjanje identitete:	7
Roki:	7
Pravice:.....	7
Pritožba pri nadzornem organu:.....	7
7. Načrt odziva na kršitev varstva osebnih podatkov	8
8. Upravljanje privolitev in nastavitev	8
9. Register pogodbenih obdelovalcev	8
10. Izjava o mednarodnih prenosih	8

Izvršni povzetek

Ta Politika skladnosti z GDPR opisuje načela, postopke ter tehnične in organizacijske ukrepe, ki jih izvaja **CYBER-SEC, informacijska in kibernetska varnost, d.o.o.** (v nadaljevanju: *CYBER-SEC*), za zakonito, pošteno in pregledno obdelavo osebnih podatkov na spletnih straneh cyber-sec.si in učni platformi academy.cyber-sec.si. Dokument združuje javno izjavo za posameznike in formalni interni akt za skladnost z **GDPR**, **ZVOP-2** in **ZEKom-2** (piškotki).

Vključuje:

- vrste osebnih podatkov, ki jih zbiramo
- namene in pravne podlage obdelave
- roke hrambe
- tehnične in organizacijske varnostne ukrepe
- pravice posameznikov in postopek uveljavljanja
- načrt odziva na kršitev varstva osebnih podatkov
- register pogodbenih obdelovalcev in mednarodne prenose (kjer je to relevantno)

Izjava o uporabnosti

Ta politika se uporablja za vse dejavnosti obdelave osebnih podatkov, ki jih izvaja CYBER-SEC v povezavi z:

- glavno spletno stranjo: <https://cyber-sec.si/>
- učno platformo: <https://academy.cyber-sec.si/>
- povezane storitve, podpora uporabnikom, gostovane vsebine, prijave na dogodke/izobraževanja in povpraševanja.

Vsi zaposleni, pogodbeni sodelavci in zunanji obdelovalci morajo spoštovati to politiko. Kršitve lahko vodijo v disciplinske ukrepe ter/ali pravne posledice.

1. Politika zasebnosti

Upravljavec

CYBER-SEC, informacijska in kibernetska varnost, d.o.o.

Tolstojeva ulica 41, 1000 Ljubljana, Slovenija

Davčna št.: SI89630777 **Matična št.:** 9827021000

E-pošta (varstvo podatkov & zahteve): gdpr@cyber-sec.si

Kontaktna točka za varstvo podatkov: gdpr@cyber-sec.si (DPO ni imenovan, ker podjetje ne izpolnjuje pogojev iz 37. člena GDPR; ob spremembah bomo politiko ustrezno posodobili). cyber-sec.si

Nameni in pravne podlage

- **Izvajanje pogodbe** (GDPR 6(1)(b)): ustvarjanje/uporaba uporabniških računov, izvedba tečajev, izdaja certifikatov, obdelava naročil/povpraševanj, komunikacija glede storitev.
- **Izvedba ukrepov pred sklenitvijo pogodbe** (GDPR 6(1)(b)): priprava ponudb na podlagi povpraševanj.
- **Zakonska obveznost** (GDPR 6(1)(c)): računovodska in davčna skladnost.
- **Zakoniti interesi** (GDPR 6(1)(f)): informacijska varnost sistemov, preprečevanje zlorab, izboljšave storitev, statistika z agregiranimi/anonymiziranimi podatki.
- **Privolitev** (GDPR 6(1)(a)): trženjska obvestila, ne-nujni piškotki/analitika. cyber-sec.si

Kategorije osebnih podatkov

- **Podatki o računu/identiteti:** ime, priimek, e-pošta, jezik vmesnika; zgoščeno geslo.
- **Učna dejavnost (Academy):** vpisi v tečaje, napredovanje, rezultati testov, certifikati, prispevki na forumu.
- **Plačila/obračuni:** ime plačnika, naslov za izstavitve računa, ID transakcije, izdajatelj plačil, zadnje štiri številke kartice (prek ponudnika plačilnih storitev).
- **Komunikacija in povpraševanja:** vsebina sporočil, podatki na obrazcih (npr. naziv podjetja, interes za izobraževanje).
- **Tehnični podatki in dnevniki:** IP naslov (pri analitiki anonimiziran), identifikatorji sej, podatki o napravi/brskalniku, nastavitve piškotkov. cyber-sec.si

Prejemniki / kategorije prejemnikov

- **Gostovanje in infrastruktura:** Hetzner (EU).
- **E-pošta in produktivnost:** Microsoft Ireland Operations Limited (EU podatkovna središča, kjer je primerno).
- **Plačila:** SaferPay → Worldline Financial Services Europe.
- **Analitika:** Google Analytics (Google Ireland Ltd.).

Obdelava pri obdelovalcih poteka na podlagi sklenjenih **pogodb o obdelavi** v skladu z 28. členom GDPR.

Hramba

- **Učni podatki (Academy):** 1 leto po zadnji aktivnosti.
- **Plačilni/računovodski podatki:** 10 let (v skladu z davčnimi predpisi RS).
- **Povpraševanja/komunikacija:** do 2 leti po zaključku komunikacije ali prej, če ugovarjate.
- **Tehnični dnevniki (spletni strežnik, požarni zid):** 90 dni.
- **Dnevniki varnostnih incidentov :** do 12 mesecev (ali dlje, če je to nujno za preiskavo incidenta/pravne obveznosti).

Po poteku rokov podatke izbrišemo ali anonimiziramo (kjer je to primerno). cyber-sec.si

Profiliranje in avtomatizirano odločanje

Ne izvajamo odločanja, ki bi temeljilo izključno na avtomatizirani obdelavi in bi imelo pravne učinke za posameznika.

2. Politika piškotkov

Načela in pravna podlaga

- **Nujni piškotki** so potrebni za delovanje strani (npr. prijava, varnost) in se nastavljajo **brez privolitve**.
- **Ne-nujni piškotki** (npr. analitika) se nastavijo **le na podlagi vaše izrecne privolitve (opt-in)**, kot zahteva **ZEKom-2, 225. člen**, in v skladu s smernicami **Informacijskega pooblaščenca**. Mehanizem omogoča **Sprejmi vse, Zavrni ne-nujne** in **Nastavitve** (granularno). Privolitev lahko kadarkoli prekličete v nastavitvah.

Kategorije

- **Nujni:** avtentikacija, varnost, ohranjanje seje.
- **Analitični:** Google Analytics (z anonimizacijo IP).

Tabela piškotkov

Kategorija	Orodje	Ime piškotka	Namen	Hramba	Ponudnik
Nujni	Seja	PHPSESSID (ali podobno)	Ohranjanje prijave/seje	Seja	CYBER-SEC
Analitični	Google Analytics	_ga	Statistika obiska (ID uporabnika)	2 leti	Google Ireland Ltd.
Analitični	Google Analytics	_gid	Statistika uporabe	24 ur	Google Ireland Ltd.
Analitični	Google Analytics	_gat	Omejevanje hitrosti zahtevkov	1 minuta	Google Ireland Ltd.
Analitični (pixel)	Google Analytics	collect	Podatki o napravi/vedenju	Seja	google-analytics.com

3. Načrt hrambe podatkov

Kategorija podatkov	Rok hrambe	Pravna podlaga	Kategorije prejemnikov
Učni podatki (Academy)	1 leto po zadnji aktivnosti	6(1)(b)	Hetzner, Microsoft
Plačilni/računovodski zapisi	10 let	6(1)(c)	Microsoft
Pisma/povpraševanja	do 2 leti po zaključku	6(1)(b)/(f)	SaferPay / Worldline
Tehnični dnevniki (spletni strežnik)	90 dni	6(1)(f)	Google Analytics
Dnevniki varnostnih incidentov (EDR)	do 12 mesecev	6(1)(f)	EDR rešitev

Z vsemi pogodbenimi obdelovalci imamo sklenjene pogodbe o obdelavi po 28. členu GDPR.

5. Tehnični in organizacijski ukrepi (TOM)

- Načela **privzete** in **vgrajene** zasebnosti (GDPR 5 in 25).
- **RBAC/least privilege** in revizijske sledi.
- **Šifriranje** pri prenosu (TLS 1.2+) in mirovanju (šifriranje podatkovnih nosilcev/baz).
- **Dvofaktorska avtentikacija** za skrbniške račune.
- **Psevdonimizacija/anonimizacija** pri analitiki.
- **Redno posodabljanje**, varnostne kopije in testiranje obnovitve.
- **Ocena tveganja** in periodični pregledi TOM.
- **Varnost obdelave** skladno z 32. členom GDPR.

6. Postopek za uveljavljanje pravic posameznikov (DSR)

Kako vložiti zahtevo:

Pišite na gdpr@cyber-sec.si. (Po potrebi lahko uporabite tudi kontaktne obrazce na strani.) Zahteva mora omogočati identifikacijo posameznika.

Preverjanje identitete:

Ustrezno preverjanje (npr. povratna potrditev preko istega e-poštnega naslova, dodatni podatki; za uporabniške račune Academy preverjanje preko prijave/2FA).

Roki:

Potrditev prejema v **72 urah**; odgovor v **1 mesecu** od prejema (možnost podaljšanja za **dodatna 2 meseca** pri kompleksnih zahtevah – obvestimo o razlogih in zamudi).

Pravice:

dostop, popravek, izbris, omejitev obdelave, prenosljivost, ugovor, umik privolitve (ne vpliva na zakonitost obdelave pred umikom).

Pritožba pri nadzornem organu:

Informacijski pooblaščenec RS, Dunajska cesta 22, 1000 Ljubljana, gp.ip@ip-rs.si, tel. 01 230 97 30, <https://www.ip-rs.si>.

7. Načrt odziva na kršitev varstva osebnih podatkov

- **Zaznava:** s pomočjo EDR in nadzornih orodij.
- **Zajezev:** izolacija sistemov, preklic kompromitiranih poverilnic, onemogočanje računov.
- **Ocena:** vrste podatkov, obseg, šifriranje/psevdonimizacija, vpliv na pravice posameznikov.
- **Obvestitev:** **IP RS v 72 urah** po seznanitvi s kršitvijo; posameznike **brez nepotrebnega odlašanja**, če obstaja **visoko tveganje** za njihove pravice in svoboščine.
- **Dokumentiranje:** vpis v **register incidentov**, analiza vzrokov in ukrepi za preprečitev ponovitev.

8. Upravljanje privolitev in nastavitvev

- **Piškotki:** privolitev/preklic preko pasice in »**Upravljanje soglasij**« v nogi strani (granularno po kategorijah; privzeto izklop ne-nujnih).
- **Trženjska obvestila:** jasen *opt-in*; odjava preko »**unsubscribe**« povezave v e-pošti ali z odgovorom na sporočilo.
- **Zapisovanje dokazil o privolitvi:** časovni žig, kategorije, verzija pasice/politike.

9. Register pogodbenih obdelovalcev

1. **Hetzner Online GmbH** - gostovanje/infrastruktura (EU).
2. **Microsoft Ireland Operations Limited** - e-poštne storitve in produktivnost (EU podatkovna središča, kjer je primerno).
3. **SaferPay → Worldline Financial Services Europe** - plačila (EU).
4. **Google Ireland Ltd.** - analitika (EU).

10. Izjava o mednarodnih prenosih

Uporabljamo storitve, pri katerih lahko pride do **prenosov v tretje države** (npr. ob uporabi določenih funkcionalnosti ponudnikov skupine Google/Microsoft). V takih primerih zagotovimo **ustrezne zaščitne ukrepe**, kot so **Standardne pogodbene klavzule (SCC)** in ocena vpliva prenosa. Podrobnosti so na voljo na zahtevo.