KORPORATIVNI COMPLIANCE PRAVILNIK O SKLADNOSTI POSLOVANJA IN UPRAVLJANJU TVEGANJ EUROPACIFIC Logistika d.o.o.

Koper, 30.10.2026

Velja z dnem sprejema

Dokument ID: COMP_EPL-2/10-2026
Verzija: 1.1, druga izdaja
Lastnik dokumenta: direktor
Datum pregleda: najmanj enkrat letno

Vsebina

KORPORATIVNI COMPLIANCE PRAVILNIK O SKLADNOSTI POSLOVANJA IN UPRAVLJANJU TVEGANJ 5

1. SPLOŠNE DOLOČBE 5

1. ČLEN(NAMEN PRAVILNIKA) 5
2. ČLEN(PODROČJE UPORABE) 5
3. ČLEN(PRAVNE PODLAGE) 6

2. COMPLIANCE NAČELA - UPRAVLJANJE SKLADNOSTI POSLOVANJA 6

4. ČLEN(NAČELO ZAKONITOSTI) 6
5. ČLEN(ODGOVORNA OSEBA ZA SKLADNOST POSLOVANJA) 7
6. ČLEN(ODGOVORNOST ZAPOSLENIH) 7
7. ČLEN(PREPOVED NEZAKONITEGA RAVNANJA) 8

3. UPRAVLJANJE TVEGANJ 8

8. ČLEN(UPRAVLJANJE TVEGANJ) 8
9. ČLEN(RISK ASSESSMENT) 9
10. ČLEN(AI GOVERNANCE – UPORABA UMETNE INTELIGENCE) 9
11. ČLEN(PREPOVED SAMOSTOJNEGA ODLOČANJA AI) 10
12. ČLEN(PREPOVED VNOSA ZAUPNIH PODATKOV V AI SISTEME) 10
13. ČLEN(EVIDENCA UPORABE AI) 11

4. INFORMACIJSKA IN KIBERNETSKA VARNOST 11

14. ČLEN(UPORABA INFORMACIJSKIH SISTEMOV) 11
15. ČLEN(VARNOSTNI UKREPI) 11
16. ČLEN(UPRAVLJANJE DOSTOPOV) 12
17. ČLEN(NIS2 IN KIBERNETSKA ODPORNOST) 12

5. VARSTVO OSEBNIH PODATKOV 13

18. ČLEN(OBDELAVA OSEBNIH PODATKOV) 13
19. ČLEN(PRAVICE POSAMEZNIKOV) 13
20. ČLEN(KRŠITVE VARSTVA OSEBNIH PODATKOV) 13

6. VAROVANJE POSLOVNIH SKRIVNOSTI 14

21. ČLEN(POSLOVNE SKRIVNOSTI) 14
22. ČLEN(VAROVANJE POSLOVNE SKRIVNOSTI) 14
23. ČLEN(OBVEZNOSTI ZUNANJIH IZVAJALCEV IN NJIHOVO NADZOROVANJE) 14

7. POSLOVNA ETIKA IN KONFLIKT INTERESOV 15

24. ČLEN(POSLOVNA ETIKA) 15
25. ČLEN(KONFLIKT INTERESOV) 15

8. INCIDENT MANAGEMENT IN WHISTLEBLOWING 16

26. ČLEN(OBVEZNOST PRIJAVE INCIDENTOV) 16
27. ČLEN(INCIDENT RESPONSE IN ESKALACIJA) 16
28. ČLEN(ZAŠČITA PRIJAVITELJEV IN NOTRANJA PRIJAVNA POT) 17

9. NADZOR, MONITORING IN REVIZIJE 18

29. ČLEN(NOTRANJI NADZOR) 18
30. ČLEN(MONITORING INFORMACIJSKIH SISTEMOV) 18
31. ČLEN(REVIZIJE IN PRESOJE SKLADNOSTI) 19

10. EVIDENTIRANJE IN HRAMBA PODATKOV 19

32. ČLEN(EVIDENCE IN DOKUMENTACIJA) 19
33. ČLEN(HRAMBA DOKUMENTACIJE) 20

11. ODGOVORNOST IN SANKCIJE 20
34. ČLEN(KRŠITVE PRAVILNIKA) 20
12. IZOBRAŽEVANJE IN OZAVEŠČANJE 21
35. ČLEN(USPOSABLJANJE IN OZAVEŠČANJE ZAPOSLENIH) 21
13. KONČNE DOLOČBE 22
36. ČLEN(SPREMEMBE PRAVILNIKA) 22
37. ČLEN(SEZNANITEV ZAPOSLENIH) 22
38. ČLEN(VELJAVNOST PRAVILNIKA) 22

Na podlagi Zakona o gospodarskih družbah (ZGD-1), Zakona o delovnih razmerjih (ZDR-1), Zakona o varstvu osebnih podatkov (ZVOP-2), Splošne uredbe o varstvu podatkov (GDPR), predpisov s področja informacijske in kibernetske varnosti, varovanja poslovnih skrivnosti in upravljanja tveganj ter drugih veljavnih predpisov Republike Slovenije in Evropske unije družbe EUROPACIFIC Logistika d.o.o., Ankaranska cesta 5, 6000 Koper sprejema naslednji

KORPORATIVNI COMPLIANCE PRAVILNIK O SKLADNOSTI POSLOVANJA IN UPRAVLJANJU TVEGANJ

1. SPLOŠNE DOLOČBE

1. člen
(namen pravilnika)

Ta pravilnik določa:

- sistem skladnosti poslovanja družbe,
- pravila korporativnega upravljanja,
- notranje compliance standarde,
- sistem upravljanja tveganj,
- pravila informacijske in AI varnosti,
- pravila varovanja poslovnih skrivnosti,
- postopke prijave incidentov in nepravilnosti,
- postopke notranjega nadzora,
- odgovornosti zaposlenih, vodstva in zunanjih sodelavcev,
- sistem upravljanja skladnosti z GDPR, AI Act in NIS2,
- ter zaščito poslovnih interesov družbe.

Namen pravilnika je:

- zagotavljanje zakonitega poslovanja,
- zmanjševanje pravnih, regulatornih, operativnih in varnostnih tveganj,
- zaščita poslovnih interesov družbe,
- zagotavljanje skladnosti z zakonodajo Republike Slovenije in Evropske unije,
- zaščita informacijskih sistemov, podatkov in poslovnih skrivnosti,
- zagotavljanje sledljivosti in odgovornosti poslovanja,
- ter vzpostavitev učinkovitega sistema korporativnega upravljanja.

2. člen
(področje uporabe)

Ta pravilnik velja za:

- vse zaposlene,
- direktorje in vodstvo družbe,
- zunanje sodelavce,
- pogodbene izvajalce,
- IT izvajalce,
- svetovalce,
- študente,

- ter vse osebe, ki dostopajo do informacijskih sistemov, podatkov ali poslovnih informacij družbe.

Določbe tega pravilnika so obvezne za vse navedene osebe.

Vsaka oseba mora biti pred pridobitvijo dostopov seznanjena z določbami tega pravilnika.

3. člen
(pravne podlage)

Ta pravilnik temelji zlasti na:

- Zakonu o gospodarskih družbah (ZGD-1),
- Zakonu o delovnih razmerjih (ZDR-1),
- Obligacijskem zakoniku (OZ),
- Zakonu o varstvu osebnih podatkov (ZVOP-2),
- Splošni uredbi o varstvu podatkov (GDPR),
- Zakonu o poslovni skrivnosti (ZPosS),
- Direktivi NIS2,
- EU AI Act,
- predpisih s področja informacijske in kibernetske varnosti,
- predpisih s področja preprečevanja korupcije,
- ter drugih veljavnih predpisih Republike Slovenije in Evropske unije.

2. COMPLIANCE NAČELA - UPRAVLJANJE SKLADNOSTI POSLOVANJA

4. člen
(načelo zakonitosti)

Družba posluje:

- zakonito, skladno zakonodajo Republike Slovenije,
- pravom Evropske unije,
- skladno s pogodbenimi obveznostmi,
- skladno z internimi pravilniki,
- transparentno,
- odgovorno,
- profesionalno,
- skladno z dobrimi poslovnimi praksami,
- ter skladno z načeli informacijske in AI varnosti.

5. člen
(odgovorna oseba za skladnost poslovanja)

Direktor družbe določi odgovorno osebo za:

- compliance nadzor,
- upravljanje tveganj,
- koordinacijo incident management postopkov,
- usklajevanje GDPR zahtev,
- koordinacijo AI governance,
- ter nadzor nad izvajanjem tega pravilnika.

Odgovorna oseba lahko sodeluje z:

- pooblaščencem za varstvo osebnih podatkov,
- zunanjimi pravnimi svetovalci,
- IT varnostnimi izvajalci,
- ter zunanjimi revizorji.

Odgovorna oseba za skladnost poslovanja mora:

- spremljati spremembe zakonodaje,
- izvajati notranje presoje skladnosti,
- pripravljati priporočila za odpravo neskladnosti,
- koordinirati odzivanje na varnostne incidente,
- sodelovati pri presojah zunanjih izvajalcev,
- ter poročati vodstvu o pomembnih tveganjih in neskladnostih.

Vodstvo družbe mora odgovorni osebi zagotoviti ustrezne organizacijske, kadrovske, tehnične in finančne vire za izvajanje nalog skladnosti poslovanja.

6. člen
(odgovornost zaposlenih)

Vsak zaposleni ali sodelavec je osebno odgovoren za:

- zakonito izvajanje svojih nalog,
- zaščito poslovnih interesov družbe,
- varovanje osebnih podatkov,
- varovanje poslovnih skrivnosti,
- preprečevanje zlorab,
- prijavo incidentov,
- ter spoštovanje tega pravilnika.

7. člen
(prepoved nezakonitega ravnanja)

Prepovedano je:

- ravnanje v nasprotju z zakonodajo,
- zloraba informacijskih sistemov,
- prikrivanje nepravilnosti,
- nepooblaščena uporaba podatkov,
- zloraba poslovnih skrivnosti,
- koruptivno ravnanje,
- nepooblaščeno razkrivanje informacij,
- uporaba neodobrenih AI sistemov,
- ter ravnanje, ki bi lahko škodovalo družbi ali njenemu ugledu.

3. UPRAVLJANJE TVEGANJ

8. člen
(upravljanje tveganj)

Družba izvaja sistem upravljanja:

- pravnih tveganj,
- informacijskih tveganj,
- AI tveganj,
- kibernetskih tveganj,
- pogodbenih tveganj,
- operativnih tveganj,
- reputacijskih tveganj,
- ter tveganj glede varstva osebnih podatkov.

Družba izvaja periodične ocene tveganj najmanj enkrat letno oziroma ob pomembnih organizacijskih ali tehnoloških spremembah.

Družba določa stopnje tveganj glede na:

- verjetnost nastanka tveganja,
- možne finančne posledice,
- vpliv na poslovanje,
- vpliv na posameznike,
- vpliv na informacijsko varnost,
- regulatorna tveganja,
- ter reputacijska tveganja.

Za pomembna tveganja se določijo odgovorne osebe, ukrepi za zmanjševanje tveganj ter roki za izvedbo ukrepov.

9. člen
(risk assessment)

Družba izvaja:

- ocene vpliva na varstvo osebnih podatkov,
- ocene AI tveganj,
- varnostne preglede,
- ocene skladnosti zunanjih izvajalcev,
- ter ocene kibernetskih tveganj.

Ocene tveganj se dokumentirajo in hranijo skladno z internimi pravili hrambe dokumentacije.

10. člen
(AI governance – uporaba umetne inteligence)

Uporaba umetne inteligence mora biti:

- zakonita,
- pregledna,
- sledljiva,
- varna,
- nadzorovana,
- nediskriminatorna,
- ter skladna z EU AI Act.

Družba mora zagotavljati:

- človeški nadzor nad AI sistemi,
- sledljivost odločitev,
- nadzor nad AI tveganji,
- zaščito podatkov,
- zaščito poslovnih skrivnosti,
- ter nadzor nad uporabo zunanjih AI storitev.

Uporaba AI sistemov mora temeljiti na načelih:

- zakonitosti,
- človekovega nadzora,
- transparentnosti,
- sledljivosti,
- nediskriminacije,
- varnosti,
- ter sorazmernosti uporabe.

Prepovedana je uporaba AI sistemov:

- brez predhodne odobritve družbe,
- za avtomatizirano sprejemanje odločitev brez človeškega nadzora,
- za obdelavo osebnih podatkov brez ustrezne pravne podlage,

- ali na način, ki bi lahko povzročil diskriminacijo ali nesorazmeren poseg v pravice posameznikov.

Uporabnik AI sistema je dolžan preveriti pravilnost, zakonitost in ustreznost rezultatov AI sistema pred njihovo uporabo ali posredovanjem tretjim osebam.

11. člen
(prepoved samostojnega odločanja AI)

AI sistemi ne smejo samostojno sprejemati:

- pravnih odločitev,
- kadrovskih odločitev,
- finančnih odločitev,
- odločitev z večjim poslovnim učinkom,
- ali drugih odločitev z bistvenim vplivom na posameznike,

brez ustreznega človeškega nadzora.

Izjemoma je vnos podatkov dovoljen:

- če je AI sistem odobren s strani družbe,
- če je zagotovljena ustrezna pogodbena zaščita podatkov,
- če je zagotovljena skladnost z GDPR,
- ter če je izvedena ustrezna ocena tveganj.

12. člen
(prepoved vnosa zaupnih podatkov v AI sisteme)

V javne ali zunanje AI sisteme ni dovoljeno vnašati:

- osebnih podatkov,
- poslovnih skrivnosti,
- internih pogodb,
- finančnih podatkov,
- API ključev,
- dostopnih podatkov,
- izvorne kode,
- ali drugih zaupnih podatkov,

razen če je to izrecno odobreno s strani družbe.

13. člen
(evidenca uporabe AI)

Družba lahko vodi evidenco:

- uporabljenih AI sistemov,
- AI ponudnikov,
- področij uporabe AI,
- ocen tveganj,
- AI incidentov,
- ter odobritev uporabe AI rešitev.

4. INFORMACIJSKA IN KIBERNETSKA VARNOST

14. člen
(uporaba informacijskih sistemov)

Informacijski sistemi družbe se smejo uporabljati izključno:

- za službene namene,
- skladno z internimi pravili,
- skladno z varnostnimi zahtevami,

ter skladno z zakonodajo.

15. člen
(varnostni ukrepi)

Vsi uporabniki morajo:

- uporabljati močna gesla,
- uporabljati večfaktorsko avtentikacijo kjer je omogočena,
- varovati dostopne podatke,
- preprečevati nepooblaščen dostop,
- zaklepati naprave,
- uporabljati odobrene informacijske sisteme,
- ter upoštevati varnostna navodila družbe.

Uporabniki ne smejo:

- deliti dostopnih podatkov,
- uporabljati neodobrenih naprav ali programske opreme,
- izklapljati varnostnih mehanizmov,
- nameščati nepooblaščenih aplikacij,
- ali obiti varnostnih pravil družbe.

Družba lahko izvaja tehnične in organizacijske ukrepe za zaščito informacijskih sistemov, podatkov in poslovnih skrivnosti.

16. člen
(upravljanje dostopov)

Dostopi do informacijskih sistemov se:

- dodeljujejo po načelu najmanjšega obsega pravic,
- periodično preverjajo,
- omejujejo glede na delovne naloge,
- prekličejo ob prenehanju sodelovanja,
- ter evidentirajo.

Družba lahko izvaja revizijo uporabniških dostopov.

17. člen
(NIS2 in kibernetska odpornost)

Družba izvaja ustrezne tehnične in organizacijske ukrepe za:

- zaščito omrežij in informacijskih sistemov,
- zaznavanje varnostnih incidentov,
- preprečevanje nepooblaščenih dostopov,
- upravljanje ranljivosti,
- neprekinjeno poslovanje,
- backup in recovery postopke,
- ter odzivanje na varnostne incidente.

Družba lahko izvaja:

- načrte neprekinjenega poslovanja,
- disaster recovery postopke,
- redno testiranje backup sistemov,
- varnostna testiranja,
- upravljanje ranljivosti,
- ter presoje dobaviteljev in zunanjih IT izvajalcev.

Kritični varnostni incidenti se obravnavajo prioritetno in se evidentirajo skladno z internimi postopki.

5. VARSTVO OSEBNIH PODATKOV

18. člen
(obdelava osebnih podatkov)

Družba obdeluje osebne podatke:

- zakonito,
- pošteno,
- transparentno,
- namensko,
- sorazmerno,
- ter skladno z GDPR in ZVOP-2.

Osebni podatki se obdelujejo samo v obsegu, ki je potreben za zakonite poslovne namene.

19. člen
(pravice posameznikov)

Družba zagotavlja posameznikom uresničevanje pravic:

- dostopa,
- popravka,
- izbrisa,
- omejitve obdelave,
- prenosljivosti,
- ugovora,
- ter drugih pravic skladno z GDPR.

20. člen
(kršitve varstva osebnih podatkov)

Vsak sum kršitve varstva osebnih podatkov mora biti nemudoma prijavljen odgovorni osebi.

Družba izvaja postopke:

- evidentiranja incidentov,
- ocene tveganj,
- poročanja nadzornim organom,
- ter obveščanja posameznikov,

kadar je to zahtevano z zakonodajo.

V primeru kršitve varstva osebnih podatkov družba izvede:

- oceno tveganja za pravice in svoboščine posameznikov,
- dokumentiranje incidenta,
- korektivne ukrepe,
- ter po potrebi prijavo nadzornemu organu v zakonsko določenih rokih.

6. VAROVANJE POSLOVNIH SKRIVNOSTI

21. člen
(poslovne skrivnosti)

Za poslovno skrivnost se štejejo zlasti:

- poslovni podatki,
- pogodbe,
- ceniki,
- izvorna koda,
- AI modeli,
- baze podatkov,
- konfiguracije sistemov,
- API ključi,
- razvojne rešitve,
- dokumentacija,
- poslovni postopki,
- ter druge informacije, katerih razkritje bi lahko škodovalo družbi ali njenim partnerjem.

22. člen
(varovanje poslovne skrivnosti)

Brez predhodnega pisnega dovoljenja ni dovoljeno:

- razkrivati poslovnih skrivnosti,
- kopirati ali prenašati kode,
- izvažati baz podatkov,
- posredovati podatkov tretjim osebam,
- uporabljati rešitev družbe za zasebne ali konkurenčne namene.

Obveznost varovanja poslovnih skrivnosti velja tudi po prenehanju sodelovanja z družbo.

23. člen
(obveznosti zunanjih izvajalcev in njihovo nadzorovanje)

Zunanji izvajalci morajo:

- spoštovati ta pravilnik,
- podpisati NDA oziroma pogodbo o zaupnosti,
- uporabljati ustrezne varnostne standarde,
- zagotavljati varovanje podatkov,
- zagotavljati skladnost z GDPR,
- zagotavljati ustrezne kibernetske ukrepe,
- ter ravnati skladno z navodili družbe.

Zunanji izvajalci morajo na zahtevo družbe predložiti:

- dokazila o varnostnih ukrepih,
- dokazila o skladnosti z GDPR,
- dokazila o usposobljenosti oseb,
- ter druge informacije, potrebne za presojo skladnosti.

Družba lahko omeji ali prepove uporabo zunanjega izvajalca, če ta predstavlja nesprejemljivo pravno, varnostno ali poslovno tveganje.

Družba lahko:

- preverja skladnost izvajalcev,
- omeji dostop do sistemov,
- izvaja varnostne preglede,
- zahteva odpravo neskladnosti,
- zahteva dokazila o skladnosti,
- ter prekine sodelovanje v primeru neskladnosti ali varnostnih tveganj.

7. POSLOVNA ETIKA IN KONFLIKT INTERESOV

24. člen
(poslovna etika)

Vsi zaposleni in sodelavci morajo ravnati:

- pošteno,
- profesionalno,
- odgovorno,
- skladno z zakonodajo,
- ter v najboljšem interesu družbe.

Prepovedano je ravnanje, ki:

- škoduje ugledu družbe,
- predstavlja konflikt interesov,
- povzroča diskriminacijo,
- omogoča korupcijo,

ali ustvarja neupravičeno osebno korist.

25. člen
(konflikt interesov)

Vsaka oseba mora brez nepotrebnega odlašanja razkriti:

- dejanski konflikt interesov,
- potencialni konflikt interesov,
- osebne, finančne ali poslovne povezave,
- ali druge okoliščine, ki bi lahko vplivale na nepristranskost poslovanja.

Brez predhodnega pisnega soglasja družbe ni dovoljeno:

- izvajati konkurenčnih dejavnosti,
- sodelovati pri konkurenčnih projektih,
- uporabljati sredstev ali informacij družbe za zasebne projekte,
- sprejemati neprimernih daril ali koristi,
- ali izkoriščati poslovnih informacij za osebno korist.

Družba lahko od zaposlenih ali sodelavcev zahteva podpis izjave o neobstoju konflikta interesov.

8. INCIDENT MANAGEMENT IN WHISTLEBLOWING

26. člen
(obveznost prijave incidentov)

Vsaka oseba mora nemudoma prijaviti:

- varnostni incident,
- AI incident,
- izgubo ali uničenje podatkov,
- sum zlorabe,
- nepooblaščen dostop,
- sum kršitve GDPR,
- sum korupcije,
- sum goljufije,
- ali drugo pomembno nepravilnost.

Incidenti se prijavljajo:

- odgovorni osebi za skladnost,
- neposredno vodstvu družbe,
- pooblaščencu za varstvo osebnih podatkov,
- ali po internih prijavnih kanalih.

V primeru večjega varnostnega incidenta mora biti vodstvo obveščeno nemudoma.

27. člen
(incident response in eskalacija)

Družba izvaja sistem upravljanja incidentov, ki vključuje:

- evidentiranje incidentov,
- klasifikacijo incidentov,
- določitev stopnje tveganja,
- eskalacijo incidentov,
- odpravo posledic,
- izvedbo korektivnih ukrepov,
- izvedbo preventivnih ukrepov,
- ter pripravo poročil o incidentih.

Incidenti se obravnavajo skladno z:

- internimi varnostnimi postopki,
- GDPR,
- NIS2,
- pogodbenimi obveznostmi,
- ter drugimi veljavnimi predpisi.

Družba lahko vodi centralni register incidentov.

Družba določi:

- stopnje kritičnosti incidentov,
- odgovorne osebe za obravnavo incidentov,
- roke za odzivanje,
- postopke eskalacije,
- ter postopke obveščanja vodstva.

Zaposleni in sodelavci so dolžni sodelovati pri preiskavi incidentov ter zagotoviti vse potrebne informacije in dokumentacijo.

28. člen
(zaščita prijaviteljev in notranja prijavna pot)

Družba zagotavlja varstvo prijaviteljev nepravilnosti in kršitev predpisov v skladu z veljavno zakonodajo, zlasti Zakonom o zaščiti prijaviteljev (ZZPri), ter Pravilnikom o notranji prijavni poti in zaščiti prijaviteljev, ki velja v družbi.

Družba zagotavlja, da se prijaviteljem, ki izpolnjujejo zakonske pogoje za zaščito, zagotovi zlasti:

- varovanje identitete in zaupnosti podatkov o prijavitelju;
- prepoved povračilnih ukrepov zaradi podane prijave;
- nepristranska, skrbna in zaupna obravnava prijave;
- omejitev dostopa do prijave in z njo povezanih podatkov na pooblaščene osebe;
- ustrezno dokumentiranje in varovanje evidenc prijav;
- obravnava prijave ter obveščanje prijavitelja v skladu z veljavno zakonodajo in internim pravilnikom.

Prepovedani so vsi neposredni ali posredni povračilni ukrepi, diskriminacija, pritiski, grožnje ali druga škodljiva ravnanja zoper prijavitelja, posrednika ali povezane osebe zaradi prijave.

Družba zagotavlja notranjo prijavno pot v skladu s svojim Pravilnikom o notranji prijavni poti in zaščiti prijaviteljev. Prijava se lahko poda na načine in prek kontaktnih podatkov, določenih v navedenem pravilniku. Anonimne prijave se obravnavajo v skladu z možnostmi in pogoji, določenimi v pravilniku in veljavni zakonodaji.

Podrobnejši postopki prejema, evidentiranja, obravnave in zaključevanja prijav, pristojnosti zaupnika ter ukrepi za zaščito prijaviteljev so določeni v ločenem internem pravilniku družbe.

9. NADZOR, MONITORING IN REVIZIJE

29. člen
(notranji nadzor)

Družba lahko izvaja:

- notranje revizije,
- varnostne preglede,
- nadzor dostopov,
- pregled aktivnosti uporabnikov,
- pregled skladnosti,
- pregled uporabe informacijskih sistemov,
- pregled uporabe AI sistemov,
- ter druge zakonite nadzorne ukrepe.

Notranji nadzor se izvaja:

- zakonito,
- sorazmerno,
- skladno z namenom nadzora,
- ter ob spoštovanju pravic posameznikov.

30. člen
(monitoring informacijskih sistemov)

Družba lahko zaradi:

- zagotavljanja informacijske varnosti,
- zaščite poslovnih skrivnosti,
- preprečevanja zlorab,
- zagotavljanja skladnosti,
- ter zagotavljanja neprekinjenega poslovanja,

izvaja monitoring informacijskih sistemov.

Monitoring lahko vključuje:

- sistemske dnevnike,
- evidence dostopov,
- evidence prijav,
- varnostne dnevnike,
- evidence aktivnosti,
- evidence AI uporabe,
- ter evidence incidentov.

Monitoring se izvaja izključno zaradi:

- zagotavljanja informacijske varnosti,
- zaščite poslovnih skrivnosti,
- zaščite informacijskih sistemov,

- preprečevanja zlorab,
- zagotavljanja zakonitega poslovanja,
- ter zagotavljanja neprekinjenega poslovanja.

Monitoring se ne izvaja za nesorazmeren nadzor zaposlenih ali nadzor njihove zasebne komunikacije v nasprotju z zakonodajo.

Dostop do evidenc je omejen na pooblaščene osebe.

Monitoring se ne sme izvajati prekomerno ali v nasprotju z zakonodajo.

31. člen
(revizije in presoje skladnosti)

Družba lahko izvaja:

- notranje compliance presoje,
- varnostne presoje,
- GDPR presoje,
- AI governance presoje,
- presoje zunanjih izvajalcev,
- ter druge postopke preverjanja skladnosti.

Zaposleni in sodelavci morajo omogočiti izvedbo zakonitih pregledov in nadzorov.

Družba lahko od zaposlenih, sodelavcev in zunanjih izvajalcev zahteva sodelovanje pri zakonitih pregledih, presojah in revizijah.

Ugotovljene neskladnosti se dokumentirajo ter po potrebi določijo korektivni in preventivni ukrepi.

10. EVIDENTIRANJE IN HRAMBA PODATKOV

32. člen
(evidence in dokumentacija)

Družba lahko vodi evidence:

- dostopov,
- varnostnih incidentov,
- AI incidentov,
- notranjih pregledov,
- compliance postopkov,
- AI ocen tveganj,
- evidenc usposabljanj,
- evidenc seznanitve zaposlenih,
- varnostnih pregledov,
- ter drugih postopkov zaradi zagotavljanja skladnosti.

Evidence se vodijo v obsegu, ki je potreben za zakonite poslovne namene.

33. člen
(hramba dokumentacije)

Dokumentacija in evidence se hranijo:

- skladno z zakonodajo,
- skladno z internimi pravili hrambe,
- skladno z načelom omejitve hrambe,
- ter samo toliko časa, kolikor je potrebno za zakonite poslovne namene.

Po preteku rokov hrambe se dokumentacija:

- izbriše,
- anonimizira,
- ali uniči na varen način.

Dostop do dokumentacije in evidenc je omejen na pooblaščene osebe.

Družba izvaja ustrezne organizacijske in tehnične ukrepe za zaščito dokumentacije pred:

- izgubo,
- uničenjem,
- nepooblaščenim dostopom,
- spremembami,
- ali zlorabami.

11. ODGOVORNOST IN SANKCIJE

34. člen
(kršitve pravilnika)

Kršitev tega pravilnika lahko predstavlja:

- kršitev delovnih obveznosti,
- hujšo kršitev delovnih obveznosti,
- razlog za disciplinski postopek,
- razlog za odpoved pogodbe,
- odškodninsko odgovornost,
- pogodbeno odgovornost,
- kazensko odgovornost,
- ali drugo pravno odgovornost.

Za hujše kršitve se štejejo zlasti:

- namerna zloraba podatkov,
- razkrivanje poslovnih skrivnosti,
- nepooblaščeno posredovanje podatkov,
- nepooblaščen dostop do sistemov,
- prikrivanje incidentov,
- uporaba neodobrenih AI sistemov,

- iznos podatkov brez dovoljenja,
- onemogočanje varnostnih ukrepov,
- ter druge hujše varnostne ali pravne kršitve.

Družba lahko v primeru kršitev:

- omeji ali prekliče dostope,
- zahteva vračilo dokumentacije ali naprav,
- izvede notranjo preiskavo,
- zahteva odpravo posledic kršitve,
- ali uvede druge zakonite ukrepe za zaščito svojih interesov.

Postopki se vodijo skladno z:

- ZDR-1,
- internimi akti družbe,
- pogodbami,
- NDA določili,
- ter veljavno zakonodajo.

12. IZOBRAŽEVANJE IN OZAVEŠČANJE

35. člen
(usposabljanje in ozaveščanje zaposlenih)

Družba lahko izvaja:

- compliance usposabljanja,
- GDPR usposabljanja,
- AI governance usposabljanja,
- usposabljanja s področja informacijske varnosti,
- phishing simulacije,
- ter druga strokovna izobraževanja.

Zaposleni so dolžni sodelovati pri obveznih usposabljanjih.

Družba lahko izvaja aktivnosti za:

- povečanje varnostne kulture,
- zmanjševanje tveganj,
- preprečevanje socialnega inženiringa,
- ozaveščanje glede AI tveganj,
- ter izboljšanje skladnosti poslovanja.

13. KONČNE DOLOČBE

36. člen
(spremembe pravilnika)

Družba lahko pravilnik kadarkoli spremeni ali dopolni zaradi:

- spremembe zakonodaje,
- organizacijskih potreb,
- tehnološkega razvoja,
- varnostnih zahtev,
- compliance zahtev,
- zahtev poslovnih partnerjev,
- ali drugih poslovnih razlogov.

37. člen
(seznanitev zaposlenih)

Vsi zaposleni in sodelavci morajo biti seznanjeni s tem pravilnikom.

Družba lahko vodi evidenco:

- seznanitve zaposlenih,
- podpisov,
- usposabljanj,

ter drugih compliance aktivnosti.

38. člen
(veljavnost pravilnika)

Ta pravilnik začne veljati z dnem sprejema.

Vsi zaposleni, sodelavci in zunanji izvajalci so dolžni ravnati skladno z njegovimi določbami.

V Kopru, dne 30.10.2026

EUROPACIFIC Logistika d.o.o.
Direktor
Rok Kobal

EUROPACIFIC LOGISTIKA d.o.o.
Ankaranska cesta 5, 6000 Koper
SLOVENIJA
ID za DDV SI77589483