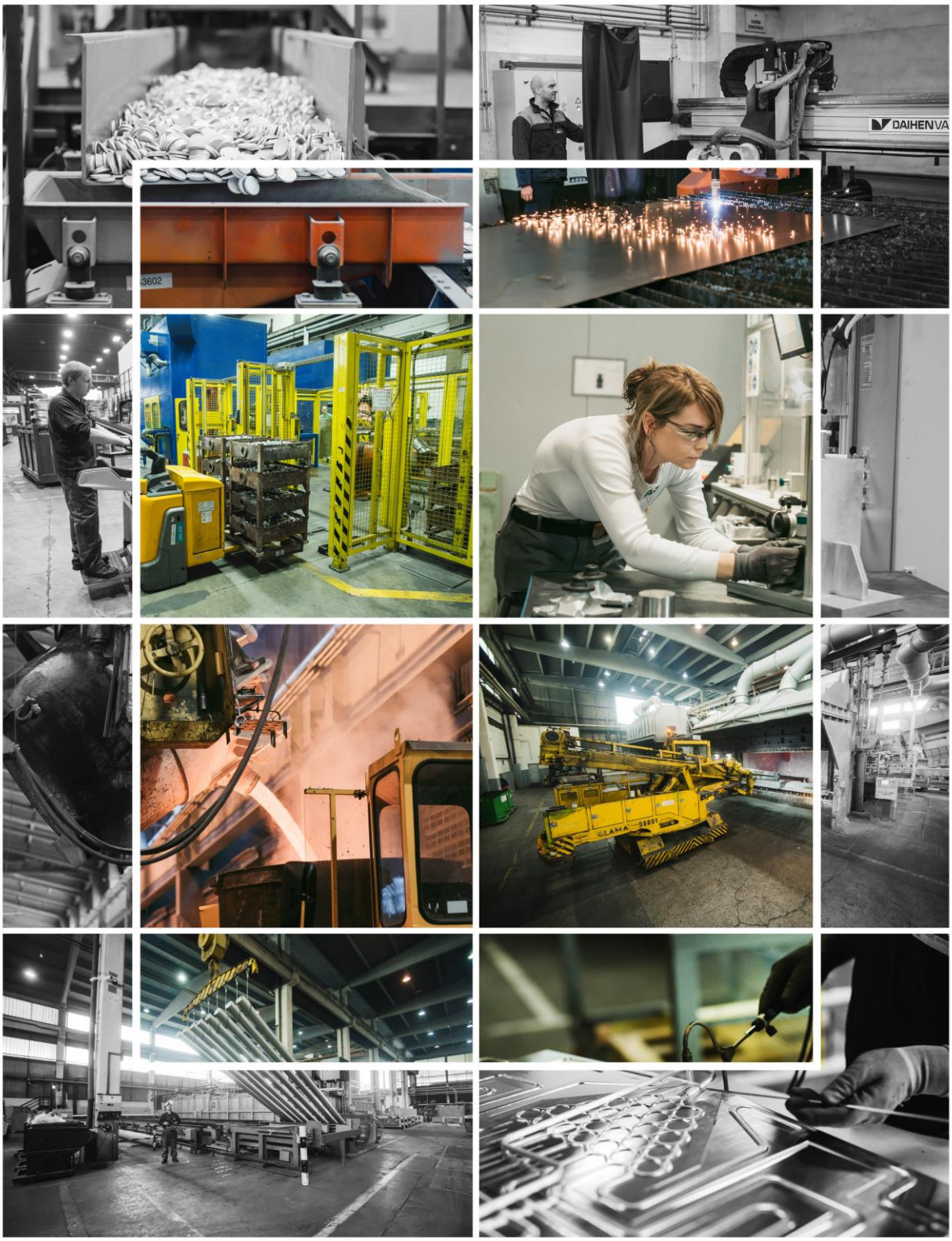
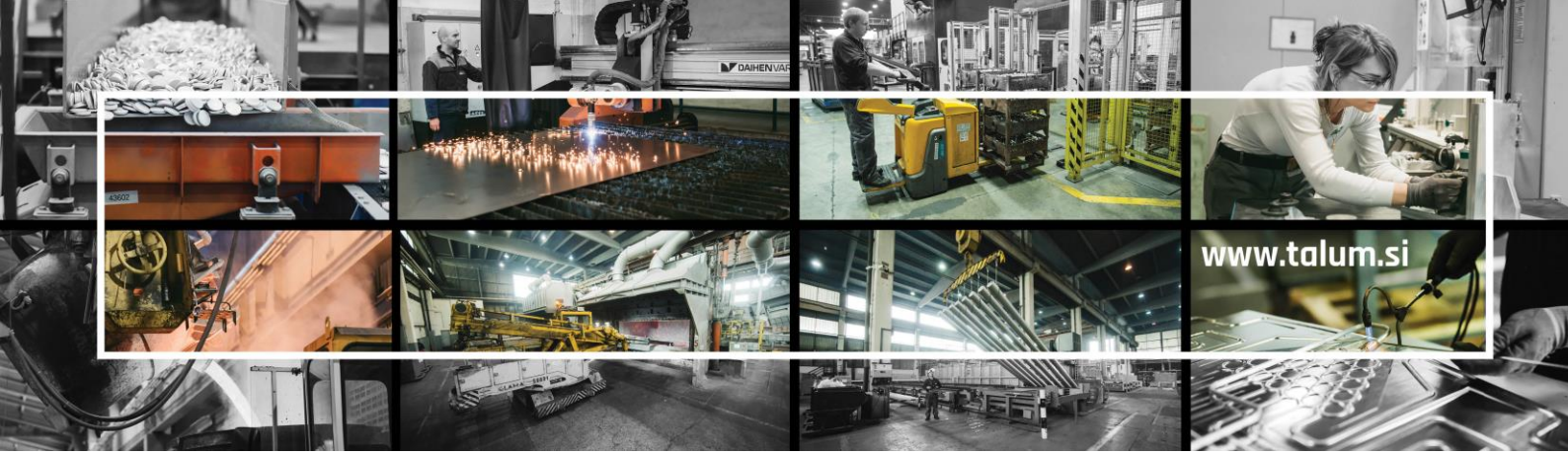
TALUM



Pravilnik korporativne integritete TALUM d.d. Kidričevo



V skladu z določbami Statuta družbe, Etičnega kodeksa SKUPINE TALUM in Slovenskimi smernicami korporativne integritete (Januar 2014), je Uprava dne 4.3.2019 sprejela čistopis akta:

Pravilnik korporativne integritete TALUM d.d. Kidričevo

1. del
I. UVODNE DOLOČBE

1. člen
(namen pravilnika)

Namen pravilnika je zagotoviti skladnost poslovanja družbe in ravnanja zaposlenih v družbi v skladu z zakonodajo, veljavnimi standardi, sprejetimi smernicami in priporočili ter z internimi pravili, predpisi in navodili družbe ter organov družbe. Pri poslovanju, družbo in zaposlene v družbi zavezujejo tudi dobri poslovni običaji ter etična načela kot izhajajo iz Etičnega kodeksa SKUPINE TALUM.

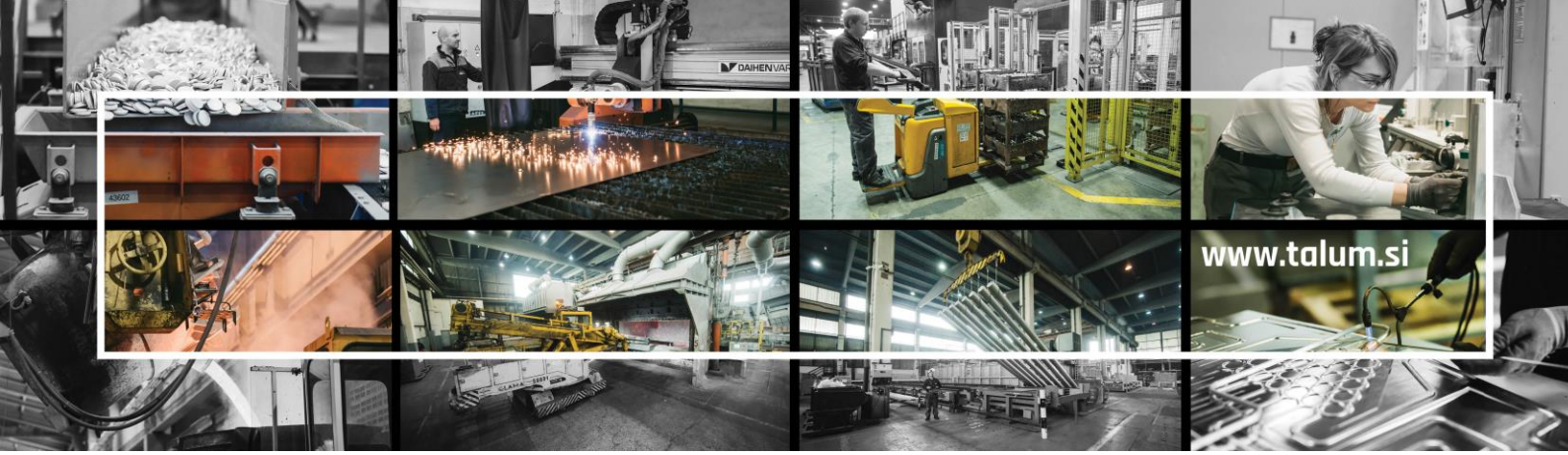
Pravilnik zavezuje k spoštovanju korporativne integritete s ciljem splošnega izboljšanja poslovnih rezultatov in krepitve družbene odgovornosti. Organi vodenja (v nadaljevanju: poslovodstvo / uprava) in organi nadzora (v nadaljevanju: nadzorni svet družbe), bodo v strateških in operativnih dokumentih ter pri svojem vsakodnevnem delu, jasno izkazovali lastno zavezo k spoštovanju korporativne integritete in etičnosti v vseh pogojih delovanja družbe.

Poslovodstvo družbe si bo prizadevalo za pozitivno motivacijo vseh zaposlenih k ravnanju, ki bo omogočalo izboljšave v sistemu korporativne integritete, vključno s primerno obravnavo utemeljenih prijav kršitev korporativne integritete.

2. člen
(uporaba pravilnika)

Ta pravilnik velja in zavezuje vse zaposlene pri opravljanju delovnih nalog v okviru in v zvezi z njihovo zaposlitvijo v družbi.

Vsi zaposleni so dolžni ravnati v skladu z zakonom, drugimi veljavnimi pravili, sprejetimi priporočili, smernicami in standardi, dobrimi poslovnimi običaji, Etičnim kodeksom in vrednotami družbe ter si prizadevati za gospodarno ravnanje s premoženjem družbe, za uspešno poslovanje in delovanje družbe.



Pravilnik določa ukrepe za spoštovanje korporativne integritete, postopek obravnavanja prijav kršitev korporativne integritete ter obveznosti poročanja in obveščanja na področju korporativne integritete.

3. člen
(poslovni partnerji)

Poslovodstvo se zavzema in pričakuje izvajanje korporativne integritete tudi od poslovnih partnerjev.

II. SPLOŠNE DOLOČBE

4. člen
(dolžnost seznanjanja in izobraževanja zaposlenih)

Poslovodstvo družbe je dolžno zagotoviti obveščenost in seznanjenost zaposlenih s tem pravilnikom in izvajanje njihovega dela v skladu s pravilnikom. Zaposlene je potrebno ob nastopu zaposlitve in redno ves čas trajanja zaposlitve, z objavami na intranetni strani ter v glasilih družbe, z obravnavo na sejah in/ali ob izvajanju drugih aktivnosti delavskih predstavništev v družbi ipd., redno seznanjati z dejavniki tveganja korporativne integritete.

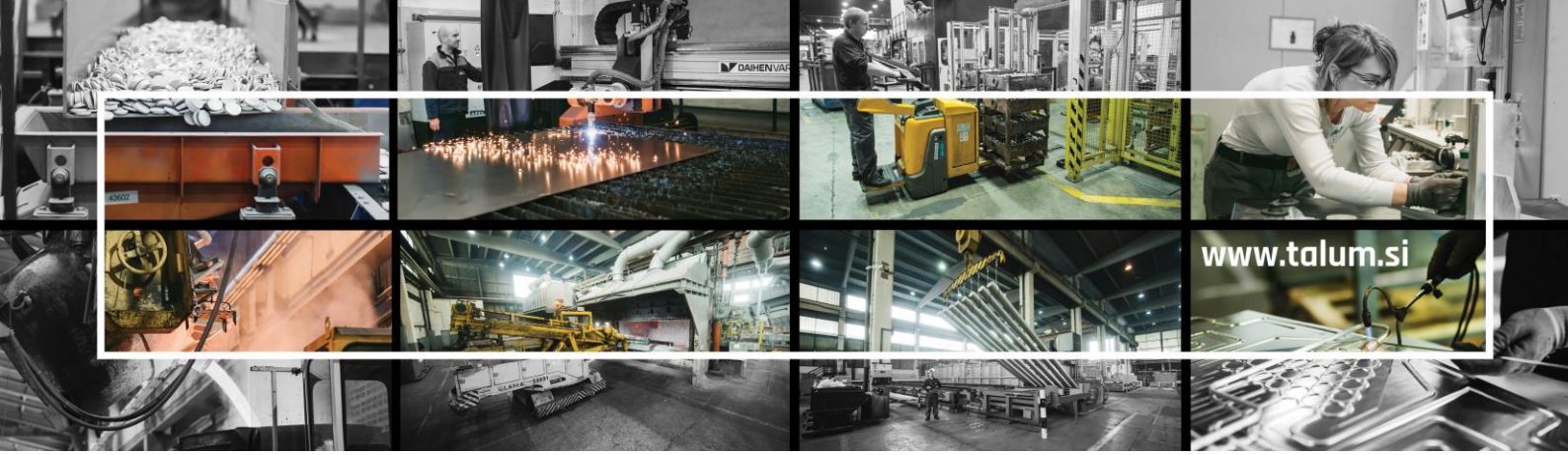
Družba bo zagotavljala izobraževanje zaposlenih o korporativni integriteti, posebej usmerjeno pa za tiste posameznike, ki opravljajo delo, potencialno bolj izpostavljeno tveganjem za korporativno integriteto.

Zaposlenim bo zagotovljena možnost obveščanja nadrejenih, pristojnih strokovnih služb in delavcev za upravljanje korporativne integritete ter poslovodstva, o kršitvah korporativne integritete ter podajanje predlogov in ukrepov za identifikacijo, obvladovanje tveganj in izboljševanje obvladovanja tveganj korporativne integritete.

5. člen
(dolžnost izogibanja nasprotju interesov in neprimernih ponudb)

Nasprotje interesov so okoliščine, v katerih zasebni interes zaposlenega vpliva ali ustvarja videz, da vpliva na nepristransko in objektivno opravljanje nalog v okviru njegove zaposlitve. Zasebni interes pomeni premoženjsko ali nepremoženjsko korist za zaposlenega, za njegove družinske člane in za druge fizične ali pravne osebe, s katerimi ima ali je zaposleni imel osebne, poslovne ali politične stike.

Zaposleni morajo biti pozorni na vsako dejansko ali možno nasprotje interesov in morajo storiti vse, da se mu izognejo. O podanem nasprotju interesov je zaposleni dolžan obvestiti neposredno nadrejenega delavca, ki je v tem primeru dolžan sprejeti ukrepe za zagotovitev zakonitega in nepristranskega izvajanje delovnih nalog.



O nasprotju interesov in sprejetih ukrepih je nadrejeni delavec dolžan nemudoma obvesti pristojno službo za upravljanje korporativne integritete.

Zaposleni pravic, obveznosti, odgovornosti in pristojnosti iz svoje zaposlitve ne smejo izvajati tako, da bi sebi ali komu drugemu uresničili nedovoljen zasebni interes. O neprimerni ponudbi je zaposleni dolžan nemudoma obvestiti pristojno službo za upravljanje korporativne integritete. Za neprimerno ponudbo se štejejo ravnanja ponujanja, dajanja ali obljubljanja nedovoljenih koristi, z namenom vplivanja na hitrost, učinkovitost ali ekonomičnost poslovanja družbe.

6. člen
(varstvo poslovnih informacij)

Zaposleni morajo skrbno varovati poslovne informacije družbe ter tudi vse druge informacije družbe s katerimi razpolagajo. S podatki morajo ravnati v skladu z zakonodajo in internimi akti družbe, tako, da ne more priti do zlorabe ali namernega izkrivljanja interpretacije podatkov. Podatkov, pridobljenih v okviru zaposlitve v družbi, zaposleni ne smejo uporabiti za to, da bi sebi ali komu drugemu pridobili kakšno premoženjsko ali nepremoženjsko korist.

Za nepooblaščeno razkrivanje poslovnih informacij družbe so zaposleni disciplinsko, kazensko in odškodninsko odgovorni.

7. člen
(prepoved in omejitve sprejemanja daril)

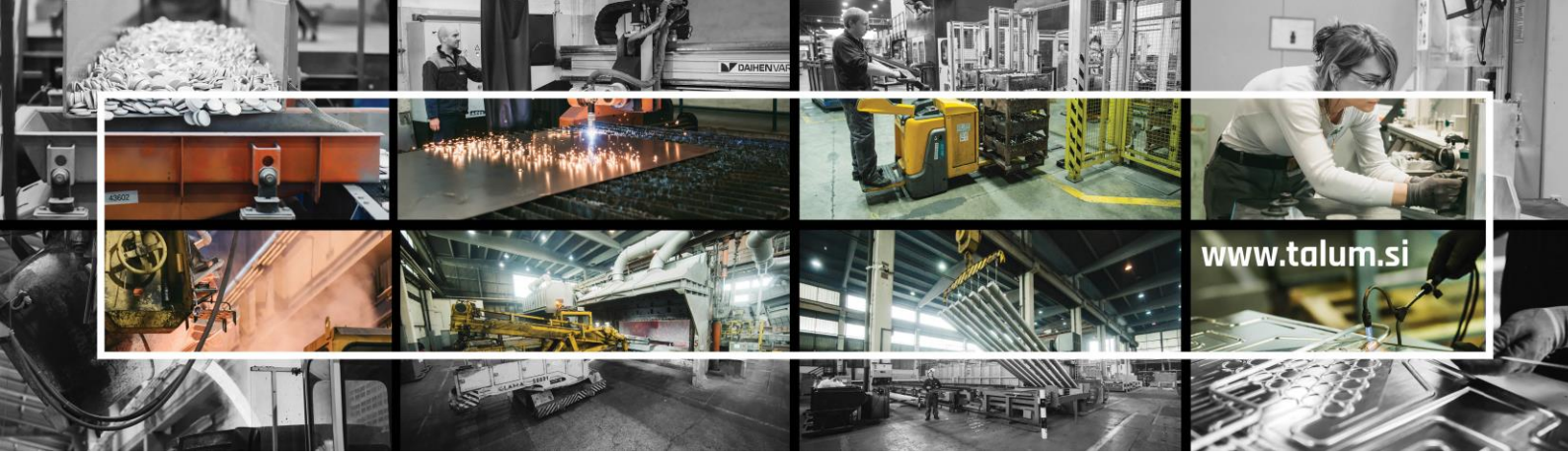
Zaposleni družbe ne smejo sprejemati daril ali drugih koristi, razen priložnostnih daril manjše vrednosti.

Priložnostna darila manjše vrednosti so darila, dana ob posebnih priložnostih, ki ne presegajo vrednosti 40 evrov in katerih skupna vrednost v posameznem koledarskem letu ne presega 100 evrov, če so prejeta od iste osebe. V nobenem primeru se kot darilo manjše vrednosti ne sme sprejeti denarja, vrednostnih papirjev ali dragocenih kovin. Sprejeta darila ne smejo vplivati na objektivnost ali nepristranskost opravljanja nalog v okviru zaposlitve. Zaposleni mora v zvezi z darili ravnati skladno z veljavnimi predpisi, ki urejajo to področje.

Darila, ki presegajo vrednost manjše vrednosti iz prejšnjega odstavka, mora zaposleni odkloniti s pojasnilom o politiki družbe do prejemanja daril.

8. člen
(prepoved dajanja daril)

Zaposleni v družbi, ne glede na položaj oz. funkcijo ali hierarhični nivo, ne smejo dajati daril ali denarja predstavnikom ali zastopnikom poslovnih partnerjev ali uradnim osebam ali zastopnikom katerihkoli



drugih oblik organiziranosti, z namenom vplivanja na njihovo razmerje do družbe. Dovoljena so darila simbolne vrednosti poslovnim partnerjem, če to ni v nasprotju z zakonodajo ali poslovnimi običaji.

9. člen
(sponzorstva in donacije)

Donacije so plačila v denarni ali materialni obliki v korist družb na področju izobraževanja, zdravja, kulture, športa in podpora nevladnim organizacijam ter se izvajajo brez pričakovane poslovne koristi vendar s pozitivnim učinkom v družbenem okolju. Sponzorstva so plačila v denarni ali materialni obliki v zameno katerih družba prejme pravice ali koristi, kot so promocija imena , izdelkov in storitev. Sponzorstva morajo odražati vrednote skupine in prispevati k krepitvi blagovne znamke ter ustvarjati ponos med zaposlenimi. Ker obstajajo tveganja prikritega podkupovanja, se morajo postopki odobravanja donacij in sponzorstev voditi transparentno in o njih poročati na letni ravni.

III. NAROČILA, IZVAJANJE INVESTICIJ IN IZVAJANJE POGODB

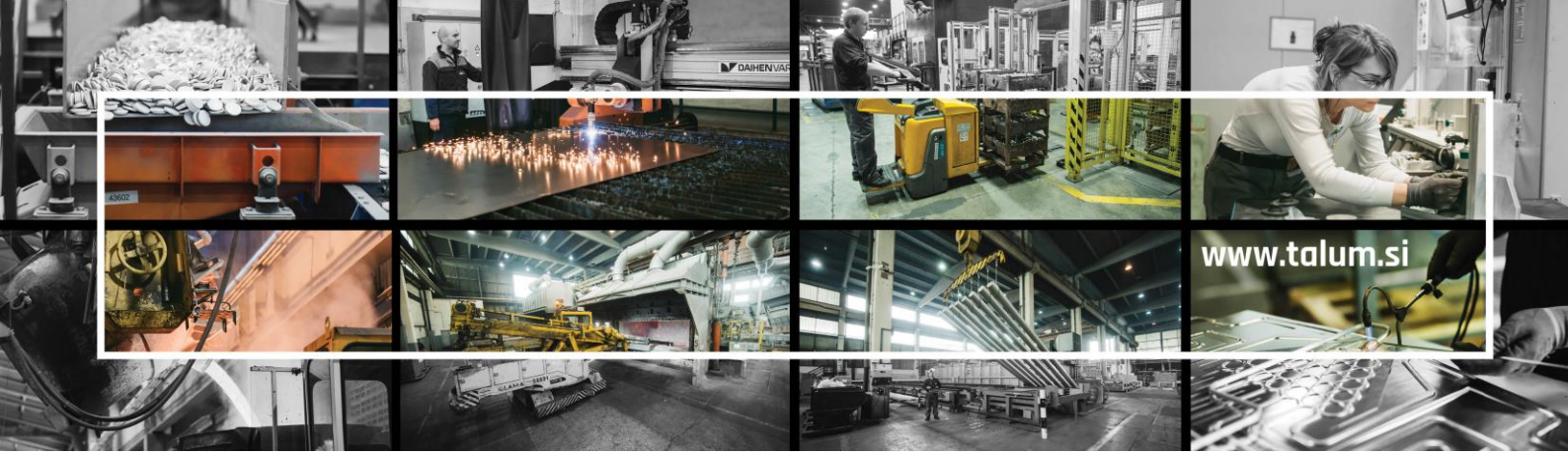
10. člen
(organizacijski predpisi družbe)

Naročanje, izvajanje investicij, sklepanje pogodb, likvidacijo računov in arhiviranje dokumentacije, urejajo in predpisujejo organizacijski predpisi (OP) in navodila za delo (ND).

11. člen
(protikorupcijska klavzula)

V vseh pogodbah s področja nabave, prodaje in/ali investicij v vrednosti nad 10.000 EUR (brez DDV), ki jih sklepa družba, se obvezno navaja in je v uporabi protikorupcijska klavzula, ki glasi: »pogodbeni stranki se zavežeta, da ne bosta obljubili, ponudili ali dali in sta seznanjeni, da ni dovoljen sprejem kakršnekoli nedovoljene koristi (npr.: darilo, plačila v denarju ali kakem drugem dragocenem predmetu, posredno ali neposredno ipd.) za namen pridobiti posel ali skleniti posel pod ugodnejšimi pogoji, za opustitev dolžnega nadzora nad izvajanjem pogodbenih obveznosti ali za drugo ravnanje ali opustitev, zaradi česar družbi nastane škoda ali je omogočena pridobitev nedovoljene koristi zaposlenemu, pogodbeni stranki ali tretji osebi.«

Protikorupcijsko klavzulo iz prvega odstavka morajo vsebovati tudi vse pogodbe med podizvajalci in izvajalci s katerimi je družba sklenila pogodbo s področja nabave, prodaje in/ali investicij.



12. člen
(omejitev poslovanja)

Zaposleni, ki opravljajo delo na področju nabave, prodaje in/ali izvajanja investicij, so pri delu dolžni ravnati s povečano skrbnostjo, t.j. s skrbnostjo dobrega strokovnjaka ter v razmerjih s poslovnimi partnerji dosledno upoštevati konkurenčno prepoved in prepoved sodelovanja v poslih s poslovnimi partnerji, ki smiselno po določbah Zakona o davku od dohodkov pravnih oseb, štejejo za povezane osebe, katerih skupna letna vrednost presega 12.000 EUR.

13. člen
(analiziranje)

Strokovna služba Strateška komerciala je zadolžena za analiziranje postopkov naročanja in pripravo 3-mesečnih in letnih poročil o stanju naročil.

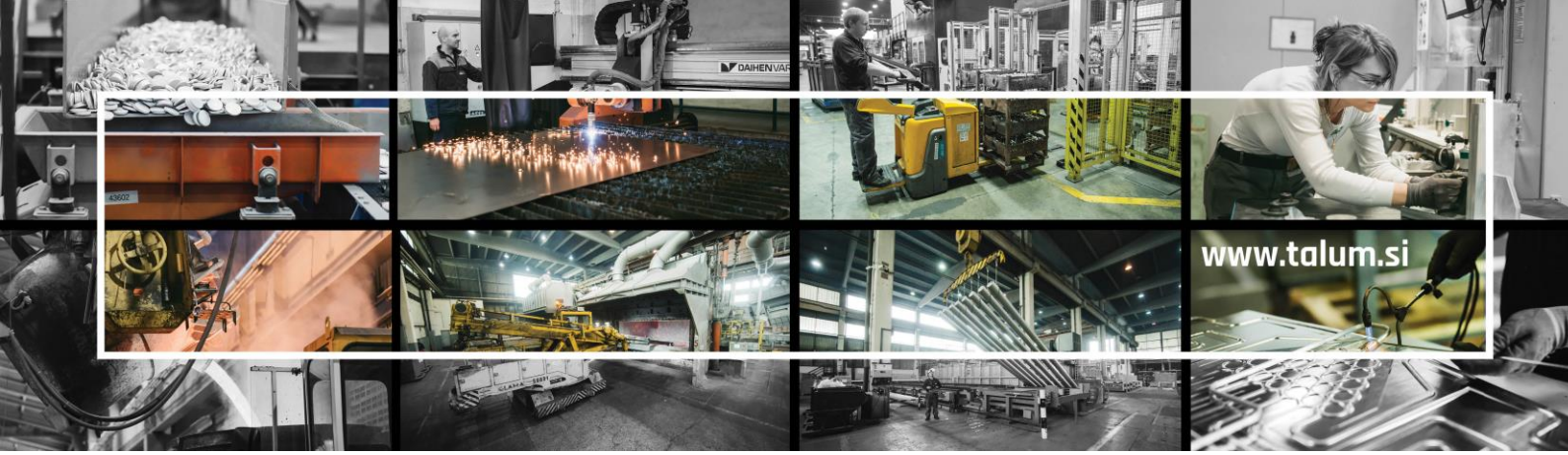
3-mesečno poročilo vsebuje vrednostne in številčne podatke o izdanih naročilnicah in tipskih pogodbah po področjih, zaključenih postopkih naročanja in/oz. sklenjenih pogodbah, reklamacijah in odstopih/odpovedih sklenjenih pogodb oz. pogodbenih razmerij.

V letnem poročilu je izvedena analiza naročil in primerjava s predhodnimi leti. Letno poročilo vsebuje vrednostne in številčne podatke. Podatki v letnem poročilu so prikazani kumulativno za obravnavano leto.

14. člen
(ocenjevanje in poročanje)

Enkrat letno Strateška komerciala izvede ocenjevanje pogodbenih partnerjev v skladu z navodili za ocenjevanje pogodbenih partnerjev.

Na osnovi ocenjevanja se izdela poročilo o ocenjevanju pogodbenih partnerjev.



2. del

IV. MEHANIZMI ZA UČINKOVITO PREPOZNAVANJE IN OBVLADOVANJE TVEGANJ KORPORATIVNE INTEGRITETE

15. člen
(upravljanje s tveganji - splošno)

Obvladovanje tveganj temelji na izpolnjevanju zahtev standarda ISO 31000:2009, ki opredeljuje načela in navodila za upravljanje tveganj kot tudi na politiki družbe o obvladovanju tveganj.

Delovanje, spremljanje, razvoj sistema in nadzor upravljanja s tveganji je delovno področje strokovne službe Upravljanje tveganj in Odbora za obvladovanje tveganj. Sestava in pristojnosti Odbora za obvladovanje tveganj določa Poslovnik kakovosti in Poslovnik o delu odbora za obvladovanje tveganj.

16.člen
(pravilnost podatkov)

Zagotavljamo polno, pošteno, natančno in razumljivo razkritje podatkov v svojih rednih računovodskih poročilih, v drugih dokumentih, predloženih regulativnim organom in agencijam, ter v drugih javnih sporočilih.

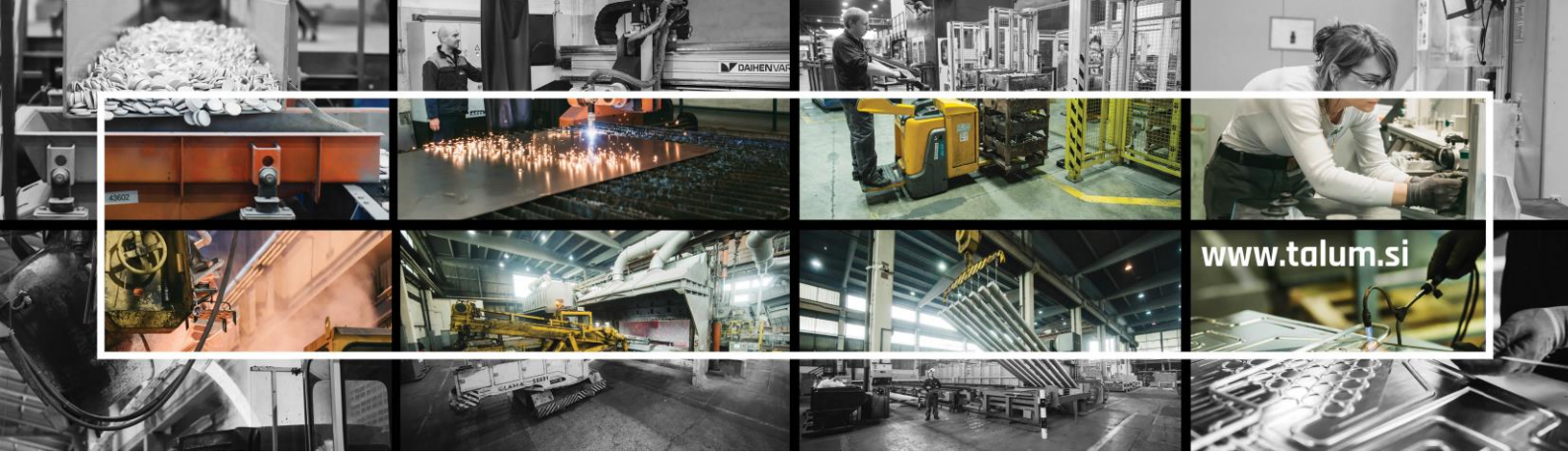
17. člen
(notranja revizija)

Družba ima vzpostavljeno notranjo revizijo.

Notranja revizija v okviru svojih pristojnosti oceni kakovost upravljanja korporativne integritete v družbi. Notranja revizija lahko uvede sistemski ali tematski nadzor. Najmanj enkrat na pet let mora notranja revizija izvesti celovito oceno kakovosti upravljanja korporativne integritete in revidirati delo strokovne službe, pristojne za upravljanje korporativne integritete.

V primeru ugotovitev pomanjkljivosti, nedelovanja ali nepravilnega delovanja mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete, lahko notranja revizija poda priporočila in/ali sprejme druge ukrepe za zagotovitev nadzora spoštovanja korporativne integritete v družbi.

Namen in naloge, načela, organiziranost ter pristojnosti in odgovornosti ter izvajanje notranje revizije, določa Pravilnik o delovanju notranje revizije.



18. člen
(mehanizem za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete)

Mehanizem za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete obsega oceno izpostavljenosti posameznih delovnih procesov in zaposlenih kršitvam korporativne integritete in korupcijskim tveganjem, identifikacijo dejavnikov tveganj za korupcijska in druga protipravna in neetična ravnanja in opredeljuje ukrepe za obvladovanje teh tveganj. Stanje korporativne integritete je potrebno vseskozi spremljati in po potrebi posodabljati, vključno z mehanizmom za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete, upoštevajoč normativne, kadrovske in organizacijske spremembe pri delovanju in poslovanju družbe.

19. člen
(strokovna služba za upravljanje korporativne integritete, samostojnost in neodvisnost)

Upravljanje korporativne integritete izvaja Služba upravljanje tveganj (v nadaljevanju: SUT).

Strokovna služba svoje naloge upravljanja korporativne integritete opravlja samostojno in neodvisno, skladno s tem pravilnikom in drugimi veljavnimi akti ter predpisi družbe.
Prepovedano je vsakršno izvajanje posrednih ali neposrednih povračilnih ukrepov proti SUT ali proti osebam, ki sodelujejo pri opravljanju nalog te službe. V primeru izvajanja kakršnihkoli povračilnih ukrepov je potrebno nemudoma obvestiti poslovodstvo, ki je dolžno zagotoviti takojšnje prenehanje izvajanja povračilnih ukrepov in ustrezno sankcioniranje odgovornih.

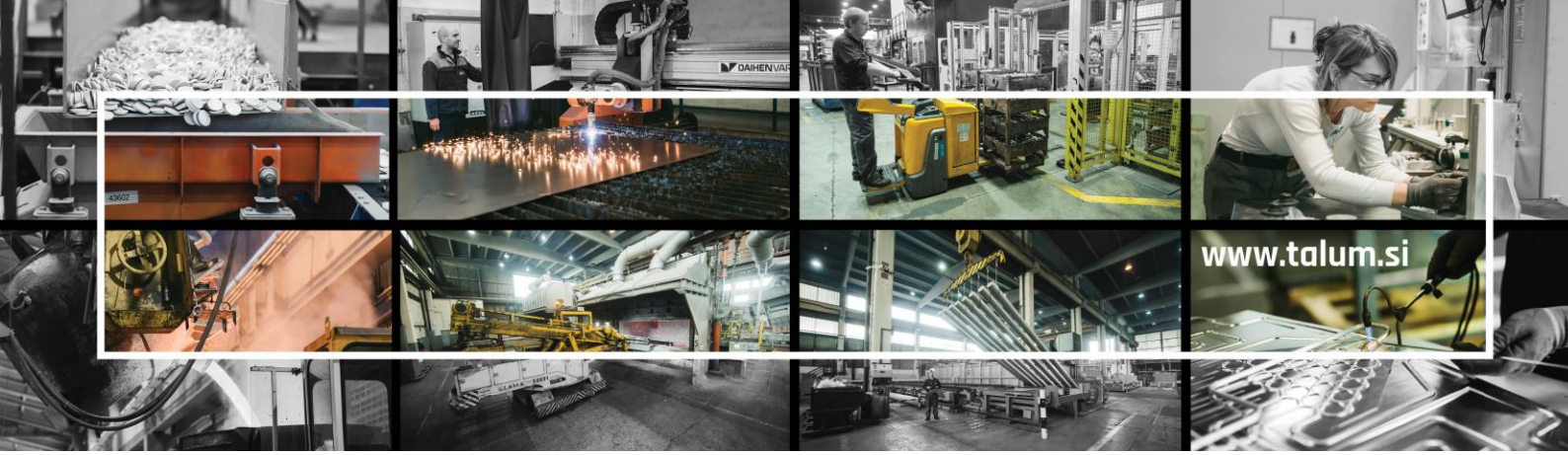
Pri upravljanju korporativne integritete uporablja SUT različne metode dela, ki so podrobneje opredeljene v mehanizmu za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete.

Službi morajo biti na voljo ustrezni prostori in materialna sredstva za nemoteno opravljanje nalog.

20. člen
(dolžnost sodelovanja pri upravljanju nalog korporativne integritete)

SUT mora biti zagotovljena ustrezna strokovna pomoč, t.j. pravica in možnost SUT, da pri upravljanju korporativne integritete sodeluje z drugimi strokovnimi službami družbe ali z zunanjimi strokovnjaki oziroma organizacijami. Strokovne službe družbe in zaposlenih v družbi so dolžni v največji možni meri sodelovati s SUT pri opravljanju nalog upravljanja korporativne integritete.

SUT ima pravico dostopa do celotne dokumentacije družbe. Zaposleni so na zahtevo SUT dolžni izročiti vso dokumentacijo, ki je last družbe ali je v zvezi s poslovanjem družbe.



21. člen
(odgovornost za izdelavo in posodabljanje mehanizma za učinkovito prepoznavanje in obvladovanje tveganj)

SUT je zadolžena za izdelavo enotnega mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete. Pri tem mora upoštevati specifične pristojnosti oziroma poslovanje posameznih organizacijskih enot, zlasti dejavnike kot so velikost, kompleksnost, število zaposlenih, specifičnost delovnih nalog, pristojnost, odgovornost, specifična tveganja ter druge dejavnike, ki zahtevajo posebno obravnavo posamezne organizacijske enote družbe.

22. člen
(delovna skupina)

Če je zaradi obsega in organizacije dela potrebno, poslovodstvo po predlogu SUT imenuje člane delovne skupine za izdelavo mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete.

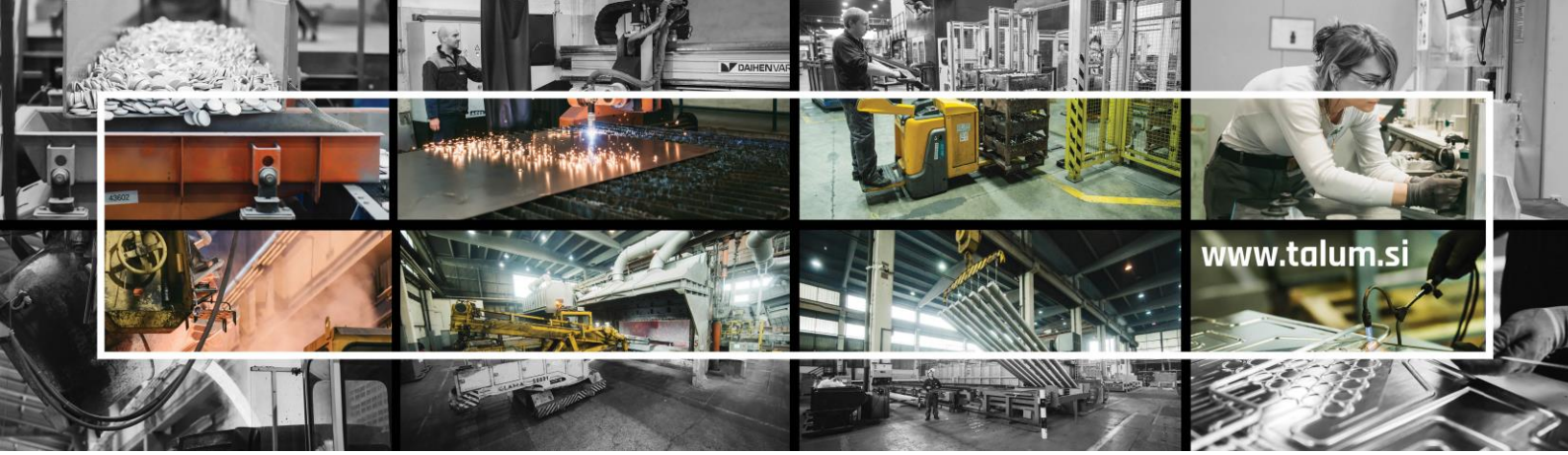
Člani delovne skupine so lahko zaposleni na različnih delovnih področjih tako, da skupaj predstavljajo vsa ključna področja delovanja družbe. V delovno skupino se ne smejo imenovati zaposleni, ki so v preteklosti na kakršenkoli način sodelovali v postopkih, za katere je bilo ugotovljeno, da so bili izvedeni v nasprotju s korporativno integriteto družbe in Etičnim kodeksom.

Po potrebi lahko v delovni skupini sodelujejo tudi posamezniki, ki niso zaposleni v družbi.

23. člen
(delovne naloge)

SUT v postopku priprave in izdelave ter izvajanja mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete:

- informira in obvešča zaposlene o začetku postopka izdelave mehanizma, o namenu in ciljih uvedbe mehanizma,
- seznanja in opozarja zaposlene o uvedbi in izvajanju mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete,
- spodbuja in motivira zaposlene k aktivnemu sodelovanju in podajanju predlogov za pridobitev informacij o dejavnikih tveganja za izdelavo mehanizma, zlasti k podajanju predlogov glede zaznavanja tveganj za korporativno integriteto in za izboljšanje stanja korporativne integritete; za dosego tega cilja se uporabljajo različne metode kot npr.: vprašalniki, intervjuji z zaposlenimi, tehnika viharjenja možganov, delo v manjših ciljno naravnanih skupinah, forumi ipd.
- objavi tudi elektronski naslov ter določi fizično lokacijo in način, kamor in kjer lahko zaposleni podajajo svoje predloge, vprašanja in opažanja,



- spodbuja zaposlene k podajanju predlogov za izboljšave in modifikacije mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete,
- podaja pojasnila glede vključitve mehanizma v delovne procese družbe,
- zbira potrebno dokumentacijo (npr. predpise družbe, poročila, analize, evidence idr.) kot vir, iz katerega se črpajo podatki in informacije o dejavnikih tveganja, za izdelavo in uvedbo mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete,
- skrbi za ozaveščanje in informiranje zaposlenih ter za svetovanje zaposlenim v zvezi s spoštovanjem korporativne integritete,
- pripravlja in izvaja ukrepe za omejevanje tveganj v zvezi s kršenjem pravil o varovanju poslovnih informacij,
- sodeluje z zunanjimi subjekti (poklicnimi organizacijami, profesionalnimi združenji, pristojnimi organi s področja integritete in preprečevanja korupcije …),
- opravlja druge naloge, ki so potrebne za pripravo in izdelavo mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete.

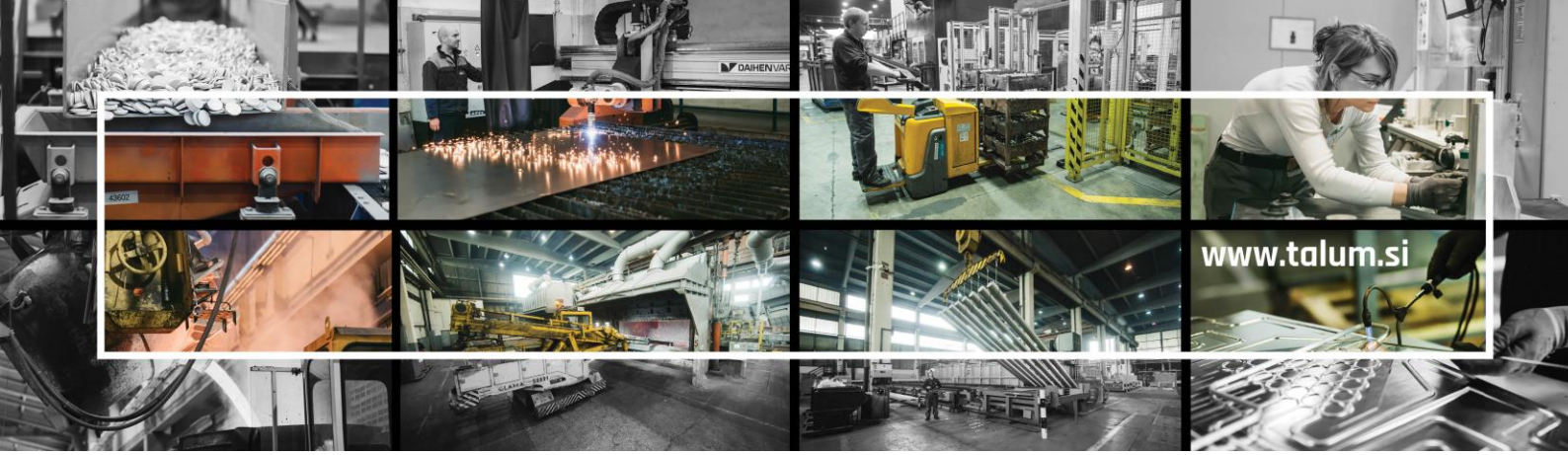
24. člen
(skupine tveganj korporativne integritete)

Mehanizem za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete mora obvezno zajeti naslednje skupine tveganj:

- skupina tveganj v zvezi s sklepanjem pogodb s področja nabave, prodaje, investicij,
- skupina tveganj v zvezi z nasprotjem interesov – v to skupino spada nasprotje interesov kot ga opredeljujejo ta pravilnik in drugi predpisi, ki urejajo institut nasprotja interesov, omejitve poslovanja, konkurenčna klavzula, konkurenčna prepoved ipd.,
- skupina tveganj v zvezi s protikorupcijsko klavzulo, spoštovanjem poslovnih skrivnosti in zaupnosti podatkov, sprejemanjem in dajanjem daril, postopki notranje revizije,
- skupina tveganj v zvezi z internimi ali zunanjimi vplivi in zahtevami - dovoljenimi in nedovoljenimi, ki bi lahko vplivali na odločitve zaposlenih pri opravljanju delovnih nalog in sprejemanju poslovnih odločitev v imenu družbe ter vplivi, ki bi lahko vplivali na osebno integriteto zaposlenih in na normativne, kadrovske, organizacijske, finančne, informacijske, nabavne postopke, postopke najema, priprave dokumentacije, sprejemanja odločitve ipd.,
- skupina tveganj v zvezi s podkupovanjem, izsiljevanjem družbe, pranjem denarja, trgovanjem z informacijami,
- skupina tveganj v zvezi z varnostjo in zdravjem pri delu, trpinčenjem na delu.

SUT preveri obstoj vzrokov oz. virov tveganj za vse skupine tveganj, v zvezi z:

- odzivanjem pri delu na zunanje okolje delovanja,
- odzivanjem pri delu na notranje okolje delovanja,
- oblikovanjem in doseganje ustreznih ciljev in ukrepov ,



- pravilnostjo procesov in pravil delovanja,
- zagotovljenostjo virov,
- določanjem in spremenljivostjo merjenja in kazalnikov,
- izvajanjem kontroliranja, nadzorovanja in usmerjanja,
- izvajanjem informiranja in poročanja,
- obvladovanjem tveganj,
- izvajanjem preverjanja, analiziranja in izboljševanja,

Obstoj tveganja za posamezno skupino tveganj je potrebno preveriti pri vseh možnih vzrokih oziroma virih tveganj.

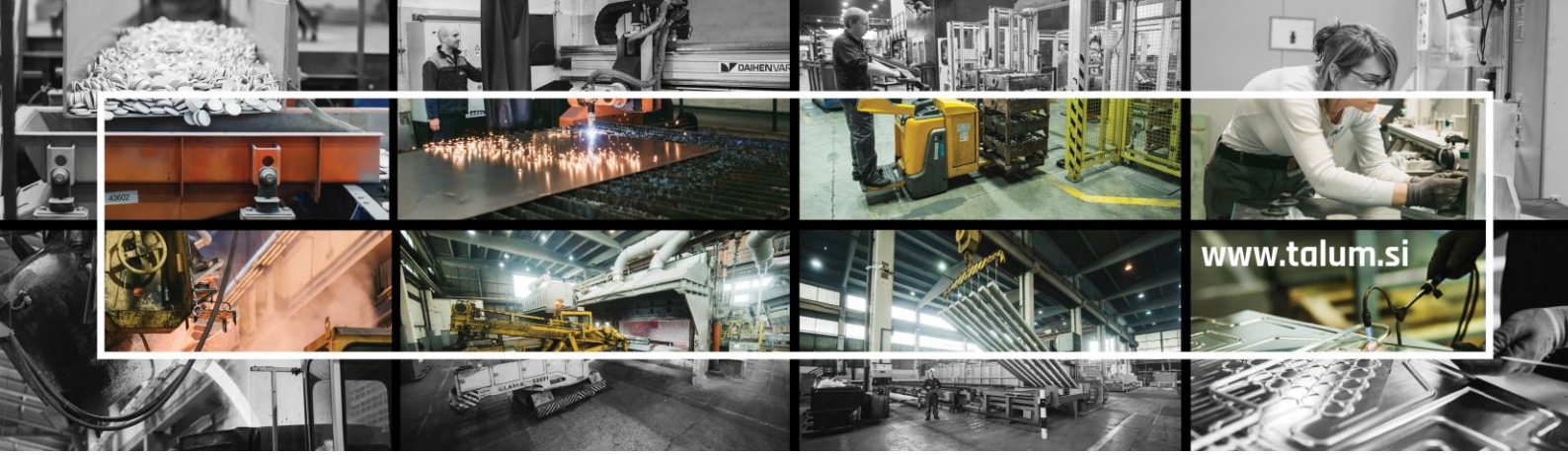
25. člen
(metode dela)

SUT pri ugotavljanju tveganj korporativne integritete uporablja različne metode dela oziroma lahko izbere katerokoli od možnih metod ali kombinacij več metod dela, glede na vrsto posamezne skupine tveganj korporativne integritete:

- sestavi ciljno usmerjene delovne skupine,
- izvede razgovore/intervjuje s sodelavci,
- izvede ankete, vprašalnike,
- uporabi metodo scenarijev za primer, da se zgodi določen dogodek,
- pregleda različna poročila in informacije iz notranjih in zunanjih virov,
- upošteva in analizira ugotovitve, usmeritve in priporočila Odbora za obvladovanje tveganj,
- analizira različne ukrepe nadzornih organov,
- analizira svoje delo na področjih, kjer ugotavlja tveganja in izkušnje glede na pretekle dogodke,
- analizira obvestila in pritožbe zaposlenih in drugih oseb,
- analizira (ne)uporabo ter dobre in slabe prakse uporabe mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete v preteklih obdobjih,
- analizira vzroke in rešitve, ki so v preteklih obdobjih že bile uveljavljene za omejevanje in preprečevanje kršitev korporativne integritete,
- spremlja oblikovanje ukrepov obvladovanja tveganj korporativne integritete,
- spremlja pomembna dogajanja v okolju, ki vplivajo na stanje korporativne integritete in predlaga posodabljanje strukture tveganj in ukrepov.

26. člen
(analiziranje tveganj korporativne integritete)

SUT analizira zaznana tveganja. Analiza vključuje preučevanje vzrokov in/oz. virov tveganja, pozitivnih in negativnih posledic, verjetnosti uresničitve tveganja ter določitev ravni tveganja.



Pri analizi se upošteva in oceni tudi že obstoječe ukrepe in kontrole, njihovo učinkovitost in uspešnost.

Pri odpravi tveganj imajo prednost tveganja z visoko stopnjo. Posebna pozornost mora biti namenjena preprečevanju podkupovanja, izsiljevanja, pranja denarja, trgovanja z informacijami in nasprotja interesov.

27. člen
(register tveganj korporativne integritete)

SUT je zadolžena za vzpostavitev registra tveganj korporativne integritete, ki obsega:

- opis tveganja,
- opredelitev vzroka oziroma vir tveganja,
- opredelitev možnih posledic, obsega škode če se tveganje uresniči,
- verjetnost tveganja,
- skupno oceno tveganja,
- predlagane izboljšave, ukrepe, priporočila, nosilce ter rok za njihovo implementacijo,
- podatke o sprejetih in implementiranih ukrepih, upoštevanju priporočil…,

Register tveganj SUT predloži poslovodstvu družbe v pregled in potrditev. Dan potrditve registra tveganj šteje za dan uvedbe mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete.

28. člen
(predstavitev mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete)

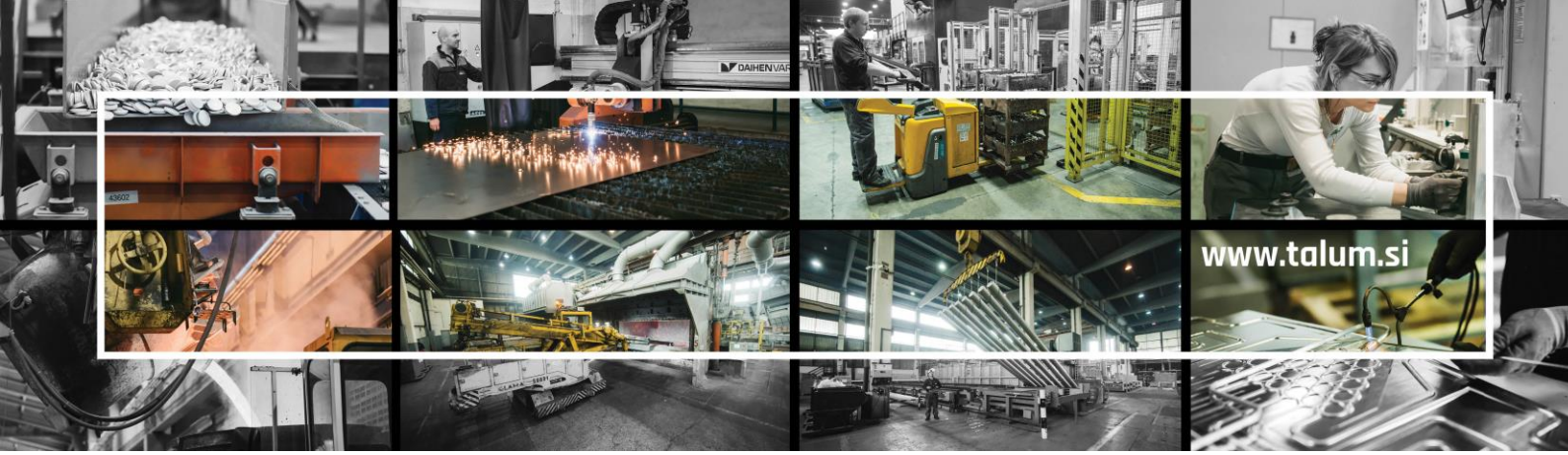
SUT zaposlene seznani z vsebino mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete.

Novo zaposlene sodelavce se z mehanizmom za učinkovito prepoznavanje in obvladovanje tveganj seznani ob nastopu zaposlitve.

29. člen
(zaposleni)

Ne glede na obliko delovnega razmerja so zaposleni oz. osebe, ki opravljajo delo v družbi, ne glede na pravno podlago svojega dela, dolžni pri opravljanju svojega dela:

- seznaniti se in se ravnati v skladu z mehanizmom za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete ter navodili SUT za spoštovanje korporativne integritete;
- seznaniti se s tveganji korporativne integritete svojega delovnega področja;
- sodelovati v procesih izobraževanja s področja korporativne integritete;



- ob zaznavi suma ali znakov korupcije, drugih protipravnih ali neetičnih ravnanj, o tem brez odlašanja obvestiti SUT;
- obveščati SUT o predlogih ukrepov za identifikacijo in obvladovanje tveganj korporativne integritete;
- sodelovati pri izvajanju in posodabljanju mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete.

30. člen
(izboljšave pri vzrokih in/oz. virih tveganj korporativne integritete)

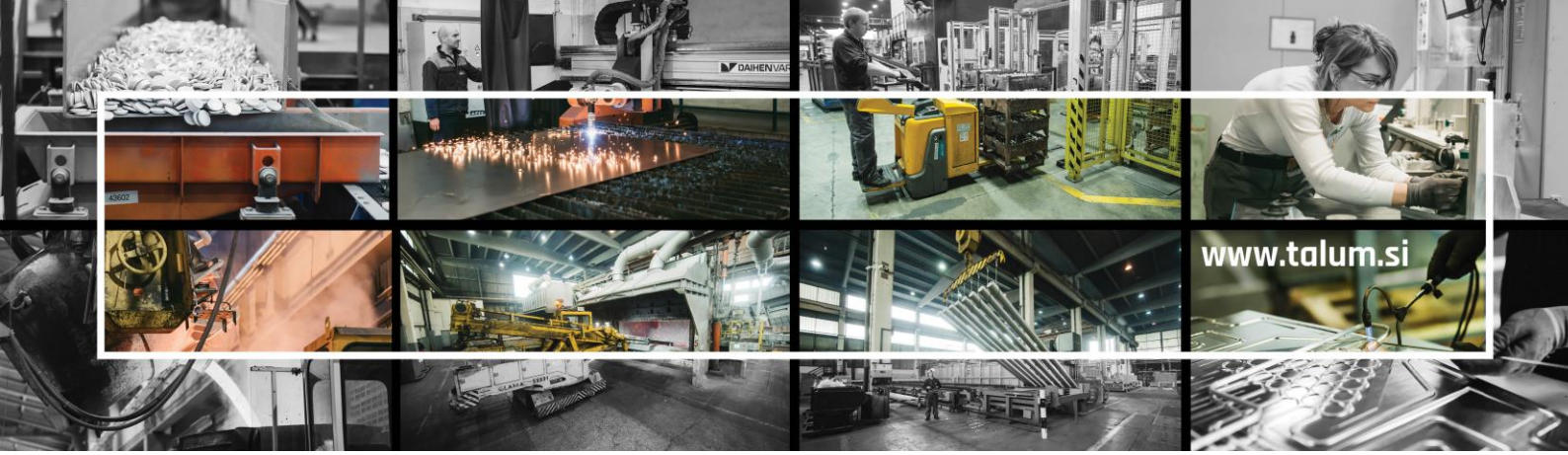
SUT predlaga izboljšave, ukrepe in poda priporočila v zvezi s/z:

- predpisi, ki se v praksi ne uporabljajo ali se ne uporabljajo dosledno ali so premalo oz. preveč obsežni,
- zaposlenimi,
- postopki izogibanja tveganju,
- odstranjevanjem in postopki odstranjevanja vira tveganja,
- spreminjanje posledic, verjetnosti tveganja,
- delovnimi procesi,
- splošnim vodenjem in upravljanjem družbe,
- finančnim poslovanjem,
- krepitvijo korporativne integritete, strokovnosti in profesionalnosti,
- drugimi vprašanji, katerih rešitve predstavljajo ukrepe za preprečevanje kršitev korporativne integritete in tveganj korupcije.

SUT pri predlaganju izboljšav, ukrepov in podajanju predlogov, upošteva stroške in trud vloženega dela v izvedbo izboljšav, ekonomsko upravičenost predlaganega ukrepa, verjetnost uresničitve tveganja in stopnjo škodljivih posledic v primeru uresničitve tveganja v primerjavi s pričakovanimi učinki izboljšave. Uporabi lahko različne možnosti obravnave, bodisi posamično ali v kombinaciji in za vsako tveganje lahko določi enega ali več ukrepov. Na podlagi mnenja uprave služba dokončno oblikuje predlagane izboljšave, ukrepe in predloge.

31. člen
(posodabljanje mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete)

SUT je zadolžena za sprotno posodabljanje in nadgrajevanje mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete. Če pride do spremenjenih okoliščin, zaradi katerih se poveča stopnja tveganja posameznih skupin tveganj ali se pojavijo oziroma odkrijejo nova tveganja oziroma skupine tveganj, je potrebno nemudoma pristopiti k posodobitvi mehanizma za učinkovito prepoznavanje



in obvladovanje tveganj. Enako je potrebno postopati v primeru spremenjenih okoliščin, ki bi lahko vplivale na že sprejete ukrepe, prioritete, roke ali nosilce.

32. člen
(usposabljanja in izobraževanja)

Zaposlenim, ki neposredno izvajajo naloge upravljanja korporativne integritete mora biti zagotovljeno ustrezno izobraževanje in usposabljanje, ki se zahteva za izvajanje teh nalog, ustrezno usposabljanje in izobraževanje pa se zagotavlja tudi drugim osebam, ki sodelujejo pri izvajanju nalog upravljanja korporativne integritete.

SUT v sodelovanju z drugim strokovnimi službami pripravi program usposabljanj in izobraževanj za korporativno integriteto za zaposlene v družbi. Po potrebi se v program vključi tudi sodelovanje z zunanjimi udeleženci (poklicnimi organizacijami, profesionalnimi združenji…).

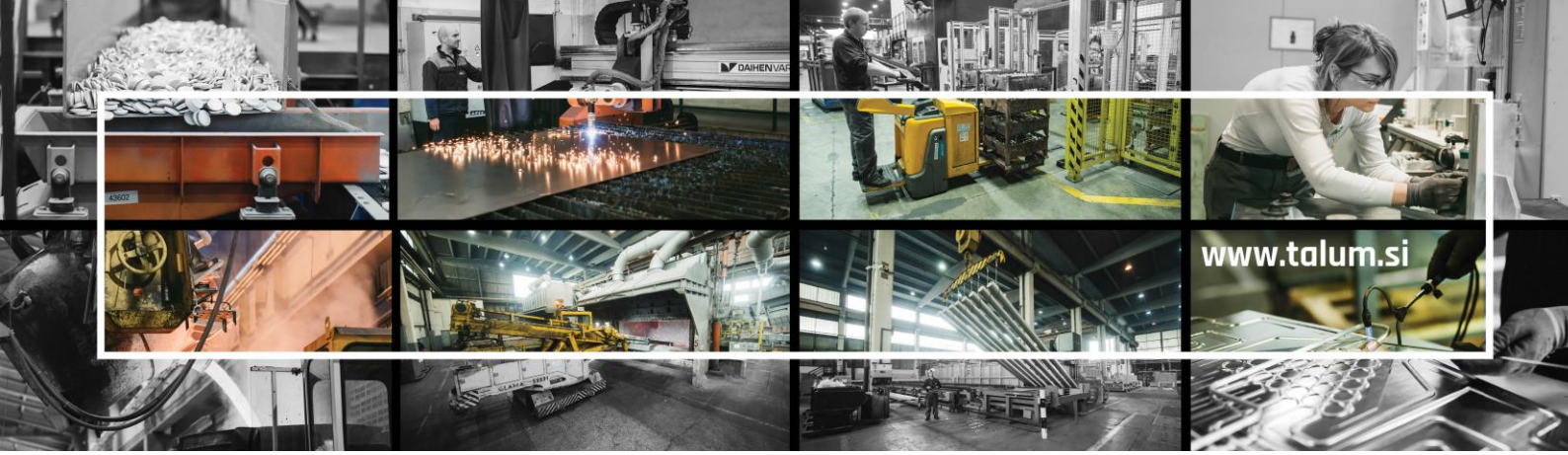
V. OBRAVNAVANJE PRIJAV KRŠITEV KORPORATIVNE INTEGRITETE TER ZAŠČITA PRIJAVITELJEV KRŠITEV KORPORATIVNE INTEGRITETE

33. člen
(prijava kršitev korporativne integritete)

Vsak zaposleni mora neposredno nadrejenemu in/ali SUT, nemudoma sporočiti vsako zaznano kršitev korporativne integritete. Nadrejeni je dolžan o vsaki prijavi obvesti SUT.

Prijavo kršitve se lahko poda v pisni ali ustni obliki. Prijavo o kršitvi je mogoče podati tudi preko elektronske pošte na naslov prijava.nepravilnosti@talum.si ali s poštno pošiljko na naslov TALUM d.d. - Služba upravljanje tveganj. Prijava se lahko poda tudi anonimno, z oddajo pisne prijave v zaprt, za ta namen določen zabojček. Lokacija zabojčka mora biti navedena na intrAnetni strani družbe, mora biti prosto dostopna in brez videonadzora tako, da je zagotovljena anonimnost.

Prijavo lahko podajo tudi druge osebe, ki zaznajo znake korupcijskega, nezakonitega oziroma neetičnega ravnanja pri poslovanju družbe ali ravnanju zaposlenih.



34. člen
(obravnava kršitev korporativne integritete)

Kršitve korporativne integritete obravnava SUT.

Obravnava se prične na podlagi prijave ali na podlagi lastne odločitve SUT kot pristojne službe za upravljanje korporativne integritete, če meni, da je podan sum kršitve korporativne integritete.

Glede na okoliščine posameznega primera lahko poslovodstvo na predlog SUT, za obravnavo prijave suma kršitve korporativne integritete imenuje delovno skupino. V delovno skupino ne smejo biti imenovane osebe, za katere je podan dvom glede njihove nepristranskosti oziroma vpletenosti v kršitev.

SUT se je na podano prijavo dolžna odzvati nemudoma oziroma najkasneje v roku 7 delovnih dni od prejema prijave.

V postopku obravnave suma kršitve korporativne integritete si mora SUT prizadevati za vsestransko razjasnitev podanega suma kršitve. Zaposlenim, domnevno vpletenim v kršitev je potrebno omogočiti zagovor, po potrebi pa tudi ostalim osebam, ki so na kakršen koli način povezane z domnevno kršitvijo. Vsi zaposleni morajo v polni meri sodelovati s SUT, da se razjasnijo vse okoliščine primera domnevne kršitve in da se zagotovi spoštovanje korporativne integritete pri poslovanju in delovanju družbe.

35. člen
(zapisnik o postopku obravnave kršitve)

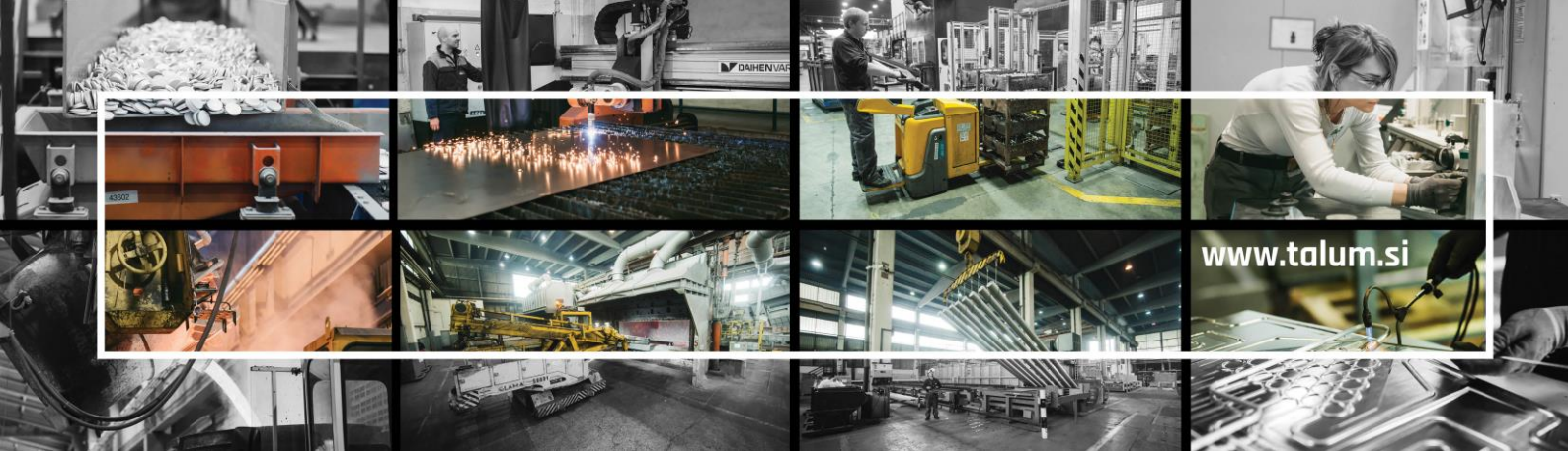
O postopku obravnave kršitve je potrebno voditi zapisnik. V zapisnik je potrebno vnesti vse bistvene okoliščine, ki so bile ugotovljene v postopku, zlasti pa:

- opis domnevne kršitve,
- osebe, ki so sodelovale v postopku,
- osebe, ki so podale izjavo ter vsebino izjave,
- potek postopka ugotavljanja dejstev in okoliščin,
- ugotovitev o obstoju in obsegu kršitve,
- sprejeti ukrepi.

Zapisnik podpiše zaposleni v SUT, ki je vodil postopek obravnave in oseba, ki je podala izjavo.

36. člen
(zaključek postopka)

SUT obravnavo prijave zaključi s sklepom o ustavitvi postopka, če ugotovi, da sum kršitev korporativne integritete ni utemeljen.



Če je sum kršitve korporativne integritete utemeljen, SUT razišče dejansko stanje in sprejme potrebne ukrepe za odpravo kršitve in preprečitev nastanka škodljivih posledic tako, da s sklepom
- poda priporočila za odpravo ugotovljenih nepravilnosti in/ali
- poda predloge za izboljšanje stanja korporativne integritete in/ali

naloži dolžnost poročanja vodstvenih delavcev o izvrševanju priporočil in stanju korporativne integritete,
- lahko predlaga nadaljnje postopanje zoper odgovorne osebe oz. kršitelje.

O sprejeti odločitvi SUT obvesti prijavitelja, če je ta poznan in poslovodstvo družbe. Prijavitelj ali poslovodstvo lahko tudi med postopkom zahteva pojasnila o poteku postopka in sprejetih ukrepih.

Če prijavljena ravnanja vsebujejo znake kaznivega dejanja, ki se preganja po uradni dolžnosti, je družba dolžna o tem obvestiti organe odkrivanja in pregona kaznivih dejanj.

37. člen
(spremljanje kršitev)

SUT posebno pozornost nameni nadzoru delovnih procesov, kjer so bile ugotovljene kršitve korporativne integritete. Od vodstvenih delavcev lahko zahteva poročilo o izvrševanju sprejetih ukrepov in stanju korporativne integritete ali določi druge ukrepe za zagotovitev spoštovanja korporativne integritete.

38. člen
(evidenca o kršitvah)

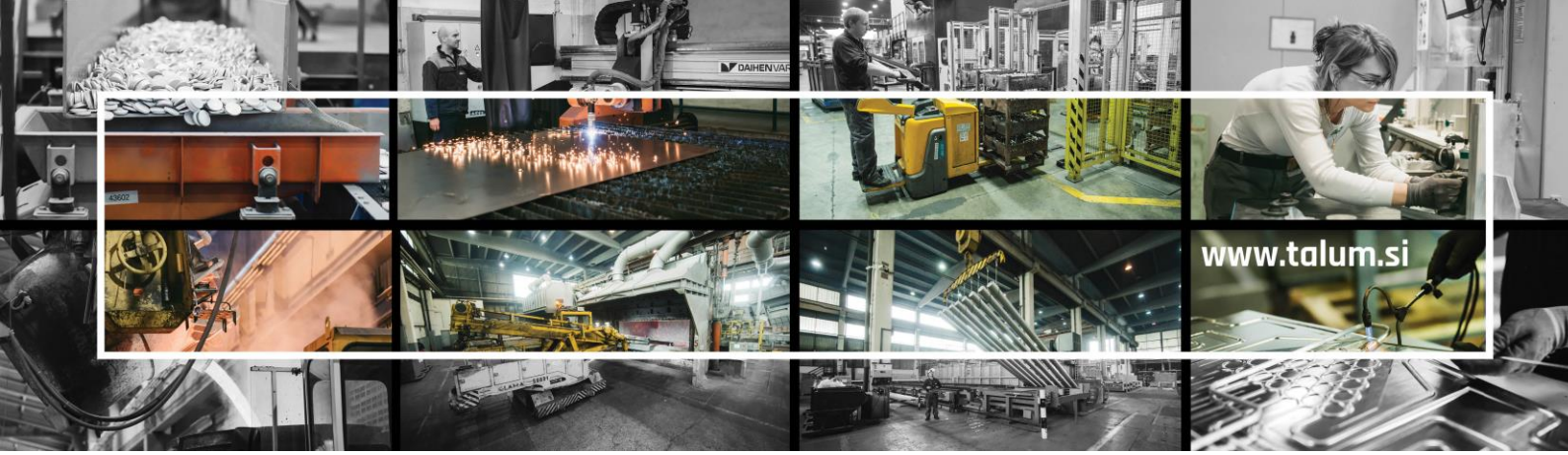
SUT vodi evidenco o vseh postopkih obravnav kršitev.

Evidenca obsega vso dokumentacijo, ki je bila zbrana tekom postopka, zlasti pa prijavo kršitve, zapisnik in sklep. Vsa dokumentacija izvedenih postopkov se arhivira.

39. člen
(zaščita prijavitelja)

Vsak dobroverni prijavitelj je upravičen do zaščite pred povračilnimi ukrepi zaradi prijave suma kršitve. Prijavitelj je v dobri veri, če v konkretnem primeru obstaja sum kršitve korporativne integritete.

SUT mora varovati identiteto dobrovernega prijavitelja in s podatki o prijavitelju ravnati zaupno. V primeru anonimne prijave identitete dobrovernega anonimnega prijavitelja ni dovoljeno ugotavljati. Identiteta prijavitelja se lahko razkrije le na podlagi sodne odločbe sodišča in/ali, če je to nujno potrebno zaradi zavarovanja javnega interesa.



SUT mora zagotoviti varstvo prijavitelja pred povračilnimi ukrepi. Zaposleni so dolžni obvestiti SUT o izvajanju povračilnih ukrepov zoper prijavitelja, ki jih zaznajo. lahko pa obvestilo poda tudi prijavitelj. Zaposlenega, ki izvaja povračilne ukrepe, je potrebno pozvati k takojšnjemu prenehanje izvajanja povračilnih ukrepov. Zoper zaposlenega, ki kljub pozivu nadaljuje s povračilnimi ukrepi, se lahko uvede disciplinski postopek.

O povračilnih ukrepih in sprejetih ukrepih za preprečitev nadaljevanje nedovoljenega ravnanja je SUT dolžna obvestiti poslovodstvo družbe.

VI. OBVEZNOST POROČANJA IN INTERNEGA OBVEŠČANJA O STANJU KORPORATIVNE INTEGRITETE

40. člen
(poročanje o stanju korporativne integritete)

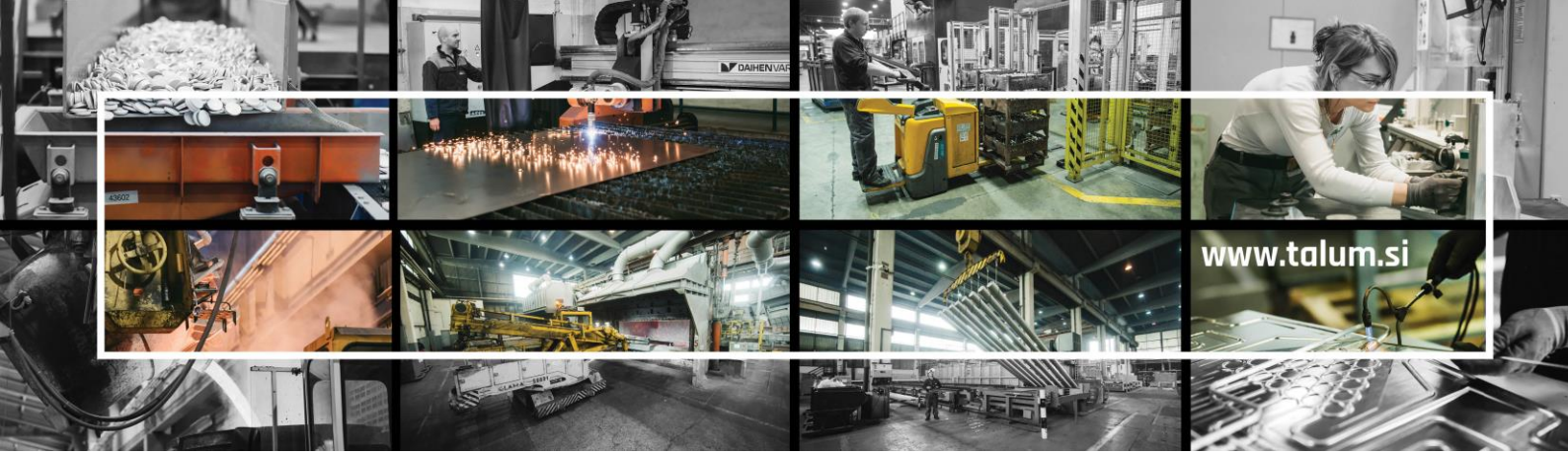
SUT je dolžna poročati o stanju korporativne integritete, rezultatih, učinkih izboljšav ter o načrtovanih posodobitvah mehanizma za učinkovito prepoznavanje in obvladovanje tveganj korporativne integritete. SUT poroča poslovodstvu vsakih šest mesecev, po lastni presoji pa lahko poroča tudi na sejah delovnih odborov družbe. Enkrat letno SUT o stanju korporativne integritete poroča nadzornemu svetu družbe.

41. člen
(letno poročilo)

Letno poročilo o stanju korporativne integritete zajema:

- številu zaznanih in obravnavanih tveganj za korporativno integriteto
- številu in vrsti uporabljenih ukrepov
- spremembah in dopolnitvah mehanizma za učinkovito prepoznavanje in obvladovanje tveganj
- številu novo identificiranih tveganj korporativne integritete in sprejetih ukrepov v minulem obdobju od zadnjega poročanja
- številu in vrsti tveganj ter ukrepov iz mehanizma za učinkovito prepoznavanje in obvladovanje tveganj, ki so jih zaznali oziroma izvedli zaposleni sami v okviru opravljanja svojih delovnih obveznosti
- predlaganih spremembah, dopolnitvah in ukrepih mehanizma za učinkovito prepoznavanje in obvladovanje tveganj.

Poročilo o stanju, napredku in predlaganih ukrepih na področju korporativne integritete je sestavni del poslovnega poročila.



VII. KONČNA DOLOČBA

42. člen
(prenehanje veljavnosti)

Z dnem začetka veljavnosti tega pravilnika prenehajo veljati Pravila za preprečevanje koruptivnih dejanj v SKUPINI TALUM in preneha mandat Komisije, imenovanje na podlagi in v skladu s citiranimi pravili.

43. člen
(Skupina Talum)

Direktorji družb, vključenih v koncern Skupina Talum (družbe v katerih ima TALUM d.d. Kidričevo, t.j. obvladujoča družba, večinski poslovni delež), s podpisom tega akta sprejmejo Pravilnik korporativne integritete TALUM d.d. Kidričevo kot splošni akt posamezne odvisne družbe, ki jo zastopajo.

Kidričevo, 4. marec 2019