



REPUBLIKA HRVATSKA
HRVATSKA AGENCIJA ZA NADZOR
FINANCIJSKIH USLUGA

Na temelju članka 74. stavka 1. Zakona o mirovinskim osiguravajućim društvima (»Narodne novine« broj 22/14, 29/18, 115/18 i 156/23), Hrvatska agencija za nadzor financijskih usluga na sjednici Upravnog vijeća održanoj 10. prosinca 2024. godine donosi

**PRAVILNIK O ORGANIZACIJSKIM ZAHTJEVIMA MIROVINSKOG OSIGURAVAJUĆEG
DRUŠTVA**

Uvodne odredbe

Članak 1.

Ovim Pravilnikom Hrvatska agencija za nadzor financijskih usluga (dalje u tekstu: Hanfa) detaljnije propisuje organizacijske zahtjeve koje mirovinsko osiguravajuće društvo treba ispunjavati s obzirom na:

1. opće organizacijske uvjete,
2. sustav upravljanja rizicima,
3. unutarnju reviziju,
4. praćenje usklađenosti s relevantnim propisima,
5. aktuarsku funkciju,
6. sukob interesa,
7. mjere za neprekidno poslovanje,
8. politike primitaka,
9. vođenje i čuvanje poslovne dokumentacije mirovinskog osiguravajućeg društva,
10. primjereno upravljanje informacijskim sustavom uključujući i kibernetičke rizike i način upravljanja istima.

Opći organizacijski uvjeti

Članak 2.

(1) Uzimajući u obzir vrstu, opseg i složenost poslovanja, mirovinsko osiguravajuće društvo dužno je:

1. ustrojiti takvu unutarnju organizacijsku strukturu kojom se osigurava pravilno obavljanje djelatnosti mirovinskog osiguravajućeg društva u skladu s odredbama Zakona o mirovinskim osiguravajućim društvima (»Narodne novine« broj 22/14, 29/2018, 115/2018 i 156/2023 dalje u tekstu: Zakon) i propisima donesenim na temelju Zakona kao i s drugim relevantnim propisima te internim odlukama, procedurama i postupcima na svim razinama mirovinskog osiguravajućeg društva,
2. ustrojiti takvu unutarnju organizacijsku strukturu kojom se osigurava neovisno obavljanje poslova upravljanja imovinom za pokriće tehničkih pričuva, na način da se poslovi podijele između najmanje sljedećih osoba i/ili jedinica i to:
 - a. front office (osobu i/ili operativnu jedinicu),
 - b. middle office (osobu i/ili jedinicu za kontrolu) i
 - c. back office (osobu i/ili jedinicu za potporu).



3. propisati, primjenjivati i redovito ažurirati interne akte kojima se uređuje unutarnja organizacijska shema mirovinskog osiguravajućeg društva i postupak donošenja odluka, iz kojih je na jasan i dokumentiran način vidljiv postupak donošenja odluka i raspodjela odgovornosti za te odluke, a koji obuhvaćaju:

- organizacijsku shemu mirovinskog osiguravajućeg društva,
- detaljan opis zaduženja i odgovornosti pojedine organizacijske jedinice,
- popis radnih mjesta i radnika unutar pojedine organizacijske jedinice,
- zaduženja i podjelu ovlasti radnika mirovinskog osiguravajućeg društva,
- postupak internog izvještavanja i donošenja odluka unutar mirovinskog osiguravajućeg društva,
- način čuvanja poslovne dokumentacije i podataka,

4. osigurati da sve relevantne osobe budu upoznate sa svim procedurama i postupcima koje su dužne primjenjivati u svrhu pravilnog obavljanja svojih dužnosti, a kada obavljaju više dužnosti u mirovinskom osiguravajućem društvu, osigurati da svaku od njih obavljaju neovisno, savjesno i profesionalno,

5. usvojiti politike kojima se propisuje zapošljavanje osobe s kvalifikacijama, znanjima i iskustvom potrebnim za obavljanje povjerenih im dužnosti,

6. usvojiti procedure za internu provjeru provedbe i funkcioniranja cjelokupne organizacije poslovanja društva.

(2) Mirovinsko osiguravajuće društvo dužno je redovito pratiti i ažurirati, unaprijediti i otklanjati nedostatke sustava poslovanja iz stavka 1. ovoga članka.

(3) Funkcija upravljanja rizicima, funkcija praćenja usklađenosti, funkcija unutarnje revizije i aktuarska funkcija iz članka 49. a. stavka 1. Zakona moraju biti hijerarhijski i funkcionalno neovisne, osim u slučajevima kada mirovinsko osiguravajuće društvo može dokazati:

1. da navedene obveze nisu razmjerne vrsti, opsegu i složenosti poslovanja mirovinskog osiguravajućeg društva,
2. da su osigurane primjerene mjere sprječavanja sukoba interesa koje omogućavaju uredno i neovisno ispunjavanje obveza pojedinih funkcija,
3. da pojedine funkcije ispunjavaju zahtjeve iz Zakona i ovoga Pravilnika.

(4) Mirovinsko osiguravajuće društvo odgovorno je za obavljanje poslova pojedinih funkcija iz članka 49. a. stavka 1. Zakona i u slučaju kada je ta funkcija izdvojena na treću osobu.

(5) Mirovinsko osiguravajuće društvo dužno je propisati i osigurati da više rukovodstvo, dakle radnik na radnom mjestu koje prema organizaciji društva pripada višem rukovodstvu, u svakom trenutku ispunjava uvjete stručnosti odnosno posjeduje odgovarajuće stručne kvalifikacije, znanje i iskustvo potrebno za ispunjavanje obveza iz svoje nadležnosti, kao i uvjete primjerenosti, odnosno ima dobar ugled i integritet i nije u sukobu interesa u odnosu na društvo, dioničare, druge članove nadzornog odbora, nositelje ključnih funkcija i više rukovodstvo društva.

(6) Mirovinsko osiguravajuće društvo je dužno organizacijski se ustrojiti na način kojim se rizik od zloporabe imovine za pokriće tehničkih pričuva, prijevare, neadekvatnog administriranja, neprimjerenog vođenja evidencija ili nemara, a što može rezultirati gubitkom ili umanjnjem vrijednosti imovine za pokriće tehničkih pričuva ili gubitkom ili smanjenjem prava u svezi s imovinom za pokriće tehničkih pričuva, ili dovesti do štete za korisnike mirovina, svodi na najmanju moguću mjeru.

Organizacijski zahtjevi za sustav upravljanja rizicima i funkciju upravljanja rizicima
Članak 3.

(1) Sustav upravljanja rizicima mora biti djelotvoran i dobro integriran u organizacijsku strukturu i procedure donošenja odluka Društva, a uključuje i sustav upravljanja rizikom od pranja novca i financiranja terorizma.

(2) Sustav upravljanja rizicima obuhvaća najmanje sljedeća područja:

1. preuzimanje rizika i oblikovanje pričuva
2. upravljanje imovinom i obvezama
3. ulaganja, posebno izvedenice, sekuritizacije i slične obveze
4. upravljanje rizicima likvidnosti i koncentracijskim rizicima
5. upravljanje operativnim rizicima
6. osiguranje i ostale tehnike smanjenja rizika
7. okolišni, socijalni i upravljački rizici povezani s portfeljem ulaganja i upravljanjem njime.

(3) Mirovinsko osiguravajuće društvo dužno je ustrojiti funkciju upravljanja rizicima koja je strukturirana na način koji olakšava provedbu sustava upravljanja rizicima.

(4) Mirovinsko osiguravajuće društvo dužno je u sklopu funkcije upravljanja rizicima osigurati obavljanje najmanje sljedećih poslova:

1. identificiranje i mjerenje rizika kojima je mirovinsko osiguravajuće društvo izloženo ili bi moglo biti izloženo u svom poslovanju,
2. praćenje rizika kojima je mirovinsko osiguravajuće društvo izloženo ili bi moglo biti izloženo u svom poslovanju,
3. upravljanje rizicima kojima je mirovinsko osiguravajuće društvo izloženo ili bi moglo biti izloženo u svom poslovanju,
4. provjeru primjene i djelotvornosti postupaka i mjera za upravljanje rizicima kojima je mirovinsko osiguravajuće društvo izloženo ili bi moglo biti izloženo u svom poslovanju,
5. izvještavanje uprave i nadzornog odbora o upravljanju rizicima,
6. sudjelovanje u izradi, provođenju i preispitivanju strategije, politika, postupaka i mjera upravljanja rizicima mirovinskog osiguravajućeg društva,
7. savjetovanje uprave vezano uz utvrđivanje profila rizičnosti mirovinskog osiguravajućeg društva te praćenje utvrđenog profila rizičnosti,
8. preispitivanje i ocjenjivanje djelotvornosti mehanizama unutarnjih kontrola,
9. davanje preporuka na temelju rezultata postupka iz točke 1. ovoga stavka,
10. provođenje ostalih provjera koje su potrebne za adekvatnu kontrolu rizika.

(5) Mirovinsko osiguravajuće društvo dužno je funkciji upravljanja rizicima osigurati potrebne ovlasti i pristup svim podacima bitnim za ispunjavanje obveza iz stavka 4. ovoga članka.

Organizacijski zahtjevi za obavljanje funkcije unutarnje revizije
Članak 4.

(1) Mirovinsko osiguravajuće društvo dužno je u sklopu funkcije unutarnje revizije osigurati obavljanje najmanje sljedećih poslova:

1. propisivanje, primjenjivanje i redovito ažuriranje plana revizije te redovito ispitivanje i procjenjivanje primjerenosti i učinkovitosti mehanizama unutarnje kontrole i ostalih elemenata organizacijskih zahtjeva mirovinskog osiguravajućeg društva, uključujući izdvojene poslove i funkcije,
2. davanje preporuka na temelju rezultata postupka iz točke 1. ovoga stavka,
3. provjeravanje usklađenosti s preporukama iz točke 2. ovoga stavka,

4. izvješćivanje uprave i nadzornog odbora u vezi poslova unutarnje revizije.

(2) Mirovinsko osiguravajuće društvo dužno je funkciji unutarnje revizije osigurati potrebne ovlasti i pristup svim podacima bitnim za ispunjavanje obveza iz stavka 1. ovoga članka.

Organizacijski zahtjevi za obavljanje funkcije praćenja usklađenosti s relevantnim propisima Članak 5.

(1) Mirovinsko osiguravajuće društvo dužno je:

1. osigurati da osobe unutar funkcije praćenja usklađenosti s relevantnim propisima imaju potrebne ovlasti, sredstva, i pristup svim bitnim podacima za obavljanje poslova praćenja usklađenosti s relevantnim propisima,

2. imenovati osobu zaduženu za praćenje usklađenosti s relevantnim propisima, a koja je odgovorna za funkciju praćenja usklađenosti s relevantnim propisima i izvješćivanje,

3. osigurati da način određivanja plaća i drugih oblika primitaka osoba uključenih u funkciju praćenja usklađenosti s relevantnim propisima ne umanjuje niti je izgledno da bi mogao umanjivati njihovu objektivnost.

(2) U sklopu funkcije praćenja usklađenosti s relevantnim propisima osigurati obavljanje najmanje sljedećih poslova:

1. praćenje i redovnu procjenu primjerenosti i učinkovitosti mjera, politika i postupaka čiji je cilj otkrivanje svakog rizika neusklađenosti s relevantnim propisima kao i povezanih rizika,

2. praćenje i redovnu procjenu aktivnosti mirovinskog osiguravajućeg društva koje se odnose na uočene propuste u poštivanju i pridržavanju obveza u skladu s relevantnim propisima,

3. savjetovanje uprave i drugih relevantnih osoba odgovornih za obavljanje djelatnosti mirovinskog osiguravajućeg društva o načinu primjene odredbi Zakona, propisa donesenih na temelju Zakona i drugih relevantnih propisa te internih akata mirovinskog osiguravajućeg društva.

Organizacijski zahtjevi za obavljanje aktuarske funkcije Članak 6.

(1) Mirovinsko osiguravajuće društvo dužno je u sklopu aktuarske funkcije osigurati obavljanje najmanje poslova iz članka 53. Zakona te poslova iz članka 3. stavka 4. ovoga Pravilnika koji se odnose na rizike izračuna mirovina, tehničkih pričuva i adekvatnosti kapitala u suradnji s funkcijom upravljanja rizicima.

(2) Mirovinsko osiguravajuće društvo dužno je aktuarskoj funkciji osigurati potrebne ovlasti i pristup svim podacima bitnim za ispunjavanje obveza iz stavka 1. ovoga članka.

Organizacijski zahtjevi radi preveniranja i otklanjanja sukoba interesa Članak 7.

(1) Razumnim koracima u smislu članka 61. stavaka 1. i 2. Zakona, osobito se smatra sljedeće:

- razdvajanje nadležnosti pojedinih organizacijskih jedinica,
- razdvajanje pojedinih funkcija iz članka 49. a. stavka 1. Zakona i zaštita tih funkcija od utjecaja koji sprječavaju objektivno, pravično i neovisno obavljanje dužnosti,
- izbjegavanje sukoba interesa kod izdvajanja poslova i funkcija,
- uspostavljanje odvojenih linija izvještavanja,

- izbjegavanje sukoba interesa između povećanja izloženosti mirovinskog osiguravajućeg društva rizicima i unutarnje kontrole,
 - ako se zbog veličine (broja zaposlenika) mirovinskog osiguravajućeg društva ne mogu razdvojiti funkcije iz članka 49. a. stavka 1. Zakona koje su međusobno nespojive, izbjegavanje sukoba interesa mora se zajamčiti na drugi način, pri čemu se mora osigurati dosljednost u vezi izabrane strategije upravljanja rizicima
- (2) Mirovinsko osiguravajuće društvo dužno je uvijek voditi računa o postojanju sukoba interesa:
- prilikom donošenja odluka o ulaganju i u svim ostalim slučajevima postupati u najboljem interesu korisnika i staviti njihove interese ispred svojih
 - kada odluka društva ide u korist uprave, dioničara društva ili s njima povezane osobe.

Politika upravljanja sukobom interesa Članak 7.a.

- (1) Mirovinsko osiguravajuće društvo dužno je propisati, primjenjivati i redovito ažurirati učinkovitu politiku upravljanja sukobom interesa. Politika upravljanja sukobom interesa mora biti primjerena veličini i organizacijskom ustroju mirovinskog osiguravajućeg društva, kao i vrsti, opsegu i složenosti djelatnosti koje mirovinsko osiguravajuće društvo obavlja.
- (2) Kada je mirovinsko osiguravajuće društvo član grupe, politika upravljanja sukobom interesa mora sadržavati sve okolnosti koje su poznate mirovinskom osiguravajućem društvu ili koje bi mu trebale biti poznate, a koje mogu dovesti do sukoba interesa koji je rezultat strukture i poslovnih aktivnosti drugih članova grupe.
- (3) Politika iz stavka 1. ovoga članka mora sadržavati:
1. okolnosti koje predstavljaju ili koje mogu dovesti do sukoba interesa na štetu korisnika mirovina, a vezano za djelatnost mirovinskog osiguravajućeg društva,
 2. procedure kojih se mirovinsko osiguravajuće društvo mora pridržavati i mjere koje mora primjenjivati za upravljanje sukobom interesa.

Organizacijski zahtjevi za provođenje mjera za neprekidno poslovanje Članak 8.

- (1) Mirovinsko osiguravajuće društvo dužno je propisati, primjenjivati i redovito ažurirati mjere za neprekidno poslovanje koje najmanje uključuju:
1. postupanje u izvanrednim okolnostima
 2. pretpostavke za primjenu mjera za neprekidno poslovanje
 3. zaduženja i odgovornosti u postupanje u izvanrednim okolnostima,
 4. pohranu sigurnosnih kopija svih zapisa koja omogućuje nesmetano obavljanje djelatnosti u izvanrednim okolnostima,
 5. ako nesmetano obavljanje djelatnosti u izvanrednim okolnostima nije moguće, pravodobnu uspostavu ključnih poslovnih aktivnosti i pristupa podacima te pravodobni nastavak obavljanja djelatnosti mirovinskog osiguravajućeg društva uz ograničavanje gubitaka u slučajevima znatnijeg narušavanja ili prekida poslovanja
 6. pravodobnu uspostavu funkcija i pristupa podacima i pravodobni nastavak obavljanja djelatnosti mirovinskog osiguravajućeg društva, ako nesmetano obavljanje djelatnosti u izvanrednim okolnostima nije moguće.
- (2) Poslovnim procesima nužnim za neprekidno i primjereno poslovanje smatraju se poslovni procesi mirovinskog osiguravajućeg društva kod kojih bi greške ili propusti pri izvršavanju znatno naštetili:

1. neprekidnom ispunjavanju uvjeta poslovanja i obveza mirovinskog osiguravajućeg društva koji su propisani Zakonom ili propisima donesenim na temelju Zakona,
2. financijskoj stabilnosti mirovinskog osiguravajućeg društva ili kontinuitetu obavljanja djelatnosti.
- (3) Poslovi koji se u smislu stavka 2. ovoga članka ne smatraju poslovnim procesima nužnim za neprekidno i uredno obavljanje djelatnosti mogu biti poslovi iz članka 10. Zakona.
- (4) Mirovinsko osiguravajuće društvo dužno je u slučaju nastupa okolnosti koje zahtijevaju pokretanje mjera za neprekidno poslovanje, bez odgode obavijestiti Hanfu o svim relevantnim činjenicama i okolnostima koje se na to odnose.
- (5) Mirovinsko osiguravajuće društvo dužno je propisati na koji način se provode mjere za neprekidno poslovanje i zaduženja zaposlenika i/ili organizacijskih jedinica u tom postupku
- (6) Mirovinsko osiguravajuće društvo dužno je propisati, primjenjivati i redovito ažurirati računovodstvene politike i procedure koje omogućavaju pravodobnu dostavu financijskih izvještaja u skladu sa Zakonom i drugim relevantnim propisima, a koji daju istinit i objektivan prikaz financijske situacije mirovinskog osiguravajućeg društva u skladu s važećim računovodstvenim standardima i pravilima.
- (7) Mirovinsko osiguravajuće društvo dužno je redovito pratiti, ažurirati, unaprjeđivati i otklanjati nedostatke internih sustava poslovanja, unutarnjih kontrola i politika i procedura.
- (8) Mirovinsko osiguravajuće društvo dužno je osigurati adekvatne resurse za neometano obavljanje djelatnosti koje obavlja.

Organizacijski zahtjevi za politike primitaka

Članak 9.

- (1) Primitak podrazumijeva sve oblike plaćanja i pogodnosti, koje mirovinsko osiguravajuće društvo (uključujući i udio u dobiti), isplaćuje članovima Uprave, osobe koje obavljaju ključne funkcije i drugim zaposlenicima ili osobama koje obavljaju poslove za mirovinsko osiguravajuće društvo čije profesionalne aktivnosti imaju značajan utjecaj na profil rizičnosti mirovinskog osiguravajućeg društva (dalje u tekstu: radnik) u zamjenu za poslove koje taj radnik obavlja, a koje uključuje:
 - a. nagrađivanje na osnovi nesamostalnog rada – plaću i diskrecijske mirovinske pogodnosti,
 - b. drugo nagrađivanje.
- (2) Diskrecijska mirovinska pogodnost je nagrađivanje ugovoreno kao izdvajanje za mirovinu koje mirovinsko osiguravajuće društvo ugovara odnosno dodjeljuje radniku na diskrecijskoj osnovi i ne isplaćuje se radniku na redovnoj osnovi, nego se utvrđuje i formira za mirovine. Diskrecijske mirovinske pogodnosti dio su radnikovih varijabilnih primitaka.
- (3) Mirovinsko osiguravajuće društvo dužno je utvrditi i primjenjivati politiku primitaka koja propisuje organizaciju kontrole: izrade, točnosti, cjelovitosti odluka ili akata mirovinskog osiguravajućeg društva koji se primjenjuju na primitke radnika što uključuje najmanje politiku nagrađivanja i procedure za njezino provođenje, odluke u svezi s nagrađivanjem te metodologiju i rezultate mjerenja uspješnosti pri utvrđivanju varijabilnih primitaka čiji rad može imati materijalno značajan utjecaj na profil rizičnosti mirovinskog osiguravajućeg društva.
- (4) Prilikom utvrđivanja i primjene politike nagrađivanja mirovinsko osiguravajuće društvo dužno je, na način i u opsegu koji je primjeren veličini i unutarnjoj organizacijskoj strukturi mirovinskog osiguravajućeg društva te vrsti, opsegu i složenosti poslovanja, voditi računa da su zaposlenici koji obavljaju poslove u funkcijama iz članka 49. a. stavka 1. Zakona neovisni o poslovnim jedinicama koje nadziru, imaju odgovarajuće ovlasti te imaju primitke koji uzimaju u obzir postignute ciljeve povezane s njihovim funkcijama, neovisno o uspješnosti poslovnih područja koja kontroliraju.
- (5) Mirovinsko osiguravajuće društvo dužno je osigurati da se kod primjene politike primitaka jasno razlikuju kriteriji za određivanje:

1. osnovnih fiksnih primitaka koji bi trebali prvenstveno odražavati relevantno profesionalno iskustvo i organizacijsku odgovornost koji su navedeni u opisu radnog mjesta radnika kao dio uvjeta zapošljavanja i

2. varijabilnih primitaka koji bi trebali odražavati održivu i riziku prilagođenu uspješnost kao i uspješnost koja prelazi okvire uspješnosti potrebne za ispunjavanje opisa radnog mjesta radnika kao dio uvjeta zapošljavanja. U varijabilne primitke uključuje se i iznos otpremnine radniku u iznosu koji prelazi zakonom propisani iznos.

(6) Mirovinsko osiguravajuće društvo dužno je utvrditi tko je u mirovinskom osiguravajućem društvu zadužen kontrolirati primjenu načela politike primitaka te sadržaj izvješća i rokove u kojima se upravi dostavljaju izvješća o provedenoj kontroli.

(7) Odredbe ovoga članka na odgovarajući način se primjenjuju i na primitke koje mirovinsko osiguravajuće društvo isplaćuje osobama koje obavljaju poslove distribucije mirovinskih programa za društvo i na primitke osobama na koje je izdvojilo poslove odnosno funkcije.

(8) Mirovinska osiguravajuća društva koja su značajna po svojoj veličini te prirodi, opsegu i složenosti poslovanja dužna su osnovati odbor za primitke kojem se omogućuje donošenje stručne i neovisne prosudbe o politikama i praksama vezanim za primitke te o utjecaju primitaka na upravljanje rizicima, uzimajući u obzir dugoročne interese mirovinskog osiguravajućeg društva i korisnika mirovine.

Organizacijski zahtjevi za vođenje i čuvanje poslovne dokumentacije i podataka

Članak 10.

(1) Sva poslovna dokumentacija i podaci koje je mirovinsko osiguravajuće društvo dužno izrađivati i prikupljati u skladu sa Zakonom i propisima donesenim na temelju Zakona kao i drugim relevantnim propisima mora se čuvati najmanje 5 godina nakon isteka poslovne godine na koju se ti podaci odnose, ako drugim propisima nije predviđen duži rok.

(2) Mirovinsko osiguravajuće društvo dužno je uspostaviti evidencije svih internih akata i njihovih izmjena.

(3) Poslovna dokumentacija i podaci iz stavaka 1. i 2. ovoga članka moraju se čuvati na mediju koji omogućuje pohranu podataka na način da budu dostupni Hanfi na zahtjev u svakom trenutku, u obliku i na način koji ispunjava sljedeće uvjete:

1. Hanfa mora biti u mogućnosti pristupiti dokumentaciji i podacima, kao i utvrditi sve ključne faze poslovnih događaja,

2. mora biti moguće jednostavno utvrditi sve ispravke ili izmjene, kao i sadržaj dokumentacije i podataka prije takvih ispravaka ili izmjena,

3. dokumentacija i podaci moraju biti zaštićeni od neovlaštenog pristupa i mogućih gubitaka u zapisu te se čuvati na način koji osigurava trajnost zapisa,

4. manipulacija dokumentacijom i podacima ili bilo kakva njihova preinaka mora biti onemogućena

5. sigurnosti čuvanja i raspolaganja pohranjenih podataka.

(4) Sigurnosne kopije svih podataka i dokumentacije mirovinsko osiguravajuće društvo dužno je čuvati izvan poslovnih prostorija mirovinskog osiguravajućeg društva na način i u rokovima propisanim ovim člankom Pravilnika.

(5) Mirovinsko osiguravajuće društvo dužno je s osobnim podacima fizičkih osoba postupati u skladu s Uredbom (EU) 2016/679, a u vezi s obradom osobnih podataka koju provodi EIOPA u okviru Direktive (EU) 2016/2341, EIOPA poštuje Uredbu (EZ) br. 45/2001.

Organizacijski zahtjevi za primjereno upravljanje informacijskim sustavom i kibernetičkim rizicima
Članak 11.

(1) Mirovinsko osiguravajuće društvo dužno je propisati, primjenjivati i redovito ažurirati politiku sigurnosti informacijskog sustava koja mora sadržavati načela, mjere i postupke kojima će se osigurati povjerljivost, cjelovitost i dostupnost podataka koji se obrađuju u informacijskom sustavu mirovinskog osiguravajućeg društva.

(2) Mirovinsko osiguravajuće društvo dužno je propisati, primjenjivati i redovito ažurirati interne akte koji uređuju primjereno korištenje informacijskog sustava mirovinskog osiguravajućeg društva.

(3) Mirovinsko osiguravajuće društvo dužno je propisati, primjenjivati i redovito održavati plan oporavka od štetnih događaja koji mora sadržavati mjere i postupke za oporavak prekinutih poslovnih sustava u razumnom roku.

(4) Mirovinsko osiguravajuće društvo dužno je testirati provedivost i učinkovitost plana oporavka od štetnih događaja najmanje jednom godišnje, a u slučaju značajnijih izmjena i češće.

(5) Mirovinsko osiguravajuće društvo dužno je organizirati informacijski sustav koji za sve poslovno važne informatičke servise ima uspostavljenu jasnu operativnu podršku te razrađen postupak uvođenja novih ili promjenu postojećih informatičkih servisa.

(6) Mirovinsko osiguravajuće društvo može izdvojiti pojedine dijelove informacijskog sustava trećim osobama ili koristiti aplikativna rješenja samo ako je ugovorno i praktično osiguran kontinuitet poslovanja za vrijeme i nakon prekida suradnje s trećom stranom.

(7) Mirovinsko osiguravajuće društvo dužno je osigurati visoku razinu sigurnosti tijekom elektroničke obrade podataka te točnost i povjerljivost evidentiranih podataka.

Članak 11.a

Mirovinsko osiguravajuće društvo je dužno u pogledu sigurnosti mrežnih i informacijskih sustava postupati u skladu sa zahtjevima iz Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011.

Članak 12.

(1) Nositelji ključnih funkcija iz čl. 49.a Zakona dužni su obavijestiti upravu i nadzorni odbor mirovinskog osiguravajućeg društva o:

1. značajnijoj povredi odredaba Zakona i/ili na temelju njega uspostavljenih propisa o poslovanju mirovinskog osiguravajućeg društva, uočenoj prilikom obavljanja poslova praćenja usklađenosti, upravljanja rizicima, aktuarskih poslova i/ili revizije poslovanja društva

2. uočenom postojanju povećanog rizika neusklađenosti mirovinskog osiguravajućeg društva s materijalno značajnim zakonskim zahtjevima, koji bi mogao utjecati na interese korisnika mirovina.

(2) Ako uprava ili nadzorni odbor mirovinskog osiguravajućeg društva ne poduzmu pravodobne i odgovarajuće mjere za otklanjanje utvrđenih povreda ili prepoznatih rizika, nositelj funkcije iz stavka 1. ovoga članka će o tome bez odgode obavijestiti Hanfu.

(3) Prilikom dostavljanja obavijesti iz stavka 2. ovoga članka Hanfa će osigurati odgovarajuću zaštitu nositelja funkcije iz stavka 1. ovoga članka koji je dostavio predmetnu obavijest, u svrhu njegove zaštite od moguće diskriminacije ili drugih oblika dovođenja u nepovoljniji položaj, odnosno pozivanja na odgovornost zbog otkrivanja navedenih podataka.

(4) Na način zaprimanja obavijesti iz stavka 2. ovoga članka i postupanje u vezi s dostavljenom obavijesti, kao i pravila o povjerljivosti podataka o osobi koja je obavijest dostavila, na odgovarajući se način primjenjuju odredbe podzakonskog propisa koje uređuju organizacijske zahtjeve kod mirovinskih društava za upravljanje dobrovoljnim mirovinskim fondovima.

Stupanje na snagu

Članak 13.

(1) Ovaj Pravilnik stupa na snagu osmoga dana od dana objave u »Narodnim novinama«, osim članka 11.a koji se počinje primjenjivati od 17. siječnja 2025. godine.

(2) Stupanjem na snagu ovog Pravilnika, prestaje važiti Pravilnik o organizacijskim zahtjevima mirovinskog osiguravajućeg društva (»Narodne novine«, broj 2/20).

KLASA: 011-01/24-11/01
URBROJ: 326-01-70-72-24-11
Zagreb, 10. prosinca 2024.

PREDSJEDNIK UPRAVNOG VIJEĆA
dr. sc. Ante Žigman