Na osnovu člana 26. stav 4. Zakona o Centralnom registru obaveznog socijalnog osiguranja ("Službeni glasnik RS", broj 30/10),

Ministar rada, zapošljavanja i socijalne politike donosi

PRAVILNIK
O ČUVANJU, ZAŠTITI I SIGURNOSTI PODATAKA U OKVIRU INFORMACIONOG SISTEMA CENTRALNOG REGISTRA OBAVEZNOG SOCIJALNOG OSIGURANJA

(Sl. glasnik RS br. 29/13)

Osnovni tekst na snazi od 06/04/2013 , u primeni od 06/04/2013

Sadržina pravilnika

Član 1.

Ovim pravilnikom uređuju se procedure čuvanja, zaštite i sigurnosti podataka informacionog sistema Centralnog registra obaveznog socijalnog osiguranja (u daljem tekstu: informacioni sistem Centralnog registra).

Ciljevi zaštite informacionog sistema

Član 2.

(1) Ciljevi zaštite informacionog sistema Centralnog registra su:

1) očuvanje poverljivosti podataka, čime se onemogućava neautorizovan uvid i korišćenje podataka iz informacionog sistema Centralnog registra;

2) zaštita integriteta podataka, čime se onemogućava izmena podataka i garantuje autentičnost podataka;

3) očuvanje raspoloživosti podataka, čime se omogućava rekonstrukcija podataka u slučaju njihovog namernog ili nenamernog oštećenja.

(2) Zaštita iz stava 1. ovog člana obezbeđuje se kroz zaštitu pristupa računarskoj opremi i mreži, koja se realizuje na mrežnom nivou kroz specijalizovane hardverske komponente i uz upotrebu protokola zaštite, kao i kroz zaštitu pristupa podacima.

Čuvanje, zaštita i sigurnost podataka Centralnog registra

Član 3.

Centralni registar je odgovoran za čuvanje, zaštitu i sigurnost podataka u okviru informacionog sistema Centralnog registra, što podrazumeva:

1) zaštitu od neovlašćenog pristupa resursima koji su predmet zaštite, njihovo neovlašćeno korišćenje ili manipulacije bazom podataka informacionog sistema od strane internih i eksternih korisnika;

2) zaštitu integriteta podataka, njihovu raspoloživost i neovlašćeni uvid u poverljive podatke;

3) zaštitu baze podataka od virusa i ostalih oblika malicioznih kodova;

4) osiguranje prenosa podataka iz Jedinstvene baze internim i eksternim korisnicima;

5) čuvanje podataka i upravljanje sigurnosnim kopijama baze podataka u okviru informacionog sistema;

6) politiku prenosnih računara u pogledu pristupa bazi podataka Jedinstvene baze i čuvanja podataka u jedinstvenoj bazi;

7) osiguranje kontinuiteta aktivnosti u slučaju požara, poplave, zemljotresa ili druge nepogode koja se smatra rezultatom više sile i koja dovodi do neuobičajenog prekida u radu informacionog sistema;

8) povraćaj sačuvanih podataka u slučaju gubitka, oštećenja ili uništenja računarske opreme informacionog sistema;

9) testiranje jedinstvene baze podataka radi otkrivanja sigurnosnih problema na redovnoj osnovi i nakon instaliranja novih verzija Jedinstvene baze podataka;

10) instaliranje softverske nadogradnje radi uklanjanja sigurnosnih problema koji se ustanove na Jedinstvenoj bazi u okviru informacionog sistema ili na povezanom softveru;

11) praćenje sigurnosnih incidenata u bazi podataka informacionog sistema radi preduzimanja korektivnih mera;

12) upravljanje sigurnosnim incidentima, edukacija i obuka svih ovlašćenih osoba radi sticanja potrebnih znanja o čuvanju i sigurnosti podataka;

13) fizički pristup i zaštita baze podataka u okviru informacionog sistema i računarske opreme;

14) održavanje računarske opreme informacionog sistema.

Mere zaštite pristupa informacionom sistemu

Član 4.

(1) Mere zaštite pristupa informacionom sistemu Centralnog registra su:

1) autentifikacija - koja predstavlja proces utvrđivanja identiteta osobe koja želi da pristupi informacionom sistemu Centralnog registra;

2) autorizaciju - koja predstavlja pravo pristupa i dozvoljenih operacija za autentifikovano lice;

3) zaštita tajnosti - što podrazumeva šifrovanje podataka u cilju sprečavanja neovlašćenog uvida;

4) neporicanje odgovornosti - što podrazumeva obezbeđenje dokaza da je neko izvršio određenu radnju, odnosno transakciju.

(2) Realizacija sistema zaštite informacionog sistema Centralnog registra podrazumeva obaveznu primenu kvalifikovanih elektronskih sertifikata za pristup preko Portala i autentifikaciju transakcija, kao i za autentifikaciju pristupa Veb servisima.

(3) Autentifikacija pristupa servisima od strane državnih organa i organizacija, sa kojima Centralni registar vrši razmenu podataka podrazumeva i obaveznu primenu serverskih sertifikata.

(4) Izuzetno, osiguranici i osigurana lica, koji imaju pravo uvida u lične podatke koji se odnose na osiguranje, mogu pristupiti informacionim sistemu Centralnog registra na osnovu jedinstvenog broja i lozinke, koje dodeljuje Centralni registar.

Pristup informacionom sistemu Centralnog registra

Član 5.

(1) Centralni registar upravlja korisničkim nalozima, pravima pristupa i korisničkim lozinkama za interne i eksterne korisnike jedinstvene baze Centralnog registra.

(2) Centralni registar dužan je da obezbedi pristup podacima u okviru informacionog sistema samo od strane ovlašćenih lica.

(3) Svaki pristup informacionom sistemu mora biti automatski zabeležen jedinstvenim identifikatorom lica u bazi podataka jedinstvenog sistema, sa tačnim vremenom pristupa.

(4) O saznanjima u vezi sa pokušajima neovlašćenog pristupa informacionom sistemu Centralnog registra, administratori Jedinstvene baze podataka dužni su da obaveste ovlašćeno lice.

Fizička zaštita podataka informacionog sistema i čuvanje bezbednosnih kopija

Član 6.

(1) Radi obezbeđenja neprekidnog funkcionisanja informacionog sistema, Centralni registar obezbeđuje fizičku zaštitu podataka primarnog informacionog sistema, formiranjem sekundarne baze podataka i sekundarnog računarskog sistema.

(2) Sekundarna baza podataka i sekundarni računarski sistem moraju biti udaljeni od mesta na kome se nalazi primarni informacioni sistem.

(3) Lokacije iz st. 1. i 2. ovog člana moraju biti na adekvatan način zaštićene od požara i poplava, kao i imati 24-satni bezbednosni sistem.

(4) Pristup lokacijama na kojima se nalaze baze podataka informacionog sistema i čuvaju bezbednosne kopije imaju samo ovlašćena lica.

Održavanje, popravka i povlačenje iz upotrebe opreme za informacioni sistem

Član 7.

(1) Centralni registar obezbeđuje održavanje računarske opreme za informacioni sistem a, u slučaju popravki, prethodno sprema bezbednosne kopije podataka, kako bi se sprečio gubitak podataka.

(2) Održavanje i popravka računarske opreme, vrši se isključivo pod nadzorom ovlašćenih zaposlenih u Centralnom registru.

(3) U slučaju povlačenja računarske opreme iz informacionog sistema, svi podaci prethodno moraju biti trajno i sigurno izbrisani.

Završna odredba

Član 8.

Ovaj pravilnik stupa na snagu osmog dana od dana objavljivanja u "Službenom glasniku Republike Srbije".

Broj 110-00-00172/2013-07
U Beogradu, 14. marta 2013. godine

Ministar,
Jovan Krkobabić, s.r.