Na osnovu člana 11. stav (5) Zakona o zaštiti ličnih podataka ("Službeni glasnik BiH" broj 49/07) i člana 17. Zakona o Vijeću ministara Bosne i Hercegovine ("Službeni glasnik BiH", broj 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08), Vijeće ministara Bosne i Hercegovine, na 93. sjednici održanoj 2. jula 2009. godine, donijelo je

PRAVILNIK

O NAČINU ČUVANJA I POSEBNIM MJERAMA TEHNIČKE ZAŠTITE LIČNIH PODATAKA

POGLAVLJE I. - OPĆE ODREDBE

Član 1.
(Predmet Pravilnika)

Pravilnikom o načinu čuvanja i posebnim mjerama tehničke zaštite ličnih podataka (u daljnjem tekstu: Pravilnik) bliže se propisuje način čuvanja i posebne mjere tehničke zaštite ličnih podataka.

Član 2.
(Pojmovi)

Pojedini pojmovi korišteni u ovom Pravilniku imaju sljedeće značenje:

a) "Administrator zbirke ličnih podataka" je fizičko lice ovlašteno i odgovorno za sistem upravljanja zbirkom ličnih podataka i za osiguranje tajnosti i zaštite obrade ličnih podataka.

b) "Izvršilac" je fizičko lice, zaposleno ili angažirano kod kontrolora koje izvršava poslove vezane za obradu ličnih podataka.

POGLAVLJE II. - NAČIN ČUVANJA LIČNIH PODATAKA

Član 3.
(Način čuvanja)

Način čuvanja ličnih podataka podrazumijeva poduzimanje organizacijskih i tehničkih mjera zaštite ličnih podataka te sačinjavanje plana sigurnosti ličnih podataka.

Član 4.
(Organizacijske mjere zaštite)

(1) Kontrolor treba da osigura organizacijske mjere zaštite ličnih podataka koje obuhvataju: informiranje i obuku uposlenih koji rade na obradi ličnih podataka, fizičke mjere zaštite radnih prostorija i opreme u kojima se vrši obrada ličnih podataka, sprečavanje neovlaštenog umnožavanja, kopiranja i prepisivanja ličnih podataka, uništavanja ličnih podataka i drugo.

(2) Nakon prijema u radni odnos, a prije otpočinjanja obavljanja radnih dužnosti, svako lice koje će u okviru poslova i zadataka obrađivati lične podatke upoznaje se sa mjerama zaštite ličnih podataka.

(3) Prije neposrednog otpočinjanja obavljanja poslova vezanih za obradu ličnih podataka, kontrolor dodatno upoznaje uposlenog sa konkretnim obavezama po pitanju zaštite ličnih podatka.

Član 5.
(Tehničke mjere zaštite)

(1) Kontrolor treba osigurati odgovarajuće mjere tehničke zaštite prostorija i opreme u kojima se vrši obrada ličnih podataka.

(2) Posebnim mjerama tehničke zaštite ličnih podataka treba onemogućiti neovlašten pristup i obradu istih.

(3) Tehničke mjere zaštite ličnih podataka, između ostalog, obuhvataju kontrolu pristupa prostorijama i opremi za obradu ličnih podatka, zaštitu od uništenja i oštećenja ličnih podataka i drugo.

Član 6.
(Plan sigurnosti ličnih podataka)

(1) Plan sigurnosti ličnih podataka sadrži organizacijske i tehničke mjere kojima se mora osigurati:

a) da samo ovlaštena lica mogu znati lične podatke - povjerljivost;

b) da za vrijeme obrade lični podaci ostanu nepromijenjeni, potpuni i ažurni - integritet;

c) da su podaci stalno dostupni, da su na raspolaganju i da se mogu ispravno obrađivati - raspoloživost;

d) da se u svako doba može utvrditi porijeklo ličnih podataka - autentičnost;

e) da se može utvrditi ko, kada, koje je lične podatke i na koji način obrađivao - mogućnost revizije;

f) da je postupak pri obradi ličnih podataka potpun, ažuran i na odgovarajući način evidentiran-transparentnost.

(2) Plan sigurnosti ličnih podataka mora sadržavati kategorije ličnih podataka koje se obrađuju i popis instrumenata zaštite odnosno organizacijske i tehničke mjere zaštite.

(3) Plan sigurnosti ličnih podataka mora biti sačinjen u pismenoj formi, ažuriran i stalno dostupan Agenciji za zaštitu ličnih podataka u Bosni i Hercegovini.

POGLAVLJE III. - ZAŠTITA LIČNIH PODATAKA U AUTOMATSKOJ OBRADI

Član 7.
(Tehničke mjere)

(1) Kontrolor pri automatskoj obradi ličnih podataka treba da osigura tehničke mjere zaštite ličnih podatka i to:

a) jedinstveno korisničko ime i lozinku sastavljenu od kombinacije minimum šest karaktera, brojeva ili slova;

b) automatsku izmjenu lozinke po utvrđenom vremenskom periodu koji ne može biti duži od šest mjeseci;

c) korisničko ime i lozinka će dozvoljavati pristup samo do dijelova sistema potrebnih izvršiocu za izvršenje njegovih radnih zadataka;

d) automatsko odjavljivanje sa sistema po isteku određenog perioda neaktivnosti, ne duže od 15 minuta, a za ponovno aktiviranje sistema potrebno je nanovo upisati korisničko ime i lozinku;

e) automatsku zabranu pristupa sistemu nakon tri neuspješna pokušaja prijavljivanja na sistem i automatsko upozorenje izvršiocu da potraži instrukciju od administratora zbirke ličnih podataka;

f) efikasnu i sigurnu antivirusnu zaštitu sistema, koje će se stalno ažurirati radi preventive od nepoznate ili neplanirane opasnosti od novih virusa;

g) kompjuterska, programska i ostala neophodna oprema na elektorenergetsku mrežu se priključuje putem uređaja za neprekidno napajanje.

(2) U slučaju iz tačke e. stav (1) ovog člana administrator zbirke ličnih podataka odobrava daljnji pristup sistemu.

(3) Izvršilac koji obavlja kadrovske poslove, treba da izvještava administratora zbirke ličnih podataka o zaposlenju ili angažiranju svakog izvršioca s pravom pristupa informacijskom sistemu, kako bi se dodijelili korisničko ime i lozinka, kao i po prestanku zaposlenja ili angažiranja, da bi se korisničko ime i lozinka izbrisali odnosno zabranio daljnji pristup.

(4) Izvještavanje iz stava (3) ovog člana vrši se i prilikom bilo koje druge promjene radnog statusa izvršioca, koja utiče na nivo ili obim pristupu zbirke ličnih podataka.

Član 8.
(Organizacione mjere)

Kontrolor pri automatskoj obradi ličnih podataka treba da osigura organizacijske mjere zaštite ličnih podataka i to:

a) potpunu tajnost i sigurnost lozinki i ostalih formi za identifikaciju pristupa ličnim podacima;

b) organizacijska pravila za pristup izvršioca internetu koja se odnose na preuzimanje i snimanje dokumenata putem elektronske pošte ili drugih izvora;

c) uništavanje dokumenata koji sadrže lične podatke po isteku roka za obradu;

d) svako iznošenje bilo kojeg medija koji sadrži lične podatke van radnih prostorija mora biti sa posebnom dozvolom i kontrolom da ne dođe do gubljenja ili nezakonitog korištenja;

e) mjere fizičke zaštite radnih prostorija i opreme gdje se obrađuju lični podaci; i

f) poštivanje tehničkih uputstava pri instaliranju i korištenju opreme koja služi za obradu ličnih podataka.

Član 9.
(Mrežna barijera)

Kontrolor je dužan da osigura odgovarajuću zaštitu - mrežnu barijeru između njegovog sistema i Internet mreže, ili bilo koje druge forme spoljne mreže, kao zaštitu protiv nedozvoljenog pokušaja ulaza u sistem.

Član 10.
(Pravo pristupa)

(1) Pristup podacima pohranjenim u zbirkama ličnih podataka dozvoljen je ovlaštenim licima uposlenim kod kontrolora ili obrađivača i ovlaštenim licima zaduženim za održavanje i razvoj sistema za vođenje zbirki ličnih podataka.

(2) Kontrolor zbirke ličnih podataka određuje lica iz stava (1) ovoga člana.

(3) Obrađivač nema ovlaštenja za određivanje lica iz stava (1) ovog člana.

(4) Zahtjev za pristup ili obradu te zahtjev za prestanak ovlaštenja za pristup zbirkama ličnih podataka ili obradu ličnih podataka podnosi se kontroloru zbirke ličnih podataka koji daje ili ukida dozvolu za pristup zbirkama.

Član 11.
(Sigurnosna kopija)

(1) Kontrolor je dužan da vrši redovno snimanje sigurnosnih kopija ili arhiviranje podataka u sistemu, da ne bi došlo do njihovog gubljenja ili uništenja.

(2) Kontrolor je obavezan provjeravati upotrebljivost sigurnosnih kopija zbirki uz provjeru postupka povrata zbirki pohranjenih na prenosivom informatičkom mediju tako da vraćeni podaci nakon izvršene provjere budu u cijelosti raspoloživi za uptrebu, bez gubitka informacija.

(3) Svaki primjerak pohranjenih podataka na prenosivom informatičkom mediju mora biti označen brojem, vrstom, datumom pohranjivanja, te imenom lica koje je pohranjivanje izvršilo.

(4) Zabranjeno je bez nadzora i odobrenja kontrolora zbirke na bilo koji način umnožavanje informatičkih medija koja sadrže podatke iz zbirki posebnih kategorija ličnih podataka.

Član 12.
(Pristup u telekomunikacijski, kompjuterski i aplikacijski sistem)

(1) Pristup u informacijski sistem za vođenje zbirki ličnih podataka ili obradu podataka iz zbirki dozvoljen je uz upotrebu odgovarajućih korisničkih imena i pripadajućih propusnica.

(2) Kontrolor će evidentirati i kontrolisati svako pravo pristupa zaposlenih vanjskim mrežama, kao i pravo pristupa kompjuterskim sistemima ili lokalnoj mreži korisnicima van kompjuterskog sistema.

(3) Modemski priključci i njihovi brojevi, koji se koriste za pristup sistemu, na kojem su pohranjene zbirke ličnih podataka ne objavljuju se u telefonskim imenicima i ne smiju biti dostupni preko službe za davanje telefonskih brojeva.

Član 13.
(Obavezna upotreba jedinstvenih korisničkih imena i propusnica za pristup sistemu)

(1) Pristup podacima pohranjenim u zbirkama ličnih podataka dozvoljen je upotrebom dodijeljenoga jedinstvenog korisničkog imena i propusnice.

(2) Ukinuto korisničko ime ne smije se dodijeliti drugom licu.

(3) Korisničko ime i pripadajuća propusnica ne smiju se odati ili dati drugom licu.

(4) Način dodjeljivanja i obavezu izmjene propusnice određuje kontrolor zbirke ličnih podataka.

Član 14.
(Evidencija, praćenje pristupa i pokušaj neovlaštenog pristupa sistemu)

(1) Svaki pristup informacijskom sistemu za vođenje zbirki ličnih podataka mora biti automatski zabilježen korisničkim imenom, datumom i vremenom prijave i odjave.

(2) Svaki pokušaj neovlaštenog pristupa sistemu mora biti automatski zabilježen korisničkim imenom, datumom i vremenom, ako je to moguće i mjestom s kojeg je takav pristup pokušan.

(3) Obrađivač, administrator zbirke ličnih podataka i izvršilac dužni su obavijestiti odgovorno lice u kontroloru zbirke ličnih podataka o svakom pokušaju neovlaštenog pristupa sistemu.

Član 15.
(Lice odgovorno za zaštitu ličnih podataka)

Za uredno provođenje mjera osiguranja, pohranjivanja i zaštite ličnih podataka odgovara administrator zbirki ličnih podataka.

Član 16.
(Lice ovlašteno za dodjeljivanje korisničkih imena i propusnica)

Kontrolor zbirke ličnih podataka određuje lice ovlašteno za dodjeljivanje i uklanjanje korisničkih imena i dodjeljivanje propusnica licima ovlaštenim za rad u sistemu, a kojima je dozvoljen pristup zbirkama ličnih podataka.

Član 17.
(Zaštita posebne kategorije ličnih podataka)

(1) Prilikom obrade posebne kategorije ličnih podataka u svim fazama obrade kontrolor označava da se radi o obradi navedene kategorije podataka.

(2) Kontrolor preduzima dopunske tehničke i organizacijske mjere pri obradi posebnih kategorija ličnih podataka.

(3) Putem dopunskih tehničkih i organizacijskih mjera pri obradi posebne kategorije ličnih podataka osigurava se:

a) mogućnost za prepoznavanje svakog pojedinačnog ovlaštenog pristupa informacijskom sistemu;

b) rad sa podacima tokom redovnog radnog vremena kontrolora; i

c) kriptozaštita podataka pri prijenosu preko telekomunikacionih sistema sa odgovarajućim softverskim i tehničkim mjerama.

Član 18.
(Sedmično, mjesečno i godišnje provjeravanje rada sistema)

Kontrolor zbirke ličnih podataka sedmično, mjesečno i godišnje provjerava rad svih dijelova sistema.

IV. PRIJELAZNE I ZAVRŠNE ODREDBE

Član 19.
(Nadzor)

Nadzor nad provedbom ovog Pravilnika vrši Agencija za zaštitu ličnih podataka u Bosni i Hercegovini.

Član 20.
(Usklađivanje s odredbama Pravilnika)

(1) Kontrolori zbirki ličnih podataka i obrađivači dužni su u roku od šest mjeseci od dana stupanja na snagu ovog Pravilnika uskladiti mjere, sredstva i uvjete osiguranja, pohranjivanja i zaštite podataka s odredbama ovog Pravilnika.

Član 21.
(Stupanje na snagu)

(1) Stupanjem na snagu ovog Pravilnika prestaje da važi Pravilnik o sigurnosti podataka ("Službeni glasnik BiH", broj 39/02).

(2) Ovaj Pravilnik stupa na snagu osmoga dana od dana objavljivanja u "Službenom glasniku BiH".

VM broj 176/09
2. jula 2009. godine
Sarajevo

Predsjedavajući
Vijeća ministara BiH
Dr. **Nikola Špirić**, s. r.
