Na temelju članka 11. stavka (5) Zakona o zaštiti osobnih podataka ("Službeni glasnik BiH" broj 49/07) i članka 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. srpnja 2009. godine, donijelo je

PRAVILNIK

O NAČINU ČUVANJA I POSEBNIM MJERAMA TEHNIČKE ZAŠTITE OSOBNIH PODATAKA

POGLAVLJE I. - OPĆE ODREDBE

Članak 1.
(Predmet Pravilnika)

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

Članak 2.
(Pojmovi)

Pojedini pojmovi korišteni u ovom Pravilniku imaju sljedeće značenje:

a) "Administrator zbirke osobnih podataka je fizička osoba ovlaštena i odgovorna za sustav upravljanja zbirkom osobnih podataka i za osiguranje tajnosti i zaštite obrade osobnih podataka.

b) "Izvršitelj" je fizička osoba, zaposlena ili angažirana kod kontrolora koja izvršava poslove vezane za obradu osobnih podataka.

POGLAVLJE II. - NAČIN ČUVANJA OSOBNIH PODATAKA

Članak 3.
(Način čuvanja)

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

Članak 4.
(Organizacijske mjere zaštite)

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

(2) Nakon prijema u radni odnos, a prije otpočinjanja obavljanja radnih dužnosti, svaka osoba koja će u okviru poslova i zadataka obrađivati osobne podatke upoznaje se sa mjerama zaštite osobnih podataka.

(3) Prije neposrednog otpočinjanja obavljanja poslova vezanih za obradu osobnih podataka, kontrolor dodatno upoznaje zaposlenog sa konkretnim obvezama po pitanju zaštite osobnih podatka.

Članak 5.
(Tehničke mjere zaštite)

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

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

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

Član 6.
(Plan sigurnosti osobnih podataka)

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

a) da samo ovlaštene osobe mogu znati osobne podatke - povjerljivost;

b) da za vrijeme obrade osobni 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 osobnih podataka - autentičnost;

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

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

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

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

POGLAVLJE III. - ZAŠTITA OSOBNIH PODATAKA U AUTOMATSKOJ OBRADI

Članak 7.
(Tehničke mjere)

(1) Kontrolor pri automatskoj obradi osobnih podataka treba da osigura tehničke mjere zaštite osobnih 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 razdoblju koje ne može biti duže od šest mjeseci;

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

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

e) automatsku zabranu pristupa sustavu nakon tri neuspješna pokušaja prijavljivanja na sustav i automatsko upozorenje izvršitelju da potraži instrukciju od administratora zbirke osobnih podataka;

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

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

(2) U slučaju iz točke e. stavka (1) ovog članka administrator zbirke osobnih podataka odobrava daljnji pristup sustavu.

(3) Izvršitelj koji vrši kadrovske poslove, treba da izvještava administratora zbirke osobnih podataka o zaposlenju ili angažiranju svakog izvršitelja s pravom pristupa informacijskom sustavu, 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 stavka (3) ovog članka vrši se i prilikom bilo koje druge promjene radnog statusa izvršitelja, koja utječe na razinu ili obim pristupu zbirke osobnih podataka.

Članak 8.
(Organizacijske mjere)

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

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

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

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

d) svako iznošenje bilo kojeg medija koji sadrži osobne podatke izvan 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 osobni podaci; i

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

Članak 9.
(Mrežna barijera)

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

Članak 10.
(Pravo pristupa)

(1) Pristup podacima pohranjenim u zbirkama osobnih podataka dozvoljen je ovlaštenim osobama zaposlenim kod kontrolora ili obrađivača i ovlaštenim osobama zaduženim za održavanje i razvoj sustava za vođenje zbirki osobnih podataka.

(2) Kontrolor zbirke osobnih podataka određuje osobe iz stavka (1) ovoga članka.

(3) Obrađivač nema ovlaštenja za određivanje osobe iz stavka (1) ovog članka.

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

Članak 11.
(Sigurnosna preslika)

(1) Kontrolor je dužan da vrši redovito snimanje sigurnosnih preslika ili arhiviranje podataka u sustavu, da ne bi došlo do njihovog gubljenja ili uništenja.

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

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

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

Članak 12.
(Pristup u telekomunikacijski, računalski i aplikacijski sustav)

(1) Pristup u informacijski sustav za vođenje zbirki osobnih podataka ili obradu podataka iz zbirki dozvoljen je uz uporabu odgovarajućih korisničkih imena i pripadajućih propusnica.

(2) Kontrolor će evidentirati i kontrolirati svako pravo pristupa zaposlenih vanjskim mrežama, kao i pravo pristupa računalskim sustavima ili lokalnoj mreži korisnicima van računalskog sustava.

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

Članak 13.
(Obvezna uporaba jedinstvenih korisničkih imena i propusnica za pristup sustavu)

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

(2) Ukinuto korisničko ime ne smije se dodijeliti drugoj osobi.

(3) Korisničko ime i pripadajuća propusnica ne smiju se odati ili dati drugoj osobi.

(4) Način dodjeljivanja i obvezu izmjene propusnice određuje kontrolor zbirke osobnih podataka.

Članak 14.
(Evidencija, praćenje pristupa i pokušaj neovlaštenog pristupa sustavu)

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

(2) Svaki pokušaj neovlaštenog pristupa sustavu 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 osobnih podataka i izvršitelj dužni su obavijestiti odgovornu osobu u kontroloru zbirke osobnih podataka o svakom pokušaju neovlaštenog pristupa sustavu.

Članak 15.
(Osoba odgovorna za zaštitu osobnih podataka)

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

Članak 16.
(Osoba ovlaštena za dodjeljivanje korisničkih imena i propusnica)

Kontrolor zbirke osobnih podataka određuje osoba ovlaštena za dodjeljivanje i uklanjanje korisničkih imena i dodjeljivanje propusnica osobama ovlaštenim za rad u sustavu, a kojima je dozvoljen pristup zbirkama osobnih podataka.

Članak 17.
(Zaštita posebne kategorije osobnih podataka)

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

(2) Kontrolor poduzima dopunske tehničke i organizacijske mjere pri obradi posebnih kategorija osobnih podataka.

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

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

b) rad sa podacima tijekom redovitog radnog vremena kontrolora; i

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

Članak 18.
(Tjedno, mjesečno i godišnje provjeravanje rada sustava)

Kontrolor zbirke osobnih podataka tjedno, mjesečno i godišnje provjerava rad svih dijelova sustava.

IV. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 19.
(Nadzor)

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

Članak 20.
(Usklađivanje s odredbama Pravilnika)

(1) Kontrolori zbirki osobnih 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.

Članak 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. srpnja 2009. godine
Sarajevo

Predsjedatelj
Vijeća ministara BiH
Dr. **Nikola Špirić**, v. r.
