
UREDBA O NAČINU POHRANJIVANJA I POSEBNIM MJERAMA TEHNIČKE ZAŠTITE POSEBNIH KATEGORIJA OSOBNIH PODATAKA

(„Narodne novine“, broj 139/2004)

Izvor: www.propisi.hr



ISSN 1846-646X

© Copyright Centar za management i savjetovanje d.o.o. Sva prava zadržana.



UREDBA O NAČINU POHRANJIVANJA I POSEBNIM MJERAMA TEHNIČKE ZAŠTITE POSEBNIH KATEGORIJA OSOBNIH PODATAKA

(NN, br. broj 139/2004)

I. OPĆE ODREDBE

Članak 1.

Ovom Uredbom određuju se mjere, sredstva i uvjeti pohranjivanja, osiguranja i zaštite te prijenosa posebnih kategorija osobnih podataka i zbirke takvih podataka, mjere održavanja i provjere ispravnosti rada računalne, telekomunikacijske i programske opreme sustava za vođenje zbirke posebnih kategorija osobnih podataka (u daljnjem tekstu: sustav), osiguranje radnih prostorija u kojima je smještena ta oprema, osobe ovlaštene za provedbu predviđenih mjera te osobe odgovorne za nadzor nad provedbom tih mjera.

Odredbe ove Uredbe na odgovarajući se način primjenjuju i na zbirke posebnih kategorija osobnih podataka koje se ručno obrađuju.

Članak 2.

Pojedini izrazi u ovoj Uredbi imaju sljedeće značenje:

1. Sustav za vođenje zbirke osobnih podataka je sustav koji se sastoji od računalne, telekomunikacijske, upravljačke i programske opreme, te svih osobnih podataka koji se tim sustavom unose, pohranjuju i prenose.
2. Računalo za vođenje zbirke je računalo u koje je ugrađena upravljačka i programska oprema sustava za vođenje zbirke osobnih podataka.
3. Središnje računalo zbirke je računalo u koje je ugrađena upravljačka i programska oprema za obradu i pohranu zbirke osobnih podataka.
4. Razvojno računalo je računalo u koje je ugrađena potrebna upravljačka i programska oprema u razvitku, oprema koja se provjerava, te oprema potpuno jednaka opremi ugrađenoj u računala za vođenje zbirke osobnih podataka.
5. Administrator zbirke osobnih podataka je osoba ovlaštena brinuti o sustavu za upravljanje zbirkama osobnih podataka i o svim vidovima osiguranja i pohranjivanja podataka.
6. Administrator mrežnog sustava je osoba ovlaštena brinuti o telekomunikacijskoj opremi, pristupnim putevima, mreži, modemskim i drugim vezama između računalnih sustava.
7. Administrator upravljačkog sustava je osoba ovlaštena brinuti o ugradnji i ispravnom radu upravljačkog sustava i druge upravljačke programske opreme.
8. Uređaj za neprekidno napajanje je uređaj koji u slučaju prekida ili nestanka električne energije omogućava nesmetan nastavak rada računala i druge opreme kroz određeno kratko vrijeme, tako da se poslovi u tijeku mogu završiti bez opasnosti za cjelovitost informacija koje se tim računalom i opremom obrađuju, a računalo i druga oprema u tom vremenu mogu uredno utrnuti.
9. Pohranjivanje podataka sustava je postupak pohranjivanja sigurnosnog primjerka podataka za slučaj gubitka, oštećenja ili uništenja podataka.
10. Povrat pohranjenih podataka je postupak vraćanja podataka u prethodno stanje sa sigurnosnog primjerka nakon gubitka, oštećenja ili uništenja podataka pri čemu tako vraćen skup podataka mora biti u posljednjem sukladnom stanju i bez gubitka informacija.
11. Obnavljanje rada računalnog sustava je skup postupaka za povratak računalnog sustava i svih započetih poslova u posljednje sukladno stanje tog sustava.
12. Ponovno uključivanje sustava u rad je skup postupaka za uključivanje računalnog sustava u rad nakon neuobičajenog prekida rada tog sustava.

**UREDBA O NAČINU POHRANJIVANJA I POSEBNIM MJERAMA TEHNIČKE
ZAŠTITE POSEBNIH KATEGORIJA OSOBNIH PODATAKA**

(NN, br. broj 139/2004)

II. MJERE ZAŠTITE

Priključenje računala i druge opreme sustava

Članak 3.

Priključenje računalne, telekomunikacijske i druge opreme sustava na energetska mreža obavlja se prema uputama proizvođača te opreme, u skladu s važećim tehničkim normama.

Obveza uporabe uređaja za neprekidno napajanje

Članak 4.

Računala za vođenje zbirke osobnih podataka i središnja računala zbirke priključuju se na energetska mreža preko uređaja za neprekinuto napajanje.

Modemski priključci za pristup sustavu

Članak 5.

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

Smještanje, postavljanje i ugradnja računala i računalne mreže

Članak 6.

Računala za vođenje zbirke osobnih podataka, središnja računala zbirke i računalnu mrežu smješta, postavlja i ugrađuje stručna osoba uz odobrenje voditelja zbirke osobnih podataka, u skladu s važećim normama, standardima i tehničkim uputama, prema projektu. Po jedan primjerak projektne dokumentacije iz stavka 1. ovog članka čuva se u radnim prostorijama voditelja zbirke osobnih podataka i izvršitelja obrade ukoliko postoji, na sigurnom mjestu, a dostavlja na uvid Agenciji za zaštitu osobnih podataka.

Mehanizmi za osiguranje posebnih kategorija osobnih podataka

Članak 7.

Računalo za vođenje zbirke za obradu posebnih kategorija osobnih podataka i središnje računalo sustava mora biti opremljeno:

- mehanizmom za sigurnosno prijavljivanje za rad s mogućnošću pohrane podataka o prijavljivanju za rad kako bi se pristup računalima mogao nadzirati i ograničiti,
- mehanizmom za sprječavanje neovlaštenog iznosa i unosa podataka uporabom prijenosnih informatičkih medija, komunikacijskih priključaka i priključaka za ispis podataka,
- mehanizmom zaštite od računalnih virusa i drugih štetnih programa,
- mehanizmom kriptološkog osiguranja posebnih kategorija osobnih podataka na prijenosnim informatičkim medijima za pohranu i u toku prijenosa takvih podataka informatičkim i telekomunikacijskim sustavima.

UREDBA O NAČINU POHRANJIVANJA I POSEBNIM MJERAMA TEHNIČKE ZAŠTITE POSEBNIH KATEGORIJA OSOBNIH PODATAKA

(NN, br. broj 139/2004)

Pristup prostorijama s računalnom i telekomunikacijskom opremom

Članak 8.

Računalna i telekomunikacijska oprema postavlja se i ugrađuje u posebno zaštićene prostorije određene projektom.

U prostorije u kojima se nalaze središnja računala zbirke osobnih podataka ili računala za vođenje zbirke osobnih podataka smiju ulaziti samo ovlaštene osobe s posebnom dozvolom za ulaz.

Voditelj zbirke osobnih podataka ili izvršitelj obrade uz suglasnost voditelja zbirke osobnih podataka određuje ovlaštene osobe koje smiju ulaziti u prostorije iz stavka 2. ovoga članka. Prostorije iz stavka 2. ovog članka moraju biti opremljene sustavom video nadzora i elektroničkim dvostranim sustavom za kontrolu prolaza na ulaznim vratima kako bi se pristup takvim prostorijama i boravak u njima mogao ograničiti i nadzirati.

Pristup podacima sustava

Članak 9.

Pristup podacima pohranjenim u zbirkama osobnih podataka dozvoljen je ovlaštenim službenicima i namještenicima voditelja zbirke ili izvršitelja obrade (u daljnjem tekstu: ovlašteni zaposlenici), ovlaštenim osobama zaduženim za održavanje i razvitak sustava za vođenje zbirke osobnih podataka (u daljnjem tekstu: ovlašteni stručnjaci).

Voditelj zbirke osobnih podataka određuje osobe iz stavka 1. ovoga članka. Izvršitelj obrade nema ovlast za određivanje osoba iz stavka 1. ovog članka.

Zahtjev za pristup ili obradu te zahtjev za prestanak ovlasti za pristup zbirkama osobnih podataka ili obradu osobnih podataka podnosi se voditelju zbirke osobnih podataka koji daje ili ukida dozvolu za pristup zbirkama.

Pristup u telekomunikacijski, računalni i aplikacijski sustav

Članak 10.

Pristup u telekomunikacijski, računalni i aplikacijski sustav za vođenje zbirke osobnih podataka ili obradu podataka iz zbirke dozvoljen je uz uporabu odgovarajućih korisničkih imena i pripadnih propusnica.

Obveza uporabe jedinstvenih korisničkih imena i propusnica za pristup sustavu

Članak 11.

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

Ukinuto korisničko ime ne smije se dodijeliti drugoj osobi.

Korisničko ime i pripadna propusnica ne smiju se odati i dati na uporabu drugoj osobi.

Članak 12.

Način dodjeljivanja i obvezu izmjene propusnice određuje voditelj zbirke osobnih podataka.

UREDBA O NAČINU POHRANJIVANJA I POSEBNIM MJERAMA TEHNIČKE ZAŠTITE POSEBNIH KATEGORIJA OSOBNIH PODATAKA

(NN, br. broj 139/2004)

Evidencija, praćenje pristupa i pokušaja neovlaštenog pristupa sustavu

Članak 13.

Svaki pristup telekomunikacijskom i računalnom sustavu za vođenje zbirke osobnih podataka mora biti automatski zabilježen korisničkim imenom, nadnevkom i vremenom prijave i odjave.

Svaki pokušaj neovlaštenog pristupa sustavu mora biti automatski zabilježen korisničkim imenom, nadnevkom i vremenom, a ako je to moguće i mjestom s kojeg je takav pristup pokušan.

Izvršitelj obrade, administrator mrežnog sustava, administrator računala i administrator zbirke osobnih podataka dužni su obavijestiti čelnika voditelja zbirke osobnih podataka o svakom pokušaju neovlaštenog pristupa sustavu.

Mjere zaštite od požara

Članak 14.

Računalna i telekomunikacijska oprema sustava mora biti smještena u prostorijama koje imaju uređaje za otkrivanje požara i automatsku dojavu o izbijanju požara.

Prostorije u kojima je smještena oprema iz stavka 1. ovoga članka moraju imati uređaje za automatsko gašenje požara (temeljene na uporabi plina halona i sl.), a u blizini, ispred i u tim prostorijama, na vidljivim i lako uočljivim mjestima moraju biti izvještene upute o postupcima u slučaju izbijanja požara.

Mjere zaštite od električnog i magnetskog polja

Članak 15.

U blizini računalne i telekomunikacijske opreme ne smije biti izvora jakog električnog ili magnetskog polja.

Mjere zaštite od ionizirajućeg zračenja

Članak 16.

U blizini računalne i telekomunikacijske opreme ne smije biti izvora ionizirajućeg zračenja.

Mjere zaštite od elektrostatičkog elektriciteta

Članak 17.

U blizini opreme osjetljive na elektrostatički elektricitet ne smije biti izvora takvog elektriciteta.

Mjere zaštite od vlage, hladnoće i topline

Članak 18.

U prostorijama u kojima je smještena računalna i telekomunikacijska oprema mora se održavati relativna vlažnost zraka između 20 i 80% i temperatura između 5 i 30°C.

UREDBA O NAČINU POHRANJIVANJA I POSEBNIM MJERAMA TEHNIČKE ZAŠTITE POSEBNIH KATEGORIJA OSOBNIH PODATAKA

(NN, br. broj 139/2004)

Mjere zaštite od nagrizajućih i lakohlapljivih tekućina, eksplozivnih sredstava i sličnih tvari

Članak 19.

U prostorijama i u blizini prostorija u kojima je smještena oprema sustava, ne smiju se nalaziti nagrizajuće i lakohlapljive tekućine, eksplozivna sredstva i slične opasne ili štetne tvari.

Mjere zaštite od prašine

Članak 20.

U prostorijama u kojima su smještena računala ne smiju se nalaziti uređaji koji u zrak ispuštaju čestice prašine. Uređaji osjetljivi na prašinu moraju biti propisno zaštićeni. Posebno osjetljivi uređaji koji se hlade zrakom, moraju imati filtere za zrak. Uređaji za koje je to dopušteno tehničkim uputama moraju se pokrivati zaštitnim pokrovima za vrijeme kada nisu u uporabi.

Mjere zaštite u slučaju potresa ili drugih elementarnih nepogoda, rata i neposredne ratneopasnosti

Članak 21.

U slučaju potresa i drugih elementarnih nepogoda, rata i neposredne ratne opasnosti voditelj zbirke dužan je odrediti premještanje računalno-komunikacijske opreme na predviđeno sigurno mjesto.

Obveza pohranjivanja podataka

Članak 22.

Voditelj zbirke je dužan pohranjivati sve posebne kategorije osobnih podataka sustava na prenosive informatičke medije uporabom metoda koje jamče sigurnost i tajnost tako pohranjenih osobnih podataka.

Za provedbu mjera pohranjivanja podataka sustava na prenosive informatičke medije odgovaraju administratori zbirke osobnih podataka.

Dnevno, tjedno, mjesečno i godišnje pohranjivanje podataka

Članak 23.

Zbirke posebnih kategorija osobnih podataka obvezno se pohranjuju na prenosive informatičke medije dnevno, tjedno, mjesečno i godišnje, po završetku svih poslova vođenja zbirke osobnih podataka za potrebe obnove zbirke u slučaju požara, poplave, potresa ili neke druge nesreće u razredu više sile.

Podaci sustava pohranjuju se u onoliko dnevnih primjeraka koliko ima radnih dana u tjednu. Tjedno pohranjivanje podataka sustava provodi se posljednji radni dan u tjednu, nakon provedbe dnevnog pohranjivanja podataka. Podaci sustava pohranjuju se u onoliko tjednih primjeraka koliko u mjesecu ima posljednjih radnih dana u tjednu (4 ili 5).

Mjesečno pohranjivanje podataka sustava provodi se posljednji radni dan u mjesecu, za svaki mjesec posebice, u 12 primjeraka godišnje.

Godišnje pohranjivanje podataka sustava provodi se posljednji radni dan u godini. Svaki primjerak godišnje pohranjenih podataka čuva se u periodu određenom posebnim propisima.

UREDBA O NAČINU POHRANJIVANJA I POSEBNIM MJERAMA TEHNIČKE ZAŠTITE POSEBNIH KATEGORIJA OSOBNIH PODATAKA

(NN, br. broj 139/2004)

Najstariji primjerak prenosivog medija za dnevno, tjedno i mjesečno pohranjivanje podataka rabi se prilikom prvog slijedećeg dnevnog, tjednog odnosno mjesečnog pohranjivanja podataka.

Svaki primjerak pohranjenih podataka na prenosivom informatičkom mediju mora biti označen brojem, vrstom (dnevno, tjedno, mjesečno, godišnje), nadnevkom pohranjivanja, te imenom osobe koja je pohranjivanje provela.

Voditelj zbirke vodi evidenciju svih primjeraka prenosivih informatičkih medija na kojima su pohranjene zbirke posebnih kategorija osobnih podataka.

Zabranjeno je bez nadzora i odobrenja voditelja zbirke na bilo koji način umnožavanje informatičkih medija koji sadrže podatke iz zbirke posebnih kategorija osobnih podataka.

Oblast za provedbu pohranjivanja podataka

Članak 24.

Voditelj zbirke ili izvršitelj obrade određuje osobu ovlaštenu za provedbu postupka pohranjivanja podataka na prenosive informatičke medije.

Udaljenost spremanja pohranjenih podataka

Članak 25.

Podaci sustava dnevno pohranjeni na prenosive informatičke medije, spremaju se u sef u radnoj prostoriji voditelja zbirke.

Podaci sustava tjedno pohranjeni na prenosive informatičke medije, spremaju se na sigurno mjesto, udaljeno najmanje 20 kilometara od zgrade u kojoj je smještena zbirka osobnih podataka.

Podaci sustava mjesečno i godišnje pohranjeni na prenosive informatičke medije spremaju se na sigurno mjesto udaljeno najmanje 50 kilometara od zgrade u kojoj je smještena zbirka osobnih podataka.

Mjesto i oprema za pohranu sigurnosnih kopija

Članak 26.

Mjesto spremanja podataka sustava pohranjenih na prenosivim informatičkim medijima mora biti osigurano od elementarnih nepogoda.

Prenosivi informatički mediji s pohranjenim zbirkama osobnih podataka moraju biti spremljeni u vodootporni i vatrootporni sef.

Način prenošenja medija s pohranjenim zbirkama

Članak 27.

Prilikom prenošenja informatičkih medija s pohranjenim zbirkama posebnih kategorija osobnih podataka koriste se vodootporni i vatrootporni kovčezi zaštićeni šifrom.

**UREDBA O NAČINU POHRANJIVANJA I POSEBNIM MJERAMA TEHNIČKE
ZAŠTITE POSEBNIH KATEGORIJA OSOBNIH PODATAKA**

(NN, br. broj 139/2004)

Provjera ispravnosti sigurnosnih kopija

Članak 28.

Uporablјivost godišnje sigurnosne kopije zbirke posebnih kategorija osobnih podataka provjerava se najmanje jednom godišnje 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.

Uporablјivost mjesečne sigurnosne kopije zbirke posebnih kategorija osobnih podataka provjerava se najmanje svakih šest mjeseci uz jednake uvjete kao u stavku 1. ovog članka.

Vremenski razmaci provjere kakvoće medija

Članak 29.

Zbirke posebnih kategorija osobnih podataka pohranjene godišnje na prenosivim informatičkim medijima moraju se obnoviti nakon isteka polovice zajamčenog roka trajanja zapisa na toj vrsti medija.

Osobe odgovorne za provedbu mjera osiguranja, pohranjivanja i zaštite zbirke posebnih kategorija osobnih podataka

Članak 30.

Za urednu provedbu mjera osiguranja, pohranjivanja i zaštite osobnih podataka odgovara administrator zbirke osobnih podataka.

Osobe ovlaštene za izradu sigurnosnih kopija i povrat podataka

Članak 31.

Voditelj zbirke osobnih podataka ili izvršitelj obrade određuje osobe ovlaštene za izradu sigurnosnih kopija i povrat zbirke osobnih podataka.

Osobe ovlaštene za iznošenje i unošenje prenosivih informatičkih medija s pohranjenim zbirkama posebnih kategorija osobnih podataka

Članak 32.

Voditelj zbirke osobnih podataka određuje osobe ovlaštene za iznošenje podataka sustava pohranjenih na prenosivim informatičkim medijima iz prostorija voditelja zbirke ili izvršitelja obrade radi spremanja na udaljeno sigurno mjesto i vraćanje tih podataka u prostorije voditelja zbirke ili izvršitelja obrade.

Osobe ovlaštene za dodjelјivanje korisničkih imena i propusnica

Članak 33.

Voditelj zbirke osobnih podataka određuje osobe ovlaštene za dodjelјivanje i uklanjanje korisničkih imena i dodjelјivanje početnih propusnica osobama ovlaštenim za rad u sustavu i kojima je dozvolјen pristup zbirkama osobnih podataka.

**UREDBA O NAČINU POHRANJIVANJA I POSEBNIM MJERAMA TEHNIČKE
ZAŠTITE POSEBNIH KATEGORIJA OSOBNIH PODATAKA**

(NN, br. broj 139/2004)

*Sustav kriptološkog osiguranja posebnih kategorija osobnih podataka u prijenosu
informatičkim i telekomunikacijskim sustavom*

Članak 34.

Voditelj zbirke posebne kategorije osobnih podataka ustrojava sustav kriptološkog osiguranja posebnih kategorija osobnih podataka u prijenosu takvih podataka informatičkim i telekomunikacijskim sustavom drugim ovlaštenim korisnicima.

Ovjera podataka koji se prenose informatičkim i telekomunikacijskim sustavom

Članak 35.

Izvaci iz zbirke posebnih kategorija osobnih podataka koji se telekomunikacijskim putem šalju ovlaštenim osobama moraju biti kriptološki osigurani i ovjereni uporabom elektroničkog potpisa koji primatelju omogućuje provjeru izvornosti primljenog izvatka.

Provjera izvornosti podataka prenesenih iz zbirke posebnih kategorija osobnih podataka

Članak 36.

Primatelji izvatka iz zbirke posebnih kategorija osobnih podataka dužni su prilikom primitka izvatka telekomunikacijskim sustavom prethodno provjeriti izvornost primljenog izvatka uporabom javnog ključa pošiljatelja.

O primljenim izvacima bez potvrde izvornosti primatelj je dužan bez odgode obavijestiti voditelja zbirke osobnih podataka.

Tjedno, mjesečno i godišnje provjeravanje rada sustava

Članak 37.

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

Provjera utvrđenih mjera, postupaka i osoba ovlaštenih za osiguranje, pohranjivanje i zaštitu sustava

Članak 38.

Mjere, postupci i osobe ovlaštene za osiguranje, pohranjivanje i zaštitu sustava određuju se, ostvaruju i provjeravaju prema planu kojeg donosi voditelj zbirke osobnih podataka a u skladu s međunarodnim preporukama za to područje (ISO 17799).

Održavanje i popravak opreme sustava

Članak 39.

Računalnu i telekomunikacijsku opremu sustava održava i popravlja osoba određena ugovorom o nabavi opreme ili drugim odgovarajućim ugovorom.

Programsku opremu sustava održava i mijenja ovlašteni stručnjak.

Članak 40.

**UREDBA O NAČINU POHRANJIVANJA I POSEBNIM MJERAMA TEHNIČKE
ZAŠTITE POSEBNIH KATEGORIJA OSOBNIH PODATAKA**

(NN, br. broj 139/2004)

Nadzor nad provedbom odredbi ove Uredbe obavlja Agencija za zaštitu osobnih podataka.

III. PRIJELAZNE I ZAKLJUČNE ODREDBE

Usklađivanje s odredbama Uredbe

Članak 41.

Voditelji zbirki osobnih podataka i izvršitelji obrade dužni su u roku od šest mjeseci od dana stupanja na snagu ove Uredbe uskladiti mjere, sredstva i uvjete osiguranja, pohranjivanja i zaštite podataka s odredbama ove Uredbe.

Stupanje na snagu

Članak 42.

Ova Uredba stupa na snagu osmoga dana od dana objave u »Narodnim novinama«.