

Na temelju Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016.), na temelju Zakona o provedbi Opće uredbe o zaštiti podataka („Narodne novine“ broj 42/18) i na temelju članka 18. Statuta Hrvatske zaklade za znanost (KLASA: 110-02/22-01/01, URBROJ: 1-02/1-22-6) Upravni odbor Hrvatske zaklade za znanost na 118. sjednici održanoj 23. prosinca 2025. godine donosi

PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA

I. OPĆE ODREDBE

Članak 1.

Ovim Pravilnikom o zaštiti podataka (dalje u tekstu: Pravilnik) propisuju se općenite procedure i mjere za zaštitu osobnih podataka, sve sa svrhom poštovanja važećih propisa, izbjegavanja neovlaštenog uništavanja podataka, njihove izmjene ili gubitka, kao i neovlaštenog pristupa, obrade, korištenja ili prijenosa osobnih podataka.

Zaposlenici Hrvatska zaklada za znanost (dalje u tekstu: Zaklada) koji u svom poslu obrađuju i koriste osobne podatke moraju biti upoznati sa važećim propisima o zaštiti osobnih podataka, Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu: „Opća uredba o zaštiti podataka“ ili „Uredba“), iz područja zakonodavstva koje uređuje pojedinačno područje njihovog posla, sadržajem krovne politike zaštite informacija, politikom zaštite i sigurnosti podataka pojedinih područja poslovanja te politikom zaštite osobnih podataka iz sadržaja ovog Pravilnika.

Izrazi koji se koriste u ovom Pravilniku, a koji imaju rodno značenje, bez obzira koriste li se u muškom ili ženskom rodu, obuhvaćaju na jednak način muški i ženski rod.

Članak 2.

Pojmovi korišteni u ovom Pravilniku imaju sljedeće značenje:

- a) Uredba - Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/ EZ (Opća uredba o zaštiti podataka);
- b) Ispitanik - pojedinac čiji je identitet utvrđen ili se može utvrditi;
- c) Pojedinac čiji se identitet može utvrditi - osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca;
- d) Osobni podaci - svi podaci koji se odnose na ispitanika;
- e) Obrada - svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, automatiziranim i/ili neautomatiziranim sredstvima, kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na

raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;

- f) Voditelj obrade - fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka, a kada su svrhe i sredstva takve obrade utvrđeni pravom Europske unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Europske unije ili pravom države članice; Hrvatska zaklada za znanost, Ilica 24, 10000 Zagreb (dalje u tekstu: „Zaklada“ ili „voditelj obrade“);
- g) Izvršitelj obrade - fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade;
- h) Primatelj - fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana;
- i) Treća strana - fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade ni osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade;
- j) Osjetljivi podaci - predstavlja posebnu kategoriju osobnih podataka - podaci koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca;
- k) Trajni nosač podataka - svako sredstvo koje omogućuje pohranu podataka i kojem se može naknadno pristupiti tijekom određenog vremena u svrhe za koje su te informacije namijenjene i koje omogućuje nepromijenjenu reprodukciju pohranjenih informacija;
- l) Informacijski sustav - svaki materijalni i nematerijalni dio koji služi za prikupljanje, obradu, pohranu ili distribuciju informacija značajnih u poslovnom procesu;
- m) Poslovna tajna - podaci koji su kao poslovna tajna određeni zakonom, drugim propisom ili općim aktom voditelja obrade;
- n) Administrator sustava - ovlaštena fizička ili pravna osoba koju voditelj obrade ovlasti za obavljanje poslova vezanih uz održavanje sustava hardvera, softvera te drugih sustava vezanih uz poslovanje voditelja obrade koji se odnose na postupak informatizacije sustava poslovanja;
- o) Ustrojstvena jedinica - u smislu ovoga Pravilnika je interna organizacijska jedinica ili treća strana koja djeluje u ime i za račun voditelja obrade kao ugovorni partner odnosno kao vanjska organizacijska jedinica, a u čijem djelokrugu poslova se obrađuju osobni podaci ispitanika;
- p) Zaposlenik - označava sve zaposlenike odnosno radnike koji rade temeljem ugovora o radu (na određeno ili neodređeno vrijeme), kao i sve druge osobe koje obavljaju poslove za Zakladu bez zasnivanja radnog odnosa (stručno osposobljavanje bez zasnivanja radnog odnosa, ugovor o djelu, ugovor o djelu redovitog studenta, ugovor o autorskom djelu itd.).

II. NAČELA OBRADE PODATAKA

Članak 3.

Zaklada osobne podatke obrađuje zakonito, pošteno i transparentno s obzirom na ispitanika (načelo zakonitosti, poštenosti i transparentnosti) što, među ostalim, znači da:

- osobne podatke prikuplja samo u posebne, izričite i zakonite svrhe te ih dalje ne obrađuje na način koji nije u skladu s tim svrhama (načelo ograničavanja svrhe),
- obrađuje samo primjerene i relevantne osobne podatke koji su ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju (načelo smanjenja količine podataka),

- osobni podaci koje Zaklada obrađuje su točni te se po potrebi ažuriraju. One osobne podatke koji nisu točni, Zaklada bez odlaganja briše ili ispravlja (načelo točnosti),
- osobne podatke obrađuje sukladno važećim propisima Republike Hrvatske i Europske unije,
- osobne podatke obrađuje isključivo na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera (načelo cjelovitosti i povjerljivosti).

Kao voditelj obrade, Zaklada je odgovorna za usklađenost s odredbama Opće uredbe o zaštiti podataka te ostalih važećih propisa u području zaštite osobnih podataka te je mora biti u mogućnosti dokazati (načelo odgovornosti).

Pravne osnove za obradu osobnih podataka

Članak 4.

Obrada osobnih podataka u Zakladi zakonita je samo ako se temelji na kojoj od sljedećih pravnih osnova:

- a) obrada je nužna za izvršavanje zadaće od javnog interesa,
- b) obrada je nužna radi poštovanja pravnih obveza,
- c) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora,
- d) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe,
- e) obrada je nužna za potrebe legitimnih interesa Zaklade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete i
- f) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha.

Pravna osnova za obradu podataka iz stavka 1. točke a) i b) ovog članka utvrđuje se u pravu Europske unije ili u pravu Republike Hrvatske.

Privola ispitanika

Članak 5.

Zaklada obrađuje osobne podatke temeljem privole ispitanika samo ako ne postoji druga pravna osnova za obradu podataka iz članka 4. stavka 1. ovog Pravilnika.

Privola ispitanika mora biti dobrovoljna, napisana razumljivim, jasnim i jednostavnim jezikom s jasno naznačenom svrhom za koju se daje i bez nepoštenih uvjeta.

Ispitanik ima pravo u svakom trenutku povući svoju privolu. Povlačenje privole ne utječe na zakonitost obrade na temelju privole prije njezina povlačenja.

Obrada u drugu sukladnu svrhu

Članak 6.

U skladu s člankom 89. stavkom 1. Opće uredbe o zaštiti podataka, smatra se da je daljnja obrada u drugu svrhu u skladu sa svrhom u koju su podaci prvotno prikupljeni u sljedećim slučajevima:

- a) u svrhe arhiviranja u javnom interesu,
- b) u svrhe znanstvenog ili povijesnog istraživanja i
- c) u statističke svrhe.

Kada Zaklada obrađuje osobne podatke temeljem pravne osnove iz članka 4. stavka 1. točaka od c) do e) ovog Pravilnika koji su prikupljeni u prvotnu svrhu, tada ih smije obrađivati u drugu svrhu samo ako utvrdi da je takva obrada u skladu sa svrhom u koju su osobni podaci prvotno prikupljeni.

Prilikom utvrđivanja činjenice je li obrada u drugu svrhu u skladu sa svrhom u koju su podaci prvotno prikupljeni, Zaklada uzima u obzir, među ostalim, sljedeće:

- a) svaku vezu između prikupljanja osobnih podataka i svrhe namjeravanog nastavka obrade,
- b) kontekst u kojem su prikupljeni osobni podaci, posebno u pogledu odnosa između ispitanika i Zaklade,
- c) prirodu osobnih podataka, osobito činjenicu obrađuju li se posebne kategorije osobnih podataka u skladu s člankom 7. ovog Pravilnika ili osobni podaci koji se odnose na kaznene osude i kažnjiva djela u skladu s člankom 8. ovog Pravilnika,
- d) moguće posljedice namjeravanog nastavka obrade za ispitanike i
- e) postojanje odgovarajućih zaštitnih mjera.

Utvrdjivanje činjenice je li obrada u drugu svrhu u skladu s prvotnom svrhom, provodi organizacijska jedinica u kojoj je nastala potreba za obradom u drugu svrhu pri čemu obvezno traži mišljenje službenika za zaštitu podataka. O utvrđenju te činjenice sastavlja se službena bilješka koju potpisuje voditelj organizacijske jedinice ili druga ovlaštena osoba od odgovorne osobe Zaklade i kojoj se prilaže mišljenje službenika za zaštitu podataka.

Službenu bilješku u slučaju da ne postoji posebno ovlaštenje iz stavka 4. ovog članka potpisuje službenik za zaštitu podataka te o istima vodi evidenciju po službenoj dužnosti.

Ako je organizacijska jedinica u kojoj je nastala potreba za obradom podataka u drugu svrhu različita od organizacijske jedinice u kojoj su podaci prvotno prikupljeni, utvrđivanje činjenice iz stavka 2. ovog članka zajednički provode obje organizacijske jedinice. U tom slučaju, o utvrđenju je li obrada u drugu svrhu u skladu sa svrhom u koju su podaci prvotno prikupljeni, sastavlja se službena bilješka te službenik za zaštitu podataka ažurira evidencije aktivnosti obrade.

Obrada posebnih kategorija osobnih podataka

Članak 7.

Zaklada obrađuje osobne podatke koji sadrže i podatke o zdravlju, etničko podrijetlo, biometrijske podatke u svrhu jedinstvene identifikacije pojedinca, podatke koji se odnose na obiteljski život pojedinca te su u odnosu na navedene kategorije podataka ispunjeni sljedeći uvjeti:

- a) ispitanik je dao izričitu privolu za obradu tih osobnih podataka za jednu ili više određenih svrha, osim ako se pravom Europske unije ili Republike Hrvatske propisuje da ispitanik ne može ukinuti zabranu obrade tih posebnih kategorija osobnih podataka,

- b) obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava Zaklade ili ispitanika u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti u mjeri u kojoj je to odobreno u okviru prava Europske unije ili prava Republike Hrvatske,
- c) obrada je nužna za zaštitu životno važnih interesa ispitanika ili drugog pojedinca ako ispitanik fizički ili pravno nije u mogućnosti dati privolu,
- d) obrada se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik,
- e) obrada je nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva Zaklade,
- f) obrada je nužna za potrebe značajnog javnog interesa na temelju prava Europske unije ili prava Republike Hrvatske koje je razmjerno željenom cilju te kojim se poštuje bit prava na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika ili
- g) obrada je nužna u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s člankom 89. stavkom 1. Opće uredbe o zaštiti podataka na temelju prava Europske unije ili prava Republike Hrvatske koje je razmjerno cilju koji se nastoji postići te kojim se poštuje bit prava na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika.

Obrada osobnih podataka koji se odnose na kaznene osude i kažnjiva djela

Članak 8.

Zaklada može provoditi obradu osobnih podataka koji se odnose na kaznene osude i kažnjiva djela ili povezane mjere sigurnosti kada je obrada odobrena pravom Europske unije ili pravom Republike Hrvatske kojim se propisuju odgovarajuće zaštitne mjere za prava i slobode ispitanika.

III. PRAVILA O UVJETIMA I NAČINU INFORMIRANJA ISPITANIKA

Transparentnost informacija i modaliteti za ostvarivanja prava ispitanika

Članak 9.

Zaklada daje ispitaniku informacije iz članaka 10. i 11., članaka od 12. do 17. na sljedeći način:

- a) u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika,
- b) u pisanom obliku ili drugim sredstvima, među ostalim, ako je prikladno, elektroničkim putem. Ako to zatraži ispitanik, informacije se mogu pružiti usmenim putem ako je to primjenjivo odnosno ako Zaklada može dokazati takvo pružanje informacije (npr. snimanjem telefonskog razgovora ili potpisivanjem službene bilješke), pod uvjetom da je drugim sredstvima utvrđen identitet ispitanika i
- c) bez nepotrebnog odgađanja i u svakom slučaju u roku od mjesec dana od dana zaprimanja zahtjeva.

Iznimno od stavka 1. točke c) ovog članka, rok od mjesec dana može se prema potrebi produžiti za dodatna dva mjeseca, uzimajući u obzir složenost i broj zahtjeva. Zaklada obavještava ispitanika o svakom takvom produženju u roku od mjesec dana od dana zaprimanja zahtjeva, uz navođenje razloga produženja roka.

Pri obavještanju ispitanika o produženju roka iz stavka 2. ovog članka ispitaniku se dostavlja Obavijest o produženju razdoblja očitovanja ispitanika pod prilogom 20. koja se, po potrebi, prilagođava ovisno o razlozima produženja.

Ako Zaklada ne postupi po zahtjevu ispitanika, dužna je bez odgađanja, a najkasnije u roku od mjesec dana od dana zaprimanja zahtjeva ispitanika, izvijestiti ispitanika o razlozima zbog kojih nije postupila te o mogućnosti podnošenja pritužbe Agenciji za zaštitu osobnih podataka (u daljnjem tekstu: „AZOP“) i pravu na sudsku zaštitu.

Informacije iz stavka 1. ovog članka Zaklada daje ispitaniku bez naknade. Ako su zahtjevi ispitanika očito neutemeljeni ili pretjerani, osobito zbog njihova učestalog ponavljanja, Zaklada može:

- a) naplatiti razumnu naknadu, uzimajući u obzir administrativne troškove pružanja informacija ili postupanja po zahtjevu ili
- b) odbiti postupiti po zahtjevu.

Teret dokaza očigledne neutemeljenosti ili pretjeranosti zahtjeva je na Zakladi.

Ako Zaklada ima sumnju u pogledu identiteta ispitanika koji podnosi zahtjev na temelju ovog Pravilnika, tada može tražiti pružanje dodatnih informacija neophodnih za potvrđivanje identiteta ispitanika.

Informacije iz stavka 1. ovog članka objavljuju se i na odgovarajućem mjestu na internetskim stranicama i/ili na drugi odgovarajući način, ako je to prikladno, kako bi se na lako vidljiv, razumljiv i jasno čitljiv način pružio smislen pregled namjeravane obrade.

Informacije iz članka od 12. do 18. ovog Pravilnika Zaklada daje putem službenika za zaštitu podataka.

Informacije koje se daju ako se osobni podaci prikupljaju od ispitanika

Članak 10.

Ako su osobni podaci koji se odnose na ispitanika prikupljeni od ispitanika, Zaklada u trenutku prikupljanja osobnih podataka daje ispitaniku sljedeće osnovne informacije:

- a) naziv i kontaktne podatke Zaklade, kao voditelja obrade,
- b) kontaktne podatke službenika za zaštitu podataka,
- c) svrhu obrade i pravnu osnovu za obradu osobnih podataka,
- d) ako se obrada temelji na članku 4. stavku 1. točki e) ovog Pravilnika, legitimne interese Zaklade ili treće strane,
- e) primatelje ili kategorije primatelja osobnih podataka, ako ih ima,
- f) ako je primjenjivo, činjenicu da Zaklada namjerava osobne podatke prenijeti trećoj zemlji ili međunarodnoj organizaciji te postojanje ili nepostojanje odluke Europske komisije o primjerenosti ili u slučaju prijenosa iz članaka 46. ili 47. ili članka 49. stavka 1. drugog podstavka Opće uredbe o zaštiti podataka, upućivanje na prikladne ili odgovarajuće zaštitne mjere i načine pribavljanja njihove kopije ili mjesta na kojem su stavljene na raspolaganje,
- g) razdoblje u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterije za utvrđivanje tog razdoblja,

- h) postojanje prava da se od Zaklade zatraži pristup osobnim podacima i ispravak ili brisanje osobnih podataka ili ograničavanje obrade koji se odnose na ispitanika ili prava na ulaganje prigovora na obradu takvih te prava na prenosivost podataka,
- i) ako se obrada temelji na članku 4. stavku 1. točki f) ili članku 7. stavku 1. točki a) ovog Pravilnika, postojanje prava da se u bilo kojem trenutku povuče privola, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije nego što je ona povučena,
- j) pravo na podnošenje pritužbe AZOP-u i
- k) informaciju o tome je li pružanje osobnih podataka zakonska ili ugovorna obveza ili uvjet nužan za sklapanje ugovora te ima li ispitanik obvezu pružanja osobnih podataka i koje su moguće posljedice ako se takvi podaci ne pruže.

Ako Zaklada namjerava dodatno obrađivati osobne podatke u svrhu koja je različita od one za koju su osobni podaci prikupljeni, Zaklada prije te dodatne obrade ispitaniku pruža informacije o drugoj svrsi te sve druge relevantne informacije iz stavka 1. točaka od g) do k) ovog članka.

Zaklada nije dužna dati ispitaniku informacije iz stavaka 1. i 2. ovog članka ako i u onoj mjeri u kojoj ispitanik već raspolaže informacijama.

Informacije koje se daju ako osobni podaci nisu dobiveni od ispitanika

Članak 11.

Ako osobni podaci nisu dobiveni od ispitanika, Zaklada daje ispitaniku sljedeće osnovne informacije:

- a) naziv i kontaktne podatke Zaklade, kao voditelja obrade,
- b) kontaktne podatke službenika za zaštitu podataka,
- c) svrhu obrade i pravnu osnovu za obradu osobnih podataka,
- d) kategorije osobnih podataka o kojima je riječ,
- e) primatelje ili kategorije primatelja osobnih podataka, prema potrebi i ako je primjenjivo, namjeru Zaklade da osobne podatke prenese primatelju u trećoj zemlji ili međunarodnoj organizaciji te postojanje ili nepostojanje odluke Europske komisije o primjerenosti, ili u slučaju prijenosa iz članka 46. ili 47., ili članka 49. stavka 1. drugog podstavka Opće uredbe o zaštiti podataka upućivanje na prikladne ili odgovarajuće zaštitne mjere i načine pribavljanja njihove kopije ili mjesta na kojem su stavljene na raspolaganje,
- f) razdoblje u kojem će se osobni podaci pohranjivati ili, ako to nije moguće, kriterije za utvrđivanje tog razdoblja,
- g) ako se obrada temelji na članku 4. stavku 1. točki e) ovog Pravilnika, legitimne interese Zaklade ili treće strane,
- h) postojanje prava ispitanika iz članaka od 12. do 17. ovog Pravilnika,
- i) ako se obrada temelji na članku 4. stavku 1. točki f) ili članku 7. stavku 1. točki a) ovog Pravilnika, postojanje prava da se u bilo kojem trenutku povuče privola, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije nego što je ona povučena,
- j) pravo na podnošenje pritužbe AZOP-u i
- k) izvor osobnih podataka i, prema potrebi, dolaze li iz javno dostupnih izvora.

Zaklada daje informacije iz stavka 1. ovog članka:

- a) unutar razumnog roka nakon dobivanja osobnih podataka, a najkasnije u roku od jednog mjeseca, uzimajući u obzir posebne okolnosti obrade osobnih podataka,
- b) ako se osobni podaci trebaju upotrebljavati za komunikaciju s ispitanikom, najkasnije u trenutku prve komunikacije ostvarene s tim ispitanikom i
- c) ako je predviđeno otkrivanje podataka drugom primatelju, najkasnije u trenutku kada su osobni podaci prvi put otkriveni.
- a) ako Zaklada namjerava dodatno obrađivati osobne podatke u svrhu koja je različita od one za koju su osobni podaci dobiveni, tada prije te dodatne obrade daje ispitaniku informacije o toj drugoj svrsi te sve druge relevantne informacije iz stavka 1. točaka od g) do l) ovog članka.
- b) nije dužna dati ispitaniku informacije iz stavaka od 1. do 3. ovog članka ako i u mjeri u kojoj:
 - ispitanik već posjeduje informacije,
 - pružanje takvih informacija je nemoguće ili bi zahtijevalo nerazmjerne napore; posebno za obrade u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, podložno uvjetima i zaštitnim mjerama iz članka 89. stavka 1. Opće uredbe o zaštiti podataka ili u mjeri u kojoj je vjerojatno da se obvezom iz stavka 1. ovog članka može onemogućiti ili ozbiljno ugroziti postizanje ciljeva te obrade. U takvim slučajevima Zaklada poduzima odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa ispitanika, među ostalim stavljanjem informacija na raspolaganje javnosti,
 - dobivanje ili otkrivanje podataka izrijeком je propisano pravom Europske unije ili pravom Republike Hrvatske, a koje predviđa odgovarajuće mjere zaštite legitimnih interesa ispitanika ili
 - ako osobni podaci moraju ostati povjerljivi u skladu s obvezom čuvanja profesionalne tajne, odnosno poslovne tajne koju uređuje pravo Europske unije ili pravo Republike Hrvatske, uključujući zakonsku obvezu čuvanja povjerljivosti informacija.

IV. PRAVA ISPITANIKA

Pravo na pristup osobnim podacima

Članak 12.

Ispitanik ima pravo dobiti od Zaklade potvrdu o tome obrađuju li se osobni podaci koji se odnose na njega te ako se takvi podaci obrađuju, pristup osobnim podacima i sljedećim informacijama:

- a) svrsi obrade,
- b) kategorijama osobnih podataka o kojima je riječ,
- c) primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, osobito primateljima u trećim zemljama ili međunarodnim organizacijama,
- d) ako je to moguće, predviđenom razdoblju u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterijima korištenima za utvrđivanje tog razdoblja,
- e) postojanju prava da se od Zaklade zatraži ispravak ili brisanje osobnih podataka ili ograničavanje obrade osobnih podataka koji se odnose na ispitanika ili prava na prigovor na takvu obradu,
- f) pravu na podnošenje pritužbe AZOP-u,
- g) ako se osobni podaci ne prikupljaju od ispitanika, svakoj dostupnoj informaciji o njihovom izvoru i postojanju ili nepostojanju automatiziranog donošenja odluka i

- h) ako se osobni podaci prenose u treću zemlju ili međunarodnu organizaciju, ispitanik ima pravo biti informiran o odgovarajućim zaštitnim mjerama u skladu s člankom 46. Opće uredbe o zaštiti podataka koje se odnose na prijenos.

Zaklada je dužna, na zahtjev ispitanika, dati ispitaniku kopiju njegovih osobnih podataka koje obrađuje. Za sve dodatne kopije koje zatraži ispitanik Zaklada može naplatiti razumnu naknadu na temelju administrativnih troškova. Ako ispitanik podnese zahtjev elektroničkim putem, informacije se pružaju u elektroničkom obliku, osim ako ispitanik zatraži drukčije.

Prilikom ostvarivanja prava ispitanika iz stavka 2. ovog članka, Zaklada osigurava da se time ne utječe negativno na prava i slobode drugih (npr. anonimiziranjem dokumenta u dijelu koji se ne odnosi na ispitanika).

Pravo na ispravak osobnih podataka

Članak 13.

Zaklada je dužna, bez nepotrebnog odgađanja, samostalno ili na zahtjev ispitanika, ispraviti osobne podatke koji se odnose na ispitanika. Uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave.

Pravo na brisanje osobnih podataka

Članak 14.

Ispitanik ima pravo od Zaklade ishoditi brisanje osobnih podataka koji se na njega odnose, a Zaklada ima obvezu obrisati osobne podatke, bez nepotrebnog odgađanja, ako je ispunjen jedan od sljedećih uvjeta:

- a) osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni,
- b) ispitanik povuče privolu na kojoj se obrada temelji, a iz zahtjeva je razvidno da ispitanik želi obrisati podatke u odnosu na čiju obradu povlači privolu te ako ne postoji druga pravna osnova za obradu,
- c) ispitanik uloži prigovor na obradu te ne postoje jači legitimni razlozi za obradu,
- d) osobni podaci nezakonito su obrađeni ili
- e) osobni podaci moraju se brisati radi poštovanja pravne obveze iz prava Unije ili prava Republike Hrvatske.

Stavak 1. ovog članka može se ne primjenjivati ili se ne primjenjuje u mjeri u kojoj je obrada nužna:

- a) radi ostvarivanja ustavnih prava ili jačih prava drugih kategorija ispitanika ili prava na slobodu izražavanja i informiranja,
- b) radi poštovanja pravne obveze kojom se zahtijeva obrada u pravu Europske unije ili pravu Republike Hrvatske ili za izvršavanje zadaće od javnog interesa,
- c) u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u mjeri u kojoj je vjerojatno da se pravom na brisanje može onemogućiti ili ozbiljno ugroziti postizanje ciljeva te obrade ili
- d) radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

Hodogram brisanja podataka pod Prilogom 18. ovog Pravilnika primjenjuje se u situacijama kada je ispitanik zatražio brisanje.

Pravo na ograničenje obrade osobnih podataka

Članak 15.

Ispitanik ima pravo zatražiti od Zaklade ograničenje obrade osobnih podataka ako je ispunjen jedan od sljedećih razloga:

- a) ispitanik osporava točnost osobnih podataka, na razdoblje kojim se Zakladi omogućuje provjera točnosti osobnih podataka,
- b) obrada je nezakonita i ispitanik se protivi brisanju osobnih podataka te umjesto toga traži ograničenje njihove uporabe,
- c) Zaklada više ne treba osobne podatke za potrebe obrade, ali ih ispitanik traži radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva ili
- d) ispitanik je uložio prigovor na obradu očekujući potvrdu nadilaze li legitimni razlozi Zaklade razloge ispitanika.

Ako je obrada ograničena prema stavku 1. ovog članka, takvi osobni podaci smiju se obrađivati samo uz privolu ispitanika i/ili na temelju drugih propisanih pravnih osnova u slučajevima u kojima je to moguće, uz iznimku pohrane, ili za postavljanje, ostvarivanje ili obranu pravnih zahtjeva ili zaštitu prava druge fizičke ili pravne osobe ili zbog važnog javnog interesa Europske unije ili Republike Hrvatske.

Ispitanika koji je ishodio ograničenje obrade na temelju stavka 1. ovog članka Zaklada izvješćuje prije nego što ograničenje obrade bude ukinuto.

Pravo na prenosivost osobnih podataka

Članak 16.

Ispitanik ima pravo zaprimiti osobne podatke koji se odnose na njega, a koje je Zaklada pružila u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te ih prenijeti drugom voditelju obrade bez ometanja od strane Zaklade samo ako su kumulativno ispunjeni sljedeći uvjeti:

- a) obrada se temelji na privoli ili na ugovoru i
- b) obrada se provodi automatiziranim putem.

Prilikom ostvarivanja svojih prava na prenosivost podataka na temelju stavka 1. ovog članka ispitanik ima pravo na izravni prijenos od Zaklade do drugog voditelja obrade ako je to tehnički izvedivo.

Ostvarivanjem prava na prenosivost osobnih podataka ne dovodi se u pitanje pravo na brisanje.

Pravo na prenosivost osobnih podataka ne primjenjuje se na obradu koja je potrebna za ostvarivanje zakonom utvrđenih ciljeva i izvršavanje zakonskih obveza Zaklade.

U osiguravanju prava na prijenos osobnih podataka ispitanika sukladno ovom članku, Zaklada mora voditi računa da se time ne utječe negativno na prava i slobode drugih.

Pravo na prigovor na obradu osobnih podataka

Članak 17.

Ispitanik ima pravo u svakom trenutku uložiti prigovor na obradu osobnih podataka koji se odnose na njega. Zaklada u tom slučaju više ne obrađuje osobne podatke, osim ako Zaklada ne dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

Zaklada izričito skreće pozornost ispitaniku na pravo na prigovor najkasnije u trenutku prve komunikacije s ispitanikom, na jasan način i odvojeno od bilo koje druge informacije.

Ako Zaklada obrađuje osobne podatke u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, ispitanik ima pravo uložiti prigovor na obradu osobnih podataka koji se na njega odnose, osim ako je obrada potrebna za ostvarivanje zakonom utvrđenih ciljeva i izvršavanje zakonskih obveza Zaklade.

Obveza izvješćivanja

Članak 18.

Zaklada priopćuje svaki ispravak ili brisanje osobnih podataka ili ograničenje obrade svakom primatelju kojem su otkriveni osobni podaci, osim ako se to pokaže nemogućim ili zahtijeva nerazmjeran napor. Zaklada obavješćuje ispitanika o tim primateljima, ako to ispitanik zatraži.

Podnošenje zahtjeva za ostvarivanje prava Ispitanika

Članak 19.

Radi ostvarenja svojih prava iz članaka od 12. do 17. ovog Pravilnika, ispitanik može podnijeti zahtjev Zakladi uporabom odgovarajućeg obrasca koji se nalazi u Prilogu 1. ovog Pravilnika i čini njegov sastavni dio.

Zahtjev iz stavka 1. ovog članka može se podnijeti i poštom na adresu Zaklade, za službenika za zaštitu podataka, ili na odgovarajuću adresu elektroničke pošte koja je objavljena na internetskoj stranici Zaklade.

U slučaju zaprimanja neurednog ili nepotpunog zahtjeva, Zaklada putem službenika za zaštitu podataka poziva ispitanika da takve nedostatke ukloni koristeći se Dopisom za pojašnjenje zahtjeva ispitanika pod Prilogom 21. ovog Pravilnika.

Postupanje po zahtjevu ispitanika

Članak 20.

Zaprimljeni zahtjev za ostvarivanje prava ispitanika iz članka 19. ovog Pravilnika, službenik za zaštitu podataka može proslijediti nadležnoj organizacijskoj jedinici ili drugoj odgovornoj osobi.

Organizacijska jedinica ili odgovorne osobe Zaklade dužne su u najkraćem mogućem roku od zaprimanja dostaviti službeniku za zaštitu podataka sve potrebne informacije u vezi sa zahtjevom.

Na temelju informacija iz stavka 2. ovog članka, službenik za zaštitu podataka daje ispitaniku tražene informacije, odnosno daje odgovor na njegov zahtjev.

Sve zahtjeve ispitanika službenik za zaštitu podataka bilježi u Evidenciji zahtjeva ispitanika pod Prilogom 15. ovog Pravilnika.

V. VODITELJ OBRADE

Članak 21.

Voditelj obrade izvršava organizacijske, tehničke i organizacijske mjere iz ovog Pravilnika i/ili iz drugih akata kojima se uređuje detaljnije pitanje tehničkih i sigurnosnih mjera zaštite i to na sljedeći način:

- a) da raspolaže prostorijama, opremom i sistemskom računalnom opremom, uključujući i uređaje za evidenciju ulaza i izlaza,
- b) da sprječava neovlašteni pristup osobnim podacima pri njihovom prijenosu, uključujući i putem telekomunikacijskih sredstava i putem mreže,
- c) da osigurava učinkovit način blokiranja, uništenja ili brisanja osobnih podataka te
- d) da osigurava organizacijsku, kadrovsku i tehničku zaštitu osobnih podataka u poslovanju voditelja obrade.

Poslove iz stavka 1. voditelj obrade provodi u skladu s mjerama koje su definirane i usvojene ovim Pravilnikom, ali i drugim aktima kojima se detaljnije uređuje pitanje provođenja sigurnosnih politika Zaklade.

VI. SIGURNOSNE MJERE, ZAŠTITA PROSTORIJA I RAČUNALNE OPREME

Članak 22.

Sigurnosne politike obuhvaćaju, ali se ne ograničavaju na mjere kojima se detaljnije uređuje način korištenja i zaštite računala, aplikacije, mrežne poslužitelje, mrežne uređaje i mrežnu infrastrukturu informacijskog sustava putem kojih se pristupa informacijskom sustavu te sistemski i korisnički softver, koji se koristi u pojedinim dijelovima informacijskog sustava.

Prostorije u kojima se nalaze trajni nosači podataka, strojna (hardver) i programska (softver) oprema, moraju biti osigurani raznim organizacijskim sredstvima koje sprječavaju neovlašteni pristup podacima (dalje: zaštićeni prostori).

Zaštićeni prostori su zaštićeni sustavom kontrole pristupa, kao i protupožarnim sustavima (u nastavku teksta: sustavi tehničke zaštite).

Voditelj obrade vodi evidencije osoba koje imaju ključeve i/ili lozinke za ulazak u zaštićene prostore.

Izvan radnog vremena i tijekom odsutnosti zaposlenika voditelja obrade ili koje druge ovlaštene osobe, računala i druga računalna oprema moraju biti ugašeni i zaključani fizički ili putem programa.

Zaposlenik koji privremeno napušta radno mjesto, dužan je programski zaključati računalno (engl. „Lock“) radi sprječavanja neovlaštenog pristupa.

Na računalima gdje to nije moguće, potrebno je završiti rad u svim aktivnim programima i odjaviti se s računala.

Sva računala moraju biti sustavno podešena na način da se automatski nakon isteka 30 minuta neaktivnosti korisnika zaključavaju.

Osobe iz stavka 6. ovog članka ne smiju davati ključeve ili lozinke trećim osobama, ne smiju ostavljati ključeve i lozinke na mjestima kojima mogu pristupiti drugi zaposlenici te ne smiju ostavljati ključ u ključanici s vanjske strane.

Osjetljivi podaci ne smiju se iznositi izvan zaštićenih prostora **Članak 23.**

Trajni nosači podataka i monitori na kojima se prikazuju osobni podaci, a koji se nalaze u prostorijama u kojima su prisutne treće strane, moraju se čuvati na način da im treće strane nemaju pristup ili uvid.

Članak 24.

Održavanje i popravak strojne i računalne opreme dopušten je pod uvjetom da se obavijesti ovlaštena osoba te se može obavljati isključivo u za to ovlaštenim servisima.

Osoblje za održavanje opreme iz stavka 1. ovog članka mora imati potpisan odgovarajući ugovor s voditeljem obrade.

Članak 25.

Osobe ovlaštene za održavanje strojne i programske opreme, posjetitelji i poslovni partneri mogu biti u zaštićenim prostorima samo uz prisutnost ovlaštene osobe voditelja obrade.

Osoblje koje pruža usluge čišćenja prostorija te zaštitarsko osoblje i druge osobe ne mogu izvan radnog vremena boraviti ili se zadržavati u zaštićenim prostorima bez prethodne najave ili odobrenja.

Zaposlenici trećih strana koje su angažirane od strane Zaklade moraju imati potpisanu izjavu o povjerljivosti u svim slučajevima u kojima imaju pristup osobnim podacima ispitanika Zaklade makar i uvidom.

VII. ZAŠTITA SISTEMSKE I KORISNIČKE RAČUNALNE OPREME TE PODATAKA KOJI SE OBRAĐUJU PUTEM RAČUNALNE OPREME

Članak 26.

Voditelj obrade je odgovoran za izradu i redovito ažuriranje dokumentacije mrežne infrastrukture u opsegu sustava koji je pod njegovim upravljanjem.

Dokumentacija mrežne infrastrukture obuhvaća, ali se ne ograničava na:

- a) dijagram trenutnog stanja računalne mreže,
- b) pristupne liste između segmenata računalne mreže i vanjskih mreža,
- c) opis sučelja prema vanjskim mrežama.

Dijagram mrežne infrastrukture mora oslikavati trenutno stanje izvedbe računalne mreže kako bi se u slučaju incidentnog događaja i/ili problema u radu računalne mreže omogućila pravovremena identifikacija problema i njegovo rješavanje.

Dijagram mrežne infrastrukture mora biti na razini detaljnosti koja omogućava jednostavnu identifikaciju svih komponenti mrežne infrastrukture, uz oznake računalnih mreža, IP adresa, DNS imena, inačica operacijskih sustava i modela uređaja.

Pristup dokumentaciji mrežne infrastrukture potrebno je omogućiti isključivo onim zaposlenicima koji za to imaju poslovnu potrebu.

Dokumentacija mora biti pohranjena na način koji će omogućiti jednostavnu i jednoznačnu identifikaciju aktualne inačice dokumentacije mrežne infrastrukture.

Članak 27.

Udaljeni pristup svim mrežnim uređajima koji imaju mogućnost upravljanja i konfiguracije, zaštićen je zaporkom.

Pristup informacijskom sustavu mora biti zaštićen na način da se pristup dopusti samo unaprijed određenim zaposlenicima ili fizičkim ili pravnim osobama koje na temelju sklopljenih ugovora pružaju određene usluge voditelju obrade (dalje u tekstu: „izvršitelji obrade“).

Zaposlenici i druge ovlaštene osobe moraju svoje ovlasti za pristup informacijskom sustavu koristiti isključivo za vlastiti rad te ne smiju drugome omogućiti njihovo korištenje.

Zaposlenici i druge neovlaštene osobe ne smiju pokušati pristupiti nijednom podatku ili programu za koji nemaju dozvolu pristupa ili izričitu suglasnost odgovorne osobe voditelja obrade.

Zabranjeno je pristupati računalnom sustavu koristeći lozinku i korisničke ovlasti druge osobe.

Pristup informacijskom sustavu imaju i tijela u slučaju provedbe nadzora nad poslovanjem voditelja obrade.

Zaposlenici ne smiju instalirati programsku opremu bez znanja osoba zaduženih za rad računalnog informacijskog sustava.

Zaposlenici bez odobrenja ovlaštene osobe i znanja osoba zaduženih za rad računalnog informacijskog sustava, ne smiju iznositi programsku opremu izvan prostorija voditelja obrade.

Članak 28.

Ispravljanje, izmjena i ažuriranje sistemske i korisničke računalne opreme dopušteno je jedino uz odobrenje ovlaštene osobe i može se provoditi samo u ovlaštenim servisima i organizacijama te s osobljem koji na temelju sklopljenih ugovora pružaju određene usluge voditelju obrade.

Ispravljanje, izmjena i ažuriranje sistemske i korisničke računalne opreme mora biti ispravno dokumentirane od strane pružatelja usluge.

Članak 29.

Za pohranu i zaštitu programske opreme na adekvatan način primjenjuju se članci ovog Pravilnika ili odredbe drugih internih akata koji uređuju postupak čuvanja podataka.

Članak 30.

Voditelj obrade odnosno osoba koja je ovlaštena od strane voditelja obrade dužna je redovito provjeravati sadržaj mrežnog diska i lokalnih direktorija, u kojima su pohranjeni osobni podaci zaštićeni od računalnih virusa.

U slučaju pojave računalnog virusa isti se mora ukloniti što je prije moguće od strane ovlaštenih osoba voditelja obrade i/ili izvršitelja obrade te se mora identificirati uzrok pojave virusa u informacijskom sustavu voditelja obrade.

Stavci 1. i 2. ovog članka primjenjuju se i u slučaju prijenosa datoteke s računala koja nisu u vlasništvu voditelja obrade.

Članak 31.

Zaposlenici ne smiju namještati programsku opremu bez znanja i dopuštenja osobe odgovorne za rad računalnog informacijskog sustava.

Nije dopušteno iznošenje programske opreme i trajnih nosača na kojima se osobni podaci čuvaju izvan prostorija voditelja obrade, bez znanja i odobrenja izravno nadređene odgovorne osobe ili osobe koju je voditelj obrade ovlastio da obavlja poslove informacijske sigurnosti.

Zaposlenici ne smiju kopirati, instalirati ili izvoditi programe kojima je svrha otkrivati sigurnosne slabosti na sustavu te ne smiju neovlašteno izvoditi programe za prikupljanje podataka o informacijskom sustavu.

U slučaju pojave potrebe za enkripcijom podataka, zaposlenik može upotrijebiti softver za enkripciju podataka koji je odobren od strane voditelja obrade.

Zaposlenici ne smiju izrađivati kopije konfiguracijskih i sistemskih datoteka, ne smiju takve datoteke neovlašteno koristiti, ne smiju ih koristiti za namjenu koja je različita od osnovne namjene te ih ne smiju neovlašteno davati na uvid drugim osobama.

Članak 32.

Pristup podacima korisničkog softvera zaštićen je korisničkim imenom i lozinkom za autorizaciju i identifikaciju programa i korisničkih podataka.

Sistem lozinke mora pružiti mogućnost naknadne procjene sljedećeg:

- a) kada su određeni osobni podaci upisani u bazu podataka, kada se koriste ili na drugi način obrađuju i
- b) tko je izvršio neku od prethodno navedenih radnji.

Administrator sustava, na temelju pisanog zahtjeva odgovorne osobe, dodjeljuje ovlaštenim zaposlenicima korisničko ime i lozinku, kako bi mogli pristupiti dijelovima informacijskog sustava.

Korisničko ime iz stavka 3. ovog članka identificira korisnika informacijskog sustava, a lozinka služi za autorizaciju prava pristupa informacijskom sustavu.

Za pristup različitim dijelovima informacijskog sustava korisnicima mogu biti dodijeljeni različiti korisnički računi i lozinke.

Korisnici su dužni lozinke redovito mijenjati i držati tajnima.

Svaki otvoreni račun za pristup informacijskom sustavu mora imati svog vlasnika, odnosno, nije dopušteno korištenje generičkih računa za ostvarivanje prava pristupa na sustav (npr. gost, admin, administrator, user i sl.).

Svaki je zaposlenik odgovoran za zaštitu svih informacija korištenih ili spremljenih posredstvom vlastitih korisničkih ovlasti.

Zaposlenici su odgovorni za sve transakcije i aktivnosti koje se obave s dodijeljenim korisničkim računom te ne smiju otkriti ili dijeliti korisničke račune i lozinke s drugim osobama.

Članak 33.

Postupak određivanja lozinki odnosno način dodjeljivanja, pohrana i mijenjanje lozinki, predlaže voditelj obrade ili osoba koju on za to ovlasti.

Pri izboru i primjeni lozinki, administrator sustava dužan je poštovati sljedeće smjernice:

- a) lozinke moraju sadržavati najmanje 10 znakova s primjenom znamenki i simbola,
- b) ne smiju sadržavati imenicu ili potpunu riječ,
- c) lozinke se moraju promijeniti najmanje nakon 12 mjeseci, a posljednje dvije lozinke neće biti dopuštene za ponovnu upotrebu.

Članak 34.

Sve lozinke i postupci koji se koriste za pristup i upravljanje mrežama, upravljanje e-mailovima i programima moraju se čuvati u zaključanim prostorijama ili ladicama ili na drugom sigurnom mjestu, moraju biti zaštićeni od neovlaštenog pristupa.

Nakon svake zloporabe ili sumnje u istu mora se odrediti nova lozinka.

Članak 35.

Za potrebe obnavljanja računalnog sustava prilikom kvara ili u slučaju bilo koje druge izvanredne situacije najmanje jednom dnevno radi se kopija sadržaja mrežnog diska i lokalnih direktorija, kao i podataka iz svih ključnih poslovnih aplikacija.

Kopije iz stavka 1. pohranjuju se u zaštićenim prostorijama ili drugim medijima, a sve sukladno odredbama ovog Pravilnika ili drugih internih akata Zaklade kojima se uređuje istovrsna problematika.

Pristup arhiviranim kopijama potrebno je ograničiti isključivo na osobe koje za to imaju poslovnu potrebu.

VIII. ODVAJANJE U MREŽI (SEGMENTIRANJE)

Članak 36.

Mreža je segmentirana u posebne logičke mrežne segmente kako bi se omogućilo definiranje posebnih prava pristupa pojedinim mrežnim resursima, informacijskim sustavima i uslugama, u skladu s poslovnim potrebama.

Segmentiranje mreže provedeno je uzevši u obzir:

- a) ustrojstvenu strukturu voditelja obrade,
- b) vrstu informacijskih resursa i informatičkih usluga kojima se treba pristupati,
- c) vrijednost i klasifikacija podataka kojima se pristupa preko tih resursa,
- d) procjenu rizika za povjerljivost, integritet i dostupnost informacija koje se prenose ili se nalaze u određenom mrežnom segmentu.

Članak 37.

Određene mreže mogu se smatrati nesigurnima.

Nesigurne mreže su, ali ne ograničavaju se na:

- Internet,
- bežične lokalne mreže
- mreže vanjskih partnera.

Kontrola pristupa zaposlenika ili izvršitelja obrade iz nesigurnih mreža na mrežnu infrastrukturu provodi se korištenjem vatrozida (engl. firewall).

Pravila pristupa na vatrozidu dozvoljavaju pristup samo određenim mrežnim segmentima i samo ograničenom broju komunikacijskih protokola.

Članak 38.

Segmentiranje mreže uz kontrolu pristupa logičkim mrežnim segmentima vrši se putem listi za kontrolu pristupa na središnjem vatrozidu.

Tehnike za segmentiranje mreže uz kontrolu pristupa logičkim mrežnim segmentima mogu biti ostvarene korištenjem VPN tehnologija, vatrozida, kontrola mrežnog usmjeravanja uz istodobnu uporabu listi za kontrolu pristupa (engl. Access Control List) itd.

Osnovni princip od kojeg se polazi kod uspostave kontrole pristupa jest da se omogućuje pristup isključivo do onih mrežno dostupnih resursa koji su potrebni za obavljanje redovitih radnih aktivnosti.

Članak 39.

Pružatelj informatičkih usluga odgovoran je za provođenje aktivnosti vezanih za segmentiranje mrežne infrastrukture i održavanje pristupnih lista mrežnih uređaja i vatrozida temeljem zahtjeva odgovornih osoba voditelja obrade.

Sve promjene na pristupnim listama mrežnih uređaja i vatrozida moraju biti evidentirane i provedene u skladu s procedurama za upravljanje promjenama na mrežnoj infrastrukturi.

O svim promjenama na pristupnim listama mrežnih uređaja i vatrozida, pružatelj informatičkih usluga (izvršitelj obrade) dužan je obavijestiti osobu koju je voditelj obrade ovlastio da obavlja poslove informacijske sigurnosti.

IX. PRISTUP INTERNETU I SADRŽAJU ELEKTRONIČKE POŠTE

Članak 40.

Pristup preko bežične lokalne mreže (eng. WLAN) je pristup definiran IEEE 802.11 skupinom standarda.

Bežični pristup internoj mreži voditelja obrade mora biti poslovno opravdan pri čemu se jasno trebaju odrediti segmenti mreže kojima se može bežično pristupiti te komunikacijski protokoli koji se mogu pri tome koristiti.

Članak 41.

Svi korisnici bežične lokalne mreže moraju se autentificirati korištenjem sigurnih autentifikacijskih protokola i mehanizama.

Odabir autentifikacijskog protokola i mehanizma autentifikacije korisnika bežične lokalne mreže mora biti pažljivo proveden uz provođenje analize mogućih rizika.

Svako spajanje korištenjem bežične lokalne mreže mora biti zabilježeno na odgovarajući način te mora biti omogućena naknadna spajanja na internu mrežu koristeći bežični pristup.

Članak 42.

Sve instalirane pristupne točke za bežični pristup u lokalnu mrežu moraju biti primjereno zaštićene od neovlaštenog pristupa.

Fizički pristup pristupnim točkama za bežičnu mrežu treba biti omogućen samo ovlaštenim osobama pružatelja informatičkih usluga (bilo to voditelj obrade ili izvršitelj obrade). Mora se voditi kontrola fizičkog ili drugog pristupa mjestima gdje su postavljene pristupne točke.

Kod odabira smještaja pristupnih točaka za bežičnu lokalnu mrežu i razine signala tih uređaja mora se voditi računa o tome da rasprostiranje signala izvan granica prostora koji pripada voditelju obrade bude minimalno.

Članak 43.

Nije dozvoljeno postavljanje pristupnih točaka za bežični pristup bez dozvole odgovorne osobe pružatelja informatičkih usluga.

Potrebno je provoditi periodičke provjere kako bi se spriječilo neautorizirano ili nekontrolirano postavljanje pristupnih točaka za bežični pristup.

Članak 44.

Za udaljeni pristup zaposlenika internoj mreži, voditelj obrade mora osigurati provjeru vjerodostojnosti.

Za udaljeni pristup iz stavka 1. koristi se TLS VPN tehnologija koja osigurava provjeru vjerodostojnosti i sigurnost (povjerljivost) komunikacijskog kanala.

VPN način udaljenog pristupa primjenjuje se na sve zaposlenike voditelja obrade, ali i izvršitelje obrada koji mogu pristupiti osobnim podacima.

Svaki udaljeni pristup informatičkom sustavu voditelja obrade poslovno je opravdan i dokumentiran te zabilježen u sustavu.

Članak 45.

Zaposlenik i druga ovlaštena osoba mogu pristupati sustavu elektroničke pošte i koristiti ga isključivo temeljem dodijeljenih korisničkih prava, svojeg korisničkog imena i pripadajuće lozinke.

Zaposlenik i druga ovlaštena osoba dužna je birati i čuvati lozinke u skladu s odredbama ovog Pravilnika.

X. ZAŠTITA OSOBNIH PODATAKA KOD UPORABE MOBILNE RAČUNALNE OPREME I RADA NA IZDVOJENOM MJESTU RADA

Članak 46.

Pod mobilnom računalnom opremom podrazumijeva se:

- prijenosno računalo
- tablet računalo
- mobilni telefon
- pametni telefoni

Rad na izdvojenom mjestu radje rad kod kojeg radnik ugovoreni posao obavlja kod kuće ili u drugom prostoru slične namjene koji je određen na temelju dogovora radnika i poslodavca, a koji nije prostor poslodavca.

Članak 47.

Razina informacijske sigurnosti koju zahtijeva voditelj obrade pri korištenju informacijskog sustava mora biti zadržana prilikom korištenja mobilne računalne opreme i pri radu na daljinu.

Ovlaštene osobe unutar voditelja obrade odgovorne su za zaduživanje, podešavanje, održavanje i razduživanje mobilne računalne opreme na kojoj se nalaze osobni podaci, a nakon čega postaju odgovornost zaposlenika.

Pristup i korištenje mobilne računalne opreme zaposlenika nije dopušteno članovima obitelji, prijateljima te bilo kojim drugim neovlaštenim fizičkim i pravnim osobama.

Članak 48.

Zaposlenik je odgovoran za zaštitu mobilne računalne opreme od krađe i neovlaštenog pristupa u svako vrijeme i na svakom mjestu.

U slučajevima kada se mobilna računalna oprema ne koristi, ona mora biti adekvatno zaštićena od krađe ili neovlaštenog pristupa.

Zaposlenik je dužan odmah prijaviti bilo kakav sigurnosni incident povezan s mobilnom računalnom opremom pružatelju informatičkih usluga ili osobi koju je voditelj obrade ovlastio da obavlja poslove informacijske sigurnosti.

Članak 49.

Pristup mobilnoj računalnoj opremi mora biti zaštićen sigurnosnim mehanizmima za identifikaciju i autorizaciju korisnika.

Prilikom rada na javnim mjestima i na mjestima na kojima postoji povećana prijetnja od nadgledanja rada od strane neovlaštene osobe, zaposlenik mora voditi računa da spriječi promatranje svog rada, osobito ako se na trajnom nosaču podataka ili monitoru nalaze osobni podaci.

Na mjestima iz stavka 2. ovog članka, obvezno je zaključavanje računala opcijom „Lock computer“ ili odjava rada iz sustava opcijom „Log off“ za vrijeme za koje se prijenosno računalo ne koristi.

Na mobilnoj računalnoj opremi zabranjeno je korištenje dijeljenih direktorija odnosno dijeljenje lokalnih direktorija na mobilnoj računalnoj opremi s drugima.

Članak 50.

Rad na izdvojenom mjestu rada zahtijeva odgovarajuću razinu zaštite od krađe opreme i podataka, neovlaštenog otkrivanja podataka, neovlaštenog udaljenog pristupa informacijskom sustavu voditelja obrade te neovlaštenog korištenja informacijskog sustava voditelja obrade.

Članak 51.

Prilikom rada na izdvojenom mjestu rada zaposleniku se ne mijenjaju poslovne odgovornosti kao ni obveze i prava koja proizlaze iz opisa njegova radnog mjesta.

Članak 52.

Korištenje bežične lokalne mreže (engl. Wireless LAN ili WLAN) u javnim prostorima (npr. zračne luke, hoteli itd.) treba biti svedeno na minimum.

U slučaju korištenja bežične lokalne mreže zaposlenici moraju biti svjesni rizika nezaštićene komunikacije na takvoj mreži.

Zaposlenici ne smiju izmjenjivati osobne podatke u nezaštićenom obliku (nekriptiranom) korištenjem bežične lokalne mreže u javnim prostorima.

Članak 53.

Autentifikacija kod udaljenog pristupa dijelovima informacijskog sustava uvijek se odnosi na individualni pristup.

Nije dopušteno korištenje tuđih ili grupnih korisničkih imena i lozinki za udaljeni pristup informacijskog sustava.

XI. SUSTAV POHRANE I ZAŠTITA OSOBNIH PODATAKA

Evidencija aktivnosti obrade

Članak 54.

Zaklada vodi evidenciju svih aktivnosti obrade osobnih podataka za koje je odgovorna (u daljnjem tekstu: Evidencija aktivnosti obrade) u elektroničkom obliku, putem službenika za zaštitu podataka.

Evidencija aktivnosti obrade, osim u slučajevima ukoliko je propisano drugačije, imaju sljedeće informacije:

- (a) naziv i kontaktne podatke Zaklade i, ako je primjenjivo, zajedničkog voditelja obrade;
- (b) ime i kontaktni podaci službenika za zaštitu podataka;
- (c) svrhe obrade;
- (d) opis kategorija ispitanika;
- (e) opis kategorija osobnih podataka;
- (f) kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije;
- (g) ako je primjenjivo, prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije te, u slučaju prijenosa iz članka 49. stavka 1. podstavka 2. Uredbe, dokumentaciju o odgovarajućim zaštitnim mjerama;
- (h) ako je to moguće, predviđene rokove za brisanje različitih kategorija podataka;
- (i) ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 21. ovog Pravilnika.

Sve organizacijske jedinice dužne su surađivati sa službenikom za zaštitu podataka i pravovremeno ga obavještavati o potrebi ažuriranja Evidencije aktivnosti obrade u odnosu na obradu osobnih podataka iz njihovog djelokruga poslova.

Obrazac za vođenje Evidencije aktivnosti obrade nalazi se u Prilogu 11. ovog Pravilnika.

Zaklada putem službenika za zaštitu podataka na zahtjev daje AZOP-u uvid u Evidenciju aktivnosti obrade.

Obzirom na stavak 2. točku (h) ovog članka, rokovi čuvanja arhivskog i dokumentarnog gradiva određeni su posebnim aktom Zaklade sukladno važećim propisima Republike Hrvatske. U odnosu na rokove čuvanja dokumentacije vezane uz obradu i zaštitu osobnih podataka koji nisu određeni posebnim aktom, Zaklada može odrediti i u Evidenciji aktivnosti obrade.

Komunikacija i suradnja s AZOP-om

Članak 55.

Odgovorne ili ovlaštene osobe Zaklade u obavljanju poslova iz svoje nadležnosti kontaktiraju i/ili surađuju s AZOP-om putem službenika za zaštitu podataka ili izravno, na način propisan u stavcima od 2. do 4. ovog članka.

Radi osiguravanja jedinstvene primjene Opće uredbe o zaštiti podataka i Zakona o provedbi Opće uredbe o zaštiti podataka, odgovorne osobe Zaklade i vanjski pružatelji usluga neće komunicirati sa nadzornim tijelom niti istome slati upite bez obavještanja i mišljenja službenika za zaštitu podataka.

Ako se upit organizacijske jedinice ili ovlaštene osobe ili treće strane u ime voditelja obrade iz stavka 2. ovog članka odnosi na tumačenje Opće uredbe o zaštiti podataka i Zakona o provedbi Opće uredbe o zaštiti podataka koje je od značaja za prava i obveze Zaklade kao voditelja i/ili izvršitelja obrade, službenik za zaštitu podataka će u roku od osam radnih dana od dana primitka obavijesti iz stavka 2. ovog članka razmotriti svrhu, način, oblik i sadržaj izravnog obraćanja AZOP-u te će obavijestiti odgovorne osobe Zaklade da je suglasan s predloženom komunikacijom ili da bi, prema njegovom mišljenju, namjeravano obraćanje AZOP-u trebalo izmijeniti ili dopuniti u sadržajnom smislu, odgoditi ili u cijelosti odustati od takvog obraćanja.

U slučaju neslaganja između organizacijske jedinice ili odgovornih osoba i službenika za zaštitu osobnih podataka, odluku donose odgovorne osobe Zaklade.

Mjere zaštite osobnih podataka

Članak 56.

Zaklada provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurala i mogla dokazati da se obrada provodi u skladu s Općom uredbom o zaštiti podataka i Zakonom o provedbi Opće uredbe o zaštiti podataka.

Najmanje jednom godišnje, a najkasnije svake dvije godine ili nakon svake izmjene u pravnom okruženju ili okruženju rizika, Zaklada preispituje tehničke i organizacijske mjere iz stavka 1. ovog članka radi utvrđenja predstavljaju li iste odgovarajuću razinu zaštite osobnih podataka.

Zaštita osobnih podataka u papirnatim dokumentima

Članak 57.

Odgovorne osobe odnosno zaposlenici Zaklade papirnatu dokumente koji sadrže osobne podatke moraju odlagati u za to određene omote, fascikle i registratore te ih pohraniti u prostorima Zaklade na odgovarajućem mjestu, osim ako je papirnata dokumentacija pod neposrednim nadzorom ovlaštene osobe Zaklade.

U slučaju da se pohrana i/ili arhiva papirnatu dokumentacije odlaže kod treće ugovorne strane nužno je da zaposlenici te treće strane potpišu izjave o povjerljivosti sukladno ovom Pravilniku.

Daljnja pravila i načini postupanja zaposlenika Zaklade s papirnatim dokumentima uređena su pozitivnim propisom Republike Hrvatske te aktom Zaklade za upravljanje dokumentarnim gradivom Zaklade a u dijelu kojim se uređuje odlaganje i čuvanje gradiva.

Zaštita osobnih podataka u elektroničkim dokumentima

Članak 58.

Zaposlenici i odgovorne osobe Zaklade čuvaju elektroničke dokumente i druge elektroničke zapise koji sadrže osobne podatke na način koji ih osigurava od neovlaštenog pristupa, brisanja, mijenjanja ili gubitka podataka, u skladu s tehničkim i organizacijskim mjerama zaštite iz ovog Pravilnika.

Daljnja pravila i načini postupanja zaposlenika Zaklade s elektroničkim dokumentima uređena su pozitivnim propisom Republike Hrvatske te aktom Zaklade za upravljanje dokumentarnim gradivom Zaklade u dijelu kojim se uređuje odlaganje i čuvanje gradiva.

Organizacijske mjere zaštite

Članak 59.

Zaposlenici i odgovorne ili ovlaštene osobe Zaklade dužni su čuvati povjerljivost osobnih podataka za koje saznaju u obavljanju svojih dužnosti i poslova te pritom poštivati odredbe Opće uredbe o zaštiti podataka, Zakona o provedbi Opće uredbe o zaštiti podataka i ovog Pravilnika.

Zaposlenici i odgovorne ili ovlaštene osobe Zaklade smiju pristupati samo onim osobnim podacima koji su im potrebni za obavljanje njihovog posla, tj. za koje postoji potreba saznanja.

Odgovorne osobe i zaposlenici ili ovlaštene treće strane dužne su bez odgađanja obavijestiti službenika za zaštitu podataka o svakoj povredi osobnih podataka.

Postupanje s privolom

Članak 60.

Ako je ispitanik privolu dostavio službeniku za zaštitu podataka, službenik za zaštitu podataka će istu bez odgađanja proslijediti nadležnoj organizacijskoj jedinici.

Ako privola ispitanika nije uredna ili potpuna, službenik za zaštitu podataka ili organizacijska jedinica će pozvati ispitanika da uočene nedostatke otkloni.

Nakon urednog zaprimanja privole, privola se bez odgađanja pohranjuje na odgovarajućem i sigurnom mjestu u organizacijskoj jedinici.

Svaka organizacijska jedinica dužna je obavještavati službenika za zaštitu podataka o svakoj zaprimljenoj privoli.

Odredbe ovog članka na odgovarajući se način primjenjuju i u slučaju povlačenja privole.

Organizacijska jedinica zadužena za prikupljanje privola zadužena je i za vođenje Evidencije o danim i povučenim privolama pod Prilogom 14. ovog Pravilnika.

Tehnička i integrirana zaštita podataka

Članak 61.

Uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, Zaklada provodi odgovarajuće tehničke i organizacijske mjere, uključujući mjere propisane internim aktima, postupanje s poslovnom tajnom i drugim povjerljivim podacima Zaklade.

Prilikom procjene odgovarajuće razine zaštite osobnih podataka, Zaklada uzima u obzir rizike koje predstavlja obrada, posebno rizike od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

Zaklada poduzima mjere kako bi osigurala da svaki zaposlenik ili drugi pojedinac koji djeluje pod njezinom odgovornošću, a koji ima pristup osobnim podacima, ne obrađuje te podatke ako to nije prema uputama Zaklade kao voditelja obrade, osim ako je to obvezan učiniti prema pravu Europske unije ili pravu Republike Hrvatske.

Procjena učinka na zaštitu podataka

Članak 62.

U slučaju potrebe uvođenja novog postupka obrade ili mogućeg povećanja rizika za prava i slobode ispitanika u postojećim postupcima obrade osobnih podataka, svaka organizacijska jedinica o tome obavještava službenika za zaštitu podataka i traži mišljenje o pitanju postoji li dužnost provođenja procjene učinka na zaštitu osobnih podataka u konkretnom slučaju.

Zaklada je dužna prije početka obrade provesti procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka, ako je vjerojatno da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode ispitanika. Jedna procjena može se odnositi na niz sličnih postupaka obrade koji predstavljaju slične visoke rizike.

Pri provođenju procjene učinka na zaštitu podataka odgovorne osobe unutar organizacijskih jedinica dužne su savjetovati službenika za zaštitu podataka.

Procjena učinka na zaštitu podataka mora sadržavati:

- a) sustavan opis predviđenih postupaka obrade i svrha obrade, uključujući, ako je primjenjivo, legitimni interes,
- b) procjenu nužnosti i proporcionalnosti postupaka obrade povezanih s njihovim svrhama,
- c) procjenu rizika za prava i slobode ispitanika i
- d) mjere predviđene za rješavanje problema rizika, što uključuje zaštitne mjere, sigurnosne mjere i mehanizme za osiguravanje zaštite osobnih podataka i dokazivanje sukladnosti s Općom uredbom o zaštiti podataka, uzimajući u obzir prava i legitimne interese ispitanika i drugih uključenih osoba.

Procjena učinka za zaštitu podataka donosi se sukladno metodologiji pod Prilogom 7. ovog Pravilnika, a provodi ju službenik za zaštitu podataka.

Procjenu učinka za zaštitu podataka potpisuje i o istoj mora dati mišljenje službenik za zaštitu podataka.

Procjena legitimnog interesa

Članak 63.

U slučajevima kada se obrada osobnih podataka vrši na temelju legitimnog interesa, prije početka obrade provest će se Procjena legitimnog interesa kako bi se osiguralo da prava i slobode ispitanika nisu narušena.

Metodologija za provođenje Procjene legitimnog interesa nalazi se pod Prilogom 8. ovog Pravilnika, a provodi ju službenik za zaštitu podataka.

Procjena legitimnog interesa mora uzeti u obzir sljedeće čimbenike:

- Postojanje legitimnog interesa voditelja obrade.
- Potrebitost obrade za ostvarivanje tog interesa.
- Procjena ravnoteže između legitimnog interesa voditelja obrade i prava i interesa ispitanika, uključujući provođenje testa proporcionalnosti i nužnosti.

Zaklada može započeti s obradom osobnih podataka na temelju legitimnog interesa samo ako rezultati procjene pokažu da obrada ne ugrožava prava i slobode ispitanika.

Prethodno savjetovanje s AZOP-om

Članak 6.

Zaklada je dužna savjetovati se s AZOP-om prije početka obrade ako bi se procjenom učinka na zaštitu podataka iz ovog Pravilnika pokazala da bi, u slučaju da Zaklada ne donese mjere za ublažavanje rizika, namjeravana obrada dovela do visokog rizika.

Prilikom savjetovanja s AZOP-om u skladu sa stavkom 1. ovog članka, Zaklada dostavlja AZOP-u:

- a) opis odgovornosti Zaklade i izvršitelja obrade, ako je uključen u obradu,
- b) svrhu i sredstva namjeravane obrade,
- c) zaštitne mjere i druge mjere za zaštitu prava i sloboda ispitanika na temelju Opće uredbe o zaštiti podataka,
- d) kontaktne podatke službenika za zaštitu podataka,
- e) procjenu učinaka za zaštitu podataka i
- f) sve druge informacije koje AZOP zatraži.

Konačnu Odluku o pokretanju prethodnog savjetovanja sa AZOP-om donose odgovorne osobe Zaklade nakon savjetovanja sa službenikom za zaštitu podataka.

XII. USLUGE KOJE PRUŽAJU VANJSKE FIZIČKE ILI PRAVNE OSOBE

Članak 65.

Ako se obrada provodi u ime Zaklade kao voditelja obrade, Zaklada koristi jedino izvršitelje obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu sa zahtjevima iz Opće uredbe o zaštiti podataka i da se njome osigurava zaštita prava ispitanika.

Svaka vanjska fizička ili pravna osoba koja obavlja poslove obrade osobnih podataka, kao što je prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, uporaba, otkrivanje, ograničavanje, brisanje ili uništavanje i koja je registrirana za obavljanje takve djelatnosti (izvršitelj obrade), mora sklopiti pisani ugovor o obradi i dijeljenju podataka s voditeljem obrade odnosno Zakladom.

Ukoliko se razmatra pružatelj usluge odnosno izvršitelj obrade sa sjedištem izvan Europske unije potrebno je provesti procjenu rizika prijenosa podataka sukladno metodologiji za provođenje procjene rizika prijenosa podataka u treće zemlje koja se nalazi u Prilogu 6. ovog Pravilnika.

Ugovor iz stavka 2. ovog članka pregledava službenik za zaštitu podataka te isti mora biti u pisanom obliku.

Predložak Ugovora o obradi i dijeljenju podataka nalazi se pod Prilogom 12. ovog Pravilnika.

Ugovor iz stavka 2. i 3. definira uvjete i mjere kojima se osigurava zaštita osobnih podataka, a odnosi se i na vanjske suradnike koji održavaju, proizvode i uvode računalnu i strojnu opremu.

Radi utvrđivanja uvjeta iz stavka 1. ovog članka, Zaklada će u postupku nabave usluga izvršitelja obrade, među ostalim obvezama propisanim važećim propisima o postupku nabave, utvrđivati ispunjava li ponuditelj kriterij korištenja odgovarajućih tehničkih i organizacijskih mjera kojima se ostvaruje stupanj zaštite osobnih podataka koji je jednak ili viši od onog stupnja zaštite koji se ostvaruje provedbom tehničkih i organizacijskih mjera zaštite od strane Zaklade i to sukladno interno donesenom Upitniku o procjeni adekvatnosti i usklađenosti vanjskog pružatelja usluga koji se nalazi u Prilogu 13. ovog Pravilnika.

Izvršitelji obrade obavljaju usluge obrade osobnih podataka u kontekstu i opsegu dozvole njihovih klijenata te podatke kojima ima pristup na temelju ugovora s voditeljem obrade ne smiju obrađivati niti na bilo koji drugi način koristiti.

Izvršitelj obrade koji pruža svoje usluge izvan prostorija voditelja obrade mora imati razinu zaštite osobnih podataka prilagođenu Općoj uredbi o zaštiti podataka i zakonskim propisima koji reguliraju obradu osobnih podataka.

Ako izvršitelj obrade angažira drugog izvršitelja obrade (podizvršitelja), za provođenje posebnih aktivnosti obrade u ime Zaklade, iste obveze za zaštitu podataka, kao one koje su navedene u ugovoru ili drugom pravnom aktu između Zaklade i izvršitelja obrade nameću se tom drugom izvršitelju obrade ugovorom ili drugim pravnim aktom u skladu s pravom Europske unije ili pravom Republike Hrvatske, a osobito obveza davanja dostatnih jamstava za provedbu odgovarajućih tehničkih i organizacijskih mjera na način da se obradom udovoljava zahtjevima iz Opće uredbi o zaštiti podataka i ovog Pravilnika.

Ako drugi izvršitelj obrade iz prethodnog stavka ovog članka ne ispunjava obveze zaštite podataka, početni izvršitelj obrade ostaje u cijelosti odgovoran Zakladi za izvršavanje obveza tog drugog izvršitelja obrade.

Nakon raskida suradnje s pružateljima usluge s kojima je sklopljen ugovor iz stavka 2. ovog članka traži se potvrda brisanja osobnih podataka sukladno Prilogu 19. ovog Pravilnika.

XIII. PRIJAM I PRIENOS OSOBNIH PODATAKA

Članak 66.

Dopušten je prijenos osobnih podataka putem informacijskih, telekomunikacijskih i drugih sredstava, samo kad se koriste postupci i mjere zaštite od neovlaštenog prisvajanja ili uništavanja podataka te neopravdano upoznavanje s njihovim sadržajem.

Zaposlenici koji su ovlašteni za prijam i evidentiranje pošte, ne otvaraju one pošiljke koje su naslovljene na drugog adresata i koje su greškom dostavljene, kao i pošiljke koje su označene kao osobni podaci, ili za koje iz označavanja na omotu proizlazi da se odnose na natječaj za zapošljavanje i/ili pozive za javnu nabavu.

Zaposlenici koji su ovlašteni za prijam i evidentiranje pošte, ne smiju otvarati pošiljke naslovljene na drugog zaposlenika, kada je na omotu navedeno da se uručuju osobno (oznaka N/R).

Stavak 3. ovog članka primjenjuje se i u slučaju pošiljaka na kojima je prvo navedeno osobno ime zaposlenika, bez naznake njegovog službenog položaja i tek nakon navedenoga adresa voditelja obrade odnosno Zaklade.

Osjetljivi podaci šalju se na određene adrese u zapečaćenoj omotnici uz potvrdu primitka.

Osobni podaci šalju se preporučenom poštom s povratnicom te je nužno osigurati da se ne može izvršiti otvaranje i uvid u sadržaj omotnice bez ostavljanja traga od otvaranja omotnice.

Omotnica u kojoj se šalju osobni podaci mora biti izrađena na način da je nemoguće vidjeti sadržaj omotnice u normalnom ili posebnom osvjetljenju.

Članak 67.

Obrada osjetljivih podataka mora biti posebno naznačena i zaštićena.

Osjetljivi podaci mogu biti poslani elektroničkom poštom samo ako se koristi neki od oblika enkripcije poruka elektroničke pošte, a koji su odobreni i podržani od strane voditelja obrade.

Članak 68.

Osobni podaci daju se na uvid primateljima koji za to imaju odgovarajuću pravnu osnovu i ovlaštenje.

Izvorni dokumenti ne smiju se prenositi trećim neovlaštenim primateljima ili bez sudske odluke.

XIV. BRISANJE PODATAKA

Članak 69.

Osobni podaci čuvaju se dok traje pravna osnova za njihovo prikupljanje i obradu.

Zaklada kao stvaratelj javnog arhivskog i dokumentarnog gradiva donijela je, sukladno pozitivnim propisima Republike Hrvatske, akte kojima uređuje područje zaštite i obrade takvog gradiva.

Zaklada će redovito odabirati arhivsko gradivo iz dokumentarnog gradiva i redovito periodički izlučivati dokumentarno gradivo kojemu su istekli rokovi čuvanja, sukladno rokovima propisanim u Popisu dokumentarnog gradiva Zaklade s rokovima čuvanja.

Članak 70.

Ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja, a voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja osim u onim slučajevima u kojima se ograničava pravo na brisanje sukladno ovom Pravilniku ili drugom aktu Zaklade ili važećim propisima Republike Hrvatske.

Članak 71.

Pravo na brisanje ne primjenjuje se u mjeri u kojoj je obrada nužna:

- a) radi ostvarivanja prava na slobodu izražavanja i informiranja;
- b) radi poštovanja pravne obveze kojom se zahtijeva obrada u pravu Europske unije ili pravu države članice kojom podliježe voditelj obrade ili za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;
- c) zbog javnog interesa u području javnog zdravlja;

- d) u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u mjeri u kojoj je vjerojatno da se pravom na brisanje može onemogućiti ili ozbiljno ugroziti postizanje ciljeva te obrade te
- e) radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

Ograničavanje svakog prava ispitanika, tako i prava na brisanje, procjenjuje se od slučaja do slučaja te je za navedeno nadležan službenik za zaštitu podataka.

XV. POSTUPANJE PRILIKOM SUMNJE NA NEOVLAŠTENI PRISTUP

Članak 72.

Zaposlenici su obvezni odmah obavijestiti odgovorne osobe voditelja obrade ili osobu koju je on ovlastio da obavlja poslove informacijske sigurnosti o aktivnostima koje se odnose na otkrivanje neovlaštenog pristupa zaštićenim podacima, kao i o zlonamjnim ili neovlaštenim korištenjima, prisvojenjima, izmjenama ili oštećenjima takvih podataka.

Zaposlenici su obvezni spriječiti bilo koju od aktivnosti koje se mogu smatrati neovlaštenim pristupom.

Voditelj obrade ili osoba koju je ovlastio za obavljanje poslova informacijske sigurnosti dužan je odmah po saznanju, o aktivnostima iz stavka 1., obavijestiti službenika za zaštitu osobnih podataka ukoliko isti nije bio ranije obaviješten o događanjima.

Voditelj obrade propisuje metodologiju i postupanje u slučaju neovlaštenog pristupa i/ili u slučaju incidenta kao što je sigurnosni incident i/ili incident koji je vezan uz zaštitu osobnih podataka, a koja se nalazi u Prilogu 5. ovog Pravilnika.

Članak 73.

Zaposlenici su dužni u najkraćem mogućem roku obavijestiti odgovorne osobe Zaklade ili osobu koju je Zaklada ovlastila za obavljanje poslova informacijske sigurnosti ili druge ovlaštene osobe o svakom događaju koji upućuje na povredu sigurnosnih mjera koje proizlaze iz ovog Pravilnika i ostalih internih akata i procedura.

Zaposlenici i druge ovlaštene osobe moraju izvijestiti i osobu ovlaštenu za obavljanje poslova informacijske sigurnosti o svakom uočenom nedostatku u sustavu sigurnosti informacijskog sustava.

Osoba ovlaštena za obavljanje poslova informacijske sigurnosti dužna je o okolnostima iz stavka 1. i 2. obavijestiti službenika za zaštitu osobnih podataka.

Sastavni dio ovog Pravilnika su Prilog 2. - Interno izvješće o povredi osobnih podataka koje popunjava osoba koja prijavljuje incident i službenik za zaštitu podataka, Prilog 3. - Registar sigurnosnih povreda i Prilog 4. - Registar incidenata/povreda.

U registru sigurnosnih povreda iz stavka 4. ovog članka evidentiraju se pojedinosti koje se odnose na sigurnosne propuste, dok u registru incidenata/povreda evidentiraju se pojedinosti koje se odnose na povredu/incident vezan uz zaštitu osobnih podataka.

Za vođenje registara iz stavka 4. ovog članka zadužen je službenik za zaštitu podataka.

Članak 74.

U slučaju da zaposlenici iz vanjskih izvora doznaju o pojavi virusa ili sigurnosnoj prijetnji, dužni su o tome obavijestiti osobe iz članka 78. ovog Pravilnika.

Zaposlenici ne smiju samostalno poduzimati aktivnosti u slučaju iz stavka 1. ovog članka te ne smiju takve obavijesti slati drugim zaposlenicima ili ovlaštenim osobama u obliku masovne ili lančane elektroničke pošte.

Izješćivanje AZOP-a o povredi osobnih podataka

Članak 75.

U slučaju povrede osobnih podataka, Zaklada putem službenika za zaštitu podataka bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izješćuje AZOP o povredi osobnih podataka, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca. Ako izješćivanje nije učinjeno unutar 72 sata, mora biti popraćeno razlozima za kašnjenje.

Izvršitelj obrade bez nepotrebnog odgađanja izješćuje Zakladu nakon što sazna za povredu osobnih podataka.

U izješćivanju iz stavka 1. ovo članka mora se barem:

- a) opisati priroda povrede osobnih podataka, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj dotičnih evidencija osobnih podataka,
- b) navesti ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija,
- c) opisati vjerojatne posljedice povrede osobnih podataka i
- d) opisati mjere koje je Zaklada poduzela ili predložila poduzeti za rješavanje problema povrede osobnih podataka, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.

Ako i u onoj mjeri u kojoj nije moguće istodobno pružiti informacije, informacije je moguće postupno pružati bez nepotrebnog daljnjeg odgađanja.

Za službeno izješćivanje AZOP-a koristiti će se službene informacije na internetskoj stranici nadzornog tijela kao i službeni obrazac prijave o povredi.

Konačnu odluku o izješćivanju AZOP-a, nakon savjetovanja sa službenikom za zaštitu podataka i osobom koju je Zaklada ovlastila da obavlja poslove informacijske sigurnosti, donose odgovorne osobe Zaklade.

Obavješćivanje ispitanika o povredi osobnih podataka

Članak 76.

U slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, Zaklada putem službenika za zaštitu podataka bez nepotrebnog odgađanja obavješćuje ispitanika o povredi osobnih podataka.

Obavijest ispitaniku o povredi osobnih podataka sadrži opis prirode povrede osobnih podataka uporabom jasnog i jednostavnog jezika te informacije i mjere koje su nužne kako ne bi došlo do daljnjeg ugrožavanja prava ispitanika.

Obavješćivanje ispitanika iz stavka 1. ovog članka nije obvezno ako je ispunjen bilo koji od sljedećih uvjeta:

- a) Zaklada je poduzela odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na osobne podatke pogođene povredom osobnih podataka, posebno one koje osobne podatke čine nerazumljivima bilo kojoj osobi koja im nije ovlaštena pristupiti, kao što je enkripcija,
- b) Zaklada je poduzela naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika iz stavka 1. ovog članka ili
- c) time bi se zahtijevao nerazmjeran napor. U takvom slučaju Zaklada o povredi prava ispitanika javno obavješćuje putem svoje internetske stranice ili na drugi odgovarajući način ovisno o tome koji podaci i koje kategorije ispitanika su zahvaćene.

Pri donošenju odluke o tome je li obavješćivanje ispitanika o povredi osobnih podataka obvezno odnosno je li ispunjen neki od uvjeta iz stavka 3. ovog članka, Zaklada traži savjet od službenika za zaštitu podataka.

XVI. SLUŽBENIK ZA ZAŠTITU PODATAKA

Imenovanje i radno mjesto službenika za zaštitu podataka

Članak 77.

Zaklada imenuje službenika za zaštitu podataka te zamjenika koji službeniku za zaštitu podataka pomaže u implementiranju procesa, mjera i drugih aktivnosti vezanih uz zaštitu osobnih podataka, privatnosti i povjerljivosti.

Kontaktne podatke službenika za zaštitu podataka Zaklada objavljuje na svojim internetskim stranicama te ih priopćuje AZOP-u.

Odgovorne osobe Zaklade podupiru službenika za zaštitu podataka u izvršavanju zadaća pružajući mu potrebna sredstva za izvršavanje tih zadaća i ostvarivanje pristupa osobnim podacima i postupcima obrade te za održavanje njegova stručnog znanja.

Ispitanici, uključujući zaposlenike Zaklade, mogu kontaktirati službenika za zaštitu podataka u pogledu svih pitanja povezanih s obradom svojih osobnih podataka i ostvarivanja svojih prava iz Opće uredbe o zaštiti podataka i Zakona o provedbi Opće uredbe o zaštiti podataka.

Službenik za zaštitu podataka obavezan je tajnošću ili povjerljivošću u vezi s obavljanjem svojih zadaća, o čemu daje posebnu pisanu izjavu o povjerljivosti.

Službenik za zaštitu podataka može ispunjavati i druge zadaće i dužnosti. Zaklada osigurava da takve zadaće ili dužnosti ne dovedu do sukoba interesa

XVII. ODGOVORNOST ZA PRIMJENU MJERA I POSTUPAKA

Članak 78.

Odgovorne osobe Zaklade kao što su voditelji ustrojstvenih jedinica i ovlaštene osobe odgovorni su, uz službenika za zaštitu podataka i zamjenika, za primjenu postupaka i mjera za zaštitu osobnih podataka kako je to uređeno ovim Pravilnikom.

Članak 79.

Svatko tko obrađuje osobne podatke dužan je postupati sukladno propisanim postupcima i mjerama radi sigurnosti i zaštite podataka, a koje mu moraju biti dostupne tijekom procesa obrade.

Obveza postupanja u skladu sa zaštitom podataka ne prestaje sa završetkom radnog odnosa ili koje druge pravne osnove.

Prije zaposlenja na radnom mjestu na kojem se obrađuju osobni podaci, zaposlenik mora potpisati posebnu Izjavu o povjerljivosti koja se nalazi pod Prilogom 10. ovog Pravilnika.

Ustrojstvena jedinica nadležna za kadrovske poslove čuva izjavu iz stavka 3. ovog članka u dokumentu osobnom očevidniku svakog zaposlenika.

Zaklada je dužna na odgovarajući način obavijestiti sve zaposlenike o obradi njihovih osobnih podataka. Obavijest o obradi osobnih podataka zaposlenika nalazi se pod Prilogom 9. ovog Pravilnika.

Putem obrasca za provjeru točnosti podataka pod Prilogom 22. ovog Pravilnika, Zaklada je dužna provjeravati točnost osobnih podataka zaposlenika minimalno jednom godišnje.

Zaklada postupa sukladno Smjernicama za zaštitu osobnih podataka u radnim odnosima pod Prilogom 23. ovog Pravilnika te iste primjenjuje u radnim odnosima.

Članak 80.

Nakon prestanka radnog odnosa ili obavljanja poslova u Zakladi zaposlenik je dužan vratiti ovlaštenoj osobi svu računalnu i komunikacijsku opremu i sve podatke (i njihove kopije) kojima je bio u posjedu tijekom rada.

Nije dozvoljeno zadržavanje računalne i komunikacijske opreme te podataka bez pisane dozvole ovlaštene osobe voditelja obrade ili izvršitelja obrade.

Zaposlenik je dužan potpisati Izjavu o vraćanju sredstva za rad pod prilogom 16. ovog Pravilnika te ispuniti Obrazac za razduživanje opreme pod prilogom 17. ovog Pravilnika.

ZAVRŠNE ODREDBE

Članak 81.

Ovaj Pravilnik objavljuje se na mrežnim stranicama Zaklade, a stupa na snagu 8 dana od dana objave.

U slučaju nesuglasja pojedinih odredbi ovog Pravilnika i/ili ovog Pravilnika sa odredbama drugih akata Zaklade, službenik za zaštitu podataka dužan je dati mišljenje.

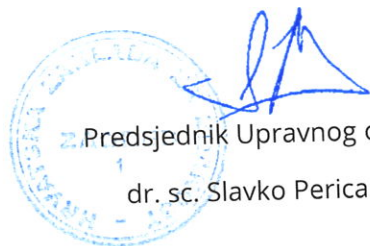
Organizacijska struktura i promjena iste ne utječe na primjenu odredbi ovog Pravilnika.

Članak 2.

Danom stupanja na snagu ovog Pravilnika prestaje važiti Procedura o obradi i zaštiti osobnih podataka Broj: O-2361-2018 donesena 5. srpnja 2018. godine.

KLASA: 110-02/25-01/01

URBROJ: 1-25-2


Predsjednik Upravnog odbora
dr. sc. Slavko Perica

Podaci o prilogima koji čine dio Pravilnika:

Naziv i šifra priloga (operativne procedure):	Podaci o odgovornim osobama za izvršenje:	Datum zadnje revizije i sadržajni opis izmjene i dopune dokumenta
OP-P-1 Obrazac zahtjeva za ostvarenje prava ispitanika	Službenik za zaštitu podataka	V1 2025
OP-P-2 Interno izvješće o povredi osobnih podataka	Službenik za zaštitu podataka	V1 2025
OP-P-3 Registar sigurnosnih povreda	Službenik za zaštitu podataka	V1 2025
OP-P-4 Registar incidenata	Službenik za zaštitu podataka	V1 2025
OP-P-5 Metodologija procjene ozbiljnosti povrede	Službenik za zaštitu podataka	V1 2025
OP-P-6 Metodologija procjene rizika prijenosa podataka u treće zemlje (TIA)	Službenik za zaštitu podatak	V1 2025
OP-P-7 Metodologija provođenja procjene učinka zaštite podataka (DPIA)	Službenik za zaštitu podataka	V1 2025
OP-P-8 Metodologija provođenje testova legitimnosti (LIA)	Službenik za zaštitu podataka	V1 2025
OP-P-9 Obavijest zaposlenicima	Službenik za zaštitu podataka	V1 2025
OP-P-10 Izjava o povjerljivosti	Službenik za zaštitu podataka	V1 2025
OP-P-11 Evidencije aktivnosti obrade	Službenik za zaštitu podataka	V1 2025
OP-P-12 Ugovor o obradi i dijeljenju podataka (dvojezična verzija)	Službenik za zaštitu podataka	V1 2025

OP-P-13 Upitnik o procjeni adekvatnosti i usklađenosti vanjskog pružatelja usluga	Službenik za zaštitu podataka	V1 2025
OP-P-14 Evidencija o danim i povučenim privolama	Službenik za zaštitu podataka	V1 2025
OP-P-15 Evidencija zahtjeva ispitanika	Službenik za zaštitu podataka	V1 2025
OP-P-16 Izjava o vraćanju sredstva za rad	Službenik za zaštitu podataka	V1 2025
OP-P-17 Obrazac za razduživanje opreme	Službenik za zaštitu podataka	V1 2025
OP-P-18 Hodogram brisanja podataka	Službenik za zaštitu podataka	V1 2025
OP-P-19 Potvrda brisanja svih podataka nakon prestanka suradnje	Službenik za zaštitu podataka,	V1 2025
OP-P-20 Obavijest o produženju razdoblja očitovanja ispitanika	Službenik za zaštitu podataka	V1 2025
OP-P-21 Dopis za pojašnjenje zahtjeva ispitanika	Službenik za zaštitu podataka	V1 2025
OP-P-22 Obrazac za provjeru točnosti podataka	Službenik za zaštitu podataka	V1 2025
OP-P-23 Smjernice za zaštitu osobnih podataka u radnim odnosima	Službenik za zaštitu podataka	V1 2025
OP-P-24 Privola za buduće selekcijske postupke	Službenik za zaštitu podataka	V1 2025

