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.

Utvrđivanje 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 obavještavanju 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 potvrđivanja 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 izrijekom 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 njihovu 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 otkloni 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 podrobnije 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 podrobnije 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 računalo (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 autentificiratikorištenjem 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 analiza 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 obavještavanja 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 papirnate 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 papirnate 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 podatka 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 uredbe 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 PRIJENOS 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 propisanima 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 kojem 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 zlonamjernim 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.

Izvješćivanje 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, izvješćuje AZOP o povredi osobnih podataka, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca. Ako izvješćivanje nije učinjeno unutar 72 sata, mora biti popraćeno razlozima za kašnjenje.

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

U izvješćivanju 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 izvješćivanje AZOP-a koristiti će se službene informacije na internetskoj stranici nadzornog tijela kao i službeni obrazac prijave o povredi.

Konačnu odluku o izvješćivanju 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 obvezan 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 prilozima 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

Hrzz
Hrvatska zaklada za znanost

Obrazac zahtjeva za ostvarenje prava ispitanika

PODACI O OSOBI (ISPITANIKU) KOJI ŽELI OSTVARITI PRAVA U VEZI SA ZAŠTITOM OSOBNIH PODATAKA[1]	
Ime i prezime	
OIB (osobni identifikacijski broj)	
Adresa prebivališta ili e-mail	

VRSTA PRAVA U DOMENI ZAŠTITE OSOBNIH PODATAKA KOJE ŽELITE OSTVARITI (molimo zaokružite redni broj)

1. Pravo na brisanje
2. Pravo na pristup
3. Pravo na ispravak
4. Pravo na ograničenje obrade
5. Pravo na prenosivost podataka
6. Pravo na prigovor
7. Prava vezana uz automatsko donošenje odluka i profiliranje
8. Pravo na povlačenje privole

NAPOMENA

_____ _____

Datum Potpis ispitanika

PODACI O ZAPRIMANJU ZAHTJEVA	
Zahtjev zaprimljen dana	
Ime, prezime i potpis zaposlenika	
Nadležna organizacijska jedinica	

[1] Podatke prikupljene u ovom obrascu Hrvatska zaklada za znanost (dalje: Zaklada) koristit će za ostvarivanje prava ispitanika u skladu s Općom uredbom o zaštiti podataka (EU 2016/679) te u svrhu davanja odgovora na upite i prigovore ispitanika u skladu s Pravilnikom o zaštiti osobnih podataka. Podaci su obvezni te u slučaju uskrate istih Zaklada neće biti u mogućnosti odgovoriti na zahtjev ispitanika. Isti podaci će se čuvati u razdoblju od 5 godina. Sve ostale informacije koje je Zaklada dužna dati ispitaniku u skladu s gore navedenom Općom uredbom o zaštiti podataka, sadržane su u Pravilniku o zaštiti osobnih podataka koji je objavljen na mrežnim stranici te dostupan u poslovnim prostorijama Zaklade.

Hrvatska zaklada za znanost

INTERNO IZVJEŠĆE O POVREDI OSOBNIH PODATAKA

1. POPUNJAVA OSOBA KOJA PRIJAVLJUJE INCIDENT

INICIJALNE INFORMACIJE	
Ime osobe koja prijavljuje incident:	
Kontakt podaci osobe koja prijavljuje incident (e-mail adresa i/ili telefonski broj):	
Datum i vrijeme incidenta:	
ROK ZA PRIJAVU POVREDE NADZORNOM TIJELU (VRIJEME SAZNANJA ZA POVREDU + 72H)	

OPIS INCIDENTA
(Opis incidenta mora sadržavati približan broj zahvaćenih ispitanika, kao i vrstu osobnih podatka vezanih uz incident. Ukoliko se radi o sigurnoj povredi molimo da istu opišete kao i sve poduzete korake.)

MOGUĆE POSLJEDICE INCIDENTA:
•

VRSTA INCIDENTA
☐ **INTERNI** ☐ **UKLJUČUJE VODITELJA OBRADE**

PODACI O VODITELJU OBRADE	
Organizacija:	**Hrvatska zaklada za znanost**
Kontakt osoba:	**Službenik za zaštitu podataka: Alen Plančić** **Zamjenik službenika za zaštitu podataka: Lana Zubović**
Kontakt podaci (e-mail adresa i/ili telefonski broj)	**alen@hrzz.hr** **lana@hrzz.hr**

PRATEĆA DOKUMENTACIJA
•
(Popis svih relevantnih dokumenata potrebnih službeniku za zaštitu podataka, uz popis molimo iste priložiti prilikom dostavljanja izvješća)

2. POPUNJAVA SLUŽBENIK ZA ZAŠTITU PODATAKA

DODATNI KOMENTARI
DODATNA DOKUMENTACIJA KOJU ZAHTIJEVA SLUŽBENIK ZA ZAŠTITU PODATAKA
•

KLASIFIKACIJA INCIDENTA
☐ SIGURNOSNI INCIDENT KOJI NE UKLJUČUJE POVREDU OSOBNIH PODATAKA ☐ POVREDA OSOBNIH PODATAKA (DATA BREACH) – OBVEZNO IZVJEŠTAVANJE NADZORNOG TIJELA ☐ POVREDA OSOBNIH PODATAKA (DATA BREACH) – BEZ POTREBE ZA IZVJEŠTAVANJEM NADZORNOG TIJELA ☐ OSTALO _____

PODUZETE ILI PREDLOŽENE MJERE ZA UMANJENJE POSLJEDICA INCIDENTA	
POST-INCIDENT AKTIVNOSTI	
ZAKLJUČAK	
Datum upisivanja incidenta u registar incidenata:	

Hrvatska zaklada za znanost

REGISTAR SIGURNOSNIH POVREDA

U registru sigurnosnih povreda Hrvatska zaklada za znanost evidentira pojedinosti koje se odnose na sigurnosne propuste.

UZROK SIGURNOSNE POVREDE	POJEDINOSTI O SIGURNOSNOJ POVREDI/VRIJEME I KRATAK OPIS	UČINCI I POSLJEDICE SIGURNOSNE POVREDE	MJERE KOJE SU PODUZETE ZA OTKLANJANJE SIGURNOSNE POVREDE

Hrzz
Hrvatska zaklada
za znanost

REGISTAR INCIDENATA/POVREDA

U registru incidenata/povreda voditelj obrade Hrvatska zaklada za znanost evidentira pojedinosti koje se odnose na povredu/incident vezan uz zaštitu osobnih podataka.

UZROK POVREDE	POJEDINOSTI O INCIDENTU/VRIJEME I KRATAK OPIS	OSOBNI PODACI NA KOJE JE POVREDA UTJECALA	UČINCI I POSLJEDICE POVREDE	MJERE KOJE SU PODUZETE ZA OTKLANJANJE POVREDE

METODOLOGIJA PROCJENE OZBILJNOSTI POVREDE OSOBNIH PODATAKA

SADRŽAJ

UVOD

Ozbiljnost povrede osobnih podataka definirana je kao procjena magnitude potencijalnog utjecaja na prava pojedinaca uzrokovana povredom osobnih podataka.

Ova Metodologija prije svega služi Hrvatskoj zakladi za znanost, Ilica 24, 10 000 Zagreb (dalje u tekstu: “voditelj obrade”) kao alat temeljem kojeg kao voditelj obrade može efikasno utvrditi ozbiljnost incidenta koji može dovesti do povrede osobnih podataka te kada je to potrebno, izvijestiti odgovarajuće nadzorno tijelo te ispitanike čiji su osobni podaci pogođeni povredom.

Metodologija predstavlja i dobar alat za brzo utvrđivanje mjera ublažavanja ako su one potrebne. Voditelj obrade vodi se putem specifičnih kvantitativnih kriterija prema stvaranju ukupne procjene povrede.

1. PREGLED METODOLOGIJE

1.1. Kriteriji

Glavni kriteriji za procjenu incidenta povrede osobnih podataka su:

- Kontekst obrade osobnih podataka **(DATA PROCESSING CONTEXT - DPC)**: Odnosi se na vrstu osobnih podataka glede kojih je povreda nastala, zajedno s nizom faktora povezanih uz cjelokupan kontekst obrade.
- Lakoća identifikacije **(EASE OF IDENTIFICATION – EI)**: Određuje koliko lako se pojedince može identificirati na temelju podataka glede kojih je povreda nastala.
- Okolnosti povrede osobnih podataka **(CIRCUMSTANCES OF BREACH – CB):** Odnosi se na specifične okolnosti povrede, što obuhvaća vrstu povrede, uključujući gubitak sigurnosti, kao i bilo kakav oblik zlonamjernog djelovanja.

1.2. Izračun ozbiljnosti povrede

Na temelju gore navedenih kriterija, pristup je sljedeći:

- Kontekst obrade osobnih podataka (DPC) je srž metodologije i ocjenjuje koliko je kritična povreda bila u kontekstu specifične obrade osobnih podataka.
- Lakoća identifikacije (EI) je korektivni faktor DPC-a. Ukupna ozbiljnost povrede može se umanjiti ovisno o vrijednosti EI-a. Drugim riječima, što je niži EI to je ukupan stupanj povrede niži.
- Okolnosti povrede osobnih podataka (CB) kvantificiraju specifične okolnosti povrede koje mogu biti povezane uz konkretnu situaciju. CB, kada postoji, može samo nadodati ozbiljnosti povrede, čime povećava ozbiljnost povrede osobnih podataka.

Na temelju iznesenog proizlazi sljedeća formula za izračun ozbiljnosti povrede:

SE = DPC X EI + CB

Rezultat se promatra unutar određenih parametara te se veže uz jedan od četiri stupnja ozbiljnosti povrede: nizak, umjeren, visok, vrlo visok. Na kraju procjene iznose se i drugi mogući elementi koji nisu uračunati u metodologiju kako bi se njihovo postojanje naglasilo nadležnima.

Bitno je naglasiti da rezultati ove metodologije služe samo za korištenje u okviru dane formule za procjenu ozbiljnosti povrede. Oni nisu namijenjeni kako bi se na temelju njih zaključivalo o određenoj vrsti podataka, a kamo li da predstavljaju pravne posljedice ili presedane o korištenju podataka u druge svrhe.

2. DETALJAN OPIS OCJENJIVANJA I RAZINE OZBILJNOSTI POVREDE

2.1. Ocjenjivanje

2.1.1. Kontekst obrade osobnih podataka (DPC)

Kako bi pravilno bodovali DPC, voditelj obrade treba pratiti sljedeće korake:

Prvi korak: Definiranje i klasifikacija vrsta osobnih podataka

a) Definiranje vrsta osobnih podataka glede kojih je povreda nastala.
b) Klasificiranje podataka u barem jednu od sljedeće 4 kategorije: jednostavni (osnovni), bihevioralni, financijski, osjetljivi podaci (kategorije objašnjene u Aneksu 1). Na ovaj način utvrđuje se preliminarni DPC rezultat.

   Navedene kategorije osobnih podataka nisu isključive, međutim, većina podataka u stvarnim slučajevima može se podvesti barem pod jednu od navedenih kategorija. Akreditacije (ovlaštenja) ne predstavljaju posebnu kategoriju podataka te se trebaju kategorizirati sukladno vrsti podataka koje obrađuje sustav za koji one osiguravaju pristup.

Drugi korak: Prilagodba kontekstualnih okolnosti vezanih uz obradu podataka

a) Procjena nastanka određenih faktora koji mogu povećati ili umanjiti osnovni rezultat (količina podataka, posebne karakteristike voditelja obrade ili pojedinaca, netočnost podataka, javna dostupnost)
b) U slučaju da takvi faktori postoje, sukladno njima potrebno je povećati/umanjiti osnovni rezultat. Tablica za procjenu 1 sadrži ljestvicu za prilagodbu prema kategorijama podataka zajedno s primjerima.

Bilješka: Iako su za potrebe ove metodologije 4 kategorije podataka rangirane, kategorizacija sama za sebe ne treba se smatrati kao generalno utvrđivanje ranga tih kategorija. Štoviše, dodatni kontekstualni faktori vezani uz obradu određene kategorije podataka moraju se uzeti u obzir.

Ako se podaci mogu svrstati u više od jedne od gore navedenih kategorija propisani koraci moraju se poduzeti za svaku od kategorija. Za konačni izračun koristit će se ona vrijednost koja prikazuje najveći stupanj povrede.

2.1.2. Lakoća identifikacije (EI)

U svrhu korištenja ove metodologije EI faktor je stupnjevan u 4 kategorije: zanemariv, ograničen, značajan i maksimalan, s linearnim povećanjem rezultata.

Kada definiramo EI, treba uzeti u obzir može li zbog povrede osobnih podataka doći do identifikacije izravno (pr. na temelju imena) ili neizravno (pr. putem broja osobne iskaznice).

Potrebno je uzeti u obzir i sva sredstva za koja se razumno može očekivati da netko može koristiti za identifikaciju pojedinaca. To uključuje informacije koje su javno dostupne, ali prikupljene i na drugi način, uključujući preko interneta, kao i putem „cross-matching" procesa s drugim dostupnim izvorima.

2.1.3. Okolnosti povrede osobnih podataka (CB)

Elementi koji se razmatraju u okviru CB-a su: gubitak sigurnosti što obuhvaća gubitak povjerljivosti, gubitak integriteta, gubitak dostupnosti, te zlonamjernost.

Gubitak povjerljivosti: Do gubitka povjerljivosti dolazi kada podacima pristupe osobe koje nisu ovlaštene ili nemaju legitimnu svrhu za pristupanjem.

Gubitak integriteta: Događa se kada se izvorni podaci izmjene, a zamjena može biti štetna za pojedinca. Najteže situacije obuhvaćaju slučajeve kada postoji ozbiljna situacija da se takvi izmijenjeni podaci koriste na način da se našteti pojedincu.

Gubitak dostupnosti: Događa se kada se ne može pristupiti izvornim podacima, a postoji potreba za pristup istima. To može biti privremeno (povrat podataka je moguć, ali je za to potrebno vrijeme što može biti štetno za pojedinca) i trajno (povrat nije moguć).

Zlonamjernost: Ovim elementom utvrđuje se je li do povrede došlo greškom, ljudskom ili tehničkom, ili je povreda učinjena namjerno. Nenamjerne povrede uključuju: slučajni gubitak, neadekvatno odlaganje, ljudsku pogrešku, softverski nedostatak ili grešku. Namjerne povrede prije svega uključuju krađu i hakiranje, ali i prodaju osobnih podataka trećima. Također, one mogu uključivati i pokušaje da se namjerno našteti voditelju obrade.

Suprotno od bodovanja DPC-a i EI-a gdje je maksimalan broj bodova određen, kod CB-a oni se dodaju ukupnom rezultatu ovisno o svakom utvrđenom elementu u pojedinom slučaju.

2.2. Razina ozbiljnosti povrede

Kao što je i prethodno navedeno, ozbiljnost povrede računa se putem formule:

SE = DPC x EI + CB

RAZINA OZBILJNOSTI POVREDE		
SE < 2	**NISKA**	Pojedinci ili neće biti zahvaćeni ili će za posljedicu imati manje neugodnosti koje će lako prevladati (vrijeme potrebno za ponovni unos podataka, neugodnosti i sl.)
2 ≤ SE < 3	**UMJERENA**	Pojedinci mogu trpjeti značajne neugodnosti koje će moći prevladati uz određene poteškoće (dodatni troškovi, strah, stres, nerazumijevanje, nemogućnost pristupa poslovnim uslugama i sl.)
3 ≤ SE < 4	**VISOKA**	Pojedinci mogu trpjeti značajne posljedice koje će moći prevladati uz ozbiljne poteškoće (pronevjera novca, stavljanje na crnu listu banaka, imovinska šteta, gubitak zaposlenja, pogoršanje zdravlja i sl.)
4 ≤ SE	**VRLO VISOKA**	Pojedinci mogu trpjeti značajne te čak i nepopravljive posljedice, a za koje postoji mogućnost da ih neće moći prevladati (financijski problemi vezani uz značajan dug, nemogućnost rada, dugoročne psihičke ili fizičke smetnje, smrt...)

2.3. Napomene („Flags“)

Kada je razina ozbiljnosti definirana, uz nju mogu se istaknuti i napomene kojima se naglašava određeni element povrede, koji iako a priori na utječe na rezultat, je bitan za konačnu procjenu. Za potrebe ove metodologije razmatrane su dvije napomene:

- **Broj pojedinaca na koje se povreda odnosi prelazi 100**. Kada je povreda podataka pojedinaca nastupila u kontekstu većeg incidenta, postoji mogućnost da se takvi podaci lakše otkriju. Istovremeno, povreda podataka velikog broja pojedinaca utječe na ukupan razmjer povrede.
- **Podaci nerazumljivi.** Nerazumljivost (podaci se nalaze u dobro kriptiranom obliku, a da pritom nije kompromitiran ključ) može umanjiti utjecaj na pojedince s obzirom da značajno smanjuje mogućnost neovlaštenog pristupa tim podacima.

3. KONTEKST OBRADE OSOBNIH PODATAKA (DPC) - BODOVANJE

3.1. Tablica za procjenu

	Pr. biografski podaci, kontakt podaci, puno ime i prezime, obiteljski život, radno iskustvo	REZ
JEDNOSTAVNI PODACI (OSNOVNI)	Osnovni rezultat kada povreda obuhvaća „jednostavne podatke“ i voditelju nisu poznati nikakvi otežavajući faktori.	1
	Rezultat može biti uvećan za 1, ako primjerice količina „jednostavnih podataka“ i/ili karakteristike voditelja obrade su takve da može biti omogućeno profiliranje pojedinaca ili se mogu izvoditi pretpostavke o socijalnom/financijskom statusu pojedinaca.	2
	Rezultat može biti uvećan za 2, primjerice kada „jednostavni podaci“ i/ili karakteristike voditelja obrade mogu dovesti do pretpostavki o zdravstvenom stanju pojedinca, vjerskim, političkim uvjerenjima ili seksualnoj orijentaciji.	3
	Rezultat može biti uvećan za 3, ako primjerice zbog određenih karakteristika pojedinaca (maloljetnici, ranjive grupe) podaci mogu biti kritični za njihovu sigurnost i fizičko/psihičko zdravlje.	4

	Pr. lokacija, podaci o prometu, podaci o osobnim preferencijama i navikama	REZ
BIHEVIORALNI PODACI	Osnovni rezultat kada povreda obuhvaća bihevioralne podatke i voditelju nisu poznati nikakvi otežavajući faktori.	2
	Rezultat može biti umanjen za 1, ako priroda podataka ne pruža značajan uvid u bihevioralne podatke pojedinaca ili se ti podaci lako mogu prikupiti (neovisno o povredi) putem javno dostupnih izvora.	1

	Rezultat može biti uvećan za 1, kada volumen bihevioralnih podataka i/ili karakteristike voditelja obrade su takve da se može kreirati profil pojedinca koji sadrži detaljne informacije o njegovom svakodnevnom životu i navikama.	3
	Rezultat može biti uvećan za 2, ako se primjerice može kreirati profil pojedinca na temelju osjetljivih podataka.	4

FINANCIJSKI PODACI	**Pr. prihodi, financijske transakcije, bankovni izvodi, kreditne kartice, računi ....**	**REZ**
	Osnovni rezultat kada povreda obuhvaća financijske podatke i voditelju nisu poznati nikakvi otežavajući faktori.	3
	Rezultat može biti umanjen za 2, ako primjerice priroda podataka ne pruža značajan uvid u financijske podatke pojedinaca (pr. činjenica da je osoba klijent određene banke bez daljnjih detalja).	1
	Rezultat može biti umanjen za 1, primjerice kada specifični skup podataka uključuje neke financijske podatke, ali i dalje ne uključuje značajan uvid u financijski status pojedinca (pr. broj bankovnog računa bez daljnjih detalja).	2
	Rezultat može biti uvećan za 1, primjerice kada svrha i/ili volumen specifičnog skupa podataka otkrije financijski status pojedinca što može omogućiti prijevaru ili ako omogući kreiranje detaljnog socijalnog/financijskog profila pojedinca.	4

OSJETLJIVI PODACI	**Pr. bilo koji oblik osjetljivih podataka, podaci o zdravlju, politička pripadnost, seksualni život....**	**REZ**
	Osnovni rezultat kada povreda obuhvaća osjetljive podatke i voditelju nisu poznati nikakvi otežavajući faktori.	4
	Rezultat može biti umanjen za 3, ako primjerice priroda podataka ne pruža značajan uvid u osjetljive podatke pojedinaca ili se isti mogu lako prikupiti	1

	(neovisno o povredi) putem javno dostupnih izvora.	
	Rezultat može biti umanjen za 2, primjerice kada priroda podataka može dovesti do donošenja općenitih pretpostavki.	2
	Rezultat može biti uvećan za 1, primjerice kada priroda podataka može dovesti do donošenja pretpostavki o osjetljivim informacijama.	3

3.2. Opis kontekstualnih faktora koje treba razmotriti prilikom ocjenjivanja

Faktori koji uvećavaju rezultat:

- **Volumen podataka (koji se odnose na istog pojedinca):** Volumen je potrebno sagledati i u kontekstu vremena (pr. ista vrsta podataka koja „curi" kroz određeno vrijeme) i sadržaja (pr. komplementarni podaci iste vrste).
- **Posebne karakteristike voditelja obrade:** Odnosi se na područje rada i aktivnosti voditelja obrade što može uvećati rezultat (pr. lista kupaca predstavlja veći rizik ako se odnosi na online ljekarnu nego kada je riječ o papirnici).
- **Posebne karakteristike pojedinaca:** Ako je riječ o pojedincima koji pripadaju socijalnim grupama sa specifičnim potrebama (to mogu biti primjerice maloljetnici, ali isto tako DPC rezultat će porasti i kod „curenja" telefonskih brojeva ako ta lista sadrži i one znanih saborskih zastupnika).

Faktori koji umanjuju rezultat:

- **Nevaljanost/netočnost podataka**: Kako bi mogao uračunati ovaj faktor, voditelj obrade mora biti siguran da su podaci nevaljani ili netočni. Primjerice lista adresa poštanske kompanije na koju pisma nisu mogla biti isporučena može se smatrati listom s netočnim podacima.
- **Javna dostupnost:** Podaci su već javno objavljeni ili ih se može lako prikupiti ili im pristupiti putem javno dostupnog izvora.
- **Priroda podataka:** Sama priroda podataka može umanjiti početni DPC rezultat. Primjerice medicinski certifikat koji samo potvrđuje da je pojedinac dobrog zdravstvenog statusa bez navođenja drugih informacija, iako početno bodovan s 4 jer je riječ o osjetljivim podacima, umanjuje se na 1, jer nema učinka na privatan

život pojedinca. Ovaj faktor potrebno je razmatrati s povećanim oprezom i uz davanje jasnog objašnjenja zašto se određeni DPC rezultat umanjuje.

4. LAKOĆA IDENTIFIKACIJE (EI) - BODOVANJE

Identifikacija može biti direktna ili indirektna te se provodi pomoću određenih identifikatora, uzimajući pritom u obzir cjelokupni kontekst obrade osobnih podataka. U nastavku se primjerično navodi lista čestih identifikatora. Važno je naglasiti da će u mnogim slučajevima povreda uključivati kombinaciju više identifikatora što automatski olakšava identifikaciju.

Ime i prezime

Smatra se najčešćim direktnim identifikatorom, a EI rezultat je različit uzimajući u obzir da samo ime i prezime ne mogu uvijek identificirati pojedinca, pa tako:

EI	IME I PREZIME	
0,25	**ZANEMARIVA**	Identifikacija na području cijele države gdje velik broj ljudi dijeli isto ime i prezime.
0,5	**OGRANIČENA**	Identifikacija na području cijele države gdje manji broj ljudi dijeli isto Ime i prezime.
0,75	**ZNAČAJNA**	Identifikacija na području malog grada gdje nekoliko ljudi ili nitko ne dijeli isto ime i prezime
1	**MAKSIMALNA**	Identifikacija na području cijele države koristeći pritom i datum rođenja i e-mail adresu.

Broj osobne iskaznice/putovnice/OIB-a

Smatraju se jedinstvenim identifikatorima te se mogu koristiti za identifikaciju pod uvjetom da je moguće te podatke usporediti s referentnom bazom podataka (povezivanje broja s konkretnom osobom).

EI	BROJ OSOBNE ISKAZNICE/PUTOVNICE/OIB-A	
0,25	**ZANEMARIVA**	Kada nema niti jednog drugog podatka o pojedincu, a nije moguće pronaći dodatne informacije bez omogućavanja pristupa referentnoj bazi.
0,75	**ZNAČAJNA**	Kada identifikator otkriva dodatne informacije o pojedincu (pr., JMBG je sadržavao u sebi datum rođenja).
1	**MAKSIMALN**	Kada su dostupni i podaci iz referentne baze (broj osobne

	A	iskaznice i puno ime i prezime i/ili slika).

Telefonski broj/kućna adresa

Oboje su indirektni identifikatori koji se mogu koristiti za komunikaciju ili pristup pojedincima. Kada se identifikacija temelji na jednom od tih faktora bodovanje je sljedeće:

EI	TELEFONSKI BROJ/KUĆNA ADRESA	
0,25	**ZANEMARIVA**	Identifikacija na području cijele države kada broj/adresa nisu dostupni putem javnog registra.
0,5	**OGRANIČENA**	Identifikacija na području manjeg grada kada broj/adresa nisu dostupni putem javnog registra (identifikaciju je moguće provesti komunikacijom).
1	**MAKSIMALNA**	Identifikacija na području cijele države kada su broj/adresa uključeni u javni registar.

E-mail adresa

Riječ je o indirektnom identifikatoru koji se koristi za komunikaciju s pojedincima, a u određenim slučajevima može sadržavati i njihovo ime i prezime.

EI	E-MAIL ADRESA	
0,25	**ZANEMARIVA**	Kada e-mail adresa ne otkriva drugi podatak putem kojeg je moguća identifikacija (pr. ime) te se ne koristi kao primarna adresa pojedinca na internetskim stranicama, forumima ili socijalnim mrežama.
0,75	**ZNAČAJNA**	Kada e-mail adresa ne otkriva drugi podatak putem kojeg je moguća identifikacija (pr. ime), ali ju pojedinac koristi kao primarnu adresu na internetskim stranicama, forumima ili društvenim mrežama.
1	**MAKSIMALNA**	Kada e-mail adresa otkriva ime pojedinca te ju on koristi kao primarnu adresu na internetskim stranicama, forumima ili društvenim mrežama.

Slika

Može biti direktni ili indirektni identifikator, ovisno o okolnostima.

EI	SLIKA	
0,25	**ZANEMARIVA**	Kada je slika nejasna ili mutna (pr. snimka nadzorne kamere s velike udaljenosti).
0,5	**OGRANIČENA**	Kada je slika nejasna ili mutna, ali uključuje dodatne informacije (pr. može se prepoznati specifična lokacija) putem kojih bi se pojedinac mogao identificirati.
0,75	**ZNAČAJNA**	Kada je slika jasna, ali nema daljnjih povezanih informacija za identifikaciju.
1	**MAKSIMALNA**	Kada je slika jasna te su uz nju vezane i daljnje informacije za identifikaciju (pr. informacije o članstvu u specifičnim organizacijama ili kućne adrese)

Kodiranje/Aliasi/Inicijali

Kodiranje se odnosi na postupak dodjeljivanja jedinstvenog identifikacijskog broja svakom pojedincu u kontekstu određene baze podataka. Korištenje aliasa je oblik pseudonimizacije, u smislu da se specifični identifikator (najčešće puno ime i prezime) zamijeni aliasom (pseudonimom). Inicijali se smatraju odlikom aliasa određenog na temelju imena i prezimena pojedinca.

EI	KODIRANJE/ALIASI/INICIJALI	
0,25	**ZANEMARIVA**	Kada kod/alias ne otkriva niti može biti povezan s bilo kojim drugim osobnim podatkom pojedinca, osim ako se omogući pristup referentnoj bazi.
0,75	**ZNAČAJNA**	Kada alias otkriva neke podatke o pojedincu (pr. ime) te je povezan s drugim osobnim podacima (pr. email adresa pojedinca).
1	**MAKSIMALNA**	Kada alias otkriva puno ime i prezime pojedinca ili su i podaci iz referentne baze također dostupni.

5. OKOLNOSTI POVREDE OSOBNIH PODATAKA (CB) - BODOVANJE

CB	GUBITAK POVJERLLJIVOSTI	
0	**PRIMJERI PODATAKA IZLOŽENIH RIZIKU GUBITKA POVJERLJIVOSTI BEZ DOKAZA DA JE BILA RIJEČ O ILEGALNOJ OBRADI**	Papirnati dokument ili laptop je izgubljen u transportu.
		Oprema je bačena bez brisanja osobnih podataka.
+ 0,25	**PRIMJERI PODATAKA IZLOŽENIH ODREĐENOM BROJU ZNANIH PRIMATELJA**	Email s osobnim podacima je pogrešno poslan određenom broju znanih primatelja.
		Neki korisnici online usluge mogli su pristupiti korisničkim računima drugih korisnika.
+ 0,5	**PRIMJERI PODATAKA IZLOŽENIH NEPOZNATOM BROJU PRIMATELJA**	Podaci su objavljeni na internetskoj oglasnoj ploči.
		Podaci su učitani na P2P (peer to peer) stranicu.
		Zaposlenik je prodao CD koji sadrži podatke o korisnicima usluga.
		Pogrešno programirana internetska stranica omogući javno dostupnim podatke o internim korisnicima.

CB	GUBITAK INTEGRITETA	
0	**PRIMJERI IZMIJENJENIH PODATAKA BEZ NEPRAVILNOG ILI NELEGALNOG KORIŠTENJA**	Baza podataka s osobnim podacima je pogrešno ažurirana, ali je ista vraćena na originalno stanje prije nego su se takvi izmijenjeni podaci koristili.

+ 0,25	**PRIMJERI IZMIJENJENIH PODATAKA UZ MOGUĆE KORIŠTENJE NA NEPRAVILAN ILI NELEGALAN NAČIN, ALI UZ MOGUĆNOST POVRATA PODATAKA**	Zapis nužan za korištenje online usluge je izmijenjen pa pojedinac mora tu uslugu zatražiti izvanmrežno.
		Zapis koji je važan za točnost dokumentacije pojedinca prilikom korištenja online usluge je izmijenjen.
+ 0,5	**PRIMJERI IZMIJENJENIH PODATAKA UZ MOGUĆE KORIŠTENJE NA NEPRAVILAN ILI NELEGALAN NAČIN BEZ MOGUĆNOSTI POVRATA PODATAKA**	Prethodni primjeri uz dodataka da ne postoji mogućnost povrata originalnih podataka.

CB	GUBITAK DOSTUPNOSTI	
0	**PRIMJERI PODATAKA KOJI SE LAKO MOGU OPET UČINITI DOSTUPNIM.**	Kopija dokumenta je izgubljena, ali postoji još kopija.
		Baza podataka je nedostupna zbog greške u sustavu, ali ju se lako može rekonstruirati putem drugih baza podataka.
+ 0,25	**PRIMJERI PRIVREMENE NEDOSTUPNOSTI**	Baza podataka je nedostupna zbog greške u sustavu, može se rekonstruirati, ali uz određenu dodatnu obradu.
		Zapis je izgubljen, ali pojedina može ponovno dati te podatke.
+ 0,5	**PRIMJERI POTPUNE NEDOSTUPNOSTI (PODACI SE NE MOGU PONOVNO PRIBAVITI NITI OD VODITELJA OBRADE NITI OD POJEDINACA)**	Dokument je izgubljen/baza podataka je nedostupna (pokvarena), ne postoji sigurnosna kopija podataka i isti se ne mogu ponovno prikupiti od pojedinaca.

CB	ZLONAMJERNOST	
+0,5	**POVREDA JE UZROKOVANA NAMJERNOM RADNJOM, TO JEST S CILJEM DA SE NAŠTETI VODITELJU OBRADU I/ILI POJEDINCIMA.**	Zaposlenik namjerno dijeli osobne podatke putem socijalnih mreža.
		Zaposlenik prodaje osobne podatke.
		Zaposlenik kao korisnik društvene mreže namjerno pošalje podatke o drugim korisnicima njihovim članovima obitelji s namjerom da im našteti.

Hrzz
Hrvatska zaklada
za znanost

PROCJENA UČINKA PRIJENOSA OSOBNIH PODATAKA

SADRŽAJ

PROCJENA UČINKA PRIJENOSA OSOBNIH PODATAKA	
Tko provodi procjenu?	Hrvatska zaklada za znanost, Ilica 24, 10 000 Zagreb
Službenik za zaštitu podataka (DPO):	alen@hrzz.hr lana@hrzz.hr
DATUM PROVOĐENJA/REVIZIJE:	
_____	

1. UVOD

Procjena učinka prijenosa osobnih podataka (dalje u tekstu: Procjena) je izrađena za Hrvatsku zakladu za znanost, Ilica 24, 10 000 Zagreb (dalje u tekstu: Zaklada ili Voditelj obrade), s ciljem utvrđivanja učinka prijenosa osobnih podataka na razinu zaštite osobnih podataka utvrđenu Općom uredbom o zaštiti podataka (EU) 2016/679 te drugom odgovarajućom pravnom regulativom.

Procjena je izrađena za interne potrebe Voditelja obrade u skladu s Općom uredbom o zaštiti podataka (EU) 2016/679 i Zakonom o provedbi Opće uredbe o zaštiti podataka (NN 42/2018).

Bilo koje korištenje ove studije mora uključivati cjelovitu studiju. Niti jedan dio ili cjeloviti dokument ne može biti citiran u bilo kojem prospektu ili drugom dokumentu, osim ako je izričito odobren od strane Zaklade.

2. POJMOVI I KRATICE

U skladu s Općom uredbom o zaštiti podataka pojedini izrazi u ovoj Procjeni imaju sljedeće značenje:

„Osobni podatak" označava sve podatke koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jest 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;

„Obrada" znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo 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;

„Sustav pohrane" znači svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi;

„Voditelj obrade" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, Voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice;

„Primatelj" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana;

„Treća strana" znači 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;

„Privola ispitanika“ znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose;

„Povreda osobnih podataka” znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani;

„Službenik za zaštitu osobnih podatka (DPO)“ – osoba koja je zadužena za savjetovanje Voditelja obrade u svezi provedbe Opće uredbe o zaštiti osobnih podataka kao i Zakona o provedbi Opće uredbe o zaštiti osobnih podataka.

„EDPB“ - European Data Protection Board (Europski odbor za zaštitu podataka)

“E.O. 12333” — Executive Order 12333 -- United States intelligence activities (Uredba predsjednika 12333 i njezine izmjene i dopune), koja se tiče proširenja ovlasti i odgovornosti američkih obavještajnih agencija.

„Enkripcija“ — Zaštita digitalnih podataka (šifriranje) simetričnim ili asimetričnim ključem na način da su podaci nečitljivi bez prethodnog dekriptiranja (dešifriranja) koje je u pravilu moguće samo uz upotrebu tog odgovarajućeg ključa.

FBI — Federal Bureau of Investigation (Savezni ured za istrage).

FISA — Foreign Intelligence Surveillance Act, 50 U.S.C. ch. 36 § 1801 *et seq.* (Zakon o nadzoru stranih obavještajnih informacija).

FISC — Foreign Intelligence Surveillance Court (Sud nadzora stranih obavještajnih informacija, osnovan na temelju FISA-e).

NSA — National Security Agency (Agencija za nacionalnu sigurnost).

PPD-28 — Presidential Policy Directive -- Signals Intelligence Activities POLICY DIRECTIVE/PPD-28 (Predsjednički ukaz br. 28).

„Schrems II“ — Presuda od 16. srpnja 2020., Schrems II, C-311/18, EU:C:2020:559.

„Uredba (EU) 2016/679“ — 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).

„Sporni zahtjev za zakonit pristup“ - zahtjev za pristup osobnim podacima od strane tijela vlasti koji je zakonit po pravu zemlje uvoznice, ali je sporan po pravu Europske unije u pogledu zaštite osobnih podataka.

Dijelovi kodeksa pozitivnog prava SAD (U.S.C.) označeni su numeracijom uobičajenom za taj kodeks.

3. PRIJENOS OSOBNIH PODATAKA

3.1. Osnovno o prijenosu

NAZIV DRUŠTVA/ORGANIZACIJE KOJEM SE PODACI PRENOSE	
STATUS ORGANIZACIJE U KONTEKSTU PRIJENOSA PODATAKA	
ZEMLJA „UVOZNIK“ PODATAKA	
PRAVNI TEMELJ PRIJENOSA OSOBNIH PODATAKA	
ODGOVARAJUĆA ZAŠTITNA MJERA PRIJENOSA OSOBNIH PODATAKA (ČL. 46 GDPR)	
RAZDOBLJE ZA KOJE SE PROVODI PROCJENA	

Kontekst obrade i prijenosa podataka.

Bi li bilo izvedivo, s praktične, tehničke i ekonomske točke gledišta da izvoznik podataka prenese predmetne osobne podatke na mjesto u zemlji unutar EEA ili zemlji za koju je donesena odluka o primjerenosti?

Je li uvoznik podataka ugovorno dužan braniti predmetne osobne podatke od pokušaja zakonitog pristupa sukladno važećim propisima zemlje u koju se osobni podaci prenose?

3.2. Osobni podaci koji se prenose

Koji osobni podaci se prenose (kategorije osobnih podataka)?

Prenose li se posebne kategorije osobnih podataka? Ako da, navedite koje.

Svrha obrade osobnih podataka.

3.3. Sigurnosne i tehničke mjere zaštite

Prenose li se predmetni osobni podaci ciljnoj nadležnosti u čistom tekstu (tj. nema odgovarajućeg šifriranja u tranzitu)?

Jesu li uvozniku podataka ili trećoj strani predmetni osobni podaci dostupni u ciljnoj nadležnosti u čistom tekstu (tj. podaci nisu odgovarajuće kriptirani ili je moguć pristup ključevima za dešifriranje)?

Jesu li predmetni osobni podaci zaštićeni mehanizmom prijenosa odobrenim primjenjivim zakonom o zaštiti podataka (npr. standardnim ugovornim klauzulama EU - a u slučaju GDPR -a) i možete li očekivati poštivanje istog, u mjeri u kojoj to dopušta ciljna nadležnost i sudska praksa (gdje je primjenjivo)?

Je li vjerojatno da je tijekom razdoblja procjene uvoznik podataka tehnički sposoban kontinuirano pretraživati podatke u običnom tekstu za izbornike (tj. pojmove za pretraživanje kao što su određeni primatelji ili pošiljatelji elektroničkih komunikacija) bez dopuštenja izvoznika podataka u sklopu spornih zahtjeva za zakonit pristup prema relevantnim lokalnim zakonima?

Navedite sigurnosne i tehničke mjere zaštite prenesenih osobnih podataka.

Jesu li uvedene dopunske mjere zaštite prijenosa sukladno smjernicama EDPB („Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance withe the EU level of protection of personal data“)

S obzirom na utvrđene mjere je li razumno za očekivati da javna tijela zemlje uvoznice mogu pristupiti osobnim podacima?

3.4. Zakonodavstvo treće zemlje

Bi li izvođenje spornog zakonitog pristupa prekršilo pravo zemlje izvoznika ili drugo primjenjivo strano pravo na način koji nije dopušten prema američkoj zakonskoj doktrini međunarodnog reciprociteta, čime se sprječavaju takvi zahtjevi?

Koji nacionalni propisi se odnose na pitanje zaštite osobnih podataka? Postoji li međunarodna regulativa vezana uz zaštitu osobnih podataka koja se primjenjuje?

Jesu li propisi na kojima se temelji obrada osobnih podataka jasni, precizni i lako dostupni?

Postoje li drugi pravni temelji prema američkom pravu koji sprječavaju sporni zakoniti pristup u ovom slučaju?

Može li se na temelju pravnih propisa zaključiti da je obrada osobnih podataka

omogućena samo kada je ista nužna, proporcionalna te sukladna postizanju legitimnih ciljeva?

Postoje li hijerarhijski nadređeni nacionalni propisi koji utječu na prava utvrđena Općom uredbom o zaštiti podataka?

Postoji li nezavisni mehanizam nadzora provođenja pravne regulative vezane uz zaštitu osobnih podataka?

Postoje li učinkoviti pravni lijekovi dostupni pojedincu za slučaj povrede prava vezanih uz zaštitu osobnih podataka?

3.5. Vjerojatnost da će inozemno tijelo uspješno izvršiti zahtjev preko davatelja usluga

Vjerojatnost da se sporni podaci prenose davatelju usluga ili njegovim kooperantima na način koji omogućuje davateljima telekomunikacijskih usluga u zemlji da ih vide u običnom tekstu kao dio uzlaznog praćenja internetskih okosnica?

Vjerojatnost da će preneseni podaci uključivati sadržaj koji su odabrali selektori (tj. pojmovi za pretraživanje obavještajnih podataka, kao što su određeni primatelji ili pošiljatelji elektroničkih komunikacija)?

Ima li uvoznik podataka u posjedu, čuvanju ili kontrolu nad predmetnim osobnim podacima u čistom tekstu i stoga mu se može (uspješno) narediti da ih dostavi ili pretraži u čistom tekstu prema relevantnim zakonima?

4. ZAKLJUČAK

PRILOZI

PROCJENA UČINKA NA ZAŠTITU PODATAKA

PROCJENA UČINKA NA ZAŠTITU PODATAKA	
Tko provodi procjenu?	Hrvatska zaklada za znanost, Ilica 24, 10 000 Zagreb
Službenik za zaštitu podataka (DPO):	alen@hrzz.hr lana@hrzz.hr (zamjenik)
DATUM I MJESTO PROVOĐENJA ANALIZE:	
_____	

SADRŽAJ

UVOD

Studija procjene utjecaja zaštite osobnih podataka (u daljnjem tekstu: Procjena) je izrađena za Hrvatsku zakladu za znanost, Ilica 24, 10 000 Zagreb.

Cilj ove procjene je dobiti odgovarajući pregled rizika i utjecaja na privatnost i zaštitu osobnih podataka vezanih uz prikupljanje podatka _____.

Studija je izrađena za interne potrebe Voditelja obrade u skladu s Općom uredbom o zaštiti podataka (EU) 2016/679 (dalje u tekstu: Opće uredba o zaštiti podataka) i Zakonom o provedbi Opće uredbe o zaštiti podataka (NN 42/2018).

Bilo koje korištenje ove studije mora uključivati cjelovitu studiju. Niti jedan dio ili cjeloviti dokument ne može biti citiran u bilo kojem prospektu ili drugom dokumentu, osim ako je izričito odobren od strane Hrvatske zaklade za znanost.

Prvo poglavlje

Opće odredbe

1. OPĆE ODREDBE

Procjena zaštite osobnih podataka predstavlja dokument dubinske analize rizika obrade osobnih podataka, u ovom slučaju obrade osobnih podataka vezanih uz prikupljanje podataka _____.

S obzirom na to da ne postoji definirana metodologija izrade, ova Procjena je izrađena u skladu s člankom 35. Opće uredbe o zaštiti podataka, te prema smjernicama radne skupine 29, uz korištenje primjera najboljih praksi u području zaštite osobnih podataka.

Cilj ove Procjene je dobiti odgovarajući pregled rizika i utjecaja na privatnost te zaštitu osobnih podataka _____, sve vezano uz prijenos i obradu osobnih podataka _____.

1.1. Odnosi i definicije

U skladu s Općom uredbom pojedini izrazi u ovoj Procjeni imaju sljedeće značenje:

„Osobni podatak" označava sve podatke koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jest 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;

„Obrada" znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo ne automatiziranim 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;

„Sustav pohrane" znači svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi;

„Voditelj obrade" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, Voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice;

„Primatelj" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana;

„Treća strana" znači 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;

„Privola ispitanika“ znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose;

„Povreda osobnih podataka” znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani;

„Službenik za zaštitu osobnih podatka (DPO)“ osoba koja je zadužena za savjetovanje voditelja obrade u svezi provedbe Opće uredbe o zaštiti osobnih podataka kao i Zakona o provedbi Opće uredbe o zaštiti osobnih podataka.

Drugo poglavlje

Obrada osobnih podataka

2. OBRADA OSOBNIH PODATAKA

2.1. Potreba za provedbom procjene učinka zaštite podataka

ZAŠTO JE POTREBNA PROVEDBA PROCJENE RIZIKA I UČINKA ZAŠTITE PODATAKA?

2.2. Detaljan opis načina obrade podataka

2.2.1. Priroda, kontekst i svrha

OPIŠITE PRIRODU OBRADE PODATAKA

KONTEKST OBRADE PODATAKA

KOJA JE SVRHA PRIKUPLJANJA INFORMACIJA UNUTAR SUSTAVA?

KORIŠTENJE IZVRŠITELJA OBRADE, PODIZVRŠITELJA OBRADE ILI ZAJEDNIČKIH VODITELJA OBRADE

PRIJENOS PODATAKA U TREĆE ZEMLJE

2.2.2. Obrada osobnih podataka

OBRADA OSOBNIH PODATAKA	KATEGORIJE ISPITANIKA	VRSTA PODATAKA	PRAVNA OSNOVA	TKO SU PRIMATELJI TIH PODATAKA	KOLIKO DUGO ĆE SE TI PODACI ČUVATI

2.3. Procjena nužnosti i razmjernosti

KOJI JE PRAVNI TEMELJ OBRADE PODATAKA?

KOJE DRUGE METODE S MANJIM STUPNJEM ZADIRANJA U PRAVO NA PRIVATNOST SU RAZMATRANE?

HOĆE LI PODACI BITI NAKNADNO OBRAĐIVANI I U DRUGE SVRHE?

PRUŽATE LI ODGOVARAJUĆE INFORMACIJE ISPITANICIMA?

POSTOJE LI PROCESI KOJIMA SE POJEDINCIMA OMOGUĆUJE DA OSTVARE SVOJA PRAVA?

2.4. Sigurnosne mjere

IMATE LI MEHANIZME KONTROLE PRISTUPA KOJI OSIGURAVAJU POVJERLJIVOST OSOBNIH PODATAKA?

IMATE LI MEHANIZME ZA ZAŠTITU INTEGRITETA PODATAKA?

IMATE LI MEHANIZME ZA SPRJEČAVANJE GUBITKA PODATAKA?

JESU LI LJUDI KOJI OBRAĐUJU OSOBNE PODATKE DOVOLJNO SVJESNI SVOJIH ODGOVORNOSTI?

Treće poglavlje

Dubinska analiza rizika

3. DUBINSKA ANALIZA RIZIKA

3.1. Metodologija analize rizika

3.1.1. Klasifikacija rizika

UNUTARNJI LJUDSKI IZVORI	Zaposlenici, menadžeri, pripravnici i dr.
VANJSKI LJUDSKI IZVORI	Primatelji osobnih podataka, ovlaštene treće strane, davatelji usluga, hakeri, posjetitelji, bivši zaposlenici, aktivisti, konkurenti, osoblje za održavanje, kriminalne organizacije i dr.
OSTALI IZVORI	Zlonamjerni kod nepoznatog porijekla (virusi, crvi itd.), voda (cjevovodi, plovni putevi itd.), zapaljivi, korozivni ili eksplozivni materijali, prirodne katastrofe, epidemije, životinje i dr.

RIZICI INFORMACIJSKE SIGURNOSTI	Povjerljivost: nelegitimna uporaba ili otkrivanje podataka
	Integritet: nelegitimna manipulacija podacima
	Dostupnost: nemogućnost pristupa ili obrade podataka
REGULATORNI RIZICI	Nelegitimna obrada osobnih podataka: nedostatak legitimne pravne osnove
	Ometanje ispitanika u ostvarenju vlastitih prava i sloboda

3.1.2. Stupnjevanje vjerojatnosti

1. ZANEMARIVA (ZA)	Ne čini se vjerojatnim da bi se odabrani izvori rizika mogli doista materijalizirati (npr. krađa papirnatih dokumenata pohranjenih u sobi zaštićenoj čitačem kartica i pristupnim kodom).
2. OGRANIČENA (O)	Čini se teško mogućim da bi se odabrani rizici mogli doista materijalizirati (npr. krađa papirnatih dokumenata pohranjenih u sobi zaštićenoj čitačem kartica).
3. ZNAČAJNA (ZN)	Čini se mogućim da bi se odabrani rizici mogli doista materijalizirati (npr. krađa papirnatih dokumenata pohranjenih u sobi kojoj se ne može pristupiti bez prethodnog javljanja na portu).
4. MAKSIMALNA (M)	Iznimno je jednostavno poduzeti radnje kojima bi se odabrani rizici materijalizirali (npr. krađa papirnatih dokumenata pohranjenih na javnom mjestu).

3.1.3. Stupnjevanje ozbiljnosti

1. NISKO(1)	Malo je vjerojatno da će to imati utjecaj na prava ispitanika (npr. gubitak vremena u ponavljanju formalnosti ili čekanje da se ispune, primanje neželjene pošte).
2. SREDNJE (2)	Vjerojatan je utjecaj na prava ispitanika, ali rizik ugrožavanja njihovih temeljnih prava i sloboda je nizak (npr. neažurirani podaci, primanje neželjene ciljane pošte koja bi mogla biti neugodna).
3. VISOKO (3)	Vjerojatan je primjetan utjecaj na ispitanike s mogućnošću ozbiljnog ugrožavanja njihovih prava i utjecaja (npr. neovlašteno prisvajanje novca koji nije nadoknađen, izgubljene mogućnosti (osiguranje, napredovanje u karijeri itd.), oštećenje imovine, gubitak podataka o ispitanicima itd.).
4. KRITIČNO (4)	Postojeća ili očekivana situacija potencijalno može biti ozbiljna ili čak i nepopravljiva ugroza za prava i slobode ispitanika (npr. fizička šteta, nesposobnost za rad ili vođenje poslova, značajan financijski gubitak).

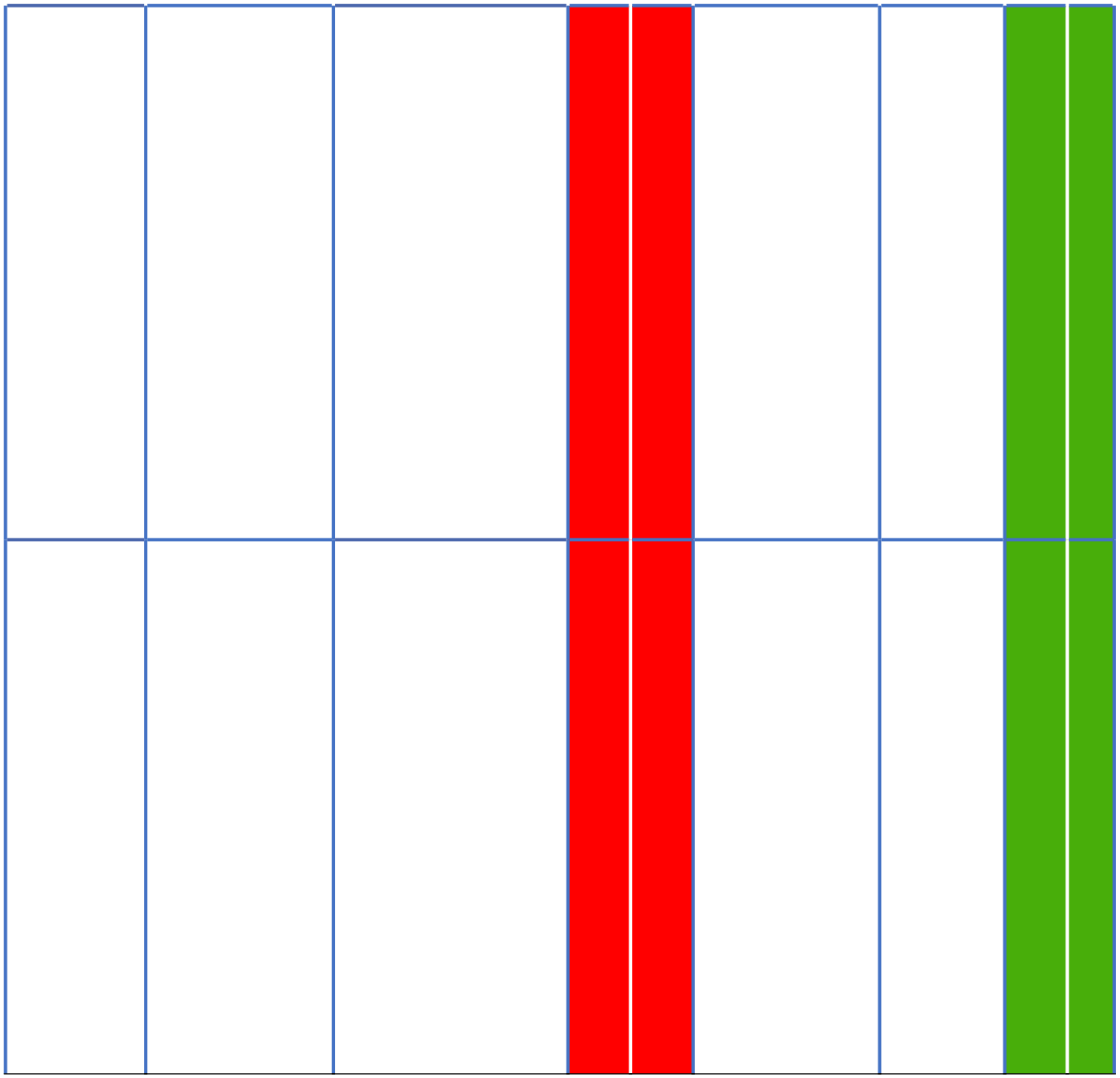
3.1.4. Utjecaj na pojedince

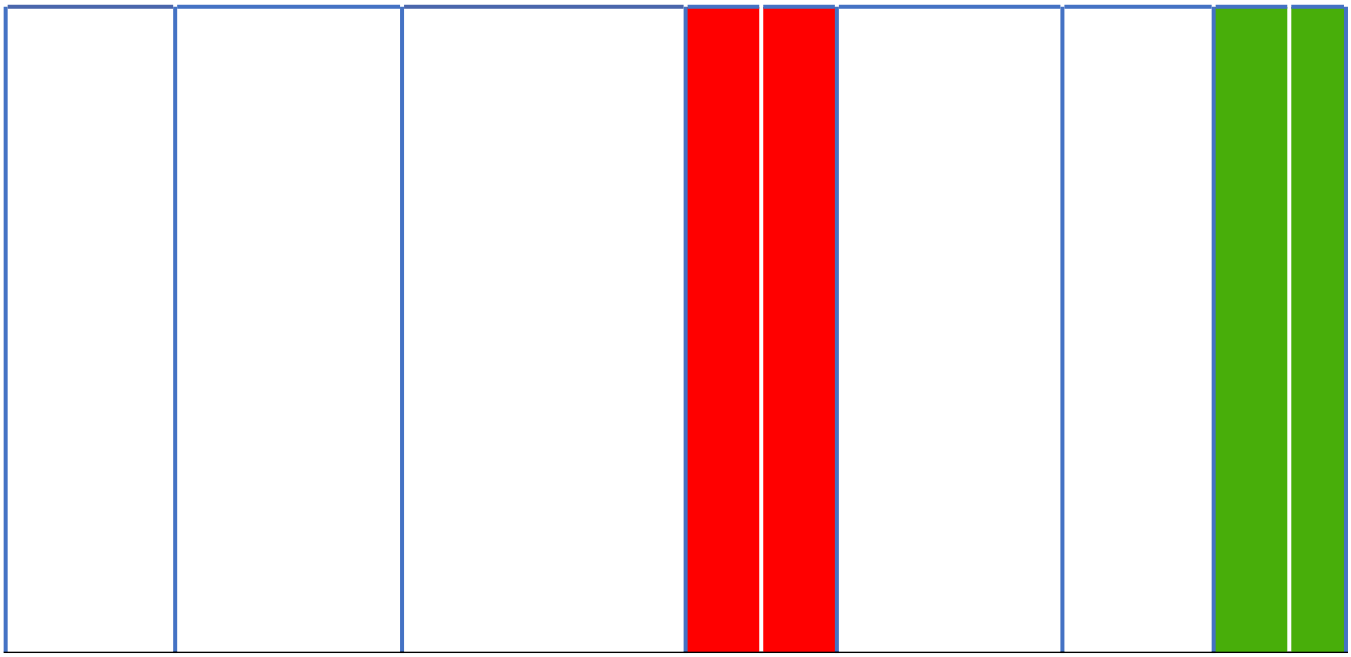
NELEGITIMAN PRISTUP OSOBNIM PODACIMA (RIZICI POVJERLJIVOSTI)	Podaci vidljivi ljudima koji ih ne trebaju vidjeti, ali ih ne mogu koristiti (npr. zloupotreba prava, krivotvorenje prava itd.). Podaci se kopiraju i spremaju na drugo mjesto.
	Podaci se dijele više nego što je potrebno i izvan kontrole ispitanika (npr. neželjeno širenje fotografije na internetu, gubitak kontrole nad informacijama objavljenim na društvenoj mreži itd.).
	Podaci se koriste u druge svrhe osim onih u koje su planirani i / ili na nepošten način (npr. u komercijalne svrhe, krađa identiteta, korištenje na štetu ispitanika itd.). Podaci su povezani s drugim informacijama koje se odnose na ispitanike (npr. korelacija adrese prebivališta i geolokacijskih podataka u stvarnom vremenu itd.).
	Podaci se šalju u treću zemlju koja ne jamči odgovarajuću razinu zaštite.
	Gubitak uređaja (telefon, prijenosna računala i sl.); vjerodajnice; pristupne kartice.
NEŽELJENA IZMJENA OSOBNIH PODATAKA (RIZICI INTEGRITETA)	Podaci se mijenjaju u valjane ili nevaljane podatke koji se neće koristiti ispravno pa obrada može izazvati pogreške, neispravnosti ili više ne pruža očekivanu uslugu (npr. narušavajući pravilan napredak važnih koraka itd.).
	Podaci se modificiraju u druge važeće podatke tako da se postupci obrade upotrebljavaju ili mogu zloupotrijebiti (npr. upotreba za krađu identiteta promjenom odnosa između identiteta pojedinaca i biometrijskih podataka drugih pojedinaca itd.).
NESTANAK OSOBNIH PODATAKA (RIZICI DOSTUPNOSTI)	Nedostaju podaci za obradu osobnih podataka što dovodi do grešaka i nepravilnosti u radu ili dovodi do pružanja usluge koja je drugačija od očekivane (npr. nedostupni su podaci bankovnog računa što dovodi do zakašnjenja u isplati plaća itd.)

	Nedostaju podaci za obradu osobnih podataka koji više ne mogu pružiti očekivanu uslugu (npr. usporavanje ili blokiranje administrativnih ili komercijalnih procesa, nesposobnost ispitanika da izvrše svoja prava itd.).

3.1.5. Shema identifikacije rizika i mjera ublažavanja

REDNI BROJ	RIZICI PRIVATNOSTI	UTJECAJ NA POJEDINCE	VJEROJATNOST	OZBILJNOST	MJERE UBLAŽAVANJA	REZULTAT RIZIKA NAKON PRIMJENE MJERA	VJEROJATNOST	OZBILJNOST





3.2. Konzultacije

JESU LI KONZULTIRANI PREDSTAVNICI ISPITANIKA?

3.3. Postupak revizije

KAKO ĆE SE OVA PROCJENA UČINKA NA ZAŠTITU PODATAKA REVIDIRATI?

3.4. Zaključak

JE LI UTVRĐENI RIZIK OBRADE PRIHVATLJIV?

Hrzz
Hrvatska zaklada
za znanost

PROCJENA LEGITIMNOG INTERESA

VODITELJ OBRADE	
HRVATSKA ZAKLADA ZA ZNANOST, ILICA 24, 10 000 Zagreb (dalje: Zaklada ili Voditelj obrade)	
KONTAKT PODACI PUTEM KOJIH SE MOGU DOBITI SVE INFORMACIJE U VEZI OBRADE I KORIŠTENJA OSOBNIH PODATAKA:	
Elektronička pošta:	Službenik za zaštitu podataka: alen@hrzz.hr Zamjenik službenika za zaštitu podataka: lana@hrzz.hr
Adresa:	Ilica 24, 10 000 Zagreb
DATUM I MJESTO PROVOĐENJA ANALIZE:	
_____	

Ova procjena legitimnog interesa provodi se za obradu podataka u kojoj Hrvatska zaklada za znanost, Ilica 24, 10 000 Zagreb prikuplja podatke _____ u svrhu _____ i ima za cilj pokazati zakonitost obrade prema članku 6., stavku 1. (f) Opće uredbe o zaštiti osobnih podataka, kako je objašnjeno u uvodnoj izjavi 47.:

Legitimni interesi voditelja obrade, među ostalim onih interesa voditelja obrade kojem se osobni podaci mogu otkriti ili treće strane, mogu predstavljati pravnu osnovu za obradu pod uvjetom da interesi ili temeljna prava i slobode ispitanika nemaju prednost, uzimajući u obzir razumna očekivanja ispitanika koja se temelje na njihovom odnosu s voditeljem obrade. Takav legitiman interes mogao bi na primjer postojati u slučaju relevantnog i odgovarajućeg odnosa ispitanika i voditelja obrade u situacijama poput one kada je ispitanik klijent voditelja obrade ili u njegovoj službi. U svakom slučaju postojanje legitimnog interesa zahtijevalo bi pažljivu procjenu, među ostalim i toga može li ispitanik u vrijeme i u kontekstu prikupljanja osobnih podataka razumno očekivati obradu u dotičnu svrhu. Interesi i temeljna prava ispitanika posebno bi mogli nadvladati interes voditelja obrade ako se osobni podaci obrađuju u okolnostima u kojima ispitanici razumno ne očekuju daljnju obradu. Budući da je zakonodavac dužan zakonski odrediti pravnu osnovu za obradu osobnih podataka koju provode tijela javne vlasti, ta pravna osnova ne bi se smjela primjenjivati na obradu koju provode tijela javne vlasti pri izvršavanju svojih zadaća. Obrada osobnih podataka koja je nužna u svrhe sprečavanja prijevara također predstavlja legitiman interes dotičnog voditelja obrade podataka. Može se smatrati da postoji legitiman interes kod obrade osobnih podataka provedene za potrebe izravnog marketinga.

Ova procjena pomaže pobliže odrediti može li se osloniti na legitiman interes pri obradi osobnih podataka, a njeni zaključci mogu biti subjektivni i trebaju se temeljiti na iskustvu i prosudbi pojedinca ili grupe koji su izvršili procjenu. Ishod procjene treba biti dokumentiran kao dokaz i mora se pregledavati povremeno, osobito kada su se kriteriji korišteni u procjeni se značajno promijenili na bilo koji način koji bi mogao utjecati na ishod.

UTVRĐIVANJE LEGITIMNOG INTERESA		
1.	Koja je svrha aktivnosti obrade?	
2.	Je li obrada potrebna za ispunjavanje jednog ili više specifičnih ciljeva Zaklade?	
3.	Je li obrada potrebna za ispunjavanje jednog ili više specifičnih ciljeva bilo koje treće strane?	
4.	Utvrđuje li Uredba, Zakon ili drugo nacionalno zakonodavstvo aktivnosti obrade kao legitimnu aktivnost?	

TEST NUŽNOSTI		
1.	Zašto je obrada važna voditelju obrade odnosno Zakladi?	
2.	Zašto je obrada važna drugim stranama kojima mogu biti otkriveni podaci, ako je to primjenjivo?	
3.	Postoji li drugi način da se postigne cilj?	

TEST URAVNOTEŽENJA		
1.	Bi li pojedinac očekivao aktivnost obrade?	

2.	Dodaje li aktivnost obrade vrijednost proizvodu ili usluzi koju pojedinac koristi?	
3.	Je li vjerojatno da će aktivnost obrade negativno utjecati na prava Ispitanika?	
4.	Je li vjerojatno da će aktivnost obrade rezultirati neopravdanom štetom ili neprilikom za pojedinca?	
5.	Hoće li neprovođenje obrade prouzrokovati štetu za voditelja obrade?	
6.	Hoće li neprovođenje obrade prouzrokovati štetu za treću stranu?	
7.	Je li obrada u interesu osobe čiji se podaci prikupljaju?	
8.	Jesu li legitimni interesi ispitanika usklađeni sa legitimnim interesom stranke koja se na njega oslanja?	
9.	Koja je veza između pojedinca i Zaklade?	
10.	Koja je priroda podataka koji se obrađuju? Imaju li podaci ove prirode posebnu zaštitu prema Uredbi?	
11.	Postoji li dvosmjerni odnos između Zaklade i ispitanika? Ako da koliko je taj odnos blizak?	
12.	Hoće li obrada ograničiti ili potkopati prava pojedinaca?	
13.	Prikupljaju li se podaci izravno od ispitanika ili neizravno?	

14.	Postoji li neravnoteža u tome tko ima moć između Zaklade i pojedinca?	
15.	Je li vjerojatno da bi pojedinac mogao očekivati da se njihovi podaci koriste u tu svrhu?	
16.	Može li se obrada smatrati nametljivom ili neprikladnom? Konkretno, može li se obrada tako shvatiti od strane pojedinca ili u kontekstu odnosa?	
17.	Je li obavijest o obradi dostavljena pojedincu, ako da, kako? Jesu li oni sigurni i jasni u odnosu na svrhu obrade?	
18.	Može li pojedinac, čiji se podaci obrađuju, kontrolirati ili prigovoriti na obradu?	
19.	Može li se opseg obrade promijeniti kako bi se smanjili / ublažili bilo kakvi temeljni rizici ili štete za privatnosti?	

MJERE ZAŠTITE I KONTROLE		
	Zaštitne mjere uključuju i niz kontrola ili mjera koje se mogu uspostaviti kako bi se zaštitio pojedinac ili smanjili bilo kakvi rizici ili potencijalno negativne učinke obrade. Ta vjerojatnost identificira se putem Procjene utjecaja na privatnost provedene u odnosu na određenu aktivnost. Na primjer: minimiziranje podataka, de-identifikacija, tehničke i organizacijske mjere,	

	privatnost dizajnom, dodavanje dodatne transparentnosti, dodatni slojevi šifriranja, provjeravanje autentičnosti više čimbenika, zadržavanje, ograničeni pristup, opcije isključivanja i druge tehničke sigurnosne metode koje se koriste za zaštitu podataka. Navedite takve mjere koje će se uspostaviti ili su već uspostavljene kako bi se zaštitila prava pojedinca.	

DONOŠENJE ODLUKE I DOKUMMENTACIJA ISHODA		
	Upotrijebite gore navedene odgovore ukoliko vjerujete da se možete osloniti na legitiman interes kao pravnu osnovu za obradu osobnih podataka. Objasnite (koristeći natuknice) možete li se ili ne osloniti na taj legitiman interes, osvrćući se na odgovore dane u ovoj procjeni.	Ishod procjene:

OBAVIJEST ZAPOSLENICIMA

Hrvatska zaklada za znanost, Ilica 24, 10000 Zagreb (dalje u tekstu: „Zaklada“ ili „poslodavac“) prikuplja osobne podatke zaposlenika (dalje u tekstu: ispitanici) te je u skladu s propisima dužna ispitanicima pružiti sljedeće informacije:

1. Voditelj obrade u odnosu na zaposlenike je Hrvatska zaklada za znanost, Ilica 24, 10000 Zagreb.

Podaci službenika za zaštitu podataka: Alen Plančić, alen@hrzz.hr.

Podaci zamjenika službenika za zaštitu podataka: Lana Zubović, lana@hrzz.hr.

2. Primatelji osobnih podataka su: Hrvatski zavod za mirovinsko osiguranje, Hrvatski zavod za zdravstveno osiguranje, Ministarstvo financija (Porezna uprava), banka u kojoj zaposlenici voditelja obrade imaju otvoreni račun za izvršenje obveza od strane voditelja obrade, a koje se tiču isplate plaće i drugih naknada iz radnog odnosa, ordinacija koja za poslodavca obavlja poslove zdravstvene skrbi-ordinacija medicine rada i sl.

3. Podaci se prikupljaju na temelju prava i obveza koje proizlaze iz Zakona o radu, ali i drugih zakona koji uređuju radne odnose, kao i prava i obveze koje proizlaze iz ugovora o radu, a sve radi izvršenja zakonskih i ugovornih obveza ili legitimnih interesa poslodavca.

Pristup Vašim osobnim podacima imaju ovlaštene osobe Zaklade te, pod određenim propisanim okolnostima i samo uz dozvolu odgovorne osobe (primjerice u slučaju kvara), konzultanti koji pomažu IT podršci. Sve osobe koje mogu pristupiti Vašim osobnim podacima prilikom vršenja svojih redovnih radnih obveza potpisali su izjave o povjerljivosti.

Nadalje, moramo naglasiti kako je moguće otkrivanje Vaših osobnih podataka ovlaštenoj trećoj strani ako to zahtijevaju ili dopuštaju obvezujući propisi (npr. državna tijela, sudovi i ostale treće strane koje se smatraju javnim tijelima).

Vaši podaci ne prenose se u treće zemlje ili međunarodne organizacije.

4. Vaši osobni podaci se čuvaju sukladno važećim propisima RH i aktima Zaklade.

Primjerice, evidencija zaposlenika – čuva se trajno kao arhivsko gradivo sukladno Pravilima za upravljanja dokumentarnim gradivom Hrvatske zaklade za znanost (dalje: Pravila), određene podatke koje smo obvezni čuvati u skladu sa Zakonom o računovodstvu – 11 godina od prestanka ugovornog odnosa, isplatne liste čuvaju se 70 godina, ugovori o radu i djelu 10 godina sukladno roku određenim u Pravilima.

Voditelj obrade obrađuje podatke kao što su ime, prezime, adresa prebivališta, OIB, IBAN, godine radnog staža, zvanje, zanimanje, podatke o privremenoj nesposobnosti za rad, podatke o radnom

vremenu, podatke o korištenju godišnjeg odmora, e-mail, spol, dob, podatke o usavršavanjima te druge podatke koji proizlaze iz radnog odnosa.

5. Vaša prava kao ispitanika su sljedeća:

Pravo na pristup: imate pravo dobiti od nas potvrdu o tome obrađuju li se vaši osobni podaci, te ako se takvi osobni podaci obrađuju, pristup osobnim podacima. Informacije o pristupu uključuju - između ostalog - svrhe obrade, kategorije osobnih podataka o kojima je riječ, primatelje ili kategorije primatelja kojima su osobni podaci bili ili će biti otkriveni. Međutim, to nije bezuvjetno pravo i interesi drugih pojedinaca mogu ograničiti Vaše pravo pristupa.

Imate pravo dobiti kopiju osobnih podataka koji se obrađuju.

Pravo na ispravak: Imate pravo ishoditi od nas ispravljanje vaših netočnih osobnih podataka. Uzimajući u obzir svrhe obrade imate pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave.

Pravo na brisanje ("pravo na zaborav"): Pod određenim uvjetima, imate pravo ishoditi od nas brisanje vaših osobnih podataka i mi možemo biti obvezni izbrisati takve osobne podatke.

Pravo na ograničenje obrade: Pod određenim uvjetima, imate pravo ishoditi od nas ograničenje obrade vaših osobnih podataka. U tom će slučaju odgovarajući podaci biti označeni i mogu biti obrađeni samo u određene svrhe.

Pravo na prigovor: Pod određenim uvjetima, imate pravo na prigovor u bilo kojem trenutku na obradu vaših osobnih podataka, iz razloga koji se odnose na vašu konkretnu situaciju ili kada se osobni podaci obrađuju u cilju izravnog marketinga te možete tražiti od nas da više ne obrađujemo vaše osobne podatke.

Pravo na prenosivost podataka: Pod određenim uvjetima, imate pravo zaprimiti osobne podatke koji se odnose na vas, koje ste nam pružili u strukturiranom, uobičajeno upotrebljivom i strojno čitljivom formatu i imate pravo prenijeti te podatke drugom voditelju obrade, bez našeg ometanja.

Uz navedena prava, voditelj obrade osigurava ovlaštenim osobama, na njihov zahtjev, dostupnost podataka iz evidencije o radnicima, i to, između ostalog, uvidom u pisani pregled osnovnih podataka za svakog radnika te uvidom u isprave, dokumente i akte vezane za radni odnos ili za ostvarivanje pojedinih prava iz radnog odnosa ili u vezi s radnim odnosom.

Također, voditelj obrade ovlaštenim osobama omogućava preuzimanje pisanog dokumenta u papirnatom ili elektroničkom obliku, s podacima o radniku koje vodi u evidenciji o radnicima ili ga čuva pohranjenog na način i u rokovima sukladno aktima Zaklade te važećim propisima Republike Hrvatske.

Detaljno o načinu ostvarenja navedenih prava možete pročitati u Pravilniku o zaštiti osobnih podataka.

6. Ako želite saznati više ili želite koristiti jedan ili više od gore navedenih prava, slobodno kontaktirajte našeg službenika za zaštitu podataka putem e-maila: alen@hrzz.hr ili lana@hrzz.hr.

7. Ako smatrate da se Vaša prava krše imate pravo podnijeti pritužbu Agenciji za zaštitu osobnih podataka (Ulica Metela Ožegovića 16, 10 000 Zagreb).

8. Vaše podatke prikupljamo radi ispunjenja zakonske obveze koja je nužna za sklapanje ugovora o radu, za prijavu Hrvatskom zavodu za mirovinsko osiguranje i Hrvatskom zavodu za zdravstveno osiguranje te primjerice radi:

- utvrđivanja zdravstvene sposobnosti zaposlenika,
- osposobljavanja zaposlenika za rad na siguran način te dobivanje potvrde o osposobljenosti zaposlenika za provođenje zaštite na radu i zaštite od požara.

9. Vaši osobni podaci obrađivat će se isključivo u gore navedene svrhe, osim ako je to neophodno za poštivanje zakonskih obveza (npr. za dostavljanje podataka sudovima ili organima kaznenog progona), ako ste pristali na odgovarajuću obradu ili ako je obrada na drugi način zakonita prema obvezujućim propisima.

Ako se podaci obrađuju u drugu svrhu, prije obrade pružit ćemo vam informacije o toj drugoj svrsi te sve druge relevantne informacije.

10. Voditelj obrade može obrađivati osobne podatke na temelju sljedećih pravnih osnova:

a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha;
b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;
c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade;
d) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe;
e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;
f) obrada je nužna za potrebe legitimnih interesa voditelja obrade 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 (iznimka - obrada koju provode tijela javne vlasti pri izvršavanju svojih zadaća).

11. Ako se obrada temelji na privoli ispitanika, ispitanik ima pravo u bilo kojem trenutku povući privolu. O povlačenju privole potrebno je obavijestiti voditelja obrade putem e-maila: alen@hrzz.hr ili lana@hrzz.hr ili na adresu koja je navedena u kontakt podacima voditelja obrade. Takvo povlačenje neće utjecati na zakonitost obrade na temelju privole prije njezina povlačenja.

12. Zaposlenik ima obvezu čuvati povjerljivima sve podatke do kojih je došao tijekom svog radnog odnosa kod voditelja obrade, a koji nisu dostupni javnosti te će se svi takvi podaci smatrati poslovnom tajnom sukladno propisima Republike Hrvatske.

Poslovnom tajnom se osobito smatraju te je iste zabranjeno otkrivati i/ili u svoju ili tuđu korist rabiti podatke o plaćama i stimulacijama zaposlenika, razvoju proizvoda i tehnologije poslovanja, o istraživanjima i projektima, know-how tehnologijama, marketinškim planovima te drugim poslovnim informacijama i svim drugim podacima koje je Zaklada tako odredila. Iznimno, zabrana ne obuhvaća informacije i podatke koji su bez odgovornosti ispitanika javno obznanjeni ili za objavu kojih je voditelj obrade prethodno dao ispitaniku pisano odobrenje.

Danom prestanka radnog odnosa zaposlenik je dužan vratiti sve izvornike i preslike poslovnih dokumenata, službenih isprava, telefona, kontakata koji su mu povjereni ili kojima je imao pristup, uključujući i poslovne bilješke zabilježene na papiru, računalu ili drugom mediju te kodove, šifre, memorandume, iskaznice, propusnice i dr.

Zaposlenik je dužan čuvati poslovnu tajnu i nakon prestanka radnog odnosa.

Zaposlenik se obavještava o pravu poslodavca na naknadu štete ako dođe do povrede pravila o tajnosti podataka koje je zabranjeno otkrivati trećim strana.

13. Ova obavijest objavit će se na oglasnoj ploči voditelja obrade, a primjerak obavijesti pohranit će se u arhivu.

Ime i prezime i potpis zaposlenika te datum zaprimanja:

_____

IZJAVA O POVJERLJIVOSTI

I.

Ovom izjavom potpisnik se obvezuje da će u skladu s propisima koji uređuju područje zaštite 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 (Opća uredba o zaštiti podataka), Zakonom o provedbi Opće uredbe o zaštiti podataka (NN 42/2018) i Pravilnikom o zaštiti osobnih podataka, čuvati povjerljivost svih osobnih podataka koje dobije na uvid ili sazna za iste prilikom obavljanja obveza iz ugovora o radu ili nekog drugog ugovora kojim se uređuju međusobna prava i obveze stranaka, kao i čuvati povjerljivost svih osobnih podataka kojima ima pravo i ovlast pristupa, a koji se nalaze u sustavima pohrane koje vodi Hrvatska zaklada za znanost u kojoj je zaposlen.

II.

Potpisnik se obvezuje odnositi prema primljenim informacijama sa strogom povjerljivosti i tajnosti, ne otkriti nijednoj trećoj (neovlaštenoj) strani bilo koju od informacija koje je doznao na radnom mjestu ili prilikom obavljanja poslova u ime i za račun Hrvatske zaklade za znanost, Ilica 24, 10000 Zagreb (dalje u tekstu: „Zaklada“ ili „Voditelj obrade“) te ne smije iskoristiti ni jednu od prikupljenih informacija na drugi način nego kako je to predviđeno ugovornim obvezama i/ili drugom svrhom obrade podataka. Ova obaveza traje i po prestanku ugovora o radu ili nekog drugog ugovora kojim se uređuju međusobna prava i obveze stranaka.

Osobni podaci ispitanika Voditelja obrade ne smiju se obrađivati u druge svrhe osim onih određenih aktima i važećim propisima Republike Hrvatske.

Voditelj obrade osobnih podataka u odnosu na zaposlenike je Zaklada.

~~V.~~III.

Potpisnik ove izjave odgovoran je ako prilikom obrade osobnih podataka namjerno ili krajnjom nepažnjom prekorači granice svojih ovlasti i/ili osobne podatke prikuplja i/ili obrađuje za drugu namjenu osim ugovorene i/ili ih daje na korištenje drugim primateljima i/ili ne osigura provođenje ugovorenih mjera zaštite osobnih podataka, a radi takve obrade dođe do imovinske, neimovinske ili druge osobne štete ispitanika te s tim u vezi i Zaklade kao voditelja obrade.

Potpisnik izričito izjavljuje da je u potpunosti svjestan kaznene odgovornosti u slučaju kršenja obveza čuvanja podataka, posebice u pogledu kaznenih djela popisanih Kaznenim zakonom (dalje u tekstu: KZ): povrede tajnosti pisama i drugih pošiljaka (čl. 142. KZ-a), odavanja i neovlaštenog pribavljanja poslovne tajne (čl. 262. KZ-a), odavanja tajnih podataka (čl. 347. KZ-a) te špijunaže (čl. 348. KZ-a).

Potpisom ove izjave, potpisnik potvrđuje da je razumio tekst ove izjave te sve obveze i prava koje iz nje proizlaze, stoga u znak prihvata prava, obveza i svih eventualnih posljedica koje proizlaze iz istoga vlastoručno je potpisuje.

Ime i prezime: _____

Datum i mjesto: _____

Potpis:

_____

NAVEDITE AKTIVNOSTI OBRADE U KOJIMA SE OSOBNI PODACI OBRAĐUJU	STATUS ORGANIZACIJE (VODITELJ/IZVRŠITELJ)	PRAVNA OSNOVA	SVRHA OBRADE OSOBNIH PODATAKA	KATEGORIJE ISPITANIKA	KATEGORIJE OSOBNIH PODATAKA	KATEGORIJE PRIMATELJA	INFORMACIJE O PRIJENOSU U TREĆE ZEMLJE ILI MEĐ. ORGANIZACIJE (AKO POSTOJI)	ROK ČUVANJA	OPĆI OPIS TEHNIČKIH I ORGANIZACIJSKIH SIGURNOSNIH MJERA

Hrvatska zaklada za znanost, Ilica 24, 10 000 Zagreb (u daljnjem tekstu: **„Voditelj obrade”**)

I

XXXXX

XXXXX (u daljnjem tekstu: **„Izvršitelj obrade**”),

zaključili su

UGOVOR O OBRADI I DIJELJENJU PODATAKA

Uvodne odredbe

Članak 1.

(1) Ovim Ugovorom utvrđuju se prava i obveze ugovornih stranaka vezanih uz svaku obradu osobnih podataka od strane Izvršitelja obrade, koja se provodi tijekom izvršavanja zasebnih ugovornih odnosa iz _____ (dalje u tekstu: Osnovni ugovor(i)) koji su na snazi ili budu sklopljeni u budućnosti između Voditelja i Izvršitelja obrade radi izvršavanja tih usluga.

(2) Postupak ugovorene obrade podataka načelno se izvodi isključivo u državi članici Europske unije (EU) ili u državi članici Europskog gospodarskog prostora (EGP). Svaki prijenos podataka u zemlju koja nije država članica EU-a ili EGP-a izvodi se samo ako je određen u opisu usluge ili ga je Voditelj obrade odobrio na neki drugi način te ako su ispunjeni specifični uvjeti iz članka 44. i ostalih članaka Opće uredbe o zaštiti podataka.

(3) Izvršitelj obrade se obvezuje obavijestiti Voditelja obrade pisanim putem i dostavlja odgovarajuće dokaze o tome kako se odgovarajuća razina zaštite za takve prijenose osigurava u svakom slučaju.

The Croatian Science Foundation, Ilica 24, 10 000 Zagreb (hereinafter: “**Data Controller**”)

And

XXXXX

XXXXX (hereinafter: “**Data Processor**”),

have concluded the following

DATA PROCESSING AGREEMENT

Introductory provisions

Article 1

(1) This Agreement establishes the rights and obligations of the Contracting Parties related to any processing of personal data by the Data Processor, which is carried out during the execution of separate contractual relationships from _____ (hereinafter: Primary contract(s)) that are in force or will be concluded in the future between the Data Controller and the Data Processor for the purpose of performing those services.

(2) The process of contracted data processing is, in principle, carried out exclusively in a member state of the European Union (EU) or in a member state of the European Economic Area (EEA). Any transfer of data to a country that is not a member state of the EU or the EEA is performed only if specified in the service description or approved by the Data Controller in some other way, and if the specific conditions from Article 44 and other articles of the General Data Protection Regulation are met.

(3) The Data Processor undertakes to inform the Data Controller in writing and provides appropriate evidence of how the appropriate level of protection for such transfers is ensured in any

(4) Vrste podataka i opis obrade nalaze se u Prilogu 1. ovog Ugovora.

Tehničke i organizacijske mjere

Članak 2.

(1) Prije početka obrade Voditelj obrade dokumentira i nalaže Izvršitelju obrade provedbu potrebnih tehničkih i organizacijskih mjera. Ako se inspekcijom/revizijom koju provede Voditelj obrade utvrdi da su potrebne izmjene i dopune, takve se izmjene i dopune moraju provesti uz međusobnu suglasnost.

(2) Izvršitelj obrade osigurava sigurnost u skladu s člankom 28. stavkom 3. točkom (c) i člankom 32. Opće uredbe o zaštiti podataka, posebno u vezi s člankom 5. stavcima 1. i 2. Opće uredbe o zaštiti podataka. Mjere koje je potrebno poduzeti su mjere za sigurnost podataka i mjere koje jamče odgovarajuću razinu zaštite s obzirom na rizik povezan s povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava. Moraju se uzeti u obzir najnovija dostignuća, troškovi provedbe te priroda, opseg i svrhe obrade, kao i vjerojatnost pojave i ozbiljnost opasnosti za prava i slobode fizičkih osoba u smislu članka 32. stavka 1. Opće uredbe o zaštiti podataka.

(3) Sigurnosne mjere koje provodi Izvršitelj obrade opisane su u Prilogu 2. ovog Ugovora. Izvršitelju obrade je dopušteno provoditi alternativne odgovarajuće mjere, ali pritom se ne smije smanjiti stupanj zaštite koji osiguravaju definirane mjere. Bitne izmjene moraju se dokumentirati.

(4) Izvršitelj obrade na zahtjev pisanim putem potpuno i detaljno obavještava Voditelja obrade o konkretnim mjerama koje su poduzete u skladu s njegovim dužnostima iz članka 3. i dodatnim dužnostima navedenima u članku 5. ovog Ugovora.

case.

(4) The types of data and a description of the processing can be found in Appendix 1 of this Agreement.

Technical and organizational measures

Article 2

(1) Before the start of processing, the Data Controller documents and instructs the Data Processor to implement the necessary technical and organizational measures. If an inspection/audit carried out by the Data Controller determines that changes and additions are necessary, such changes and additions must be carried out with mutual consent.

(2) The Data Processor ensures security in accordance with Article 28 paragraph 3(c) and Article 32 of the General Data Protection Regulation, in particular in connection with Article 5 paragraphs 1 and 2 of the General Data Protection Regulation. The measures that need to be taken are measures for data security and measures that guarantee an adequate level of protection with regard to the risk associated with the confidentiality, integrity, availability and resilience of the system. The latest developments, costs of implementation and the nature, extent and purposes of processing, as well as the likelihood of occurrence and the seriousness of the threat to the rights and freedoms of natural persons in the sense of Article 32 paragraph 1 of the General Data Protection Regulation must be taken into account.

(3) The security measures implemented by the Data Processor are described in Appendix 2. to this Agreement. The Data Processor is allowed to implement alternative appropriate measures, but the degree of protection provided by the defined measures must not be reduced. Significant changes must be documented.

(4) Upon request, the Data Processor shall inform the Data Controller fully and in detail in writing about the specific measures taken in accordance with his duties from Article 3 and additional duties

Ispravljanje, ograničavanje i brisanje podataka

Članak 3.

(1) Izvršitelj obrade ne smije ispravljati ili brisati podatke koji se obrađuju u ime Voditelja obrade niti ograničavati njihovu obradu prema vlastitom nahođenju, nego samo na temelju dokumentiranih uputa Voditelja obrade.

(2) Ako ispitanik izravno kontaktira Izvršitelja obrade u vezi s ispravljanjem, brisanjem ili ograničenjem obrade podataka, Izvršitelj obrade će zahtjev ispitanika bez odgode proslijediti Voditelju obrade.

(3) Ako je to uključeno u opseg usluga, Izvršitelj obrade bez odgode osigurava pravo brisanja, „pravo na zaborav", ispravak, prenosivost podataka i pristup podacima u skladu s dokumentiranim uputama Voditelja obrade.

Osiguranje kvalitete i ostale dužnosti izvršitelja obrade

Članak 4.

(1) Osim pridržavanja pravila utvrđenih u ovom Ugovoru, Izvršitelj obrade je dužan poštovati obveze iz članaka 28. do 33. Opće uredbe o zaštiti podataka te u skladu s time, Izvršitelj obrade posebno osigurava usklađenost sa sljedećim zahtjevima:

a) Pisano imenovanje službenika za zaštitu podataka, koji izvršava svoje dužnosti u skladu s člancima 38. i 39. Opće uredbe o zaštiti podataka.
b) Voditelju obrade se pružaju njegovi podaci za kontakt u svrhu izravnog kontaktiranja. Voditelja obrade se odmah obavješćuje o svakoj promjeni službenika za zaštitu podataka.

☐ Izvršitelj obrade je imenovao

specified in Article 5 of this Agreement.

Correction, restriction and deletion of data

Article 3

(1) The Data Processor may not correct or delete the data processed on behalf of the Data Controller or limit their processing at its own discretion, but only based on the documented instructions of the Data Controller.

(2) If a data subject directly contacts the Data Processor regarding the correction, deletion or restriction of data processing, the Data Processor will forward the data subject's request to the Data Controller without delay.

(3) If this is included in the scope of the services, the Data Processor ensures without delay the right to deletion, "right to be forgotten", correction, data portability and data access in accordance with documented instructions of the Data Controller.

Quality assurance and other duties of the Data Processor

Article 4

(1) In addition to complying with the rules set forth in this Agreement, the Data Processor is obliged to comply with the obligations from Articles 28 to 33 of the General Data Protection Regulation and accordingly, the Data Processor particularly ensures compliance with the following requirements:

a) Written appointment of a data protection officer, who performs his duties in accordance with Articles 38 and 39 of the General Data Protection Regulation.
b) The Data Controller is provided with his contact information for the purpose of direct contact. The Data Controller is immediately notified of every change of the data protection officer.

g./gđu …….. *[unesite: ime, prezime, kontakt podatke]* službenikom za zaštitu podataka. Voditelja obrade se odmah obavješćuje o svakoj promjeni službenika za zaštitu podataka.

(2) Izvršitelj obrade obvezuje se da podaci službenika za zaštitu osobnih podataka budu uvijek točni te da su navedeni i lako dostupni na mrežnoj stranici Izvršitelja obrade ili drugi odgovarajući način.

Podugovaranje

Članak 5.

(1) Podugovaranje se za potrebe ovog Ugovora tumači kao usluge koje se izravno odnose na pružanje glavne usluge. To ne obuhvaća pomoćne usluge kao što su poštanske ili usluge prijevoza, usluge održavanja/čišćenja poslovnih prostora i fizičke sigurnosti. Izvršitelj obrade je, međutim, obvezan sklopiti odgovarajuće i zakonski obvezujuće ugovore te poduzeti prikladne inspekcijske mjere da bi osigurao zaštitu i sigurnost podataka Voditelja obrade, čak i u slučaju eksternaliziranih pomoćnih usluga.

(2) Izvršitelj obrade može angažirati podizvršitelje (dodatne ugovorne izvršitelje obrade) samo nakon pribavljanja prethodne izričite pisane ili dokumentirane suglasnosti Voditelja obrade (Prilog 3 – Popis podizvršitelja.)

(3) Voditelj obrade pristat će na angažiranje podizvršitelja uz uvjet sklapanja ugovora u skladu s člankom 28. stavcima 2. do 4. Opće uredbe o zaštiti podataka odnosno na način da ga se obavijesti o nazivu, adresi, zemlji te uslugama.

(4) Angažiranje podizvršitelja ili promjena

☐ The Data Processor has appointed Mr./Ms. …….. [enter in: first name, last name, contact information] as data protection officer. The Data Controller is immediately notified of every change of the data protection officer.

(2) The Data Processor undertakes that the information regarding the data protection officer is always correct and that it is listed and easily accessible on the website of the Data Processor or in another appropriate way.

Subcontracting

Article 5

(1) For the purposes of this Agreement, subcontracting is interpreted as services directly related to the provision of the main service. This does not include ancillary services such as postal or transportation services, maintenance/cleaning services for business premises and physical security. The Data Processor is, however, obliged to enter into appropriate and legally binding contracts and take appropriate inspection measures to ensure the protection and security of the Data Controller's data, even in the case of outsourced ancillary services.

(2) The Data Processor may hire subprocessors (additional contractual data processors) only after obtaining the prior express written or documented consent of the Data Controller (Appendix 3 – List of subprocessors).

(3) The Data Controller will agree to the engagement of a subprocessor with the condition that a contract has been concluded in accordance with Article 28, paragraphs 2 to 4 of the General Data Protection Regulation, that is, with informing him of the name, address, country and services.

(4) Contracting a subprocessor or changing an

postojećeg podizvršitelja dopušteni su:

a) ako Izvršitelj obrade dovoljno unaprijed obavijesti Voditelja obrade o takvom angažiranju podizvršitelja u pisanom ili elektroničkom obliku, i
b) ako Voditelj obrade nije uložio prigovor na planiranu eksternalizaciju u pisanom ili elektroničkom obliku do datuma predavanja podataka Izvršitelju obrade, i
c) ako je podugovaranje utemeljeno na ugovoru u skladu s člankom 28. stavcima 2. do 4. Opće uredbe o zaštiti podataka.

(5) Prijenos osobnih podataka podizvršitelju i obrada podataka koju provodi podizvršitelj smiju početi tek nakon što se osigura usklađenost sa svim zahtjevima iz članka 28. Opće uredbe o zaštiti podataka i ovog Ugovora.

(6) Ako podizvršitelj pruža ugovorenu uslugu izvan EU-a/EGP-a, Izvršitelj obrade pomoću odgovarajućih mjera osigurava usklađenost s propisima o zaštiti podataka u EU. Isto vrijedi ako će se angažirati pružatelji usluga u smislu stavka 1. ovog članka.

(7) Daljnja eksternalizacija koju provodi podizvršitelj nije dopuštena.

Nadzorne ovlasti Voditelja obrade

Članak 6.

(1) Voditelj obrade ima pravo nakon savjetovanja s Izvršiteljem obrade provesti inspekcije ili ih povjeriti revizoru koji će se imenovati u svakom pojedinom slučaju. Voditelj obrade ima pravo provjeriti usklađenost Izvršitelja obrade i njegova poslovanja s ovim Ugovorom putem nasumičnih provjera koje se obično moraju pravovremeno najaviti.

(2) Izvršitelj obrade pruža razumnu pomoć kako bi Voditelj obrade mogao provjeriti usklađenost s obvezama Izvršitelja obrade u skladu s

existing subprocessor is allowed:

a) if the Data Processor notifies the Data Controller sufficiently in advance of such hiring of subprocessors in written or electronic form, and
b) if the Data Controller has not objected to the planned outsourcing in written or electronic form by the date of handing over the data to the Data Processor, and
c) if the subcontracting is based on a contract in accordance with Article 28 paragraphs 2 to 4 of the General Data Protection Regulation.

(5) The transfer of personal data to the subprocessor and data processing by the subprocessor may begin only after ensuring compliance with all requirements from Article 28. of the General Data Protection Regulation and this Agreement.

(6) If the subprocessor provides the contracted service outside the EU/EEA, the Data Processor ensures compliance with EU data protection regulations using appropriate measures. The same applies if service providers will be engaged in the sense of paragraph 1 of this Article.

(7) Further outsourcing by a subcontractor is not allowed.

Supervisory powers of the Data Controller

Article 6

(1) The Data Controller has the right, after consultation with the Data Processor, to carry out inspections or entrust them to an auditor who will be appointed in each individual case. The Data Controller has the right to check the compliance of the Data Processor and its operations with this Agreement by means of random audits which must usually be announced in a timely manner.

(2) The Data Processor provides reasonable assistance so that the Data Controller can verify compliance with the Data Processor's obligations

člankom 28. Opće uredbe o zaštiti podataka. Izvršitelj obrade se obvezuje na zahtjev dostaviti Voditelju obrade potrebne informacije kako bi dokazao izvršenje tehničkih i organizacijskih mjera.

in accordance with Article 28 of the General Data Protection Regulation. The Data Processor undertakes to provide the Data Controller with the necessary information upon request to prove the execution of technical and organizational measures.

Komunikacija u slučaju povreda koje je počinio Izvršitelj obrade

Članak 7.

(1) Izvršitelj obrade pomaže Voditelju obrade u ispunjavanju obveza u pogledu zaštite osobnih podataka, zahtjeva za izvještavanje o povredi podataka, procjena učinka na zaštitu podataka i prethodnog savjetovanja iz članaka 32. do 36. Opće uredbe o zaštiti podataka. To uključuje:

a) osiguravanje primjerene razine zaštite pomoću tehničkih i organizacijskih mjera koje uzimaju u obzir okolnosti i svrhe obrade te predviđenu vjerojatnost i ozbiljnost moguće povrede zakona uslijed sigurnosnih propusta i koje omogućuju trenutno otkrivanje relevantnih slučaja povrede,
b) obvezu izvještavanja Voditelja obrade o povredi osobnih podataka bez odgode,
c) dužnost pružanja razumne pomoći Voditelju obrade u vezi s obvezom pružanja informacija ispitanicima i ostvarivanja njihovih prava, te pružanja svih relevantnih informacija o tome Voditelju obrade bez dogode,
d) pružanje podrške Voditelju obrade u procjeni učinka na zaštitu podataka,
e) pružanje podrške Voditelju obrade u pogledu prethodnog savjetovanja s nadzornim tijelom.

(2) Izvršitelj obrade će za vrijeme i nakon isteka Ugovora nadoknaditi štetu (uključujući pravne troškove), a koja je vezana uz kršenje obveza ovog Ugovora od strane Izvršitelja obrade i/ili bilo koji

Communication in case of violations committed by the Data Processor

Article 7

(1) The Data Processor assists the Data Controller in fulfilling obligations regarding personal data protection, data breach reporting requirements, data protection impact assessments and prior consultation from Articles 32 to 36 of the General Data Protection Regulation. This includes:

a) ensuring an adequate level of protection by means of technical and organizational measures that take into account the circumstances and purposes of processing and the predicted probability and severity of a possible violation of the law due to security flaws and that enable the immediate detection of relevant cases of violation,
b) the obligation to report a personal data breach to the Data Controller without delay,
c) the duty to provide reasonable assistance to the Data Controller in connection with the obligation to provide information to Data Subjects and exercise their rights, and to provide all relevant information about this to the Data Controller without delay,
d) providing support to the Data Controller for data protection impact assessments,
e) providing support to the Data Controller regarding prior consultation with the supervisory authority.

(2) During and after the expiration of the Agreement, the Data Processor shall compensate for damages (including legal costs) related to the breach of obligations of this Agreement by the Data

incident vezan uz osobne podatke za koji je odgovoran Izvršitelj obrade.

Ovlast Voditelja obrade za izdavanje uputa

Članak 8.

(1) Voditelj obrade odmah potvrđuje usmene upute u pisanom ili elektroničkom obliku.

(2) Izvršitelj obrade bez odgode obavješćuje Voditelja obrade ako smatra da neka uputa krši propise o zaštiti podataka; međutim, samo prihvaćanje upute ne potvrđuje niti implicira da je ta uputa u skladu s propisima o zaštiti podataka. Izvršitelj obrade tada ima pravo obustaviti izvršavanje relevantnih uputa dok ih Voditelj obrade ne potvrdi ili izmijeni.

Brisanje i vraćanje osobnih podataka

Članak 9.

(1) Kopije ili duplikati podataka nikada se ne smiju izrađivati bez znanja Voditelja obrade, uz iznimku sigurnosnih kopija ako su nužne za osiguravanje uredne obrade podataka, kao i podataka potrebnih za ispunjavanje regulatornih zahtjeva za zadržavanje podataka.

(2) Nakon završetka ugovorenog posla ili prije, na zahtjev Voditelja obrade, a najkasnije nakon završetka trajanja Ugovora o pružanju usluga, Izvršitelj obrade će Voditelju obrade predati ili, ovisno o prethodnoj suglasnosti, uništiti sve dokumente, rezultate obrade i korištenja te skupove podataka povezane s Ugovorom koji su došli u njegov posjed, na način usklađen sa zaštitom podataka. Isto vrijedi za sve povezane ispitne, otpadne, redundantne i odbačene materijale. Zapisnik o uništenju ili brisanju dostavlja se na zahtjev.

(3) Dokumentaciju koja se upotrebljava kao dokaz uredne obrade podataka u skladu s narudžbom Izvršitelj obrade pohranjuje dulje od trajanja ovog

Processor and/or any incident related to personal data for which the Data Processor is responsible.

Authority of the Data Controller to issue instructions

Article 8

(1) The Data Controller immediately confirms verbal instructions in written or electronic form.

(2) The Data Processor shall notify the Data Controller without delay if it considers that an instruction violates data protection regulations; however, mere acceptance of an instruction does not confirm or imply that the instruction complies with data protection regulations. The Data Processor then has the right to suspend the execution of the relevant instructions until the Data Controller confirms or changes them.

Deleting and returning personal data

Article 9

(1) Copies or duplicates of data may never be made without the knowledge of the Data Controller, with the exception of backup copies if they are necessary to ensure proper data processing, as well as data required to meet regulatory data retention requirements.

(2) After the end of the contracted work, or before at the request of the Data Controller, and at the latest after the end of the Service Agreement, the Data Processor shall hand over to the Data Controller or, depending on prior consent, destroy all documents, results of processing and use, and data sets related to the Agreement which came into his possession, in a manner compliant with data protection. The same applies to all related test, waste, redundant and discarded materials. A record of destruction or deletion is provided upon request.

(3) Documentation that is used as evidence of proper data processing in accordance with the order is stored by the Data Processor for longer

Ugovora u skladu s odgovarajućim razdobljima zadržavanja. Izvršitelj obrade takvu dokumentaciju po završetku trajanja ovog Ugovora može predati Voditelju obrade da bi se oslobodio te ugovorne obveze.

than the duration of this Agreement in accordance with the appropriate retention periods. The Data Processor may hand over such documentation to the Data Controller at the end of the term of this Agreement in order to be released from this contractual obligation.

Hrvatska zaklada za znanost	**XXXXXX**
_____	_____
Mjesto, datum	Mjesto, datum

The Croatian Science Foundation	**XXXXXX**
_____	_____
Place, date	Place, date

Prilog 1. Opis obrade osobnih podataka

KATEGORIJE ISPITANIKA ČIJI SE OSOBNI PODACI OBRAĐUJU	CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS PROCESSED
_____	_____
KATEGORIJE OSOBNIH PODATAKA	CATEGORIES OF PERSONAL DATA
_____	_____
SVRHA OBRADE	PURPOSE OF PROCESSING
_____	_____
PRIRODA OBRADE (npr. prikupljanje, strukturiranje, pohrana, obavljanje uvida)	NATURE OF PROCESSING (e.g., collection, structuring, storage, inspection)
_____	_____
RAZDOBLJE U KOJEM ĆE SE OSOBNI PODACI ČUVATI ILI KRITERIJI NA TEMELJU KOJIH SE UTVRĐUJE TO RAZDOBLJE	THE PERIOD FOR WHICH PERSONAL DATA WILL BE KEPT OR THE CRITERIA ON THE BASIS OF WHICH THAT PERIOD IS DETERMINED
_____	_____

Appendix 1. Description of personal data processing

Prilog 2. – Tehničke i organizacijske mjere koje

Appendix 2. Technical and organizational

poduzima Izvršitelj obrade

1. **<u>ORGANIZACIJA INFORMACIJSKE SIGURNOSTI: POLITIKE I STANDARDI INFORMACIJSKE SIGURNOSTI</u>**

   Izvršitelj obrade će održavati korporativnu organizaciju za informacijsku sigurnost koja će biti zadužena za upravljanje politikama informacijske sigurnosti Izvršitelja obrade.

   a. Organizacija za informacijsku sigurnost biti će odgovorna za:

      i. Izvođenje periodičnih procjena sigurnosnih rizika na licu mjesta (i) postrojenja za obradu podataka, sistema i aplikacija Izvršitelja obrade te (ii) postrojenja za obradu podataka, sistema i aplikacija izvođača obrade (kao podizvršitelja obrade) u mjeri u kojoj izvođači obrađuju podatke ili imaju interakciju sa okruženjima za obradu od Izvršitelja obrade ili onih od suradnika Izvršitelja obrade.

      ii. Organizirati procjene sigurnosti provedene od strane neovisne treće strane (kao što je procjena ranjivosti, procjena politike informacijske sigurnosti ili penetracijsko testiranje) na godišnjoj razini.

      iii. Savjetovati izvršno rukovodstvo, revizijsku komisiju Izvršitelja obrade, te njegov upravni odbor o politikama informacijske sigurnosti Izvršitelja obrade, potencijalnim rizicima i planovima za ublažavanje učinaka.

      iv. Proglasiti i održavati razumne i prikladne politike informacijske sigurnosti, procedure i standarde koji adekvatno osiguravaju povjerljivost, integritet i dostupnost podataka koje obrađuje Izvršitelj obrade. Takve politike, procedure i standardi će uključivati bez ograničenja, one koji su dizajnirani da zaštite podatke koji su obrađeni sa udaljenih lokacija, uključujući postrojenja i lokacije za

measures undertaken by the Data Processor

1. **<u>INFORMATION SECURITY ORGANIZATION: INFORMATION SECURITY POLICIES AND STANDARDS</u>**

   The Data Processor shall maintain a corporate information security organization that will be in charge of managing the Data Processor's information security policies.

   a. The information security organization shall be responsible for:

      i. Performing periodic on-site security risk assessments of (i) Data Processor's data processing facilities, systems and applications; and (ii) data processing facilities, systems and applications of processing contractors (as data subprocessors) to the extent that the contractors process the data or interact with the processing environments of the Data Processor or those of the Data Processor's associates.

      ii. Organize security assessments conducted by an independent third party (such as vulnerability assessment, information security policy assessment, or penetration testing) on an annual basis.

      iii. Advise the executive management, the audit committee of the Data Processor, and its board of directors on the information security policies of the Data Processor, potential risks and mitigation plans.

      iv. Adopt and maintain reasonable and appropriate information security policies, procedures and standards that adequately ensure the confidentiality, integrity and availability of data processed by the Data Processor. Such policies, procedures, and standards will include, without limitation, those designed to protect data processed from remote locations, including employee remote work facilities and

daljinski rad zaposlenika.

v. Periodički procjenjivati i ažurirati politike informacijske sigurnosti Izvršitelja obrade, njegove procedure i standarde kako bi se adresirale nove i nastajuće prijetnje i promjene zakonskih uvjeta i industrijskih standarda.

vi. Pružiti rukovodstvu usmjerenje i potporu za informacijsku sigurnost u skladu sa zahtjevima u poslovanju i relevantnim zakonima i pravilima.

b. Izvršitelj obrade trebao bi dokumentirati zasebnu namjensku sigurnosnu politiku u pogledu obrade osobnih podataka. Sigurnosnu politiku treba odobriti uprava i priopćiti je svim zaposlenicima i relevantnim vanjskim stranama. Sigurnosna politika trebala bi se barem odnositi na: uloge i odgovornosti osoblja, osnovne tehničke i organizacijske mjere usvojene za sigurnost osobnih podataka, podizvršitelje obrade podataka ili druge treće strane uključene u obradu osobnih podataka. Inventar posebnih politika/postupaka koji se odnose na sigurnost osobnih podataka trebao bi se stvoriti i održavati na temelju opće sigurnosne politike. Uloge i odgovornosti u vezi s obradom osobnih podataka trebaju biti jasno definirane i raspoređene u skladu sa sigurnosnom politikom. Sigurnosnu politiku obrade osobnih podataka trebalo bi preispitivati i po potrebi revidirati semestralno.

c. Treba izvršiti jasno imenovanje osoba zaduženih za posebne sigurnosne zadatke, uključujući imenovanje službenika za sigurnost. Službenik za sigurnost trebao bi biti službeno imenovan (dokumentiran). Zadaće i odgovornosti službenika za sigurnost također bi trebali biti jasno postavljeni i dokumentirani.

d. Sukobljene dužnosti i područja odgovornosti, na primjer uloge službenika za sigurnost, revizora sigurnosti i službenika za zaštitu podataka, trebale bi se odvojiti kako bi se smanjile mogućnosti za neovlaštenu ili nenamjernu izmjenu ili zlouporabu osobnih podataka.

locations.

v. Periodically evaluate and update the information security policies of the Data Processor, its procedures and standards in order to address new and emerging threats and changes in legal requirements and industry standards.

vi. Provide management with guidance and support for information security in accordance with business requirements and relevant laws and regulations.

b. The Data Processor should document a separate dedicated security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties. The security policy should at least refer to: the roles and responsibilities of personnel, the baseline technical and organizational measures adopted for the security of personal data, the data subprocessors or other third parties involved in the processing of personal data. An inventory of specific policies/procedures related to the security of personal data should be created and maintained, based on the general security policy. Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy. The personal data processing security policy should be reviewed and revised, if necessary, on a semester basis.

c. Clear appointment of persons in charge of specific security tasks should be performed, including the appointment of a security officer. The security officer should be formally appointed (documented). The tasks and responsibilities of the security officer should also be clearly set and documented.

d. Conflicting duties and areas of responsibility, for example the roles of security officer, security auditor, and DPO, should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of personal data.

2. **SIGURNOST LJUDSKIH RESURSA**

a. Izvršitelj obrade trebao bi osigurati da su svi zaposlenici na odgovarajući način obaviješteni o sigurnosnim kontrolama informacijskog sustava koje se odnose na njihov svakodnevni rad. Zaposlenici uključeni u obradu osobnih podataka također bi trebali biti pravilno informirani o relevantnim zahtjevima zaštite podataka i zakonskim obvezama kroz redovne kampanje podizanja svijesti. Izvršitelj obrade trebao bi osigurati da svi zaposlenici razumiju svoje odgovornosti i obveze u vezi s obradom osobnih podataka. Uloge i odgovornosti trebaju biti jasno priopćene tijekom procesa prije zaposlenja i/ili uvođenja u posao. U gore navedene svrhe, Izvršitelj obrade trebao bi imati strukturirane i redovne godišnje programe obuke za osoblje, uključujući posebne programe za uvođenje (u pitanja zaštite podataka) novog osoblja.

b. Programi obuke trebali bi obrazovati i informirati zaposlenike, izvođače i druge vanjske korisnike mreže, sustava i aplikacija Izvršitelja obrade o (i) prijetnjama i brigama u informacijskoj sigurnosti; (ii) zahtjevima politike informacijske sigurnosti; te (iii) njihovim zaduženjima i odgovornostima u odnosu na obradu podataka, uključujući osobne podatke.

c. Izvršitelj obrade će opremiti zaposlenike, izvođače radova, te druge vanjske korisnike njegove mreže, sistema i aplikacija sa odgovarajućim alatima i opremom koja podupire implementaciju zahtjeva organizacijske sigurnosne politike u tijeku redovnog rada, uključujući u odnosu na daljinski pristup infrastrukturi Izvršitelja obrade (kao što je daljinski rad ili lokacije klijenata).

d. Tijekom unutarnjih reorganizacija ili otkaza i promjena zaposlenja, opoziv prava i odgovornosti s odgovarajućim postupcima primopredaje trebao bi biti jasno definiran. To znači da će Izvršitelj obrade osigurati da zaposlenici, izvođači radova i korisnici treće strane napuštaju organizaciju ili mijenjaju ulogu na uredan način, te da će pristup osobnim podacima biti uklonjen kada zaposlenici izađu

2. **HUMAN RESOURCES SECURITY**

a. The Data Processor should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns. The Data Processor should ensure that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities should be clearly communicated during the pre-employment and/or induction process. For the above stated purposes, the Data Processor should have structured and regular yearly training programs for staff, including specific programs for the induction (to data protection matters) of newcomers.

b. Training programs should educate and inform employees, contractors and other external users of the Data Processor's network, systems and applications about (i) information security threats and concerns; (ii) the requirements of the information security policy; and (iii) their responsibilities and obligations in relation to the processing of data, including personal data.

c. The Data Processor shall equip employees, contractors, and other external users of its network, systems and applications with appropriate tools and equipment to support the implementation of the organizational security policy requirements during its regular operation, including in regards to remote access to the Data Processor's infrastructure (such as remote work or customer locations).

d. During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures should be clearly defined. This means that the Data Processor will ensure that employees, contractors and third party users leave the organization or change roles in an orderly manner, and that access to personal data is removed when employees leave the organization or change position to a position

iz organizacije ili promijene poziciju u poziciju za koju nije potreban pristup takvim podacima.

e. Prije nego što preuzmu svoje dužnosti, od zaposlenika treba zatražiti da pregledaju i usuglase se sa sigurnosnom politikom Izvršitelja obrade i potpišu odgovarajuće ugovore o povjerljivosti i tajnosti podataka. Zaposlenici uključeni u visokorizičnu obradu osobnih podataka trebali bi biti vezani posebnim klauzulama o povjerljivosti (prema njihovom ugovoru o radu ili drugom pravnom aktu).

3. **UPRAVLJANJE IMOVINOM/RESURSIMA**

a. Izvršitelj obrade će osigurati prikladne kontrole za zaštitu organizacijske imovine koja obrađuje podatke, uključujući osobne podatke. Uz to, Izvršitelj obrade će održavati sustav klasifikacije podataka koji je industrijski standard i koji je dizajniran da osigura da će podaci, uključujući osobne podatke biti zaštićene adekvatnom razinom zaštite u svako vrijeme.

b. Izvršitelj obrade treba imati registar IT resursa koji se koriste za obradu osobnih podataka (hardver, softver i mreža). Registar bi trebao sadržavati barem sljedeće podatke: IT resurs, vrstu (npr. poslužitelj, radna stanica), lokaciju (fizičku ili elektroničku). Određenoj osobi treba dodijeliti zadatak za održavanje i ažuriranje registra (npr. informatički službenik).

c. Uloge koje imaju pristup određenim resursima trebaju biti definirane i dokumentirane.

d. IT resurse treba pregledavati i ažurirati godišnje.

4. **FIZIČKA I LOKACIJSKA SIGURNOST**

Izvršitelj obrade će spriječiti neovlašteni fizički pristup, štetu i smetnju svojim prostorijama, te će poduzeti mjere za sprječavanje gubitka, štete, krađe ili kompromitiranja imovine, te smetnje njegovih aktivnosti vezanih za obradu podataka. Sve lokacije u kojima informacijski sustavi sadrže podatke, uključujući osobne podatke, moraju imati odobrene sigurnosne sustave uspostavljene kako bi se kontrolirao i ograničio pristup takvim podacima.

that does not require access to such data.

e. Prior to up taking their duties employees should be asked to review and agree on the security policy of the Data Processor and sign respective confidentiality and non-disclosure agreements. Employees involved in high risk processing of personal data should be bound to specific confidentiality clauses (under their employment contract or other legal act).

3. **ASSET/RESOURCE MANAGEMENT**

a. The Data Processor shall provide appropriate controls to protect the organizational assets that process data, including personal data. In addition, the Data Processor will maintain an industry standard data classification system designed to ensure that data, including personal data, is protected by an adequate level of protection at all times.

b. The Data Processor should have a register of the IT resources used for the processing of personal data (hardware, software, and network). The register should include at least the following information: IT resource, type (e.g., server, workstation), location (physical or electronic). A specific person should be assigned the task for maintaining and updating the register (e.g., IT officer).

c. Roles having access to certain resources should be defined and documented.

d. IT resources should be reviewed and updated on annual basis.

4. **PHISYCAL AND LOCATION SECURITY**

The Data Processor shall prevent unauthorized physical access, damage, and interference to its premises, and will take measures to prevent the loss, damage, theft or compromise of property, and interference with its data processing activities. All locations where information systems contain data, including personal data, must have approved security systems in place to control and restrict access to such data. This includes implementing the following measures:

To uključuje provedbu sljedećih mjera:

a. Fizičko područje infrastrukture IT sustava ne smije biti dostupno neovlaštenom osoblju.

b. Gdje je primjereno, potrebno je uspostaviti jasnu identifikaciju, putem odgovarajućih sredstava, na primjer identifikacijskih oznaka, za svo osoblje i posjetitelje koji pristupaju prostorijama Izvršitelja obrade.

c. Sigurne zone treba definirati i zaštititi odgovarajućim kontrolama ulaska. Fizički dnevnik ili elektronički revizorski trag svih pristupa trebali bi se sigurno održavati i nadzirati.

d. Sustave otkrivanja uljeza treba instalirati u svim sigurnosnim zonama.

e. Fizičke prepreke treba, prema potrebi, izgraditi kako bi se spriječio neovlašteni fizički pristup.

f. Prazna zaštićena područja treba fizički zaključati i povremeno pregledavati.

g. Automatski sustav za gašenje požara, namjenski sustav klimatizacije zatvorene kontrole i neprekidno napajanje (UPS) trebaju biti implementirani u poslužiteljskoj prostoriji.

h. Osoblju vanjske službe za podršku treba odobriti ograničen pristup zaštićenim područjima.

5. **UPRAVLJANJE KOMUNIKACIJAMA I OPERACIJAMA**

Izvršitelj obrade će osigurati ispravan i siguran rad objekata za obradu podataka, uključujući korištenjem odgovarajuće firewall i enkripcijske tehnologije; te koliko je god moguće, logiranje i praćenje svih transmisija podataka.
Izvršitelj obrade će implementirati i održavati odgovarajući nivo informacijske sigurnosti i dostave usluga u skladu s ugovorima o dostavi usluge trećih strana.

6. **SIGURNOST SERVERA, RADNIH STANICA I PRIJENOSNIH UREĐAJA**

a. Korisnici ne bi trebali moći deaktivirati ili zaobići sigurnosne postavke.

b. Protuvirusne aplikacije i uzorke za detekciju

a. The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel.

b. Clear identification, through appropriate means e.g., ID badges, for all personnel and visitors accessing the premises of the Data Processor should be established, as appropriate.

c. Secure zones should be defined and be protected by appropriate entry controls. A physical log book or electronic audit trail of all access should be securely maintained and monitored.

d. Intruder detection systems should be installed in all security zones.

e. Physical barriers should, where applicable, be built to prevent unauthorized physical access.

f. Vacant secure areas should be physically locked and periodically reviewed.

g. An automatic fire suppression system, closed control dedicated air conditioning system and uninterruptible power supply (UPS) should be implemented at the server room.

h. External party support service personnel should be granted restricted access to secure areas.

5. **COMUNICATIONS AND OPERATIONS MANAGEMENT**

The Data Processor will ensure the correct and secure operation of data processing facilities, including the use of appropriate firewall and encryption technology; and, as much as possible, logging and tracking of all data transmissions.
The Data Processor will implement and maintain an appropriate level of information security and service delivery in accordance with third party service delivery agreements.

6. **SERVER, WORKSTATION AND PORTABLE DEVICE SECURITY**

a. Users should not be able to deactivate or bypass security settings.

b. Anti-virus applications and detection signatures should be configured on a daily

treba svakodnevno konfigurirati.

c. Korisnici ne bi trebali imati privilegije za instaliranje ili aktiviranje neovlaštenih softverskih aplikacija.

d. Sustav bi trebao imati prekide sesije kada korisnik nije bio aktivan određeno vremensko razdoblje.

e. Kritična sigurnosna ažuriranja koja je izdao developer operativnog sustava trebala bi se redovito instalirati.

f. Postupke upravljanja mobilnim i prijenosnim uređajima treba definirati i dokumentirati uspostavljajući jasna pravila za njihovu pravilnu uporabu. Treba jasno definirati posebne uloge i odgovornosti u pogledu upravljanja mobilnim i prijenosnim uređajima.

g. Mobilni uređaji kojima je dopušten pristup informacijskom sustavu trebaju biti unaprijed registrirani i prethodno autorizirani.

h. Mobilni uređaji trebali bi biti podvrgnuti istim razinama postupka kontrole pristupa (sustavu za obradu podataka) kao i druga terminalna oprema.

i. Izvršitelj obrade bi trebao moći daljinski izbrisati osobne podatke (koji se odnose na postupak obrade) na mobilnom uređaju koji je ugrožen.

j. Mobilni uređaji trebali bi podržavati odvajanje privatne i poslovne upotrebe uređaja putem sigurnih softverskih spremnika.

k. Mobilni uređaji trebaju biti fizički zaštićeni od krađe kada se ne koriste.

l. Za pristup mobilnim uređajima treba implementirati dvofaktorsku autentifikaciju.

m. Osobni podaci pohranjeni na mobilnom uređaju (kao dio operacije obrade podataka Izvršitelja obrade) trebaju biti enkriptirani.

n. Potpuno kriptiranje diska trebalo bi biti omogućeno na pogonima operacijskog sustava radne stanice.

o. Servere baze podataka i aplikacija treba konfigurirati za rad pomoću zasebnog računa, s minimalnim ovlastima OS-a za ispravno

basis.

c. Users should not have privileges to install or activate unauthorized software applications.

d. The system should have session time-outs when the user has not been active for a certain time period.

e. Critical security updates released by the operating system developer should be installed regularly.

f. Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use. Specific roles and responsibilities regarding mobile and portable device management should be clearly defined.

g. Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.

h. Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.

i. The Data Processor should be able to remotely erase personal data (related to its processing operation) on a mobile device that has been compromised.

j. Mobile devices should support separation of private and business use of the device through secure software containers.

k. Mobile devices should be physically protected against theft when not in use.

l. Two factor authentication should be implemented for accessing mobile devices.

m. Personal data stored at the mobile device (as part of the Data Processor's data processing operation) should be encrypted.

n. Full disk encryption should be enabled on the workstation operating system drives.

o. Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly.

p. Database and applications servers should only

funkcioniranje.

p. Serveri baze podataka i aplikacija trebaju obrađivati samo osobne podatke koji su stvarno potrebni za obradu kako bi se postigle svrhe obrade.

q. Treba implementirati enkripciju pogona za pohranu radnih stanica i servera.

r. Tehnike pseudonimizacije trebale bi se primijeniti razdvajanjem podataka od izravnih identifikatora kako bi se izbjeglo povezivanje sa ispitanikom bez dodatnih informacija.

7. **UPRAVLJANJE MREŽNOM SIGURNOSTI**

Izvršitelj obrade će osigurati zaštitu svih podataka Voditelja obrade, uključujući osobne podatke, u svojim mrežama (i mrežama svojih pružatelja usluga), te će osigurati zaštitu potporne infrastrukture.

a. Izvršitelj obrade će održavati zaštitu (uključujući antivirusnu zaštitu) od malicioznog koda.

b. Kad god se pristup vrši putem Interneta, komunikaciju treba šifrirati kriptografskim protokolima (TLS/SSL).

c. Općenito bi se trebao izbjegavati daljinski pristup IT sustavu. U slučajevima kada je to apsolutno potrebno, to bi trebalo biti učinjeno samo pod kontrolom i nadzorom određene osobe iz organizacije (npr. IT administrator/službenik sigurnosti) putem unaprijed definiranih uređaja.

d. Bežični pristup IT sustavu trebao bi biti dopušten samo određenim korisnicima i procesima. Treba ga zaštititi mehanizmima enkripcije.

e. Promet prema IT sustavu i iz njega trebao bi se pratiti i kontrolirati putem vatrozida i sustava za otkrivanje upada.

f. Pristup informacijskom sustavu trebaju imati samo prethodno odobreni uređaji i terminalna oprema pomoću tehnika kao što su MAC filtriranje ili kontrola pristupa mreži (NAC).

g. Radne stanice koje se koriste za obradu osobnih podataka po mogućnosti ne bi trebale biti povezane s internetom osim ako su na snazi

process the personal data that are actually needed to process in order to achieve its processing purposes.

q. Encryption of workstation and server storage drives should be implemented.

r. Pseudonymization techniques should be applied through separation of data from direct identifiers to avoid linking to data subject without additional information.

7. **NETWORK SECURITY MANAGEMENT**

The Data Processor will ensure the protection of all data of the Data Controller, including personal data, in its networks (and the networks of its service providers), and will ensure the protection of the supporting infrastructure.

a. The Data Processor will maintain protection (including antivirus protection) against malicious code.

b. Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).

c. Remote access to the IT system should in general be avoided. In cases where this is absolutely necessary, it should be performed only under the control and monitoring of a specific person from the organization (e.g. IT administrator/security officer) through pre-defined devices.

d. Wireless access to the IT system should be allowed only for specific users and processes. It should be protected by encryption mechanisms.

e. Traffic to and from the IT system should be monitored and controlled through Firewalls and Intrusion Detection Systems.

f. Access to the IT system should be performed only by pre-authorized devices and terminal equipment using techniques such as MAC filtering or Network Access Control (NAC).

g. Workstations used for the processing of personal data should preferably not be connected to the Internet unless security measures are in place to prevent unauthorized processing, copying and transfer of personal

sigurnosne mjere za sprječavanje neovlaštene obrade, kopiranja i prijenosa osobnih podataka koji su spremljeni.

h. Mrežu informacijskog sustava koji se koristi za obradu osobnih podataka treba odvojiti od drugih mreža Izvršitelja obrade.

8. **RUKOVANJE MEDIJIMA**

Izvršitelj obrade će održavati odgovarajuće procese i postupke za sprječavanje neovlaštenog otkrivanja, modifikacije, brisanja ili uništenja imovine, te prekida u poslovnoj aktivnosti. Kada se mediji moraju zbrinuti ili ponovo upotrijebiti, procedure su implementirane za sprječavanje bilo kakvog naknadnog dohvaćanja informacija spremljenih na njima prije nego što su povučeni iz inventara. To podrazumijeva sljedeće:

a. Provesti će se uništavanje papira i prijenosnih medija koji se koriste za pohranu osobnih podataka.

b. Prije odlaganja, na svim medijima treba izvršiti softversko prepisivanje više puta. Nakon softverskog brisanja, potrebno je provesti dodatne mjere na hardveru, poput demagnetiziranja. Ovisno o slučaju, treba razmotriti i fizičko uništenje.

c. Ako se usluge treće strane koriste za sigurno uništenje medija ili papirnatih zapisa, trebao bi postojati ugovor o usluzi i prema potrebi sastaviti zapisnik o uništavanju podataka. U ovom slučaju treba uzeti u obzir da se proces odvija u prostorijama Izvršitelja obrade (i izbjegavati prijenos osobnih podataka izvan tog mjesta).

d. Ne smije se dopustiti prijenos osobnih podataka s radnih stanica na vanjske uređaje za pohranu (npr. USB, DVD, vanjski tvrdi diskovi).

9. **RAZMJENA INFORMACIJA**

Izvršitelj obrade održat će sigurnost podataka, uključujući osobne podatke i softver koji se razmjenjuju unutar organizacije i s bilo kojim vanjskim subjektom.

10. **USLUGE ELEKTRONIČKOG POSLOVANJA**

Izvršitelj obrade će implementirati odgovarajuće

data on store.

h. The network of the information system used to process personal data should be segregated from the other networks of the Data Processor.

8. **MEDIA HANDLING**

The Data Processor shall maintain appropriate processes and procedures to prevent unauthorized disclosure, modification, deletion or destruction of assets, and business interruptions. When media need to be disposed of or reused, procedures are implemented to prevent any subsequent retrieval of information stored on them before they are withdrawn from inventory. This includes the following:

a. Shredding of paper and portable media used to store personal data shall be carried out.

b. Multiple passes of software-based overwriting should be performed on all media before being disposed. Following the software erasure, additional hardware based measures such as degaussing should be performed. Depending on the case, physical destruction should also be considered.

c. If a third party's services are used to securely dispose of media or paper based records, a service agreement should be in place and a record of destruction of records should be produced as appropriate. In this case it should be considered that the process takes place at the premises of the Data Processor (and avoid off-site transfer of personal data).

d. It should not be allowed to transfer personal data from workstations to external storage devices (e.g. USB, DVD, external hard drives).

9. **EXCHANGE OF INFORMATION**

The Data Processor will maintain data security, including of the personal data and software exchanged within the organization and with any external entity.

10. **ELECTRONIC BUSINESS SERVICES**

The Data Processor will implement appropriate measures to ensure the security of e-business services, including mobile devices and their safe

mjere za pružanje sigurnosti usluga elektroničkog poslovanja, uključujući mobilne uređaje i njihovo sigurno korištenje. Izvršitelj obrade će održavati djelotvorne procedure praćenja dovoljne da otkriju neovlaštene aktivnosti u odnosu na podatke.

11. **KONTROLE PRISTUPA**

a. Izvršitelj obrade će održavati odgovarajuće procedure kontrole pristupa za osiguranje ovlaštenog pristupa korisnika i za sprječavanje neovlaštenog pristupa, krađe ili gubitka podataka, uključujući osobnih podataka, iz informacijskih sustava, uključujući mreže, aplikacije i operativne sustave. Treba implementirati sustav kontrole pristupa primjenjiv na sve korisnike koji pristupaju IT sustavu. Sustav bi trebao omogućiti stvaranje, odobravanje, pregled i brisanje korisničkih računa.

b. Pravila kontrole pristupa trebaju biti detaljna i dokumentirana. Izvršitelj obrade trebao bi u tom dokumentu odrediti odgovarajuća pravila kontrole pristupa te prava pristupa i ograničenja za posebne uloge korisnika u vezi s procesima i postupcima koji se odnose na osobne podatke.

c. Svakoj ulozi (uključenoj u obradu osobnih podataka) treba dodijeliti precizna prava unutar kontrole pristupa slijedeći načelo ograničenog pristupa.

d. Odvajanje uloga kontrole pristupa (npr. zahtjev za pristup, autorizacija pristupa, administracija pristupa) treba biti jasno definirano i dokumentirano.

e. Uloge s širokim pravima pristupa trebaju biti jasno definirane i dodijeljene ograničenim određenim članovima osoblja.

f. Treba izbjegavati upotrebu zajedničkih korisničkih računa. U slučajevima kada je to potrebno, treba osigurati da svi korisnici zajedničkog računa imaju iste uloge i odgovornosti.

g. Treba uspostaviti mehanizam provjere autentičnosti koji omogućuje pristup IT sustavu (na temelju tog sustava i pravila kontrole pristupa). Kao minimum treba koristiti

use. The Data Processor will maintain effective monitoring procedures sufficient to detect unauthorized activities in relation to the data.

11. **ACCESS CONTROLS**

a. The Data Processor shall maintain appropriate access control procedures to ensure authorized user access and to prevent unauthorized access, theft or loss of data, including personal data, from information systems, including networks, applications and operating systems. An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, reviewing and deleting user accounts.

b. An access control policy should be detailed and documented. The Data Processor should determine in this document the appropriate access control rules, access rights and restrictions for specific user roles towards the processes and procedures related to personal data.

c. Specific access control rights should be allocated to each role (involved in the processing of personal data) following the need to know principle.

d. Segregation of access control roles (e.g., access request, access authorization, access administration) should be clearly defined and documented.

e. Roles with excessive access rights should be clearly defined and assigned to limited specific members of staff.

f. The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities.

g. An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). As a minimum a username/password combination should be used. Passwords should respect a

kombinaciju korisničko ime/lozinka. Lozinke trebaju poštivati određenu (podesivu) razinu složenosti.

h. Sustav kontrole pristupa trebao bi imati mogućnost otkrivanja i sprječavanja upotrebe lozinki koje ne poštuju određenu (podesivu) razinu složenosti.

i. Treba definirati i dokumentirati određena pravila lozinki. Pravila bi trebala uključivati najmanje duljinu lozinke, složenost, razdoblje valjanosti, kao i broj prihvatljivih neuspješnih pokušaja prijave.

j. Korisničke lozinke moraju biti pohranjene u "hash" obliku.

k. Za pristup sustavima koji obrađuju osobne podatke treba koristiti dvofaktorsku provjeru autentičnosti. Faktori autentifikacije mogu biti lozinke, sigurnosni tokeni, USB ključevi s tajnim tokenom, biometrija itd.

12. **ZAPISNICI DOGAĐAJA**

a. Datoteke zapisnika trebaju biti aktivirane za svaki sustav/aplikaciju koja se koristi za obradu osobnih podataka. Oni bi trebali uključivati sve vrste pristupa podacima (prikaz, izmjena, brisanje).

b. Datoteke zapisnika trebaju biti vremenski označene i na odgovarajući način zaštićene od neovlaštenih izmjena i neovlaštenog pristupa. Sat treba sinkronizirati s jednim referentnim izvorom vremena.

c. Radnje administratora sustava i operatora sustava, uključujući dodavanje/brisanje/promjenu korisničkih prava, trebaju biti zabilježene.

d. Ne smije postojati mogućnost brisanja ili izmjene sadržaja datoteka zapisnika. Pristup datotekama zapisnika također bi trebao biti zabilježen uz nadzor radi otkrivanja neobičnih aktivnosti.

e. Sustav za nadzor trebao bi obraditi datoteke zapisnika i izraditi izvješća o statusu sustava te obavijestiti o potencijalnim upozorenjima.

13. **KRIPTOGRAFSKA KONTROLA**

certain (configurable) level of complexity.

h. The access control system should have the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity.

i. A specific password policy should be defined and documented. The policy should include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts.

j. User passwords must be stored in a "hashed" form.

k. Two-factor authentication should be used for accessing systems that process personal data. The authentication factors could be passwords, security tokens, USB sticks with a secret token, biometrics etc.

12. **EVENT LOGGING**

a. Log files should be activated for each system/application used for the processing of personal data. They should include all types of access to data (view, modification, deletion).

b. Log files should be timestamped and adequately protected against tampering and unauthorized access. Clocks should be synchronized to a single reference time source.

c. Actions of the system administrators and system operators, including addition/deletion/change of user rights should be logged.

d. There should be no possibility of deletion or modification of log files content. Access to the log files should also be logged in addition to monitoring for detecting unusual activity.

e. A monitoring system should process the log files and produce reports on the status of the system and notify for potential alerts.

Izvršitelj obrade poduzet će odgovarajuće mjere za zaštitu baze podataka, uključujući osobne podatke, počevši od čitanja podataka (pristup podacima), kopiranja, izmjena ili brisanja od strane neovlaštenih osoba tijekom procesa ažuriranja ili prijenosa podataka. Izvršitelj obrade pobrinut će se za sigurnost podataka, povjerljivost, autentičnost i integritet podataka, uključujući osobne podatke, bilo u fazi prijenosa ili tijekom pohrane ili upotrebe, posebno tijekom cijelog procesa, koristeći pouzdane metode i kriptografska sredstva koja su se pokazala kao najsigurnija u industriji. Izvršitelj obrade će, u skladu sa svojim mogućnostima, osigurati da se kriptografski protokoli mijenjaju prema potrebi u skladu s tehnološkim razvojem i novim potencijalnim prijetnjama. Nadalje, Izvršitelj obrade cijelo će vrijeme održavati i upravljati ključevima za enkripciju te ih ni u kojem slučaju neće otkriti trećim stranama, uključujući državna tijela ili agencije za zaštitu podataka, u skladu s odredbama ugovora.

14. **UPRAVLJANJE TEHNIČKIM NEDOSTACIMA**

a. Izvršitelj obrade održat će sigurnost aplikacijskog softvera praćenjem i omogućavanjem (usvajanjem) sustava za upravljanje procesima i postupcima za smanjenje rizika od zlouporabe i otkrivanja tehničkih nedostataka.

b. Izvršitelj obrade pravodobno će ukazati na nedostatke informacijskog sustava i sigurnosti podataka, dajući dovoljno vremena da se nedostaci isprave i otklone.

15. **UPRAVLJANJE INCIDENTIMA**

a. Izvršitelj obrade uskladit će odgovarajuće propise, postupke i radnje radi sprječavanja slučajnog, neovlaštenog ili nezakonitog uništavanja, izmjene, oštećenja, gubitka ili pristupa osobnim podacima te radi osiguranja dostupnosti i integriteta podataka. Treba definirati plan odgovora na incidente s detaljnim postupcima kako bi se osigurao učinkovit i uredan odgovor na incidente koji se odnose na osobne podatke. Plan odgovora na incidente treba dokumentirati, uključujući popis mogućih mjera ublažavanja posljedica i jasnu dodjelu uloga.

13. **CRYPTOGRAPHIC CONTROL**

The Data Processor will take appropriate measures to protect the database, including personal data, starting from reading data (data access), copying, modification or deletion by unauthorized persons during the process of updating or transferring of the data. The Data Processor will take care of data security, confidentiality, authenticity and data integrity, including personal data, whether in the transmission phase or when in storage or use, in particular throughout the process, using reliable methods and cryptographic means that have proven to be the most secure in the industry. The Data Processor will, in accordance with its capabilities, ensure that cryptographic protocols are changed as necessary to comply with technological developments and new potential threats. Furthermore, the Data Processor will maintain and manage the encryption keys at all times and will in no case disclose them to third parties, including government authorities or data protection agencies, in accordance with the provisions of the contract.

14. **MANAGEMENT OF TECHNICAL DEFECTS**

a. The Data Processor will maintain the security of the application software by monitoring and enabling (adopting) a system to manage processes and procedures to reduce the risks posed by misuse and disclosure of technical deficiencies.

b. The Data Processor will point out the shortcomings of the information system and data security in a timely manner, giving sufficient time for the deficiencies to be corrected and remedied.

15. **INCIDENT MANAGEMENT**

a. The Data Processor will harmonize appropriate regulations, procedures and acts to prevent accidental, unauthorized or unlawful destruction, alteration, damage, loss or access to personal data, and to insure the availability and integrity of data. An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data. The

b. Incidente i povrede osobnih podataka treba zabilježiti zajedno s pojedinostima o događaju i naknadnim provedenim mjerama ublažavanja. Povrede osobnih podataka trebaju se odmah prijaviti upravi. Trebali bi biti uspostavljeni postupci obavještavanja za prijavljivanje povreda nadležnim tijelima i ispitanicima, u skladu s čl. 33 i 34 GDPR-a.

c. Izvršitelj obrade trebao bi uspostaviti glavne kontrole i postupke koje treba slijediti kako bi se osigurala potrebna razina kontinuiteta i dostupnost IT sustava koji obrađuje osobne podatke u slučaju incidenta/povrede osobnih podataka.

d. Potrebno je imenovati posebno osoblje s potrebnom odgovornošću, ovlastima i sposobnostima za upravljanje kontinuitetom poslovanja u slučaju incidenta/povrede osobnih podataka.

16. **UPRAVLJANJE POSLOVNIM PROCESIMA**

a. Organizacija bi se trebala pobrinuti da sve promjene u IT sustavu registrira i prati određena osoba (npr. IT ili sigurnosni službenik). Trebalo bi redovito pratiti ovaj proces. Trebalo bi uspostaviti detaljna i dokumentirana pravila promjena. Ona bi trebala uključivati: postupak uvođenja promjena, uloge/korisnike koji imaju prava raditi promjene, rokove za uvođenje promjena. Pravila promjena treba redovito ažurirati.

b. Izvršitelj obrade poduzet će sve potrebne mjere kako bi spriječio poremećaje radnih procesa i zaštitio važne poslovne procese od kvara informacijskog sustava ili nesreća te će se pobrinuti da na vrijeme pronađe odgovarajuće načine za uklanjanje gore navedenog.

c. PKP (plan kontinuiteta poslovanja) treba biti detaljan i dokumentiran (slijedeći opća sigurnosna pravila). To bi trebalo uključivati jasne radnje i dodjelu uloga. U PKP-u treba definirati razinu zajamčene kvalitete usluge za temeljne poslovne procese koji se tiču sigurnosti osobnih podataka.

d. Izvršitelj obrade će imati uspostavljena alternativna, rezervna postrojenja kako bi se osigurao integritet i pristupačnost podataka i

incidents' response plan should be documented, including a list of possible mitigation actions and clear assignment of roles.

b. Incidents and personal data breaches should be recorded along with details regarding the event and subsequent mitigation actions performed. Personal data breaches should be reported immediately to the management. Notification procedures for the reporting of the breaches to competent authorities and data subjects should be in place, following art. 33 and 34 GDPR.

c. The Data Processor should establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data in the event of an incident/personal data breach.

d. Specific personnel with the necessary responsibility, authority and competence to manage business continuity in the event of an incident/personal data breach should be nominated.

16. **BUSINESS PROCESS MANAGEMENT**

a. The organization should make sure that all changes to the IT system are registered and monitored by a specific person (e.g., IT or security officer). Regular monitoring of this process should take place. A detailed and documented change policy should be in place. It should include: a process for introducing changes, the roles/users that have change rights, timelines for introducing changes. The change policy should be regularly updated.

b. The Data Processor will take all necessary measures to prevent disruption of work processes and protect important business processes from failure of the information system or accidents and make sure to find a way to eliminate the above in a timely manner.

c. A BCP (business continuity plan) should be detailed and documented (following the general security policy). It should include clear actions and assignment of roles. A level of guaranteed service quality should be defined in the BCP for the core business processes that provide for personal data security.

objekata za obradu podataka.

17. **SIGURNOSNE KOPIJE PODATAKA**

a. Postupci sigurnosnog kopiranja i vraćanja podataka trebaju biti definirani, dokumentirani i jasno povezani s ulogama i odgovornostima.

b. Sigurnosnim kopijama treba dati odgovarajuću razinu fizičke i zaštite okoliša u skladu sa standardima koji se primjenjuju na izvorne podatke.

c. Izvođenje sigurnosnih kopija treba nadzirati kako bi se osigurala potpunost.

d. Cijele sigurnosne kopije treba redovito provoditi.

e. Sigurnosne medije treba redovito testirati kako bi se osiguralo da se na njih može osloniti za hitnu uporabu.

f. Zakazane inkrementalne sigurnosne kopije trebale bi se provoditi barem svakodnevno.

g. U slučaju da se koristi usluga treće strane za sigurnosno kopiranje pohrane, kopija mora biti enkriptirana prije nego što se prenese od Izvršitelja obrade.

h. Inačice sigurnosnih kopija trebale bi biti enkriptirane i sigurno pohranjene izvanmrežno na različitim lokacijama.

18. **PODIZVRŠITELJI OBRADE**

a. Izvršitelj obrade će osigurati da njegovi kooperanti, kao podizvršitelji obrade podataka, osiguraju odgovarajuću razinu zaštite osobnih podataka, ekvivalentnu zaštiti propisanoj ovim ugovorom. U tu svrhu, formalne smjernice i postupci koji se tiču obrade osobnih podataka od strane podizvršitelja obrade (izvođači/vanjski izvođači) trebaju biti definirani, dokumentirani i dogovoreni između Izvršitelja obrade i podizvršitelja obrade prije početka aktivnosti obrade. Ove smjernice i postupci trebali bi obvezno uspostaviti istu razinu sigurnosti osobnih podataka koju propisuju sigurnosna pravila Izvršitelja obrade.

b. Nakon što sazna za povredu osobnih podataka, podizvršitelj obrade će bez nepotrebnog odgađanja obavijestiti Izvršitelja obrade.

d. The Data Processor will have in place adequate alternative, back-up facilities to ensure the integrity and accessibility of information and information processing facilities.

17. **DATA BACKUP**

a. Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities.

b. Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.

c. Execution of backups should be monitored to ensure completeness.

d. Full backups should be carried out regularly.

e. Backup media should be regularly tested to ensure that they can be relied upon for emergency use.

f. Scheduled incremental backups should be carried out at least on a daily basis.

g. In case a third party service for back up storage is used, the copy must be encrypted before being transmitted from the Data Processor.

h. Copies of backups should be encrypted and securely stored offline in different locations.

18. **DATA SUBPROCESSORS**

a. The Data Processor shall ensure that its subcontractors, as data subprocessors, provide an adequate level of personal data protection, equivalent to the protection prescribed in this contract. For this purpose, formal guidelines and procedures covering the processing of personal data by data subprocessors (contractors/outsourcing) should be defined, documented and agreed between the Data Processor and the data subprocessor prior to the commencement of the processing activities. These guidelines and procedures should mandatorily establish the same level of personal data security as mandated in the Data

c. Formalni zahtjevi i obveze trebali bi biti formalno dogovoreni između Izvršitelja obrade i podizvršitelja obrade. Podzvršitelj obrade trebao bi pružiti dovoljno pisanih dokaza o usklađenosti.

d. Organizacija Izvršitelja obrade trebala bi redovito provjeravati usklađenost podizvršitelja obrade s dogovorenom razinom zahtjeva i obveza.

e. Zaposlenici podizvršitelja obrade koji obrađuju osobne podatke trebali bi biti subjekti posebnih pisanih ugovora o povjerljivosti/neotkrivanju podataka.

Processor's security policy.

b. Upon finding out of a personal data breach, the data subprocessor shall notify the Data Processor without undue delay.

c. Formal requirements and obligations should be formally agreed between the Data Processor and the data subprocessor. The data subprocessor should provide sufficient documented evidence of compliance.

d. The Data Processor's organization should regularly audit the compliance of the data subprocessor to the agreed level of requirements and obligations.

e. The employees of the data subprocessor who are processing personal data should be subject to specific documented confidentiality/ non-disclosure agreements.

Prilog 3. Popis podizvršitelja

Naziv podizvršitelja	Adresa sjedišta	Kategorije podataka koje se dijele s podizvršiteljem, pravni osnov i rokovi čuvanja	Stvarna lokacija obrade

(*Uputa: Popunjava Izvođač odnosno Izvršitelj obrade*)

Appendix 3. List of subprocessors

Name of subprocessor	Address of headquarters	Categories of data shared with the subprocessor, legal basis and retention periods	Actual processing location

(Instruction: Filled in by the Contractor, that is, the Data Processor)

GDPR – Upitnik za samoprocjenu

1 Tablica obrade osobnih podataka

Molimo Vas unesite sve aktivnosti vezane uz obradu osobnih podataka koje izvršavate u ime Hrvatske zaklade za znanost, sve u skladu s Vašim evidencijama aktivnosti obrade prema članku 30. Opće uredbe o zaštiti podataka:

Aktivnost obrade	*Svrha obrade*	*Kategorije ispitanika*	*Vrsta osobnih podataka/ vrijeme čuvanja*	*Temeljni ugovor/ pravni osnov obrade*	*IT sustavi uključeni u obradu/ sigurnosne i tehničke mjere zaštite*	*Angažirani podizvođači*	*Mjesto obrade / dijeljenje s trećima / primatelji*

2 Tehničke i organizacijske mjere

Molimo Vas označite kvačicom i/ili opišite implementirane mjere:

2.1 Organizacijska i instruktivna kontrola

☐	Uspostavljena odobrenja za pristup zaposlenicima i trećim osobama, uključujući i odgovarajuću dokumentaciju	☐	Specifična sigurnosna područja s vlastitom kontrolom pristupa („closed shops“)
☐	Smjernice za organizaciju datoteka podataka	☐	Interna pravila i postupci za obradu osobnih podataka, smjernice, instrukcije za rad, opisi procesa i pravila za programiranje, testiranje i objavu podataka
☐	Osobni se podaci obrađuju samo prema dokumentiranim uputama voditelja obrade, uključujući prijenos osobnih podataka u treću zemlju ili međunarodnu organizaciju	☐	Postojanje koncepta sigurnosti podataka
☐	Obvezujuća pravila i postupci za zaposlenike izvršitelja obrade vezano uz obradu podataka	☐	Na zahtjev, izvršitelj obrade može voditelju obrade u kratkom roku omogućiti pristup svim informacijama potrebnim za dokazivanje da je njegovo (izvršiteljevo) postupanje u skladu s DPA-om. (maksimalan rok 48 h)
☐	Na zahtjev, izvršitelj obrade će omogućiti pristup voditelju obrade kako bi putem revizije ili inspekcije provjerio postupa li izvršitelj u skladu s ugovorom	☐	Postojanje plana za hitne slučajeve
☐	Odvajanje funkcija između IT odjela i drugih odjela	☐	Smjernice za zaposlenike na temu obrade osobnih podataka
☐	Imenovanje službenika za sigurnost	☐	Redovna edukacija zaposlenika o zaštiti osobnih podataka
☐	Jasno razgraničenje ovlasti između voditelja obrade i izvršitelja obrade	☐	Pisana obveza zaposlenika da poštuju povjerljivost podataka ili zaposlenici podliježu zakonskim obvezama o povjerljivosti u skladu s člankom 28. stavkom 3. točkom b GDPR
☐	Utvrđena procedura za slučaj povrede osobnih podataka		

Dodatne mjere/objašnjenja:

_____

_____

_____

_____

2.2 Fizička kontrola pristupa

☐	Isključivo ovlašteni zaposlenici imaju pristup sustavima obrade podataka	☐	Nadzor pristupa trećih (posjetitelji, klijenti, servis za čišćenje ...)
☐	Savjestan izbor osoba koje obavljaju zaštitarske i čuvarske dužnosti I poslove čišćenja	☐	Propusnice za posjetitelje
☐	Biometrijske ulazne barijere/svjetlosne barijere/detektori kretanja	☐	Omogućavanje zaključavanja svih prostorija vezanih uz obradu podataka (uključuje pristup prostorijama i kompjuterskoj i drugoj opremi koja se koristi za obradu podataka)
☐	Biometrijske propusnice	☐	Fizičko osiguranje prostora u kojima s nalaze prijenosnici podataka
☐	Obvezno nošenje identifikacijskih iskaznica ili kodnih kartica	☐	Utvrđivanje identitet na ulazu (recepciji)
☐	Restrikcije vezane uz dostupnost ključeva	☐	Sigurnosni alarm i druge odgovarajuće sigurnosne mjere uključene i izvan radnog vremena
☐	Pravila o zaporkama	☐	Decentralizacija opreme za obradu podataka i osobnih kompjutera
☐	Identifikacija osoba koje su ovlaštene za pristup	☐	Zaštita i ograničenje pristupa putem automatskog sustava kontrole pristupa
☐	Protuprovalne brave, električne brave, chip kartice/ elektronički sustav zaključavanja	☐	Fizičke mjere zaštite (Ograđivanje, zaključana vrata, ulazna vrata, prozori)

☐	Izvješćivanje u pristupu	☐	Alarmni signal u slučaju neovlaštenog ulaska u sobu sa serverima.
☐	Utvrđivanje prostora u kojima se prijenosnici podataka mogu/moraju nalaziti.		

Dodatne mjere/objašnjenja:

_____

_____

_____

_____

2.3 Pristup podacima i kontrola korisnika

☐	Uspostavljanje autorizacije pristupa za zaposlenike, uključujući odgovarajuću dokumentaciju	☐	Proces provjere i puštanja programa u rad
☐	Davanje pristupa samo individualno određenim pojedincima	☐	Enkripcija podataka i nosača podataka (uključujući smartphone) i nivo enkripcije _____
☐	Odgovarajuća pravila za treće strane (pr. IT podršku)	☐	Pseudonimizacija podataka i vrsta pseudonimizacije _____
☐	Zaključavanje terminala	☐	Zaštita unutarnjih mreža od neautoriziranog pristupa (pr. putem vatrozida)
☐	Alokacija individualnih terminala i/ili određivanje karakteristika korisnika terminala i identifikacija istih za specifične svrhe.	☐	Implementacija i održavanje antivirusnih programa na svim uređajima koji se korite za obradu podataka
☐	Funkcionalna i/ili vremenski ograničeno korištenje terminala i/ili karakteristike korisnika terminala i identifikacija	☐	Logiranje i prijava pristupa

☐	Korisničke šifre za podatke i programe	☐	Dodjeljivanje i čuvanje identifikacijskih kodova
☐	Utvrđen način kodiranja za podatke	☐	Ograničavanje prava na pristup samo ograničenom broju administratora
☐	Diferencirana pravila pristupa (pr. djelomično blokiranje)	☐	Identifikacija karakteristika koje se odnose samo na specifičnu funkciju
☐	Korisnička imena i šifre (smjernice koje uključuju duljinu i vrijeme izmjene istih)	☐	Autentifikacija ovlaštenih osoba
☐	Redovno brisanje podataka s nosača podataka prije ponovne upotrebe	☐	Mjere zaštite za umetanje podataka, čitanje, blokiranje i brisanje pohranjenih podataka
☐	Automatsko isključivanje korisničkog imena nakon što je nekoliko puta pogrešno upisana šifra	☐	Specifična pravila pristupa procedurama, kontrolne kartice, metode kontrole postupaka, autorizacija katalogiziranja programa
☐	Automatsko odlogiranje korisničkog imena koje nije korišteno kroz značajniji period	☐	Korištenje VPN tehnologije
☐	Automatsko zaključavanje čuvara zaslona nakon određenog vremena	☐	Korisnička imena i šifre na svim uređajima
☐	Dokumentiranje pristupa aplikacijama (posebice umetanje, modifikacija, brisanje i uništavanje podataka)	☐	Smjernice za izradu sigurnih šifri dostavljene svim zaposlenicima
☐	Korištenje dnevničke datoteke za događaje (nadzor pokušaja provale u sustav)	☐	Vođenje evidencije o korištenju podataka
☐	Pravila o organizaciji dokumenata	☐	Odvajanje proizvodnog i testnog okruženja za banku podataka i podatke
☐	Logiranje i analiza korištenja dokumenata	☐	Korištenje sustava detekcije upada, anti virusnog sustava, vatrozida za hardver i softver, kao i centralnog administrativnog softvera za smartphone (pr. vanjsko brisanje podataka)
☐	Specijalna kontrola u vezi korištenja programa pomoći u opsegu u kojem mobu izbjeći sigurnosne mjere	☐	Brisanje i uništenje svi izbrisivih podataka i elektroničkih medija (laptopa, hard diskova, CD-a, DVD-a, USB stickova....) nakon isteka ugovorene obrade podataka

☐			

Dodatne mjere/objašnjenja:

_____

_____

_____

_____

2.4 Kontrola prijenosa

☐	Korištenje uništavača dokumenata ili pružatelja takve usluge	☐	Zabrana unošenja torbi, i sl., unutar osiguranog prostora kao i efektivna kontrola nad tim
☐	Implementacija mjera filtriranja (URL filter, filtriranje mailova, privitaka i sl.)	☐	Elektronički potpis
☐	Ograničenje korištenja uređaja s vanjskom pohranom podataka (posebice USB, eksterni hard disk, SD kartice i sl.) tehničkim sredstvima (pr. softver za nadzor sučelja)	☐	Nadzor uklanjanja nosača podataka
☐	Nadzor potpunosti i točnosti prijenosa podataka („end to end“ provjera)	☐	Sigurna pohrana i predaja nosača podataka samo ovlaštenim osobama
☐	Savjestan izbor dostavnih službi, osobne dostave i izvršenja transfera	☐	Redovna kontrola dokumenata, kontrolirano i dokumentirano uništenje nosača podataka
☐	Pravila za slanje pošiljki	☐	Zaključavanje povjerljivih nosača podataka
☐	U slučaju povrede osobnih podataka izvršitelj obrade će odmah obavijestiti voditelj obrade	☐	Enkripcija e-mailova
☐	Enkripcija nosača podataka / odvojen transfer dekripcijskih ključeva	☐	Pohrana / prijenos podataka u kriptiranom obliku
☐	Prijenos podataka u anonimiziranom / pseudonimiziranom obliku	☐	Dokumentiranje primatelja, vremena korištenja, utvrđenog vremena brisanja

☐	Implementacija iznajmljenih linija / VPN tunela	☐	Dokumentiranje izdvojenih lokacija / destinacija na koje je prijenos usmjeren te put prijenosa
☐	Formalizirana obrada podataka koja uključuje popis pristupa i procesa prijenosa		

Dodatne mjere/objašnjenja:

_____

_____

_____

_____

2.5 Kontrola unosa

☐	Elektronička evidencija obrade podataka, posebice korištenje, modifikacije i brisanje podataka	☐	Evidencija programa prijenosa i vraćanja podataka
☐	Elektronička evidencija korištenja administrativnih alata	☐	Zapis aktivnosti pohranjen _____ (vrijeme)
☐	Razvoj pregleda aplikacija koje se mogu koristiti za izmjenu i brisanje podataka	☐	Dodjela prava vezanih uz unos, izmjenu i brisanje podataka temeljna na konceptu autorizacije
☐	Transparentnost unosa, izmjena i brisanja podataka od strane individualnog korisničkog imena (bez grupe korisnika)	☐	Pohrana oblika iz kojih su preuzeti podaci namijenjeni automatskoj obradi

Dodatne mjere/objašnjenja:

_____

_____

_____

_____

2.6 Kontrola dostupnosti

☐	Pravila za nadzor nad stvaranjem sigurnosnih kopija	☐	Formalna pravila otpisa hardvera i softvera te odgovarajuće IT procedure
☐	Centralna nabava hardvera i softvera	☐	Prostorije sa serverima ne nalaze se ispod sanitarnog čvora
☐	Ažuriranje softvera	☐	Postojanje plana za hitne slučajeve
☐	Interna pravila o zaštiti osobnih podataka, smjernice, instrukcije za rad, opis procesa i pravila za programiranje, testiranje puštanja podataka	☐	Pohrana sigurnosnih kopija izvan IT odjela na sigurnoj lokaciji
☐	Stvaranje sigurnosnih kopija u pravilnim razmacima	☐	Alternativne lokacije za slučaj nužde
☐	Provjera uspostave sigurnosnih kopija u pravilnim razmacima	☐	Na područjima opasnosti od poplava, prostorije sa serverima nalaze se iznad crte vodene granice
☐	Sigurnosna utičnica u prostoriji sa serverima	☐	Otpornost IT sustava, čak i za slučajeve (jako) velikog stupnja korištenja
☐	Postavljanje servera u odvojenu osiguranu prostoriju ili podatkovni centar	☐	Mjere zaštite od požara (detektori vatre i dima, vatrogasni aparat u prostoriji sa serverima)
☐	Drugi server na mjestu različitom od prvog	☐	Generator električne energije za slučaj nužde
☐	Izvor električne energije koji nije moguće prekinuti	☐	Procedure za povrat podataka
☐	Zrcaljenje podataka	☐	Uređaji koji nadziru temperaturu i vlagu u prostorijama sa serverima
☐	Klima uređaj u prostoriji sa serverom		

Opis vremenskih intervala, nosača podataka, kao i roka pohrane i mjesta sigurnosnih kopija

_____

_____

_____

Dodatne mjere / objašnjenja

_____

_____

_____

_____

2.7 Odvajanje podataka

☐	Odvajanje produktivnog i testnog sustava	☐	Vezano za pseudonimizaciju: odvajanje datoteke o dodjeli i pohrana podataka u zaseban siguran IT sustav
☐	Utvrđivanje prava na baze podataka	☐	Pohrana podataka različitih voditelja obrade u zasebne sakupljače podataka (fizička razdvojenost)
☐	Skupovi podataka opremljeni prilagođavanjem svrhe / polja podataka	☐	Logično odvajanje klijenata (temeljeno na softveru)

Dodatne mjere / objašnjenja:

_____

_____

_____

_____

2.8 Evaluacija

☐ Mehanizam za redovite provjere, procjene i evaluacije efektivnosti gore spomenutih tehničkih i organizacijskih mjera potrebnih za osiguranje sigurnosti.
Molim naznačite koliko često se evaluacija provodi: Svakih _____ mjeseci/godina.

3 Podizvršitelji

☐	Ili: Prethodno pribavljanje posebnog ovlaštenja voditelja obrade za svaki angažman podizvršitelja	☐	Ugovorene kazne za slučaj povrede
☐	Ili: Izvršitelj obrade obavještava voditelja obrade o svakoj promjeni koja se tiče dodavanja ili mijenjanja drugih podizvršitelja, omogućujući voditelju da prigovori takvim promjenama	☐	Voditelju obrade se daju prava izravnog kontroliranja podizvršitelja
☐	Savjestan izbor podizvršitelja posebice imajući u vidu sigurnost podataka	☐	Zaposlenici podizvršitelja imaju obvezu čuvanja tajnosti podataka
☐	Prethodna revizija mjera poduzetih od strane podizvršitelja	☐	Uništavanje podataka nakon okončanja ugovora
☐	Podizvršitelji moraju poštovati ista ograničenja i odredbe ugovora kao i izvršitelj u vezi s obradom podataka voditelja obrade	☐	Konstantan nadzor podizvršitelja i njegova rada

Dodatne mjere / objašnjenja:

_____

_____

_____

_____

4 Obrada izvan EU/EEA

☐	Obrada se odvija isključivo unutar prostora EU/EEA
☐	Obrada se odvija izvan zemlje članice Europske unije (EU) ili zemlje članice Europskog gospodarskog prostora (EEA), a podatke obrađujemo kao izvršitelji obrade. Države: _____
☐	Jedan ili više podugovaratelja obavlja obradu na području izvan zemalja članica EU (EU) ili zemalja članica Europskog gospodarskog prostora (EEA) Države: _____

Svaka obrada izvan EU/EEA zaštićena je (moguće je označiti više odgovora):

- ☐ Odluka Europske komisije o primjerenosti (Bijela lista zemalja);
- ☐ Obvezujuća korporativna pravila;
- ☐ Standardne ugovorne klauzule;
- ☐ Kodeks ponašanja (sukladno članku 40. Uredbe);
- ☐ Certificiranje (sukladno članku 42. Uredbe);
- ☐ zaštita je ostvaren na drugi način: _____

Dodatne mjere / objašnjenja:

_____

_____

_____

_____

5 Omogućavanje ostvarenja prava ispitanika

Tehnički i organizacijski omogućeno je ostvarenje sljedećih prava ispitanika vezanih za obradu osobnih podataka:

☐	Pravo na pristup (čl. 15. GDPR)
☐	Pravo na ispravak (čl. 16. GDPR)
☐	Pravo na brisanje (čl. 17. GDPR)
☐	Pravo na ograničenje obrade (čl. 18. GDPR)
☐	Pravo na prenosivost podataka (čl. 20. GDPR)

Dodatne mjere / objašnjenja:

_____

_____

_____

_____

6 GDPR – specifični zahtjevi

☐	Vođenje odgovarajućih evidencija aktivnosti obrade sukladno čl. 30. Uredbe
☐	Provođenje potrebe procjene učinka na zaštitu podataka sukladno čl. 35 Uredbe
☐	Implementacija zaštite podataka, dizajnirane i utvrđene prema zadanim postavkama u pruženoj usluzi

Dodatne mjere / objašnjenja:

_____

_____

_____

_____

7 Certificiranje i kodeks ponašanja

☐	Certificiranje prema DIN/ISO 9002 (molim dostavite svu relevantnu dokumentaciju)
☐	Valjana certifikacija putem valjanog mehanizma za zaštitu osobnih podataka (oznaka/pečat) upisanog u javni registar Europskog obora za zaštitu podataka
☐	Valjana certifikacija putem službeno akreditiranog tijela za certificiranje (sukladno čl. 43. Uredbe)
☐	Pridržavanje odobrenog kodeksa ponašanja u smislu čl. 40., st. 2., točke (h), Uredbe

Dodatne mjere / objašnjenja:

_____

_____

_____

8 Imate li uspostavljene procedure vezane uz zaštitu osobnih podataka?

☐ Provodite li reviziju stupnja implementacije sa zahtjevima iz Opće uredbe minimalno jednom godišnje?

_____

_____

_____

☐ Imate li uspostavljene procedure i usvojene metodologije provođenja testova procjene učinka na zaštitu podataka ispitanika (DPIA)?

_____

_____

_____

☐ Molimo dostavite jedan primjerak DPIA i navedite kada ste provodili zadnji test procjene učinka ako (za koju vrstu obrade, datum, rizici, rezultati)?

_____

_____

_____

☐ Imate li uspostavljene procedure ostvarivanja prava ispitanika? Molimo ukratko ih opišite.

_____

_____

_____

☐ Imate li uspostavljene procedure vezane uz povredu osobnih podataka i/ili druge incidente? Molimo Vas ukratko opišite procedure te nam dostavite metodologiju po kojoj procjenjujete rizike povrede odnsono incidenta?

_____

_____

_____

☐ Imate li uspostavljene evidencije aktovnosti obrade I Koliko često ih revidirate?

Imate li uspostavljene procedure brisanja podataka? Molimo ukratko opišite iste.

_____

_____

_____

☐ Imate li Pravila privatnosti i Pravila o korištenju kolačića? Molimo dostavite ih.

_____

_____

_____

☐ Opišite nam procedure i mjere vezane uz ˝Privacy by design˝ i ˝Privacy by default˝ (mjere tehničke I integrirane zaštite podataka)? Molimo da nam ukratko opišete oba koncepta, na koji način ih provodite u praksi.

_____

_____

_____

☐ Dijelite li podatke s trećim stranama? Ukoliko da molimo navedite nazive trećih strana koje su relevantne u odnosu na podatke koji se dijele na temelju osnovnog Ugovora?

_____

_____

_____

☐ Jeste li angažirali u odnosu na temeljni ugovor podizvođače? Ukoliko da molimo da ih navedete te dostavite sklopljene Ugovore o obradi i dijeljenju podataka s njima.

_____

_____

_____

☐ Prenosite li podatke u SAD? Ukoliko da na kojem pravnom osnovu ih prenosite. Molimo dostavite procjenu utjecaja prijenosa podataka (TIA)

_____

_____

_____

☐ Održavate li edukacije zaposlenika vezano uz zaštitu osobnih podataka te koliko često?

_____

_____

_____

☐ Na koji način ste uspostavili procedure obavještavanja voditelja obrade u slučaju povrede ili zahtjeva za ostvarivanjem prava od strane ispitanika koji zaprimite u ime voditelja obrade?

_____

_____

_____

Kontakt podaci

i. Kontaktna točka za komunikaciju s DPO-om

Odgovorna osoba: _____

Položaj u organizaciji: _____

E-mail adresa: _____

ii. Službenik za zaštitu podataka (samo za zemlje izvan EU)

Ime i prezime: _____

E-mail adresa: _____

b. Molimo Vas dokument isprintajte i pošaljite nam potpisanu verziju e-mailom (scan)

_____ _____

Datum Odgovorna osoba za popunjavanje upitnika

_____

Položaj u kompaniji

_____

Telefon i e-mail adresa

Potpisivanjem ovog dokumenta potvrđujete implementaciju navedenih mjera.

_____

Potpis

BROJ	IME I PREZIME KOPČANKA	MJESNI BROJ KUPOVANJA	R. BROJ ULOŽENE KUPOVANJA	DATUM ISKAZIVANJA PRAVA	DATUM POVLAČENJA PRAVA (ako je primjenjivo)	DATUM ISKORIŠTENJA ZAHTJEVA	IME I PREZIME OSOBE KOJA JE OBAVILA POVLAČENJE PRAVA

Hrvatska zaklada za znanost

EVIDENCIJA ZAHTJEVA ISPITANIKA

Br.	Tip zahtjeva (npr. zahtjev za brisanje, zahtjev za pristup itd.) i osnovni podaci zahtjeva (npr. ispitanikovo obrazloženje)	Identitet ispitanika (ime i prezime, ostali detalji potrebni za identifikaciju osobe)	Datum primitka zahtjeva	Može li se zahtjevu udovoljiti? (da/ne). Ako ne, navesti razloge.	Složeni zahtjev koji uzrokuje kašnjenje u davanju odgovora? (da/ne). Ako da, navesti razloge.	Ako je primjenjivo, datum obavijesti o kašnjenju odgovora na zahtjev	Datum odgovora na zahtjev	Ako je primjenjivo, naknada za pretjeran/očito neutemeljen zahtjev i razlozi za naplaćivanje ispitaniku	Radnje poduzete po zahtjevu	Podatak je li Službenik za zaštitu podataka bio uključen u proces (da/ne)
1.										
2.										
3.										
4.										
5.										
6.										

*Popunjava Službenik za zaštitu podataka

IZJAVA O VRAĆANJU OSNOVNOG SREDSTVA ZA RAD

Ovom izjavom ja, _____, potvrđujem da sam dana

_____ godine vratio/vratila

_____.

Jasno mi je kao potpisniku ove izjave da su svi podaci kao i osnovno sredstvo za rad u vlasništvu Hrvatske zaklade za znanost te da odgovorne osobe mogu raditi provjeru istih u bilo kojem trenutku ako postoji sumnja u zlouporabu opreme ili u kršenje važećih propisa i internih akata/politika Hrvatske zaklade za znanost.

U Zagrebu, dana _____ godine.

Ovaj dokument je izrađen u 2 (dva) primjerka od kojih svaka strana zadržava po 1 (jedan) primjerak.

Predao:

_____

Primio:

_____

OBRAZAC ZA RAZDUŽIVANJE OPREME

_____ (ime i prezime, OIB), zaposlen/zaposlena do prestanka radnog odnosa na radnom mjestu _____, svojim potpisom se obvezuje da će u skladu s propisima koji uređuju područje zaštite osobnih podataka, odnosno 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 (Opća uredba o zaštiti podataka), Zakonom o provedbi Opće uredbe o zaštiti podataka (NN 42/18), Pravilnikom o zaštiti podataka i drugim internim aktima i važećim propisima, čuvati povjerljivost svih osobnih podataka koje je dobio/dobila tijekom obavljanja obveza iz Ugovora o radu koji uređuje prava i obveze i/ili koje proizlaze iz istog odnosno drugog ugovora koji uređuje prava i obveze i/ili koje proizlaze iz istog.

Uz navedeno, svojim potpisom se obvezuje sve podatke iz službene opreme koju je koristio/koristila za vrijeme radnog odnosa, a osobito u slučaju da mu/joj ista nakon prestanka radnog odnosa ostaje na raspolaganju, prije samog odlaska iz Hrvatske zaklade za znanost, Ilica 24, 10 000 Zagreb (dalje u tekstu: Zaklada), spremiti na sigurno, šifrom (poznatoj odgovornoj osobi u Zakladi) zaštićeni vanjski medij, bez izrade kopije, kako bi sve informacije i dalje ostale u vlasništvu Zaklade.

Potpisom također jamči odnositi se prema svim primljenim informacijama sa strogom povjerljivosti i tajnosti, ne otkriti ni jednoj trećoj strani bilo koju od informacija koje je doznao/doznala na radnom mjestu i/ili u obavljanju poslova za Zakladu te da neće iskoristiti ni jednu od tih informacija na drugi način nego kako je to predviđeno ugovornim obvezama i/ili drugom svrhom prikupljanja podataka.

Na kraju, svojim potpisom prihvaća materijalnu i kaznenu odgovornost ako prilikom obrade osobnih podataka i nakon prestanka radnog odnosa u Zakladi, namjerno ili krajnjom nepažnjom prekorači granice svojih ovlasti i/ili osobne podatke prikuplja i/ili obrađuje za drugu namjenu osim ugovorene i/ili ih daje na korištenje drugim primateljima i/ili ne osigura provođenje ugovorenih mjera zaštite osobnih podataka i/ili sam/sama protivno uputi odgovorne osobe Zaklade zadrži, obrađuje i distribuira podatke u vlasništvu Zaklade, a radi takve obrade dođe do imovinske, neimovinske ili druge štete za Zakladu kao voditelja obrade te s tim u vezi i štete za ispitanika.

_____ (ime i prezime osobe) vratio/vratila i razdužio/razdužila je sljedeće stvari, koje su mu/joj bile predane za korištenje u službene svrhe:

NAZIV STVARI:

Ovaj dokument je izrađen u 2 (dva) primjerka od kojih svaka strana zadržava po 1 (jedan) primjerak.

U Zagrebu, _____ (datum)

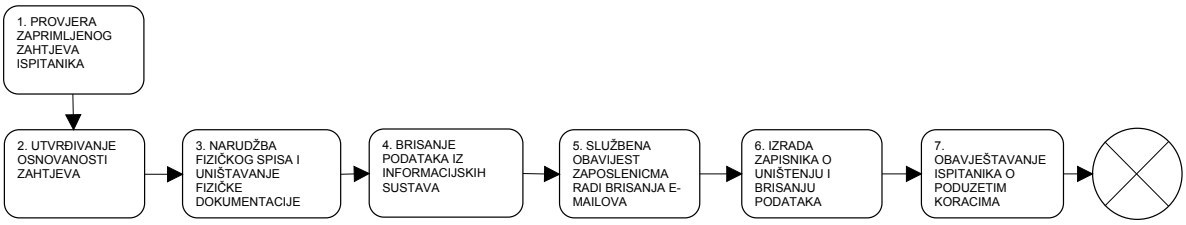
Odgovorna osoba u Zakladi

_____

Zaposlenik:

_____

HODOGRAM BRISANJA OSOBNIH PODATAKA



Poštovani,

nastavno na prekid suradnje ovim putem podsjećamo kako se sve odredbe vezane uz tajnost kao i uz zaštitu privatnosti naših ispitanika, u skladu s važećim propisima primjenjuju trajno.

Molimo da nam pisanim putem potvrdite kako ste sve podatke koje ste imali u vezi s našim ispitanicima ili poslovanjem obrisali sa svih medija i iz vaših internih sustava.

Za sva pitanja možete se obratiti i našem službeniku za zaštitu podataka: Alen Plančić, alen@hrzz.hr ili zamjenici službenika za zaštitu podataka: Lana Zubović, lana@hrzz.hr.

Srdačan pozdrav,

Hrvatska zaklada za znanost
Ilica 24,
10000 Zagreb

OBAVIJEST O PRODUŽENJU RAZDOBLJA ZA OČITOVANJE

Za: _____ (*Ispitanik*)

Predmet: Vaš zahtjev za ostvarenje prava ispitanika

Poštovani,

zahvaljujemo Vam što ste uputili zahtjev za ostvarenje prava ispitanika, kako je naznačeno u [*npr. e-pošti od datuma, tijekom telefonskog poziva na datum*].

Hrvatska zaklada za znanost ima zaduženi tim zaposlenika i službenika za zaštitu podataka koji će istražiti Vaš zahtjev i poslati Vam očitovanje.

Pregledom Vašeg zahtjeva utvrdili smo kako je riječ o složenom zahtjevu, budući da obuhvaća opsežno pretraživanje velikog broja dokumenata i drugih podataka pohranjenih u elektroničkom obliku. S obzirom na to da ti dokumenti mogu sadržavati osobne podatke, ne samo o Vama, nego i o drugim ispitanicima, bit će potrebno dodatno vrijeme da provedemo odgovarajuće analize i provjere radi utvrđenja točnih informacija.

Stoga će rješavanje Vašeg zahtjeva zahtijevati ulaganje dodatnog vremena te ćemo morati produžiti vrijeme kako bi Vam mogli pružiti odgovarajuće očitovanje. Namjeravamo odgovoriti na Vaš zahtjev najkasnije u roku od tri mjeseca od primitka, s tim da ćemo nastojati odgovoriti i prije isteka tog roka.

Ako imate dodatnih pitanja ili nedoumica, u bilo kojem nam se trenutku tijekom tog razdoblja možete obratite putem sljedećih kontakt podataka:

- telefonski broj: +385 51 228 690
- adresa e-pošte: alen@hrzz.hr (službenik za zaštitu podataka ili lana@hrzz.hr (zamjenik službenika za zaštitu podataka)
- poštanska adresa Hrvatske zaklade za znanost: Ilica 24, 10 000 Zagreb.

Više o Vašim pravima možete pročitati na [*staviti link na tekst obavijesti iz članka 13. ili 14. Opće uredbe odnosno Pravila privatnosti*].

S poštovanjem,

Hrvatska zaklada za znanost,

Ilica 24

10 000 Zagreb

DOPIS ZA POJAŠNJENJE ZAHTJEVA

Za: _____ (*Ispitanik*)

Predmet: Vaš zahtjev za ostvarenje prava ispitanika

Poštovani,

zahvaljujemo Vam što ste uputili zahtjev za ostvarenje prava ispitanika, kako je naznačeno u [*npr. e-pošti od datuma, tijekom telefonskog poziva na datum*].

Hrvatska zaklada za znanost ima zaduženi tim zaposlenika i službenika za zaštitu podataka koji će istražiti Vaš zahtjev i poslati Vam očitovanje.

Međutim, kako bismo ispravno odgovorili na Vaš zahtjev, želimo utvrditi na koje pravo iz Opće uredbe o zaštiti podataka (ili više prava) se Vaš zahtjev odnosi.

Imajte na umu da u skladu s Općom uredbom o zaštiti podataka imate sljedeća prava: (i) pravo na pristup Vašim osobnim podacima, (ii) pravo na ispravak Vaših osobnih podataka ako su netočni ili nepotpuni, (iii) pravo na brisanje Vaših osobnih podataka (poznatije kao "pravo na zaborav"), (iv) pravo na ograničenje obrade, (v) pravo prigovora na obradu osobnih podataka, (vi) pravo na prenosivost podataka i (vii) pravo da ne budete predmetom automatiziranog individualnog donošenja odluka, uključujući izradu profila.

Nakon što odredite na koje od navedenih prava iz Opće uredbe o zaštiti podataka se Vaš zahtjev odnosi, nastavit ćemo s njegovom obradom u zakonskom roku (tj., ovisno o složenosti zahtjeva, u roku od jednog mjeseca ili najviše tri mjeseca od primitka Vašeg zahtjeva).

Ako ne specificirate Vaš zahtjev ni nakon dva zahtjeva za specifikacijom koje Vam upućuje Hrvatska zaklada za znanost, nećemo moći donijeti oduku u vezi Vašeg zahtjeva.

Ako imate dodatnih pitanja ili nedoumica, u bilo kojem nam se trenutku tijekom tog razdoblja možete obratite putem sljedećih kontakt podataka:

- telefonski broj: +385 51 228 690
- adresa e-pošte: alen@hrzz.hr (službenik za zaštitu podataka ili lana@hrzz.hr (zamjenik službenika za zaštitu podataka)
- poštanska adresa Hrvatske zaklade za znanost: Ilica 24, 10 000 Zagreb.

Više o Vašim pravima možete pročitati na [*staviti link na tekst obavijesti iz članka 13. ili 14. Opće uredbe odnosno Pravila privatnosti*].

S poštovanjem,

Hrvatska zaklada za znanost,

Ilica 24

10 000 Zagreb

OBRAZAC ZA PROVJERU TOČNOSTI PODATAKA

Ovim Vas putem obavještavamo kako u skladu s obvezama koje imamo kao poslodavac, provjeravamo točnost Vaših podataka. Provjerom točnosti izvršavamo obveze koje proizlaze iz Opće uredbe o zaštiti podataka, a koje su u vezi s Vama kao našim zaposlenicima.

Obrada podataka je nužna kako bismo ispunili svoje obveze koje imamo kao voditelj obrade, prilikom čega moramo redovito održavati točnost i ažurnost podataka. Slijedom navedenog, Hrvatska zaklada za znanost, Ilica 24, 10 000 Zagreb (dalje u tekstu: „Zaklada“) kao voditelj obrade je, u skladu s važećim propisima, dužna ispitanicima pružiti sljedeće informacije:

Pristup Vašim osobnim podacima mogu imati zaposlenici Zaklade, konzultanti koji pomažu IT podršci i koji pomažu u obradi osobnih podataka tijekom korištenja IT sustava te ovlaštene osobe Zaklade. Moguće je također otkrivanje Vaših osobnih podataka ovlaštenoj trećoj strani ako to zahtijevaju ili dopuštaju obvezujući propisi (npr. državna tijela, sudovi, vanjski savjetnici i ostale treće osobe koje se smatraju javnim tijelima).

Vaša prava su sljedeća:

- Pravo na pristup
- Pravo na ispravak
- Pravo na brisanje ("pravo na zaborav")
- Pravo na ograničavanje obrade
- Pravo na prigovor
- Pravo na prenosivost podataka.

Detaljno o načinu ostvarenja navedenih prava možete pročitati u Pravilniku o zaštiti osobnih podataka, Pravilima privatnosti objavljenim na mrežnim stranicama Zaklade ili zatražite da Vam informacije dostavimo putem e-maila ili na adresu stanovanja.

Ako želite saznati više ili želite koristiti jedan ili više od gore navedenih prava, slobodno kontaktirajte službenika za zaštitu podataka putem e-maila: alen@hrzz.hr ili poštom na adresu: Ilica 24, 10 000 Zagreb.

Vaši osobni podaci obrađivat će se ili se mogu obrađivati isključivo u gore navedene svrhe, osim ako je to neophodno za poštivanje zakonskih obveza (npr. za dostavljanje podataka sudovima ili organima kaznenog progona), ako ste pristali na odgovarajuću obradu ili ako je obrada na drugi način zakonita prema obvezujućim propisima. Ako se podaci obrađuju u drugu svrhu, prije obrade pružit ćemo Vam informacije o toj drugoj svrsi te sve druge relevantne informacije.

OBRAZAC ZA PROVJERU TOČNOSTI PODATAKA

Ime:	
Prezime:	
Datum i mjesto rođenja:	
Općina/Grad	
Ulica i kućni broj	
Broj i naziv pošte	
Boravište:*	
Zanimanje/zvanje:	
Stručna sprema:	
IBAN:	
Zaštićeni račun	

Kontakt podaci za slučaj nužde/nezgode na radu ili drugih izvanrednih okolnosti	
E-mail adresa za komunikaciju **	

* upisuju zaposlenici koji imaju prijavljeno privremeno boravište
** upisuju zaposlenici koji nemaju službenu e-mail adresu već im se za potrebe izvršenja obveza i prava koja proizlaze iz radnog odnosa obavijesti i dokumenti šalju na privatne e-mail adrese koje se brišu odmah po prestanku radnog odnosa kod poslodavca.

Posebna napomena: u slučaju promjene nekog od podataka, radnik je dužan u roku od 8 sata obavijestiti poslodavca o nastalim promjenama sukladno Pravilniku o sadržaju i načinu vođenja evidencije o radnicima zaposlenim kod poslodavca (NN 55/2024).

SMJERNICE ZA ZAŠTITU OSOBNIH PODATAKA U RADNIM ODNOSIMA

Dana 25. svibnja 2018. stupila je na snagu 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). Ova Uredba uvodi nove obveze za poslodavce zbog osjetljivosti odnosa poslodavca i zaposlenika, odnosno zbog odnosa podređenosti zaposlenika. Cilj ove upute je pokriti sve situacije u kojima postoji radni odnos, bez obzira na to je li odnos utemeljen na ugovoru o radu.

Hrvatska zaklada za znanost, Ilica 24, 10000 Zagreb (dalje u tekstu: „Zaklada" ili „poslodavac") koristit će ove upute kao Smjernice u obradi osobnih podataka.

1. Obveze poslodavca i glavna načela

Obveza poslodavca je da:

- osigura da se podaci obrađuju za određene i zakonite svrhe koje su razmjerne i nužne;
- uzme u obzir načelo ograničavanja svrhe te da istodobno osigura da su podaci prikladni, relevantni te da nisu prekomjerno prikupljeni;
- primjenjuje načela razmjernosti i supsidijarnosti bez obzira na pravnu osnovu;
- bude transparentan sa zaposlenicima o korištenju i svrhama tehnologije praćenja;
- omogući ostvarivanje prava na pristup podacima te pod određenim pretpostavkama pravo na ispravljanje, brisanje, prenosivost i ograničenje obrade osobnih podataka;
- održava podatke točnima i ne čuva ih više nego što je potrebno;
- poduzima sve potrebne mjere za zaštitu podataka od neovlaštenog pristupa i osigurava da su zaposlenici dovoljno svjesni obveze zaštite podataka.

U skladu s navedenim, glavna načela za obradu osobnih podataka zaposlenika su: svrhovitost, transparentnost, legitimnost, proporcionalnost, povjerljivost i čuvanje podataka, sigurnost, svijest zaposlenika.

Svrhovitost - podaci se moraju prikupljati za određenu, izričitu i legitimnu svrhu te se ne mogu dalje obrađivati na način koji je nespojiv s tim ciljevima.

Primjer - osobne adrese zaposlenika prikupljene u svrhu isplate plaće ne mogu se dalje koristiti ili obrađivati u svrhu izravnog marketinga bez posebnog pristanka zaposlenika. Kompatibilna svrha bila bi npr. dodatna obrada podataka kako bi se izračunale i uključile nove putne naknade u plaću.

Transparentnost - obrada podataka u kontekstu radnih odnosa može dovesti do kršenje pravila o zaštiti podataka, ne zato što je takva obrada sama po sebi nezakonita, već zato što zaposlenici nisu

pravilno obaviješteni o njima. Zaposlenici moraju znati koje podatke poslodavac prikuplja i u koju svrhu.

Transparentnost je također zajamčena dodjeljivanjem zaposleniku prava na pristup njegovim osobnim podacima i mogućnošću da se obrati nadzornom tijelu.

Primjer - poslodavac može imati legitiman interes u kontroli rada svojih zaposlenika procjenom radne učinkovitosti (npr. koliko slučajeva je zaposlenik riješio, na koliko telefonskih poziva je odgovorio itd.); međutim, uzevši u obzir načelo proporcionalnosti, poslodavac će moći obrađivati takvu vrstu podataka ako je zaposlenik o takvoj obradi propisno obaviješten.

Legitimnost - bilo koji proces obrade, čak i ako je potpuno transparentan, može se poduzeti jedino ako je legitiman.

Primjer - poslodavac ima legitimni interes da procijeni učinak rada svog zaposlenika, a u sklopu toga nužno je da poslodavac obradi osobne podatke zaposlenika. Taj kriterij će biti zadovoljen tek kada praćenje učinka rada neopravdano ne krši prava i slobode zaposlenika.

Proporcionalnost - poslodavci uvijek trebaju obrađivati osobne podatke zaposlenika tako da najmanje zadiru u osobnu sferu pojedinca, uzimajući u obzir rizike koji su u pitanju, količinu podataka koji su uključeni i svrhe obrade.

Primjer - poslodavci moraju znati, za određena radna mjesta, imaju li potencijalni zaposlenici auto i vozačku dozvolu. Poslodavac je ovlašten tražiti takvu informaciju, ali bilo bi suprotno ovom načelu pitati za model ili boju auta.

Povjerljivost i čuvanje podataka - evidencija o zaposlenicima mora se čuvati sukladno Pravilima za upravljanja dokumentarnim gradivom Hrvatske zaklade za znanost (KLASA: 110-02/24-01/01; URBROJ: 1-24-3)

Poslodavci mogu osigurati točnost osobnih podataka zaposlenika, npr. pružajući zaposlenicima godišnji ispis njihovih evidencija.

Sigurnost - posebnu zaštitu treba osigurati zbog neovlaštenog otkrivanja ili pristupa. Danas tehnologija nudi razumna sredstva za sprečavanje ovakvog neovlaštenog pristupa ili otkrivanja, omogućujući u svakom slučaju identifikaciju osoblja koje pristupa datotekama. Mora postojati ugovor između poslodavca i treće strane, odnosno izvršitelja, kojim se osiguravaju jamstva da izvršitelj djeluje samo prema uputama poslodavaca.

Neke od propisanih mjera sigurnosti su: korištenje lozinki odnosno identifikacijskih sustava za pristup računalnim evidencijama o zapošljavanju, prijava i praćenje neovlaštenog pristupa i otkrivanja, sigurnosne kopije, enkripcije poruka, osobito kada se podaci prenose izvan organizacije.

Svijest zaposlenika - bez prikladne edukacije zaposlenika o načinu rukovanju osobnim podacima, neće se moći u potpunosti poštivati zaštita osobnih podataka na radnom mjestu. Poslodavac stoga osigurava edukacije zaposlenika.

Uvažavajući navedena načela, poslodavac se treba voditi trima glavnim principima: pravni temelj, transparentnost i automatiziranost odluka.

1. *Pravni temelj*

Za većinu obrada osobnih podataka na poslu, pravna osnova ne može i ne bi trebala biti suglasnost, odnosno privola zaposlenika zbog prirode odnosa između poslodavca i zaposlenika. Obrada osobnih podataka može biti neophodna za izvršenje ugovora u slučajevima kada poslodavac mora obraditi osobne podatke zaposlenika u ispunjavanju takvih obveza. Nacionalnim zakonodavstvom propisane su zakonske obveze poslodavca koje zahtijevaju obradu osobnih podataka (npr. Zakon o radu, Zakon o mirovinskom osiguranju i dr.), no u takvim slučajevima zaposlenik mora biti jasno i potpuno informiran o takvoj obradi.

Ako su osobni podaci koji se odnose na zaposlenika prikupljeni od samog zaposlenika, poslodavac u trenutku prikupljanja osobnih podataka zaposleniku pruža sve sljedeće informacije:

1. identitet i kontaktne podatke poslodavca

2. kontaktne podatke službenika za zaštitu podataka, ako je primjenjivo;

3. svrhe obrade radi kojih se upotrebljavaju osobni podaci kao i pravnu osnovu za obradu;

4. ako je obrada nužna za potrebe legitimnih interesa poslodavca ili treće strane, informacije o legitimnim interesima poslodavca ili treće strane;

5. primatelje ili kategorije primatelja osobnih podataka, ako ih ima;

6. ako je primjenjivo, činjenicu da poslodavac namjerava osobne podatke prenijeti trećoj zemlji ili međunarodnoj organizaciji te postojanje ili nepostojanje odluke Komisije o primjerenosti; ili u slučaju prijenosa koji podliježu odgovarajućim zaštitnim mjerama ili kod obvezujućih korporativnih pravila ili kada je prijenos nužan za izvršavanje ugovora između ispitanika i voditelja obrade, kao i za provedbu predugovornih mjera na zahtjev ispitanika, upućivanje na prikladne ili odgovarajuće zaštitne mjere i načine pribavljanja njihove kopije ili mjesta na kojem su stavljene na raspolaganje.

Osim navedenih informacija, poslodavac u trenutku kada se osobni podaci prikupljaju pruža zaposleniku sljedeće dodatne informacije potrebne kako bi se osigurala poštena i transparentna obrada:

1. razdoblje u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterije kojima je utvrđeno to razdoblje;

2. postojanje prava da se od poslodavca zatraži pristup osobnim podacima i ispravak ili brisanje osobnih podataka ili ograničavanje obrade, koji se odnose na ispitanika ili prava na ulaganje prigovora njihovu obradu te prava na prenosivost podataka;

3. ako se obrada temelji na privoli zaposlenika danoj za jednu ili više svrha obrade ili na temelju izričite privole zaposlenika dane za obradu posebnih kategorija osobnih podataka, postojanje prava da se u bilo kojemu trenutku povuče privola, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije nego što je ona povučena;

4. pravo na podnošenje prigovora nadzornom tijelu;

5. informaciju o tome je li pružanje osobnih podataka zakonska ili ugovorna obveza ili uvjet prijeko potreban za sklapanje ugovora te ima li zaposlenik obvezu pružanja osobnih podataka i koje su moguće posljedice ako se takvi podaci ne pruže;

6. postojanje automatiziranog donošenja odluka, što uključuje izradu profila te smislene informacije o tome o kojoj je logici riječ, kao i važnost i predviđene posljedice takve obrade za zaposlenika.
Navedeno se ne primjenjuje u onoj mjeri u kojoj zaposlenik već raspolaže navedenim informacijama.

Primjeri evidencija o radniku koji obično uključuju obradu osobnih podataka:

- prijave na natječaj i radne reference,
- isprava o obračun plaće i porezne informacije - porezne i socijalne naknade,
- podaci o bolovanju,
- godišnji odmor,
- neplaćeni dopust/plaćeni dopust,
- godišnja procjena/izvještaj o ocjenjivanju,
- podaci koji se odnose na promaknuće, premještaj, edukacije i disciplinska pitanja,
- podaci o ozljedama na radu,
- podaci prikupljeni od strane računalnih sustava,
- evidencija ulazaka i izlazaka,
- članovi obitelji,
- nadoknada troškova, za npr. putovanje.

Ako se poslodavac oslanja na legitiman interes, svrha obrade mora biti legitimna - odabrana metoda ili specifična tehnologija mora biti potrebna, razmjerna i provedena na najmanje nametljiv način zajedno sa sposobnošću da poslodavac može dokazati da su uspostavljene odgovarajuće mjere kako bi se osigurala ravnoteža s temeljnim pravima i slobodama zaposlenika. Procesi obrade moraju također biti transparentni, a zaposlenici trebaju biti jasno i potpuno informirani o obradi osobnih podataka, uključujući i postojanje bilo kakvog nadzora. Potrebno je usvojiti odgovarajuće tehničke i organizacijske mjere kako bi se osigurala sigurnost obrade.

a) Suglasnost/privola

Privola ispitanika znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika (zaposlenika) kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose. Da bi se privola smatrala valjanom, zaposlenik bi je trebao moći opozvati u bilo koje doba i bez ikakve štete, odnosno negativnih posljedica.

Zbog činjenice da je zaposlenik u podređenom položaju u odnosu na poslodavca, za većinu slučajeva obrade osobnih podataka zaposlenika, pravna osnova te obrade ne može i ne bi trebala biti suglasnost zaposlenika pa je potrebna druga pravna osnova.

Štoviše, čak i u slučajevima kada bi se moglo reći da privola predstavlja valjanu pravnu osnovu takve obrade (ako se nesumnjivo može zaključiti da je pristanak slobodno dan), to mora biti specifičan i informiran pokazatelj volje zaposlenika. Zadane postavke na uređajima i/ili instalacija softvera (kao što je unaprijed označena kvačica) ne mogu se smatrati dobrovoljnom suglasnošću

za obradu osobnih podataka od strane zaposlenika jer pristanak zahtijeva aktivnu radnju. Nedostatak aktivne radnje (npr. kada se ne mijenjaju zadane postavke) ne može se smatrati posebnom suglasnošću za dopuštanje takve obrade.

Važno je navesti kako zaposlenici rijetko mogu slobodno dati, odbiti ili opozvati privolu, s obzirom na ovisnost koja proizlazi iz odnosa poslodavca i zaposlenika. Osim u iznimnim situacijama, poslodavci će se morati osloniti na drugu pravnu osnovu osim privole - kao što je nužnost obrade podataka za njihov legitimni interes. Međutim, legitiman interes sam po sebi nije dovoljan kada uzrokuje prekoračenje prava i sloboda zaposlenika.

Bez obzira na pravnu osnovu obrade, prije samog početka trebalo bi provesti test proporcionalnosti kako bi se razmotrilo je li obrada neophodna za postizanje legitimne svrhe, kao i određivanje koje se mjere moraju poduzeti kako bi se osiguralo da su kršenje prava na privatni život i tajnost komunikacija svedeni na minimum.

b) Legitiman interes

Ako se poslodavac želi osloniti na legitiman interes kao pravnu osnovu za obradu osobnih podataka, svrha obrade mora biti legitimna, a odabrana metoda ili specifična tehnologija pomoću koje se obrada vrši, mora biti nužna za legitiman interes poslodavca. Obrada mora biti razmjerna poslovnim potrebama, tj. svrsi obrade. Obrada podataka u radnim odnosima trebala bi se svesti na najmanju moguću mjeru i trebala bi biti usmjerena na specifično područje rizika.

Da bi se poslodavac oslonio na legitiman interes kao pravnu osnovu obrade osobnih podataka zaposlenika, bitno je da postoje posebne mjere ublažavanja kako bi se osigurala odgovarajuća ravnoteža između legitimnog interesa poslodavca i temeljnih prava i sloboda zaposlenika. Takve mjere, ovisno o obliku nadzora trebale bi uključivati ograničenja nadzora kako bi se zajamčilo da se ne krši privatnost zaposlenika. Takva ograničenja mogu biti: geografska (npr. praćenje samo na određenim mjestima, odnosno zabrana praćenja osjetljivih područja kao što su vjerska mjesta, sanitarne zone i prostorije za odmor); usmjerena na određenu vrstu podataka (osobne elektronske datoteke i komunikaciju ne bi trebalo pratiti) i vremenska (npr. periodično umjesto kontinuiranog praćenja).

2. Transparentnost

Zaposlenici moraju biti obaviješteni o postojanju bilo kakvog nadzora, svrsi za koju će se obrađivati osobni podaci i bilo kakve druge informacije potrebne za jamstvo pravedne obrade.

S novim tehnologijama potreba za transparentnošću postaje sve vidljivija jer omogućuju prikupljanje i daljnju obradu mogućih velikih količina osobnih podataka na tajan način.

3. Automatizirane odluke

Zaposlenici imaju pravo da ne podliježu odlukama koje su utemeljene isključivo na automatiziranoj obradi osobnih aspekata (kao što je primjerice učinkovitost na radu), osim ako odluka proizlazi iz nekog obvezujućeg propisa.

2. Procjena rizika i propisivanje posebnih pravila

Poslodavac prije obrade mora provesti procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka, osobito tamo će gdje vrsta obrade, posebice korištenjem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe same obrade, vjerojatno rezultirati visokim rizikom za prava i slobode fizičkih osoba. Primjer je slučaj sustavne i opsežne procjene osobnih aspekata vezanih uz fizičke osobe temeljene na automatiziranoj obradi, uključujući profiliranje, a na kojima se donose odluke koje stvaraju pravne učinke u vezi s fizičkom osobom ili na sličan način značajno utječu na fizičku osobu. Ako poslodavac utvrdi da ne može efikasno riješiti identificirane rizike, tj. da su preostali rizici i dalje visoki, mora se konzultirati s nadzornim tijelom (Agencijom za zaštitu osobnih podataka („AZOP")) prije početka obrade.

Poslodavac može posebnim aktom osigurati detaljnija pravila kako bi se osigurala zaštita prava i sloboda u pogledu obrade osobnih podataka zaposlenika u kontekstu radnog odnosa. Konkretno, ta se pravila mogu predvidjeti u svrhu:

- zapošljavanja,
- izvršavanja ugovora o radu,
- upravljanja, planiranja i organizacije rada,
- jednakosti i raznolikosti na radnom mjestu,
- zdravlja i sigurnosti na poslu,
- zaštite imovine poslodavca,
- ostvarivanja prava i koristi vezanih uz zapošljavanje,
- prestanka radnog odnosa.

Sva takva pravila trebaju uključivati prikladne i specifične mjere za zaštitu ljudskog dostojanstva, legitimnih interesa i temeljnih prava zaposlenika, s posebnim osvrtom na transparentnost obrade, prijenos osobnih podataka unutar skupine poduzetnika ili grupe poduzeća koja se bave zajedničkom gospodarskom djelatnošću i sustava nadzora na radnom mjestu.

Moderne tehnologije omogućuju putem različitih uređaja praćenje zaposlenika tijekom i izvan radnog vremena, na putu od mjesta rada do njihova mjesta stanovanja. Takvi uređaji mogu biti npr. pametni telefon, računalo, tablet, vozilo. Ako ne postoje ograničenja za obradu, odnosno ako obrada nije transparentna, postoji visoki rizik da se legitimni interes poslodavaca za zaštitom svoje imovine pretvori u neopravdano i nametljivo praćenje.

Opsežna uporaba tehnologije često znači gubitak anonimnosti, što dovodi do sve manjeg broja prijava nepravilnosti i nezakonitosti koje čine nadređeni i drugi zaposlenici. Anonimnost je često nužna kako bi se zaposlenik aktivirao i prijavio takve situacije. Praćenje koje krši prava privatnosti zaposlenika može dovesti do nemogućnosti podnošenja pritužbi odgovarajućim zaposlenicima. U takvom slučaju, uspostavljena sredstva za unutarnju kontrolu mogu postati neučinkovita.

U ovakvim situacijama poslodavci bi trebali razmotriti je li:

- djelatnost obrade neophodna, i ako je tako, pravni temelj koji se primjenjuje;
- predložena obrada osobnih podataka pravedna prema zaposlenicima;
- obrada proporcionalna riziku

~ aktivnost obrade transparentna.

Obrada posebnih kategorija osobnih podataka

Postoje posebne kategorije podataka, kao npr. one koje otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska uvjerenja, biometrijski podaci, genetski podaci, sindikalno članstvo te one koje se odnose na zdravlje, spolni život i seksualnu orijentaciju.

U kontekstu radnog odnosa osjetljivi podaci koje najvjerojatnije posjeduju poslodavci uključuju

- zdravlje - primjerice, vezano za isplate plaću tijekom bolovanja, ispunjavanje zdravstvenih i sigurnosnih zahtjeva, pružanje zdravstvenog sustava zaštite zdravlja i osiguranja ili osiguranja mirovina;
- kaznena djela - primjerice, u vezi s istragom pokrenutom protiv zaposlenika zbog kaznenog djela prijevare, takav zaposlenik ne može obavljati poslove koje zahtijevaju povjerenje;
- sindikalno članstvo.

Poslodavac ima legitimni interes za obradu osobnih podataka svojih zaposlenika u zakonite i legitimne svrhe potrebne za uobičajeni razvoj radnog odnosa i poslovnih operacija.

Postavlja se pitanje koju količinu osobnih podataka o potencijalnom zaposleniku poslodavac može prikupljati? Odgovor na ovo pitanje bio bi vrlo različit npr. drugačiji su kriteriji za odabir osobe koja će se baviti procjenom rizika klijenata neke banke, u odnosu na zaposlenika u kantini iste banke.

3. Nadzor zaposlenika preko društvenih mreža

Korištenje društvenih mreža od strane pojedinaca je široko rasprostranjeno i relativno je često da se profili korisnika mogu javno vidjeti, ovisno o postavkama koje je odabrao korisnik. Posljedično, poslodavci vjeruju da bi provjeravanje profila na društvenim mrežama potencijalnih kandidata moglo biti opravdano tijekom njihovog procesa zapošljavanja. To također može biti slučaj i za druge javno dostupne informacije o potencijalnom zaposleniku.

Međutim, poslodavci ne bi smjeli pretpostavljati da im je, samo zbog toga što je profil na društvenim mrežama javno dostupan, dopušteno obraditi te podatke u poslovne svrhe. Za tu obradu potrebna je pravna osnova, poput legitimnog interesa. U tom kontekstu poslodavac treba - prije pregleda profila na društvenim mrežama - uzeti u obzir je li profil na društvenoj mreži podnositelja zahtjeva vezan uz poslovne ili privatne svrhe jer to može biti važan pokazatelj pravne dopustivosti obrade podataka. Osim toga, poslodavcima je dopušteno prikupljati i obrađivati osobne podatke koji se odnose na podnositelje zahtjeva u onoj mjeri u kojoj je prikupljanje tih podataka potrebno i relevantno za obavljanje posla koji se traži.

Podaci prikupljeni tijekom procesa zapošljavanja trebaju biti općenito izbrisani čim postane jasno da odluka o zaposlenju pojedinih zaposlenika neće biti donesena ili da neće biti prihvaćena. Pojedinac se također mora pravilno obavijestiti o takvoj obradi prije nego što se uključe u proces zapošljavanja.

Ne postoji pravni temelj za poslodavca da potencijalnim zaposlenicima podnese "zahtjev za prijateljstvo" na društvenim mrežama ili da na drugi način osigura pristup sadržaju njihovih profila. Samo ako je za posao potrebno pregledati informacije o kandidatu na društvenim medijima, na primjer, kako bi se mogli ocijeniti specifični rizici koji se tiču kandidata za određenu funkciju, a kandidati se pravilno informiraju (primjerice u oglasu za posao), poslodavac može imati pravnu osnovu za pregled javno dostupnih informacija o kandidatima, odnosno potencijalnim zaposlenicima.

Dokle god poslodavac može dokazati da je takvo praćenje potrebno za zaštitu njegovih legitimnih interesa, da nema dostupnih drugih, manje drastičnih sredstava i da su bivši zaposlenici bili adekvatno informirani o opsegu redovitog promatranja njihovih profila na javnim mrežama, poslodavac se može osloniti na navedenu pravnu osnovu.

Primjer - poslodavac prati LinkedIn profile bivših zaposlenika tijekom trajanja ugovorne zabrane natjecanja. Svrha ovog praćenja je provjera usklađenosti s takvim ugovorom. Praćenje je ograničeno samo na bivše zaposlenike obuhvaćene ugovorom.

Poslodavac ne može od zaposlenika tražiti korištenje isključivo njegovog poslovnog profila na društvenim mrežama. Čak i kad je to u opisu njegova posla (npr. glasnogovornik), zaposlenik mora zadržati opciju privatnog profila koji može koristiti umjesto službenog profila povezanog s poslodavcem.

4. Elektroničko praćenje zaposlenika

Praćenje elektroničkih, službenih komunikacija na radnom mjestu (npr. telefon, internet pregledavanje, e-pošta, *instant messaging*, itd.) smatra se glavnom prijetnjom za privatnost zaposlenika, no nije zabranjeno.

Primjer - poslodavac namjerava implementirati inspekcijski alat za dešifriranje i pregled prometa osiguranog TLS protokolom (Transport Layer Security), s ciljem otkrivanja zlonamjernog prometa. Alat također može snimiti i analizirati cjelokupnu aktivnost zaposlenika na mreži poslodavca.

Korištenje šifriranih komunikacijskih protokola sve se više provodi kako bi se zaštitili mrežni tokovi osobnih podataka od malicioznih presretanja. Međutim, to također može predstavljati probleme jer šifriranje onemogućuje praćenje dolaznih i odlaznih podataka. TLS inspekcijska oprema dešifrira tok podataka, analizira sadržaj u sigurnosne svrhe i kasnije ponovno šifrira tok.

U ovom primjeru poslodavac se oslanja na legitimne interese - nužnost zaštite mreže i osobnih podataka zaposlenika i korisnika koji se nalaze unutar te mreže od neovlaštenog pristupa ili curenja podataka.

U mjeri u kojoj se neko prisluškivanje TLS prometa može kvalificirati kao strogo nužno, uređaj treba biti konfiguriran na način da se spriječi trajno bilježenje aktivnosti zaposlenika, na primjer blokiranjem sumnjivog dolaznog ili odlaznog prometa i preusmjeravanja korisnika na informacijski

portal na kojem on ili ona mogu tražiti pregled takve automatske odluke. Ako se neko opće bilježenje ipak smatra strogo neophodnim, uređaj se također može konfigurirati da ne pohranjuje zapisničke podatke, osim ako uređaj signalizira pojavu incidenta, uz minimalizaciju prikupljenih podataka.

Poslodavac bi trebao moći ponuditi alternativni pristup zaposlenicima, odnosno pristup podacima koji se ne nadziru. To se može učiniti nudeći besplatno WiFi ili samostalne uređaje (uz odgovarajuće mjere zaštite kako bi se osigurala tajnost komunikacija), gdje zaposlenici mogu ostvariti i svoje legitimno pravo korištenja radnih uređaja za neku privatnu upotrebu. O navedenom odlučuje poslodavac i primjenjuje se samo ako poslodavac dopusti korištenje službenih uređaja i u privatne svrhe.

U nekim slučajevima, praćenje zaposlenika često se događa u situacijama kada se od zaposlenika očekuje korištenje online aplikacije poslodavca, a koja obrađuje osobne podatke. Primjer toga je upotreba uredskih aplikacija temeljenih na tzv. *cloud-u* (npr. uređivači dokumenata, kalendari, itd.). Treba osigurati da zaposlenici mogu odrediti privatne prostore na koje poslodavac ne može pristupiti osim u izuzetnim okolnostima. Ovo je primjerice relevantno za kalendare, koji se često koriste i za privatne sastanke. Ako zaposlenik postavi opciju na "Privatno" ili bilježi to u samom nazivu, poslodavcima (i ostalim zaposlenicima) nije dopušteno da pregledaju sadržaj sastanka.

Primjer - poslodavac nudi svojim zaposlenicima kao dar uređaj za praćenje kretanja. Uređaji računaju broj koraka koje zaposlenici poduzimaju i registriraju njihova otkucaja srca i uzorke spavanja tijekom vremena. Dobiveni zdravstveni podaci trebaju biti dostupni samo zaposleniku, ali ne i poslodavcu. Svi podaci preneseni između zaposlenika (kao ispitanika) i uređaja/davatelja usluga (kao voditelj podataka) tiču se samo tih stranaka.

Budući da bi zdravstvene podatke moglo obrađivati i društvo koja je proizvelo uređaje ili koje nudi uslugu poslodavcima, prilikom odabira uređaja ili usluge poslodavac treba procijeniti politiku zaštite proizvođača i/ili davatelja usluga kako bi se osigurao da ne rezultira nezakonitom obradom zdravstvenih podataka zaposlenika.

Nadalje, uobičajeno je da poslodavci mogu ponuditi zaposlenicima mogućnost rada na daljinu, npr. od kuće ili dok su na putu. Dok rad na daljinu može biti pozitivan, on također predstavlja prostor dodatnog rizika za poslodavca. Primjerice, zaposlenici koji imaju vanjski pristup infrastrukturi poslodavca nisu vezani fizičkim sigurnosnim mjerama koje mogu postojati u prostorijama poslodavca. Jasno rečeno: bez provođenja odgovarajućih tehničkih mjera povećava se opasnost od neovlaštenog pristupa i može dovesti do gubitka ili uništenja informacija, uključujući osobne podatke zaposlenika ili korisnika, koje poslodavac može imati.

Da bi se ublažio rizik, poslodavci uglavnom smatraju da postoji opravdanje za implementaciju softverskih paketa koji imaju sposobnost, primjerice, prijaviti upotrebe tipkovnice i miša, prijaviti snimanje zaslona (slučajno ili u određenim vremenskim razmacima), bilježenja korištenih aplikacija (i koliko ih se upotrebljava), snimanje web kamerama te prikupljanje snimaka. Takve su tehnologije naširoko dostupne, uključujući i od trećih strana.

Ključ je rješavanje rizika na razmjeran i umjeren način, bez obzira na tehnologiju koja se predlaže, osobito ako su granice između poslovne i privatne uporabe fluidne.

Također, u kontekstu radnih odnosa, sve je prisutnija uporaba vlastitih uređaja, poput mobitela ili računala za obavljanje rada (tzv. *bring your own device* ili *BYOD*). Međutim, rizici privatnosti BYOD-a obično su povezani s tehnologijama koje prikupljaju identifikatore kao što su MAC adrese (*Media Acces Control*) ili u slučajevima kada poslodavac pristupa uređaju zaposlenika pod opravdanjem da izvršava sigurnosne provjere prisutnosti zlonamjernih programa (malware). S obzirom na potonje, postoje brojna komercijalna rješenja koja omogućuju skeniranje privatnih uređaja, no njihova upotreba može potencijalno pristupiti svim podacima na tom uređaju pa stoga moraju biti pažljivo vođeni. Npr. dijelovima uređaja za koje se pretpostavlja da se koriste samo u privatne svrhe (npr. folder koja pohranjuje fotografije sa ljetovanja) poslodavac ne bi trebao pristupiti. Praćenje lokacije i prometa takvih uređaja može se smatrati da služi legitimnom interesu za zaštitu osobnih podataka za koje je poslodavac odgovoran kao voditelj obrade podataka, no to može biti nezakonito kada se radi o osobnom uređaju zaposlenika, ako takvo praćenje također obuhvaća podatke koji se odnose na privatni i obiteljski život zaposlenika. Kako bi se spriječilo praćenje privatnih podataka, moraju postojati odgovarajuće mjere pomoću kojih bi se razlikovala privatna i poslovna upotreba uređaja.

Sustavi koji omogućuju poslodavcima da kontroliraju tko može ući u njihove prostorije, također mogu omogućiti praćenje aktivnosti zaposlenika. Iako takvi sustavi postoje već dugi niz godina, nove tehnologije namijenjene za praćenje vremena, ulazak i izlazak zaposlenika sve se šire primjenjuju, uključujući i one koji prate biometrijske podatke.

Primjer - Poslodavac ima posebnu prostoriju u kojoj su pohranjeni poslovni podaci, osobni podaci o zaposlenicima i osobni podaci koji se odnose na kupce putem *webshop*a. Kako bi se udovoljilo pravnim obvezama osiguranja podataka od neovlaštenog pristupa, poslodavac je instalirao sustav kontrole pristupa koji bilježi ulaz i izlaz zaposlenika koji imaju odgovarajuće dopuštenje za ulazak u prostoriju. Ako nestane bilo kakva oprema ili ako bilo koji podatak podliježe neovlaštenom pristupu, gubitku ili krađi, evidencije koje vodi poslodavac omogućuju im da utvrde tko je imao pristup prostoriji u to vrijeme. S obzirom na to da je obrada nužna i ne nadmašuje pravo na privatnost zaposlenika, ona kao pokriće ima legitiman interes, ako su zaposlenici na odgovarajući način obaviješteni o postupku obrade. Međutim, kontinuirano praćenje učestalosti i točnog vremena ulaska i izlaska zaposlenika ne može se opravdati ako se ti podaci koriste i za drugu svrhu, kao što je ocjenjivanje rada zaposlenika.

S druge strane, u skladu s mogućnostima koje nam pruža video analitika, poslodavac može nadzirati izraze lica automatskim sredstvima, prepoznati odstupanja od unaprijed definiranih uzoraka kretanja (npr. tvornički prostor) i još mnogo toga. To bi bilo neproporcionalno pravima i slobodama zaposlenika, a time i nezakonito. Obrada također vjerojatno uključuje profiliranje i, eventualno, automatizirano odlučivanje. Stoga se poslodavci trebaju suzdržati od upotrebe tehnologija prepoznavanja lica.

Poslodavac može biti obvezan instalirati tehnologiju praćenja u vozilima kako bi pokazao sukladnost s ostalim zakonskim obvezama, npr. kako bi se osigurala sigurnost zaposlenika koji

upravljaju tim vozilima. Poslodavac također može imati legitiman interes da locira vozila u bilo koje vrijeme. Čak i ako bi poslodavci imali legitimni interes za postizanje tih ciljeva, prvo treba procijeniti je li obrada u te svrhe potrebna i je li u skladu s načelima proporcionalnosti i supsidijarnosti. Kada je dopuštena i privatna uporaba službenog vozila, najvažnija mjera koju poslodavac može poduzeti kako bi osiguralo poštivanje ovih načela jest ponuda *opt-out*-a: u principu, zaposlenik bi trebao imati mogućnost privremeno isključiti opciju praćenja lokacije kada posebne okolnosti opravdaju to isključivanje, kao što je, primjerice, posjet liječniku. Na taj način, zaposlenik može na vlastitu inicijativu zaštititi određene podatke kao privatne. Poslodavac mora osigurati da se prikupljeni podaci ne koriste za neovlaštenu daljnju obradu, kao što je praćenje i evaluacija zaposlenika.

Poslodavac također mora jasno obavijestiti zaposlenike o tome da su uređaji za praćenje instalirani u vozilima poslodavca kojima se služe te da se njihovi pokreti bilježe tijekom korištenja tog vozila (te da se, ovisno o uključenoj tehnologiji, njihovo ponašanje u vožnji također može snimiti). Poželjno je da takve informacije budu jasno vidljive u svakom vozilu, u vidokrugu vozača.

Važno je za napomenuti da uređaji za praćenje vozila nisu uređaji za praćenje osoblja. Njihova je funkcija pratiti vozilo ili pratiti mjesto vozila na kojima su ugrađeni. Poslodavci ih ne bi trebali smatrati uređajima kojima bi se pratilo ponašanje ili gdje se nalaze vozači ili drugi zaposlenici, primjerice slanje upozorenja u odnosu na brzinu vozila.

Primjer - transportna tvrtka oprema sva vozila s video kamerom unutar kabine koja snima zvuk i video. Svrha obrade tih podataka je poboljšati vještine vožnje zaposlenika. Kamere su konfigurirane da zadrže snimke kad god se dogode incidenti poput naglog kočenja ili nagle promjene smjera. Tvrtka smatra da ima zakonsku osnovu za obradu, odnosno da je legitiman interes zaštita sigurnosti zaposlenika i sigurnosti drugih vozača. Međutim, legitimni interes tvrtke da prati vozače ne prevladava nad pravima tih vozača na zaštitu njihovih osobnih podataka. Neprestano praćenje zaposlenika s takvim kamerama predstavlja ozbiljno miješanje u njihovo pravo na privatnost. Postoje i druge metode (npr. ugradnja opreme koja sprečava uporabu mobilnih telefona) i drugi sigurnosni sustavi kao što su napredni sustav za hitne kočnice ili sustav za upozorenje kod nenamjernog napuštanja prometne trake, a koji se mogu koristiti za sprečavanje nesreća te koji mogu biti prikladniji. Nadalje, takav videozapis ima veliku vjerojatnost da će rezultirati obradom osobnih podataka trećih strana (poput pješaka), a za takvu obradu legitiman interes tvrtke nije dovoljan da opravda obradu.

Sve je češće da tvrtke prenose svoje podatke o zaposlenicima svojim korisnicima u svrhu osiguranja pouzdane usluge. Ti podaci mogu biti prilično prekomjerni, ovisno o opsegu pruženih usluga (kada je, primjerice, uključena fotografija zaposlenika). Međutim, zaposlenici nisu u stanju, s obzirom na neravnotežu moći, dati dobrovoljni pristanak na obradu njihovih osobnih podataka od strane svog poslodavca, a ako obrada podataka nije proporcionalna, poslodavac nema pravni temelj.

Primjer - trgovačko društvo koje se bavi dostavom pošiljaka šalje svojim korisnicima e-poštu s imenom i lokacijom dostavljača). Društvo je također namjeravalo pružiti isporučitelju fotografiju s putovnice zaposlenika. Poslodavac je pretpostavio da će u svom legitimnom interesu imati pravni temelj za obradu, omogućujući korisniku da provjeri je li isporučitelj doista prava osoba. Međutim,

nije potrebno navesti ime i fotografiju isporučitelja korisnicima. Budući da nema druge legitimne osnove za ovu obradu, društvo ne smije pružiti te osobne podatke korisnicima.

5. Prijenos podataka u treće zemlje

Poslodavci sve više koriste aplikacije i usluge temeljene na *cloud*-u, poput onih dizajniranih za rukovanje podacima o ljudskim resursima i internetske aplikacije. Korištenje većine tih aplikacija rezultirat će međunarodnim prijenosom podataka zaposlenika. Prijenos osobnih podataka u treću zemlju izvan EU može se odvijati samo ako ta zemlja osigura odgovarajuću razinu zaštite. To utvrđuje Komisija kada donosi odluku o primjerenosti ili ako potpada pod odgovarajuće zaštitne mjere. Međutim, ako ne postoji odluka o primjerenosti ili odgovarajuće zaštitne mjere, što uključuje obvezujuća korporativna pravila, prijenos podataka u treću zemlju ili međunarodnu organizaciju ostvaruje se samo pod jednim od sljedećih uvjeta:

- ako je zaposlenik izričito pristao nakon što je bio obaviješten o svim mogućim rizicima takvog prijenosa za zaposlenika zbog nepostojanja odluke o primjerenosti i odgovarajućih zaštitnih mjera,
- ako je prijenos nužan za izvršavanje ugovora između poslodavca i zaposlenika,
- ako je prijenos nužan radi sklapanje ili izvršavanje ugovora sklopljenog u interesu zaposlenika između poslodavca i druge fizičke ili pravne osobe,
- ako je prijenos nužan iz važnih razloga javnog interesa,
- ako je prijenos nužan za postavljanje, ostvarivanje ili obranu pravnih zahtjeva,
- ako je prijenos nužan za zaštitu životno važnih interesa zaposlenik, ako zaposlenik fizički ili pravno ne može dati privolu,
- ako se prijenos obavlja iz registra koji služi pružanju informacija javnosti, odnosno koji je otvoren na uvid javnosti ili bilo kojoj osobi koja može dokazati neki opravdani interes, ali samo u mjeri u kojoj su ispunjeni uvjeti propisani u pravu Unije ili pravu državu članice za uvid u tom posebnom slučaju.

6. Vrijeme čuvanja

Općenito je pravilo da se podaci čuvaju onoliko koliko je to potrebno, u skladu sa svrhama obrade. Iako opseg osobnih podataka određenog zaposlenika normalno završava na kraju radnog odnosa, obrada njegovih osobnih podataka od strane bivšeg poslodavca može se nastaviti. Poslodavci obično vode evidenciju o radnom odnosu u određenom vremenskom razdoblju, u mnogim slučajevima radi poštivanja zakonske obveze čuvanja dokumentacije iz radnog odnosa.

Svi rokovi koji se odnose na dokumentaciju zaposlenika, općenito radne odnose, propisani su Pravilima za upravljanja dokumentarnim gradivom Hrvatske zaklade za znanost (KLASA: 110-02/24-01/01; URBROJ: 1-24-3) i možete ih saznati kontaktirajući službenika za zaštitu podataka.

7. Zaključak

Konačno, prilikom obrade osobnih podataka zaposlenika, poslodavci trebaju imati na umu da:

- se poštuju temeljna načela zaštita podataka, bez obzira na tehnologiju koja se koristi;
- temeljna načela zaštite osobnih podataka moraju biti primijenjena kod svih oblika komunikacije;
- nije vjerojatno da će privola biti pravna osnova za obradu osobnih podataka, osim ako zaposlenici mogu odbiti davanje privole bez štetnih posljedica;
- se ponekad mogu pozvati na izvršavanje ugovora i legitimni interes kao pravne osnove za obradu osobnih podataka, pod uvjetom da je obrada strogo neophodna u legitimnoj svrsi i da je u skladu s načelima proporcionalnosti i supsidijarnosti;
- bi zaposlenici trebali dobiti učinkovite informacije o praćenju koji se odvija;
- bi se svaki međunarodni prijenos podataka zaposlenika trebao odvijati samo ako je osigurana odgovarajuća razina zaštite.

Hrvatska zaklada za znanost kao poslodavac pridržava se svih načela i navedenih smjernica.

OBAVIJEST O OBRADI OSOBNIH PODATAKA

Voditelj obrade je Hrvatska zaklada za znanost, Ilica 24, 10000 Zagreb (dalje u tekstu: „Zaklada“).

Imamo službenika za zaštitu osobnih podataka, a možete ga kontaktirati putem e-mail-a: alen@hrzz.hr ili na našoj adresi na način da pošaljete dopis sa naznakom ˝Za službenika za zaštitu osobnih podataka˝.

Vaše osobne podatke obrađujemo temeljem privole. Ukoliko pristajete da Vas kontaktiramo nakon završenog natječaja, za potrebe popunjavanja otvorenih radnih mjesta u budućnosti, privolu dajete označavanjem kvačice u praznom polju i upisivanjem Vašeg imena i prezimena, broja mobitela ili e-maila.

Prikupljeni podaci i dokumentacija obrađivat će se u svrhu provedbe selekcijskog postupka za odabir kandidata koji najbolje odgovara traženom radnom mjestu u budućnosti.

Osobne podatke ćemo obrađivati do povlačenja Vaše privole. Ukoliko ne povučete privolu Vaše osobne podatke ćemo brisati nakon proteka dvije godine od kada ste nam dali privolu da Vaše osobne podatke koristimo za potrebe popunjavanja otvorenih radnih mjesta u budućnosti. Ukoliko je pokrenut sudski, upravni ili izvansudski postupak, osobni se podaci mogu pohraniti do kraja takvog postupka, uključujući i moguće razdoblje za izjavljivanje pravnih lijekova.

Niste obvezni dati svoju privolu za korištenja Vaših osobnih podataka u gore navedene svrhe. Ukoliko ne želite dati svoju privolu, nećemo obrađivati Vaše osobne podatke za potrebe popunjavanja otvorenih radnih mjesta u budućnosti. Odbijanjem davanja privole nećete snositi negativne posljedice.

Vaši osobni podaci obrađivat će se u gore navedene svrhe, osim ako je to neophodno za poštivanje zakonskih obveza (npr. za dostavljanje podataka sudovima ili organima kaznenog progona), ako ste pristali na odgovarajuću obradu ili ako je obrada na drugi način zakonita prema obvezujućim propisima. Ukoliko se podaci obrađuju u drugu svrhu, prije obrade pružit ćemo Vam informacije o toj drugoj svrsi te sve druge relevantne informacije.

Imate pravo u bilo kojem trenutku povući privolu. O povlačenju privole potrebno je obavijestiti voditelja obrade putem kontakt podataka navedenih na početku ove Izjave. Takvo povlačenje neće utjecati na zakonitost obrade na temelju privole prije njezina povlačenja.

Pristup vašim osobnim podacima mogu imati konzultanti s kojima surađujemo na održavanju našeg poslovnog sustava. Moguće je otkrivanje Vaših osobnih podataka ovlaštenoj trećoj strani ako to zahtijevaju ili dopuštaju obvezujući propisi (npr. državna tijela, sudovi, vanjski savjetnici i druge treće osobe koje se smatraju javnim tijelima).

Vaši podaci ne prenose se u treće zemlje niti u međunarodne organizacije.

Vaša prava su slijedeća: pravo na pristup, pravo na ispravak, pravo na brisanje, pravo na ograničenje obrade, pravo na prigovor, pravo na prenosivost podataka. Ako smatrate da su Vaša prava povrijeđena imate pravo podnijeti prigovor Agenciji za zaštitu osobnih podataka.

Ukoliko želite saznati više ili želite koristiti jedan ili više od gore navedenih prava, slobodno kontaktirajte službenika za zaštitu podataka na kontakt podatke navedene na početku ove Obavijesti o obradi osobnih podataka.

PRIVOLA

Ovime ja,

_____

_____ (*ime i prezime, broj telefona ili e-mail*)

dajem pristanak Hrvatskoj zakladi za znanost za obradu osobnih podataka uključenih u moj životopis i drugu priloženu dokumentaciju u svrhu budućih selekcijskih procesa u periodu od dvije godine od datuma potpisa ove privole.

U _____(*mjesto*),_____(*datum*)

_____

(potpis kandidata)