ZAŠTITA OBRADE OSOBNIH PODATAKA

ZAŠTITA OBRADE OSOBNIH PODATAKA

OPĆE ODREDBE

Osobne podatke fizičkih osoba društvo FIMA Invest d.o.o., Zagreb, Gradišćanska ulica 34, u svojstvu voditelja obrade osobnih podataka (dalje: Društvo) obrađuje u skladu s odredbama 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, o stavljanju izvan snage Direktive 95/46/EZ (dalje: Uredba) te sukladno odredbama Zakona o provedbi Opće uredbe o zaštiti podataka (NN 42/2018).

DEFINICIJE

1. „**Osobni podaci**" su svi podaci 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;
2. **„Obrada"** predstavlja 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;
3. **„Voditelj obrade"** je fizička ili pravna osoba koja obrađuje osobne podatke ispitanika;
4. **„Izvršitelj obrade"** je fizička ili pravna osoba koja obrađuje osobne podatke u ime voditelja obrade;
5. **„Sustav pohrane"** predstavlja svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi;
6. **„IT-služba"** je jedinstvena kontaktna točka za sve IT potrebe uključujući traženje rješenja za IT problem, podnošenje ili prosljeđivanje na višu razinu zahtjeva za podršku, kontaktiranje IT podrške;
7. **„Glavna služba"** je jedinstvena kontaktna točka za svekoliku obradu osobnih podataka unutar Društva, a vodi ga osoba nadležna za GDPR koja odgovara Upravi Društva;
8. **„Dokument"** je bilo koja isprava koja sadrži osobne podatke koji mogu biti u elektroničnom i materijalnom obliku, čuvani na mediju ili na informacijsko-komunikacijskoj opremi te korišteni u obradi podataka, dostavljeni putem e-maila i/ili preneseni putem elektroničke komunikacijske mreže;
9. **„Identifikacija"** je bilo koja radnja informacijskog sustava vezana uz identifikaciju ovlaštenih osoba;
10. **„Informacijska infrastruktura"** je cjelokupna informacijsko-komunikacijska mreža Društva u okviru koje se informacije prikupljaju, obrađuju i pohranjuju;
11. **„Informacijski sustav"** je svaki sustav koji se koristi u obradi osobnih podataka kako bi podaci bili lakše dostupni i primjenjivi za svakoga tko ima pravo i potrebu da ih kao takve koristi;
12. **„Incident"** je svaka nepravilnost koja utječe ili bi potencijalno mogla utjecati na tajnost i zaštitu osobnih podataka;
13. **„Kontrola pristupa"** je svaka radnja za dodjeljivanje pristupa osobnim podacima ili informacijsko-komunikacijskoj opremi ovlaštenoj osobi u svrhu kontrole;

14. **„Ispitanik“** je svaka fizička osoba na koju se obrađeni podaci odnose;
15. **„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;
16. **„Nadležna osoba za GDPR“** je osoba koja je zaposlena ili angažirana u Društvu, a koja jedina ima ovlašteni pristup dokumentima i informacijsko - komunikacijskom sustavu u službi osobnih podataka;
17. „**Treća strana**” predstavlja fizičku ili pravnu osobu, tijelo javne vlasti, agenciju 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;
18. **„Treća zemlja“** je svaka zemlja koja nije članica Europske unije ili članica Europskog gospodarskog prostora;
19. **„Lozinka“** je povjerljiva informacija koja se sastoji od broja znakova koji se koriste za provjeru ovlaštenih osoba;
20. **„Medij“** je svaki materijalni uređaj u informacijskom sustavu koji se koristi u obradi osobnih podataka i na koji se podaci mogu pohraniti ili s kojeg se podaci mogu preuzeti;
21. **„Kontrola“** je svaka radnja vezana uz provjeru ovlaštene osobe informacijskog sustava;
22. **„Sigurnosna kopija“** je svaka kopija osobnih podataka koja se nalazi u elektroničkom dokumentu koji je pohranjen na mediju u svrhu njegova preuzimanja;
23. **„Korisnik“** je svaka osoba koja ima pristup obradi osobnih podataka unutar subjekta.

PRAVA ISPITANIKA

Ispitanici ostvaruju sljedeća prava:

1. Pravo na pristup (članak 15. Uredbe)

Ispitanik od Društva ima pravo dobiti informaciju o tome obrađuju li se osobni podaci koji se odnose na njega, te ako se obrađuju ima pravo na pristup osobnim podacima i sljedećem informacijama: svrsi obrade, kategorijama osobnih podataka o kojima je riječ, primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, osobito primateljima u trećim zemljama ili međunarodnim organizacijama; ako je to moguće, predviđenom razdoblju u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterijima korištenima za utvrđivanje tog razdoblja; postojanju prava da se od voditelja obrade zatraži ispravak ili brisanje osobnih podataka ili ograničavanje obrade osobnih podataka koji se odnose na ispitanika ili prava na prigovor na takvu obradu, pravu na podnošenje pritužbe nadzornom tijelu; ako se osobni podaci ne prikupljaju od ispitanika, svakoj dostupnoj informaciji o njihovu izvoru.

2. Pravo na ispravak (članak 16. Uredbe)

U slučaju netočnih podataka ispitanik ima pravo od Društva zatražiti odgovarajući ispravak osobnih podataka koji se na njega odnose. U slučaju nepotpunosti osobnih podataka ispitanik ima pravo dopuniti iste, između ostaloga i davanjem dodatne izjave. Društvo je dužno ispitaniku priopćiti svaki ispravak osobnih podataka osim ako se to pokaže nemogućim ili zahtijeva nerazmjeran napor.

3. Pravo na brisanje (članak 17. Uredbe)

Ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja te voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako je ispunjen jedan od sljedećih uvjeta: osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni; ispitanik povuče privolu na kojoj se obrada temelji i ako ne postoji druga pravna osnova za obradu; ispitanik uloži prigovor na te ne postoje jači legitimni razlozi za obradu, ili ispitanik uloži prigovor na obradu u skladu s člankom 21. stavkom 2.; osobni podaci nezakonito su obrađeni; osobni podaci moraju se brisati radi poštovanja pravne obveze iz prava Unije ili prava države članice kojem podliježe voditelj obrade;Ovim putem skrećemo pažnju da pravo na brisanje nije apsolutno pravo, te Uredba poznaje slučajeve kada Društvo neće biti u obvezi brisati Vaše osobne podatke. Tako, u slučaju ostvarivanja prava na slobodu izražavanja i informiranja;radi poštovanja pravne obveze kojom se zahtijeva obrada u pravu Unije ili pravu države članice kojem podliježe voditelj obrade ili za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;zbog javnog interesa u području javnog zdravlja u skladu s člankom 9. stavkom 2. točkama (h) i (i) kao i člankom 9. stavkom 3. Uredbe.;u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s člankom 89. stavkom 1. u mjeri u kojoj je vjerojatno da se pravom iz stavka 1. može onemogućiti ili ozbiljno ugroziti postizanje ciljeva te obrade; radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

4. Pravo na ograničenje obrade (članak 18. Uredbe)

Na zahtjev ispitanika, Društvo će ograničiti obradu osobnih podataka pod sljedećim uvjetima:u slučaju da ispitanik osporava točnost podataka na razdoblje kojim se Društvu omogućuje provjera točnosti osobnih podataka,osobni podaci Društvu više nisu potrebni, ali ih ispitanik traži radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva, ispitanik je uložio prigovor na obradu podataka na osnovi legitimnih interesa te se čeka odgovor na taj prigovor. Ako ispitanik uspije ishoditi ograničenje obrade, Društvo ga je dužno obavijestiti o postavljanju i o ukidanju tog ograničenja.

5. Pravo na prenosivost podataka (članak 20. Uredbe)

Na zahtjev ispitanika Društvo može u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu dati osobne podatke radi prijenosa drugom voditelju obrade, pod uvjetom da se obrada podataka temelji na privoli ili je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzela radnja na zahtjev ispitanika prije sklapanja ugovora te ako se obrada provodi automatiziranim putem. Prijenos se može provesti direktno, ako je to tehnički izvedivo.

6. Pravo na prigovor (članak 21. Uredbe)

U slučaju da Društvo obrađuje osobne podatke ispitanika s osnove postojanja legitimnog interesa Društva ili je takva obrada nužna za izvršavanje zadaće od javnog interesa, ispitanik može podnijeti prigovor Društvu na obradu osobnih podataka u svakom trenutku.

Način ostvarivanja prava:

- Porukom elektroničke pošte na adresu elektroničke pošte: info@fimainvest.com
- Osobnim dolaskom u sjedište Društva na adresi: Gradišćanska ulica 34, Zagreb
- Dostavom pisanog zahtjeva na prethodno navedenu adresu sjedišta Društva.

7. Pravo na pritužbu nadzornom tijelu

Svaki ispitanik ima pravo uložiti pritužbu na obradu osobnih podataka koju provodi Društvo.
Pritužba se podnosi nadzornom tijelu za zaštitu osobnih podataka. Nadzorno tijelo na području Republike Hrvatske je Agencija za zaštitu osobnih podataka (dalje: Agencija) sa sjedištem u Zagrebu.
Preporučujemo da prije podnošenja pritužbe Agenciji provjerite na njenim mrežnim stranicama koji je sadržaj potreban za dostavu pritužbe, odnosno na koji se način i kome pritužba podnosi. Društvo ne snosi nikakvu pravnu odgovornost u slučaju da ispitanik uputi pritužbu koja ne sadržava sve što je potrebno da bi Agencija o njoj mogla odlučivati, odnosno da pritužbu uloži na pogrešnu adresu.

OBRADA OSOBNIH PODATAKA

Zaštita obrade osobnih podataka primjenjuje se na:

- djelomično ili u potpunosti automatiziranu obradu osobnih podataka i
- ostalu ručnu obradu osobnih podataka kao dio stalnog prikupljanja osobnih podataka ili kojoj je namjena postati dio takvog prikupljanja osobnih podataka.

TEHNIČKE I ORGANIZACIJSKE MJERE

Društvo primjenjuje tehničke i organizacijske mjere koje pružaju sigurnost i zaštitu obrade osobnih podataka u skladu s prirodom obrađenih podataka i potencijalnim rizicima za vrijeme obrade.

TEHNIČKE MJERE

Prilikom automatske obrade podataka poduzimaju se sljedeće tehničke mjere za zaštitu obrade osobnih podataka:
1. Svaka osoba zaposlena/angažirana od strane Društva ima na raspolaganju odvojeno osobno (prijenosno) računalo za izvršavanja radnih zadataka i pristup odvojenoj radnoj stanici. Radna stanica je radni prostor namijenjen za dugotrajni uredski posao koji izvršava jedna osoba, s vodoravnom radnom površinom, podesivom radnom stolicom te pristupom električnoj energiji, podacima i telefonu, a nalazi se u prostorima općih uredskih radnih jedinica. Radna jedinica može biti dodijeljena ili mobilna.
Dodijeljena radna jedinica je radna jedinica u otvorenim prostorijama koja je dodijeljena jednom radniku. Mobilna radna jedinica je radna jedinica u otvorenim prostorijama koja je dostupna svima kao jedinica koja se ne može rezervirati te funkcionira na principu „tko prvi dođe, prvi koristi“;

2. Jedinstveno korisničko ime i lozinka zahtijevaju pristupnu lozinku od 5 (pet) znakova za prijavu u operacijski sustav Windows te e-mail račun. Prijenosna računala imaju isto korisničko ime i lozinku za Windows i za e-mail. Osim zadane duljine pristupna lozinka mora sadržavati 3 od 4 vrste znakova: velika slova, mala slova, simbole i brojeve. Jedinstvena lozinka stvorena od strane svake zasebne ovlaštene

osobe na računalu, koje se koristi za radne zadatke, a koje računalo je u vlasništvu Društva, pod pretpostavkom da svaka osoba zaposlena/angažirana od strane Društva ima različitu lozinku za računalo koje je u vlasništvu Društva, samo za računalo dano na raspolaganje od strane Društva za izvršavanje radnih zadataka, pod pretpostavkom da:
- lozinka dozvoljava pristup osobi zaposlenoj od strane Društva samo dijelovima sustava koji su joj potrebni za izvršavanje radnih zadataka;
- lozinka je tajna te se ne smije davati trećim osobama izvan Društva ni pod kojim uvjetima, niti se smije davati međusobno između osoba zaposlenih/angažiranih od strane društva;
- nijedna osoba zaposlena/angažirana od strane Društva ne smije koristiti računalo druge osobe zaposlene/angažirane od strane Društva i koje je dano na raspolaganje od strane Društva za izvršavanje radnih zadataka; i
- Društvo mora periodično mijenjati pristupne lozinke. Svi računi za interakciju s korisnicima moraju imati postavljen rok trajanja od najviše 3 (tri) mjeseca te ih se mora smjesta promijeniti ako se sumnja u ugroženost.
Mora postojati postupak za izmjenu lozinki računa za usluge te se ni u kojem slučaju ne smije premašiti trajanje od najviše 3 (tri) mjeseca. Lozinke računa za usluge se moraju smjesta promijeniti ako se sumnja u ugroženost;

3. Automatska odjava iz sustava na svakom zasebnom osobnom računalu nakon isteka određenog perioda neaktivnosti od 15 (petnaest) minuta te je za ponovnu aktivaciju sustava na osobnom računalu potrebno ponovno unijeti lozinku;

4. Ako se korisnik ne uspije prijaviti (unosom nevažećeg korisničkog imena ili lozinke) u sustav nakon 3 (tri) pokušaja, isti će se morati javiti Ovlaštenoj osobi za GDPR koja će zatražiti podršku za izmjenu lozinke od „IT-službe“;

5. Učinkovit i siguran antivirusni i protušpijunski program instaliran na svakom prijenosnom računalu u Društvu, redovito ažuriran putem internetske veze s najnovijim zaštitnim definicijama u svrhu zaštite od nepoznatih i nepredvidivih prijetnji od novih virusa itd.; IT služba zahtijeva da svi sustavi imaju instaliran odobreni antivirusni softverski paket s najnovijom ažuriranom verzijom. Društvo je odobrilo antivirusni softver po operativnom sustavu. Radne stanice i osobna računala s Windowsom (32 i 64 bitna verzija) koriste Windows Defender;

6. Bilježenje i čuvanje odgovarajuće dokumentacije za softver za obradu osobnih podataka i svih promjena;

7. Instalacija usmjerivača između informacijskog sustava i interneta kao zaštitna mjera protiv neovlaštenog i/ili zlonamjernog pokušaja ulaska i/ili proboja u sustav;

8. Ako postoji potreba za korištenjem računala izvan prostorija Društva (rad od kuće, sastanak, itd.), tada se primjenjuju prikladne sigurnosne mjere za danu situaciju (VPN i enkripcija);

9. Spajanje opreme u sobi za informatičku tehnologiju (IT) na energetsku mrežu putem uređaja za neprekidno napajanje (UPS);

10. Licencirani programi – Microsoft Office 365 (uključujući sve programe potrebne za rad na računalu za izvršavanje zadataka) za sva računala koja se koriste u potrebe Društva i koja su u vlasništvu istog, uključujući antivirusne i protušpijunske sustave. Svi programi potrebni za rad su instalirale osobe koje su zaposlene/angažirane od strane Društva uz mogućnost pomoći od strane „IT-službe“. Samovoljna instalacija programa, aplikacija i slično od strane osoba koje je zaposlilo/angažiralo Društvo, a da instalaciju istih nije odobrila Uprava društva, je zabranjena;

11. Osobe zaposlene/angažirane od strane Društva imaju pravo osigurati održavanje (ažuriranje softvera, 1 razina provjere) njihovih osobnih računala s mogućnošću pristupa od strane „IT-službe“ za održavanje i popravke velikih problema, ali cijeli sustav računala je vlasništvo Društva. Svaki popravak odnosno održavanje osobnih računala se bilježi te se izvješće dostavlja Upravi Društva;

12. Putem web stranice Društva ne prikupljaju se osobni podaci.

DODATNE TEHNIČKE MJERE

Dodatne tehničke i organizacijske mjere za vrijeme obrade osobnih podataka omogućuju:
1. Klasifikaciju osobnih podataka na osnovnu, srednju i visoku razinu tajnosti, kao i određivanje pristupa grupi podataka i načina ophođenja istom;
2. Prepoznavanje svakog zasebnog pristupa informacijskom sustavu putem verifikacije i autorizacije svake ovlaštene osobe;
3. Evidenciju svakog ovlaštenog pristupa koji sadrži sljedeće podatke:
   a) Ime i prezime ovlaštenog osoblja;
   b) Poslovnu jedinicu za pristup informacijskom sustavu;
   c) Datum i vrijeme pristupa;
   d) Osobne podatke kojima se pristupilo;
   e) Vrstu pristupa s radnjama poduzetima za vrijeme obrade podataka;
   f) Dnevnik pristupa sa svim pristupima;
   g) Dnevnik sa svim neovlaštenim pristupima i registracijom automatskih odbijanja informacijskog sustava;
4. Evidenciju s podacima za identifikaciju informacijskog sustava koji je pokušao izvršiti vanjski pristup operacijskim funkcijama ili osobnim podacima bez potrebne razine ovlasti;
5. Ograničen pristup za sve ovlaštene osobe samo onim bazama podataka ili osobnim podacima koji su potrebni za izvršavanje poslovnih zadataka;
6. Enkripciju podataka koji se mogu prenijeti putem telekomunikacijske mreže (internetska mreža, bežične mreže) ili bilo koja druga vrsta veze s odgovarajućim softverom i tehničkim mjerama.

SIGURNOSNE KOPIJE

Sigurnosne su kopije obvezne na kraju svakog radnog dana i radnog tjedna te se kreiraju putem automatiziranog sustava sigurnosnih kopija osobnih računala. Dohvat podataka sa sigurnosnih kopija vrši se od strane ovlaštene osobe u „IT-Službi“.

Osnovne kopije e-mail korespondencije koje sadrže osobne podatke brišu se unazad šest mjeseci, a aktualna e-mail korespondencija obrađuje se u skladu sa računalnim standardima sigurnosti obrade osobnih podataka.

Sigurnosne se kopije čuvaju na sigurnoj, neobjavljenoj lokaciji u Društvu. Točne lokacije se ne objavljuju i poznate su samo imenovanoj odgovornoj osobi za GDPR u društvu.

PRIJENOS PODATAKA

Prijenos osobnih podataka vrši se na sljedeći način:

1. Kod materijalnog oblika (tiskana kopija – papir) uvijek se mora pripaziti da dokumenti koji sadrže osobne podatke nisu vidljivi trećim osobama te ih se dostavlja samo ovlaštenim osobama, posebice kada se isti nose izvan prostorija Društva te se na taj način osigurava da se takvi podaci ne otkrivaju neovlaštenim osobama;
2. Kod prijenosa osobnih podataka u elektroničkom obliku putem medija za prijenos podataka, podaci se štite, ovisno o obliku podataka, lozinkom i enkripcijom u skladu s uputama koje se nalaze u politikama kriptografije i standardu korištenja kriptografije Društva te standardima koji su navedeni u sigurnosnim specifikacijama prijenosa fizičkim medijima.
3. Za vrijeme prijenosa osobnih podataka izvan teritorija Europske unije, tj. u treće zemlje, obraća se pozornost na sljedeće:
   - opseg i sadržaj podataka moraju biti u skladu s ciljem i svrhom njihova prijenosa, tj. šalju se samo najpotrebniji podaci. To se osobito odnosi na to da OIB bude slabije dostupan i vidljiv, kao i ostali osjetljivi podaci;
   - provjera postoji li potreba za dobivanjem privole ispitanika te postoji li već takva privola prije slanja podataka;
   - provjera posjeduje li osoba koja treba primiti podatke odgovarajuće ovlaštenje za pristup prenesenim podacima;
   - provjera postoji li potreba za davanjem mišljenja od strane Agencije za zaštitu osobnih podataka.

ORGANIZACIJSKE MJERE

Odgovorna osoba za GDPR poduzima organizacijske mjere za zaštitu automatske obrade osobnih podataka predstavlja ujedno Upravu Društva i ovlaštene osobe, a ista osigurava fizičku zaštitu radnih prostora i opreme te zaštitu informacijskog sustava u cijelosti, uključujući i prijenos podataka.

Uprava je odgovorna za koordinaciju i kontrolu postupaka i vođenje dokumentacije tehničkih i organizacijskih pravila te osobne evidencije obrade. Njemu/njoj će pomoći osoba odgovorna za IT odnosno IT-služba.

OSOBNA EVIDENCIJA OBRADE

Svaki radnik kao nadležna osoba na radnom mjestu vodi osobnu evidenciju obrade u obliku Word-datoteke u koju evidenciju upisuje:
- koji se podaci prikupljaju i u koju svrhu;

- gdje se čuvaju prikupljeni podaci;
- tko još ima pristup prikupljenim podacima;
- postoji li za iste privola;
- koliko dugo se čuvaju prikupljeni podaci te
- kako se uništavaju prikupljeni podaci.

Za radna mjesta na kojima se ne provodi prikupljanje, obrada, čuvanje ili pohrana osobnih podataka, ne postoji obveza iz prethodnog stavka.

FIZIČKA DOKUMENTACIJA

Fizička dokumentacija osoba se čuva u sjedištu Društva u zasebnim mapama i registratorima zaštićenima u zasebnim ormarićima otpornima na vodu i vatru do kojih je pristup ograničen te se popis s brojevima registratora kao i imena svake osobe, a koji podliježe zaštiti osobnih podataka, čuva u elektroničkom obliku na računalnoj mreži Društva, a pristup istom je dozvoljen samo ovlaštenim osobama.

Dokumenti svih osoba u fizičkom obliku se čuvaju i ne uništavaju, a elektronički oblici istih su pohranjeni na računalu u zasebnoj zaštićenoj datoteci u Društvu. Uprava Društva je odgovorna za čuvanje dokumenata u razdoblju koje je propisano Zakonom o računovodstvu, Zakonu o obveznim odnosima ili drugim zakonskim propisima koji nalažu čuvanje osobnih podataka.

Prilikom sklapanja ugovora s fizičkim osobama potrebno je ishoditi njihovu izričitu suglasnost na prikupljanje, obradu i čuvanje osobnih podataka, pogotovo ako se navedeni ugovori prosljeđuju u svrhu obrade i čuvanja trećim osobama.

Pravila obrade, pohranjivanja (čuvanja) i pristupa podacima su zasebno uređeni procedurama u pojedinim osobnim evidencijama obrade osobnih podataka. Sve nadležne osobe su upoznate s istim, a svaka nadležna osoba dužna je voditi osobnu evidenciju obrade podataka na zasebnoj datoteci na osobnom računalu.

Razdoblje čuvanja dokumenata ispitanika osobnih podataka određuje se u skladu sa odgovarajućim zakonskim propisima vezano uz bilo koji oblik osobnih podataka.

Potrebno je koristiti rezače papira za uništavanje nepotrebnih papira, materijala i podataka nakon isteka roka čuvanja predmetne dokumentacije te na taj način spriječiti bacanje dokumenata izvan prostorija.

Dostava dokumenata koji su uručeni i/ili dostavljeni suradnicima Društva ili kojim drugim ispitanicima se izvršava zatvorenom kuvertom s točno navedenim imenom i prezimenom/titulom ispitanika kojemu se dostavlja kuverta, a primitak se potvrđuje potpisom.

Svi podaci navedeni u dokumentima izrađenim od strane Društva, a koji se dostavljaju nadležnom sudu, upravnom tijelu, ministarstvu i drugim institucijama ili drugim korisnicima izdaju se isključivo u skladu sa zakonom, legitimnim interesom ili po primitku izričite pisane privole ispitanika.

NEPOSREDNO KORIŠTENJE OSOBNIH PODATAKA U RADNIM PROCESIMA

Društvo će onemogućiti pristup radnim prostorima u Društvu trećim osobama koje nisu u pratnji radnika Društva ili bilo koji drugi kontakt (fizički ili vizualni) takvim osobama s osobnim podacima, datotekama i drugim dokumentima.

Izjava o tajnosti je izjava koju potpisuje radnik te se čuva u osobnom spisu radnika. Životopisi kandidata za postojeća ili buduća radna mjesta čuvaju se samo uz izričitu privolu ispitanika u zasebnoj datoteci među datotekama radnika Društva.

Društvo provodi neprekidno obavještavanje radnika za neposredne obveze i odgovornosti za zaštitu osobnih podataka.

ŠKOLOVANJE RADNIKA

Prije početka rada, radnici/osobe angažirane od strane Društva upoznat će se s obvezama čuvanja osobnih podataka prilikom obrade te s cjelokupnom dokumentacijom tehničkih i organizacijskih mjera te potpisuju izjavu kojom potvrđuju da prihvaćaju obveze i odgovornost vezane uz zaštitu osobnih podataka, a naznačena izjava je sastavni dio Ugovora o radu.
U ugovore o radu / ugovore o angažmanu za provođenje radova u Društvu uključene su obveze i odgovornosti za zaštitu osobnih podataka te svaki radnik mora pristupiti odgovarajućim uvodnim treninzima uz neke dodatne treninge, ovisno o njihovom poslu, kako bi se osigurali specifični uvjeti za zaštitu osobnih podataka.

Osobe koje su odgovorne za prikupljanje i obradu podataka pohađaju redovita školovanja radi aktualizacije njihovih saznanja o novijoj normativnoj aktivnosti zakonodavca i upravnih tijela, a stečena znanja prenose na ostale radnike unutar Društva.

MJERE PRILIKOM NEPOSREDNOG KONTAKTA SA ISPITANICIMA

Kada u izvršavanju ugovornih obveza Društvo prikuplja osobne podatke putem svojih djelatnika ili podizvođača u svojstvu izvršitelja obrade na način da od svake osobe zatraži osobne podatke koji su potrebni za izvršenje naloga.

Društvo će za vrijeme obrade osobnih podataka poduzeti sljedeće dodatne tehničke i organizacijske mjere:

1. Prije prikupljanja osobnih podataka, svaka će se osoba obavijestiti o:
- cilju
- načinu obrade osobnih podataka
- voditelju i izvršitelju
- pravilima privatnosti
- načinu i razdoblju čuvanja

- prijenosu podataka
- pravima i obvezama voditelja, izvršitelja i ispitanika te
- mogućnosti podnošenja pritužbe Agenciji za zaštitu osobnih podataka.

2. Svaka osoba koja neposredno prikuplja osobne podatke mora se ispitaniku predstaviti osobnim imenom i prezimenom.

3. Svaka osoba koja od ispitanika neposredno prikuplja osobne podatke mora voditi računa o opsegu osobnih podataka koje prikuplja, tj. da prikuplja samo onaj opseg osobnih podataka koji je nužan za ispunjenje svrhe u koju se osobni podaci prikupljaju (načelo razmjernosti), a sve kako se ne bi prikupljali osobni podaci u prekomjernom opsegu.

4. Na zahtjev ispitanika/građana, odnosno njihovih zakonskih zastupnika ili punomoćnika nadležna osoba dužna je najkasnije u roku od 30 (trideset) dana od podnošenja zahtjeva omogućiti ostvarivanje prava ispitanika/građana na uvid u njihove osobne podatke, odnosno dostaviti obavijesti, izvatke, potvrde i ispise u vezi osobnih podataka koji se obrađuju.

5. Svaki ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja, a o tome je Društvo dužno upoznati svakog ispitanika.

POVREDA OSOBNIH PODATAKA (INCIDENT)

U slučaju povrede osobnih podataka Uprava Društva bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izvješćuje Agenciju za zaštitu osobnih podataka ako je voditelj obrade i to 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.

U izvješćivanju Agencije u slučaju potrebe, mora se:

- opisati priroda incidenta, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj dotičnih evidencija osobnih podataka;
- navesti ime i kontaktne podatke kontaktne točke od koje se može dobiti još informacija;
- opisati vjerojatne posljedice incidenta;
- opisati mjere koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.

Uprava Društva dokumentira sve povrede osobnih podataka, uključujući činjenice vezane za povredu osobnih podataka, njezine posljedice i mjere poduzete za popravljanje štete. Ta će dokumentacija nadzornom tijelu omogućiti provjeru poštivanja procedura za prijavu povrede osobnih podataka.

OBAVJEŠTAVANJE ISPITANIKA O POVREDI OSOBNIH PODATAKA (INCIDENTU)

U slučaju povrede osobnih podataka koje bi mogao prouzročiti visok rizik za prava i slobode pojedinaca, osoba nadležna za GDPR bez nepotrebnog odgađanja obavještava ispitanika o povredi osobnih podataka.

Obavještavanjem ispitanika opisuje se priroda povrede osobnih podataka uporabom jasnog i jednostavnog jezika te ono sadržava barem informacije i mjere iz članka 34. GDPR-e.

NADZOR

Nadzor nad provedbom zakona sukladno Uredbi za zaštitu osobnih podataka i Zakonu o provedbi Opće uredbe o zaštiti podataka u Republici Hrvatskoj provodi Agencija za zaštitu osobnih podataka.

Društvo je dužno omogućiti Agenciji za zaštitu osobnih podataka pristup spisima i drugoj dokumentaciji te sredstvima obrade osobnih podataka.