



DRUŠTVO GRAĐEVINSKIH INŽENJERA ZAGREB

Berislavićeva 6, Zagreb, OIB: 08954544114

Tel./fax: 01 4872 498, e-mail: dgiz@zg.t-com.hr, www.dgiz.hr

PRAVILNIK O POLITICI ZAŠTITE OSOBNIH PODATAKA

DRUŠTVA GRAĐEVINSKIH INŽENJERA ZAGREB

Temeljem članka 18. Statuta Društva građevinskih inženjera Zagreb, Berislavićeva 6, Zagreb (u daljnjem tekstu: DGIZ) i Opće uredbe u zaštiti podataka (Uredba EU 2016/679), Predsjedništvo DGIZ-a na sjednici održanoj 8. svibnja 2018. godine donio je dokument

PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA

I. POJMOVNIK

Osobni podatak – podatci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi.

Ispitanik – jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podatci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca. U kontekstu DGIZ-a, ispitanik može biti član, bivši član, korisnik usluga, fizička osoba kojoj DGIZ nudi svoje proizvode ili usluge, zaposlenik, kandidat za zaposlenika ili zaposlenik partnera.

Obrada osobnih podataka – 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

Voditelj obrade – znači fizička ili pravna osoba, koja samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka. U kontekstu DGIZ-a, DGIZ je

Voditelj obrade. Predsjedništvo može donijeti odluku o imenovanju i fizičke osobe
Voditelja obrade, ukoliko se pokaže potreba za istim.

Izvršitelj obrade – znači fizička ili pravna osoba, koja obrađuje osobne podatke u ime
voditelja obrade. U kontekstu DGIZ, DGIZ je Izvršitelj obrade. Upravni odbor može
donijeti odluku o imenovanju i fizičke osobe Izvršitelja obrade, ukoliko se pokaže
potreba za istim.

Informacijski sustav – sveobuhvatnost tehnološke infrastrukture, organizacije, ljudi i
postupaka za prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz te distribuciju
informacija kao i raspolaganje njima.

Nadzorno tijelo – neovisno tijelo javne vlasti koje je osnovala Republika Hrvatska u
svrhu kontrole i osiguranja provođenja Uredbe.

Povjerljivost – svojstvo informacija (podataka) da nisu dostupne ili otkrivene
neovlaštenim subjektima.

Integritet – svojstvo informacija (podataka) i procesa da nisu neovlašteno ili
nepredviđeno mijenjani.

Privola – 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.

Pseudonimizacija – obrada osobnih podataka na način da se osobni podatci više ne
mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom
da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i
organizacijskim mjerama kako bi se osiguralo da se osobni podatci ne mogu pripisati
pojedincu čiji je identitet utvrđen ili se može utvrditi.

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.

Izrada profila – svaki oblik automatizirane obrade osobnih podataka koji se sastoji od
uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s
pojedincem, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom,
ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću,

ponašanjem, lokacijom ili kretanjem tog pojedinca.

Treće strane – 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.

Distributivni kanali – predstavljaju sredstva i načine preko kojih je omogućena komunikacija s ispitanicima (članovima, pretplatnicima i drugim osobama koje svojevolumno postanu ispitanici), te pristup informacijama, ugovaranje i korištenje proizvoda i usluga Društva, a obuhvaćaju aktivnosti podružnica, sekcija i drugih entiteta, mrežnu stranicu Društva: www.hdki.hr, te ostale aktivnosti koje se jasno i jednoznačno mogu povezati s Društvom.

II. TEMELJNE ODREDBE

Ovim Pravilnikom definiraju se osnovna načela i pravila zaštite osobnih podataka u skladu s poslovnim i sigurnosnim zahtjevima DGIZ-a, kao i zakonskim propisima, najboljim praksama i međunarodno prihvaćenim standardima.

Pravilnik o politici zaštite osobnih podataka (u daljnjem tekstu: Pravilnik) temeljni je akt koji opisuje svrhu i ciljeve prikupljanja, obrade i upravljanja osobnim podacima unutar DGIZ-a, a koji se temelji na vodećim svjetskim praksama iz područja zaštite osobnih podataka. Pravilnik osigurava adekvatnu razinu zaštite podataka u skladu s Općom uredbom o zaštiti podataka*

(u nastavku: Uredba) i drugim primjenjivim važećim

zakonima vezanim uz zaštitu osobnih podataka što Društvo dodatno osigurava detaljnim internim Aktima.

III. OPSEG I CILJ

Pravilnik o politici zaštite osobnih podataka je temeljni akt DGIZ-a koji za svrhu ima uspostavljanje okvira zaštite osobnih podataka sukladno Općoj uredbi o zaštiti podataka. Pravilnik utvrđuje pravila povezana sa zaštitom pojedinaca u pogledu prikupljanja i obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka.

* UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u svezi s

obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ

Cilj Pravilnika je uspostaviti primjerene procese zaštite i upravljanja osobnim podacima ispitanika, poslovnih partnera i drugih osoba čiji se osobni podatci obrađuju.

Pravilnik se primjenjuje na sve obrade osobnih podataka unutar DGIZ-a, osim u slučajevima gdje se obrađuju anonimizirani podatci ili su obrade takve prirode da se radi o statističkim analizama iz kojih nije moguće identificirati pojedinca.

IV. NAČELA OBRADE PODATAKA

Načela obrade podataka su osnovna pravila kojih se DGIZ-a pridržava prilikom obrade osobnih podataka ispitanika, a obrade koje se provode sukladno niže navedenim načelima smatraju se zakonitima.

Svaka organizacijska jedinica DGIZ-a dužna je osigurati pridržavanje niže navedenih načela unutar vlastite domene i prilikom obrade osobnih podataka za koje je organizacijska jedinica voditelj obrade.

DGIZ-a osobne podatke obrađuje u skladu sa sljedećim načelima obrade:

1. Zakonito i pošteno – s obzirom na ispitanike i njihova prava, DGIZ-a će obrađivati osobne podatke ispitanika sukladno važećim zakonima i pokrivajući sva prava ispitanika.
2. Transparentno – DGIZ-a će osigurati transparentnost obrada osobnih podataka te će, sukladno Uredbi, pružiti ispitanicima sve potrebne informacije i na zahtjev osigurati ispitanicima uvid u njihove podatke, obrazloženja obrada, temelje i zakonitosti obrade i sl. Kroz ovaj Pravilnik, ali i kroz druge kanale koje će biti dostupni ispitanicima, DGIZ-a će osigurati informacije kako se osobni podatci koji se odnose na njih prikupljaju, upotrebljavaju, daju na uvid ili na drugi način obrađuju, kao i do koje se mjere ti osobni podatci obrađuju ili će se obrađivati. Ispitanik će pravovremeno, odnosno prije samog prikupljanja podataka, biti upoznat sa svim relevantnim informacijama.
3. Uz ograničenje svrhe – osobni podatci moraju biti prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama.

4. Uz ograničenje pohrane – DGIZ-a osigurava da su osobni podatci ispitanika čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podatci obrađuju. DGIZ-a osobne podatke može pohraniti i dulje, ali za to mora imati jasnu svrhu u smislu zakonske obveze (npr. Zakona o arhivskom gradivu i arhivima) ili legitimni interes (npr. u slučaju sudskog spora).

5. Koristeći samo potrebne podatke (smanjenje količine podataka) – DGIZ osobne podatke prikuplja i obrađuje na način da su primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju. Od ispitanika se mogu tražiti i drugi podatci, no ispitanik ih nije dužan dati.

6. Točnost – DGIZ osigurava da su podatci točni i prema potrebi ažurni; mora se poduzeti svaka razumna mjera radi osiguravanja da se osobni podatci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja izbrišu ili isprave. DGIZ osigurava primjenu ovog načela na način da je uspostavila redovite kontrole, ali i transparentan proces komunikacije s ispitanicima kroz koji se može zatražiti ispravak podataka u slučaju da ispitanik primijeti da neki od njegovih osobnih podataka nije ispravno naveden.

7. Osigurava sigurnost, nadzor i kontrolu nad podacima i obradama podataka (Cjelovitost i povjerljivost) – DGIZ prikuplja i obrađuje podatke 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. DGIZ je implementiralo IT sustave koji imaju za cilj detekciju i sprječavanje curenja podataka, sustave za anonimizaciju/pseudonimizaciju podataka, metode nadzora nad pristupom podataka, ograničenja pristupa podacima sukladno potrebi radnog mjesta i sl. Sukladno navedenim načelima, podacima ispitanika pristupat će administratori i časnici DGIZ-a ovisno o njihovim ovlaštenjima. Također dio usluga za DGIZ obavljaju i druge pravne osobe s kojima će podatci ispitanika biti podijeljeni samo ako su oni nužni za potrebe ispunjenja obveza iz zajedničkih Ugovora. Primjer toga je računovodstvo, izrada poreznih

kartica, pohrane dokumentacije ili slanje dokumentacije na kućne adrese.

DGIZ će podatke ispitanika proslijediti i Udruženjima ili državnim institucijama u slučaju kada za to postoji zakonska osnova (primjerice za potrebe obrade poreznih obveza).

V. ZAKONITOST OBRADE

DGIZ osobne podatke ispitanika smatra njihovim vlasništvom te se prema njima tako i odnosi. Međutim, kako bi DGIZ bilo u mogućnosti pružiti uslugu ispitaniku, a sukladno niže navedenim zakonitostima, potrebno je obrađivati minimalan set podataka nužan za kvalitetno pružanje pojedine usluge. U suprotnom, odnosno ako ispitanik odbije ustupiti traženi set podataka, DGIZ vo neće biti u mogućnosti pružiti mu uslugu (primjerice ukoliko kandidat za članstvo odbije dati OIB ili nužne kontakt podatke, članstvo će biti odbijeno).

Sukladno tome, osobni podatci ispitanika obrađuju se kada je zadovoljen jedan od niže navedenih uvjeta:

- a) obrada je nužna za izvršavanje službenog odnosa DGIZ-a i ispitanika.
- b) obrada je nužna radi poštovanja pravnih obveza DGIZ-a (važeci zakonski propisi prema kojima je DGIZ dužno postupati) – u svakom trenutku kada zakon DGIZ ovlašćuje ili obvezuje na određenu obradu, DGIZ će temeljem tog zakona obrađivati osobne podatke ispitanika.
- c) obrada je nužna za potrebe legitimnih interesa DGIZ –a 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. Pod legitimnim interesom DGIZ-a podrazumijeva obrade koje služe kako bi se unaprijedilo poslovanje, ponudili proizvodi i usluge za koje je razvidno da bi mu olakšale poslovanje s DGIZ-om, unaprijedilo njegovo upravljanje vlastitim financijama te u korist rješavanja sudskih sporova.
- d) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha – privola mora biti dokaziva i dobrovoljna, napisana lako razumljivim jezikom i ispitanik ima pravo u svakom trenutku povući svoju privolu (povlačenje privole mora biti jednako jednostavno kao i davanje privole).

DGIZ će ispitanika zatražiti privole za obrade podataka i kontaktiranje u svrhe promotivnih i marketinških akcija putem kontakt podatka koje je ispitanik ustupio. Presentaciju novih proizvoda i usluga, nedostupnosti određene usluge koje Banka komunicira putem dostupnih distributivnih kanala DGIZ smatra dijelom osnovne usluge te za to neće zatražiti privolu ispitanika dok je sama obrada u skladu s načelima obrade navedenih u točki V. te se temelji na nekoj od navedenih zakonitosti obrade.

e) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe.

f) obrada je nužna za izvršavanje službene zadaće ili zadaće od javnog interesa.

g) Svaka organizacijska jedinica DGIZ-a dužna je identificirati zakonitost za svaku obradu koja je u njihovoj poslovnoj domeni. Pri identifikaciji zakonitosti obrade konzultirat će se nadležna osoba imenovana od Predsjedništva, koji će prema jasnim i unaprijed definiranim kriterijima savjetovati organizacijsku jedinicu prilikom identifikacije zakonitosti obrada.

VI. PRAVA ISPITANIKA

DGIZ je svjesno kako su osobni podatci ispitanika njegovo vlasništvo te iako su ti podatci nužni za pružanje usluge, ispitanici u svakom trenutku zadržavaju određena prava u odnosu na obrade njihovih podataka te DGIZ podatke prikuplja i obrađuje samo uz postojanje gore navedenih zakonitosti obrade. Društvo će u trenutku prikupljanja informacija od ispitanika pružiti sljedeće informacije: svrhe obrade radi kojih se upotrebljavaju osobni podatci kao i pravnu osnovu za obradu, legitimne interese, namjeru prijenosa osobnih podataka trećim zemljama (ako postoji), razdoblje pohrane podataka ili kriterije koji definiraju to razdoblje, prava vezana uz privole, potencijalno postojanje automatiziranog donošenja odluka što podrazumijeva i izradu profila (smislene informacije o kojoj je logici obrade riječ te potencijalnim posljedicama i važnosti same obrade za ispitanika) te postojanje niže navedenih prava. U slučaju da se podatci ne prikupljaju izravno od ispitanika, uz navedene podatke navodi se i izvor osobnih podataka. DGIZ osobne podatke obrađuje sukladno pravima ispitanika definiranim unutar Uredbe, a koja su navedene u nastavku:

Pravo na brisanje („pravo na zaborav“) – ispitanik ima pravo od DGIZ-a ishoditi brisanje osobnih podataka koji se na njega odnose, a DGIZ ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako je ispunjen jedan od sljedećih uvjeta:

- a) osobni podatci 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 ne postoji druga pravna osnova za obradu
- c) ispitanik uloži prigovor na obradu, a legitimni razlozi za realizaciju prava na brisanje imaju veću težinu od legitimnog interesa DGIZ-a za obradu i/ili čuvanje osobnih podataka
- d) osobni podatci nezakonito su obrađeni
- e) osobni podatci moraju se brisati radi poštovanja pravne obveze

Pravo na pristup podacima – ispitanik ima pravo dobiti od DGIZ-a potvrdu obrađuju li se njegovi osobni podatci te ako se takvi osobni podatci obrađuju, pristup osobnim podacima i svrsi obrade, kategorijama podataka, potencijalnim primateljima kojima će osobni podatci biti otkriveni, i sl.

Pravo na ispravak – ispitanik ima pravo bez nepotrebnog odgađanja ishoditi od DGIZ-a ispravak netočnih osobnih podataka koji se na njega odnose. Uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave. Dodatno, ispitanici imaju obvezu ažuriranja osobnih podataka u poslovnom odnosu s DGIZ-om.

Pravo na prijenos podataka – ispitanik ima pravo zaprimiti osobne podatke koji se odnose na njega, a koje je pružio DGIZ-u u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade. Potrebno je uzeti u obzir da se pravo prijenosa odnosi isključivo na osobne podatke ispitanika.

Pravo na prigovor – ispitanik ima pravo na temelju svoje posebne situacije u svakom trenutku uložiti prigovor na obradu osobnih podataka koji se odnose na njega. DGIZ u takvoj situaciji više ne smije obrađivati osobne podatke osim ako dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika ili

radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva. Nadalje, ako se osobni podatci obrađuju za potrebe izravnog marketinga, ispitanik u svakom trenutku ima pravo uložiti prigovor na obradu osobnih podataka koji se odnose na njega za potrebe takvog marketinga, što uključuje izradu profila u mjeri koja je povezana s takvim izravnim marketingom.

Pravo na ograničenje obrade – ispitanik ima od DGIZ-a pravo tražiti pravo na ograničenje obrade u slučaju da osporava točnost osobnih podataka, kada smatra da je obrada nezakonita te se protivi brisanju osobnih podataka i umjesto toga traži ograničenje njihove uporabe, te u slučaju kada je ispitanik uložio prigovor na obradu i očekuje potvrdu nadilaze li legitimni razlozi voditelja obrade razloge ispitanika. Ispitanik ima pravo u svakom trenutku zahtijevati realizaciju bilo kojeg od gore navedenih prava.

DGIZ ispitaniku na zahtjev pruža informacije o poduzetim radnjama vezanim uz navedena prava, najkasnije u roku od 3 mj. od zaprimanja zahtjeva – svi zahtjevi će se pokušati adresirati unutar 1 mjeseca te će rok produljiti najviše za dodatna 2 mjeseca kada je to nužno. Ako DGIZ ne postupi po zahtjevu ispitanika, bez odgađanja i najkasnije jedan mjesec od primitka zahtjeva izvijestit će ispitanika o razlozima zbog kojih nije postupila. Razlozi za ne postupanje podrazumijevaju postojanje zakonitosti obrade koja DGIZ onemogućava u postupanju. Dodatno, ispitanik ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu, osim ako je ta odluka:

- potrebna za sklapanje ili izvršenje ugovora između ispitanika i DGIZ-a
- dopuštena zakonom
- temelji na izričitoj privoli ispitanika

VII. OBVEZE DRUŠTVA SUKLADNO UREDBI

DGIZ kontinuirano provodi odgovarajuće tehničke i organizacijske mjere zaštite uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode ispitanika. Spomenute mjere uključuju provedbu odgovarajućih politika zaštite podataka:

- Osobni podatci ispitanika čuvaju se u skladu s internim standardima sigurnosti

DGIZ-a, koje kontinuirano poduzima organizacijske i tehničke mjere kako bi zaštitila osobne podatke ispitanika. Gdje je to primjenjivo, DGIZ primjenjuje kriptografske metode zaštite podataka te se kontinuirano radi na unaprjeđenju sigurnosnih mjera. Uz navedeno, koriste se napredni alati za zaštitu i sprječavanje curenja podataka, nadziru se kritični sustavi unutar Društva i sl.

– DGIZ ne dopušta neovlašteno prikupljanje, obradu ili korištenje osobnih podataka. Primjenjuje se pravilo ograničavanja pristupa podacima samo na one podatke koji su potrebni za obavljanje pojedinih poslovnih zadataka. U skladu s tim, jasno su definirane uloge i odgovornosti unutar DGIZ-a. Administratorima i časnicima je strogo zabranjeno korištenje osobnih podataka ispitanika u bilo koju svrhu koja nije u skladu s uvjetima definiranim u poglavlju IV. Zakonitost obrade.

– Osobni podatci se štite od neovlaštenog pristupa, korištenja, izmjene te gubitka. Mehanizmi zaštite se primjenjuju na osobne podatke unutar DGIZ-a bez obzira u kojem se obliku oni čuvaju – papirnatom ili elektroničkom.

VIII. OBRADA POSEBNIH KATEGORIJA OSOBNIH PODATAKA

DGIZ ne obrađuje podatke koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu ili seksualnoj orijentaciji pojedinca.

DGIZ posebno štiti osobne podatke djece, budući da djeca mogu biti manje svjesna rizika, posljedica i predmetnih zaštitnih mjera te svojih prava u vezi s obradom osobnih podataka. Djecom se smatraju osobe mlađe od šesnaest godina.

IX. AUTOMATSKA OBRADA PODATAKA

Donošenje odluka temeljem automatske obrade podataka je sastavni dio poslovanja DGIZ-a i kao takva je nužna, a provodi se:

- sukladno važećim zakonima kojima podliježe DGIZ
- u slučaju potrebe osiguravanja sigurnosti i pouzdanosti usluge koju pruža DGIZ
- ako je nužno za sklapanje ili izvršavanje ugovora između ispitanika i voditelja obrade što uključuje umanjeње rizika u poslovanju, unaprjeđenje poslovanja, određenih prekonoćnih obrada koje su sastavni dio IT sustava i sl.
- kada je ispitanik izričito dao svoju privolu

U skladu s Uredbom, DGIZ omogućava ispitanicima pravo prigovora na automatsku, ali i ručnu, obradu podataka u svrhu izravnog marketinga, uključujući izradu profila u mjeri u kojoj je povezana s takvim izravnim marketingom, bilo u odnosu na početnu ili daljnju obradu, u bilo koje vrijeme i besplatno.

X. PRIJENOS OSOBNIH PODATAKA

Prijenos osobnih podataka je moguć i partnerima DGIZ-a kojima je ugovorom povjereno obavljanje određenih usluga u ime DGIZ-a ili u slučaju postojanja zajedničkih aktivnosti.

Prilikom prijenosa podataka ispitanika DGIZ-a vanjskim partnerima strogo se poštuje načelo ograničenja obrade uz prijenos minimalne količine podataka koja je potrebna kako bi se realizirala tražena usluga. Dodatno, DGIZ je uspostavilo kontrolne mehanizme koji od partnera zahtijevaju minimalno jednaku razinu zaštite osobnih podataka kao i sami DGIZ.

Prema potrebi, a isključivo temeljem uvjeta navedenih u poglavlju IV. Zakonitost obrade, DGIZ podatke prenosi trećim zemljama ili međunarodnim organizacijama. U takvim situacijama se primjenjuju dodatne kontrole i zaštitne mjere za iznošenje osobnih podataka sukladno Uredbi. Te mjere mogu podrazumijevati pravno obvezujući i provedivi instrument, obvezujuća korporativna pravila, certificiranje i sl.

XI. POSLOVANJE S POSLOVNIM KORISNICIMA

Poslovni ispitanici unutar DGIZ-a mogu biti svaka pravna osoba, tijelo državne vlasti, jedinica lokalne ili područne samouprave te njihova tijela, udruga i društvo (sportsko, kulturno, dobrotvorno i sl.), kao i svaka fizička osoba (nepotrošač) koja djeluje unutar područja svoje registrirane gospodarske djelatnosti ili slobodnog zanimanja. DGIZ prikuplja i obrađuje podatke o poslovnim ispitanicima, transakcijama, korištenju proizvoda i usluga i osobne podatke fizičkih osoba (nepotrošača) koje djeluju unutar područja svoje registrirane gospodarske djelatnosti ili slobodnog zanimanja te osobne podatke fizičkih osoba (potrošača) koje su povezane s poslovnim ispitanicima.

Povezane osobe s poslovnim ispitanikom u kontekstu ovog Pravilnika mogu biti fizičke osobe vlasnici poslovnog ispitanika, osobe ovlaštene za zastupanje poslovnog

ispitanika, prokuristi, opunomoćenici poslovnog ispitanika, predstavnici poslovnog ispitanika i druge fizičke osobe čije je osobne podatke poslovni ispitanik dao DGIZ-u na korištenje za svrhe uspostave i održavanja poslovnog odnosa. DGIZ prikuplja, obrađuje i dijeli podatke o poslovnim ispitanicima koji uključuju osobne podatke poslovnih ispitanika i povezanih osoba u skladu sa zakonitostima iz točke V. Zakonitost obrade ovog Pravilnika.

DGIZ može obrađivati prikupljene podatke poslovnih ispitanika koji uključuju osobne podatke fizičkih osoba (neispitanika) koje djeluju unutar područja svoje registrirane gospodarske djelatnosti ili slobodnog zanimanja i povezanih osoba koje joj je na korištenje dao poslovni ispitanik za sljedeće slučajeve:

- Utvrđivanje identiteta
- Procjena rizika uspostave i održavanja poslovnog odnosa
- Prevencija rizika koji mogu proizaći iz poslovnog odnosa
- Usklađivanje sa zakonskim i regulatornim propisima unutar i izvan područja RH
- Ugovaranje i korištenje proizvoda i usluga koje DGIZ pruža
- Izvršenje svih vrsta bankovnih transakcija unutar i izvan područja Republike Hrvatske
- Izvještavanje
- Statističke obrade
- Razvijanje i poboljšanje proizvoda i usluga kako bi poslovnim ispitanicima omogućili bolje iskustvo korištenja
- Definiranje proizvoda i usluga koji bi poslovnim ispitanicima DGIZ-a bili od koristi
- Kontaktiranje u svrhe ispunjenja ugovornih odnosa unutar DGIZ-a
- Kontaktiranje u marketinške svrhe.

DGIZ može podijeliti podatke o poslovnim ispitanicima koji uključuju osobne podatke fizičkih osoba (neispitanika) koje djeluju unutar područja svoje registrirane gospodarske djelatnosti ili slobodnog zanimanja i povezanih osoba koje joj je na korištenje dao poslovni ispitanik uz zadovoljenje zakonitosti obrada definiranih u točki V. Zakonitost obrade te sukladno načelima obrade definiranim u točki IV. Načela obrade podataka i to prema:

- Nekoj od članica Grupe
- Zakonodavnim, nadzornim i regulatornim tijelima unutar i izvan područja Republike Hrvatske
- Financijskim institucijama s kojima DGIZ surađuje
- Ministarstvima, jedinicama lokale i područne samouprave s kojima DGIZ surađuje
- Ostale agencije, institucije, udruge, osiguravajuće kuće i tvrtke partneri s kojima DGIZ ima sklopljen ugovor o poslovnoj suradnji temeljem kojeg poslovnici ispitanici mogu ugovarati i koristiti proizvode i usluge koje DGIZ pruža itd.

XII. SLUŽBENIK ZA ZAŠTITU PODATAKA (DPO)

Sukladno uredbi EU 2016/679, DGIZ u trenutku izrade Pravilnika nije bilo obvezatno imenovati Službenika za zaštitu podataka (Data Protection Officer, DPO).

U slučaju promjene okolnosti koje će zahtijevati imenovanje DPO, Predsjedništvo će ga imenovati posebnom odlukom.

XIII. PROCJENA UČINKA

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, DGIZ prije obrade provodi procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka, ako je u ulozi voditelja obrade. Jedna procjena može se odnositi na niz sličnih postupaka obrade koji predstavljaju slične visoke rizike.

Dodatno, DGIZ će provesti procjenu učinka na sve obrade koje su trenutno aktivne, a odgovaraju navedenim kategorijama.

DGIZ obvezatno provodi procjenu učinka na zaštitu podataka u slučaju:

- sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila, i na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili značajno utječu na pojedinca
- opsežne obrade posebnih kategorija osobnih podataka
- sustavnog praćenja javno dostupnog područja u velikoj mjeri
- u slučajevima obrada koje propiše nadzorno tijelo (Agencija za zaštitu osobnih

podataka)

Procjena učinka sadrži minimalno:

- sustavan opis predviđenih postupaka obrade i svrha obrade, uključujući legitimni interes DGIZ-a
- procjenu nužnosti i proporcionalnosti postupaka obrade povezanih s njihovim svrhama
- procjenu rizika za prava i slobode ispitanika iz stavka
- mjere predviđene za rješavanje problema rizika, što uključuje zaštitne mjere, sigurnosne mjere i mehanizme za osiguravanje zaštite osobnih podataka i dokazivanje sukladnosti s Uredbom, uzimajući u obzir prava i legitimne interese ispitanika i drugih uključenih osoba

XIV. REGISTAR OBRADA OSOBNIH PODATAKA

DGIZ vodi evidenciju aktivnosti obrada za koje je odgovorna, odnosno u slučajevima kada je u ulozi voditelja obrade ili zajedničkog voditelja obrade. Ta evidencija je u elektroničkom obliku i sadržava najmanje sljedeće informacije:

- ime i kontaktne podatke voditelja obrade
- svrhe obrade
- opis kategorija ispitanika i kategorija osobnih podataka
- kategorije primatelja kojima su osobni podatci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije
- prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući ime treće zemlje ili naziv međunarodne organizacije
- predviđene rokove za brisanje različitih kategorija podataka, ako je to moguće
- opći opis tehničkih i organizacijskih sigurnosnih mjera

Voditelj obrade podataka odgovoran je za održavanje registra obrada, a sve organizacijske jedinice unutar DGIZ-a su odgovorne za dostavu točnih i pravovremenih informacija kako bi se registar obrada adekvatno popunio.

XV. INCIDENTI / CURENJE PODATAKA I PRAVO NA PRITUŽBU

DGIZ poduzima značajne procesne i tehnološke mjere kako bi zaštitila osobne podatke ispitanika. Dodatno, sve ovlaštene osobe DGIZ-a imaju dužnost obavijestiti

odgovorne osobe u slučaju incidenta vezanog uz zaštitu osobnih podataka, a u slučaju povrede osobnih podataka DGIZ je incident dužno prijaviti Agenciji za zaštitu osobnih podataka unutar 72 sata nakon saznanja o povredi, ako je to izvedivo. DGIZ je dužan obavijestiti odgovorne osobe direktno ako je u ulozi voditelja ili zajedničkog voditelja obrade, a u ulozi izvršitelja obrade obavještavanje se provodi putem voditelja obrade koji je primarna točka za kontakt.

U slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, DGIZ bez nepotrebnog odgađanja obavještava ispitanika.

Iznimno, DGIZ neće obavijestiti ispitanika u slučaju povreda osobnih podataka ako je ispunjen barem jedan od sljedećih uvjeta:

- DGIZ je poduzelo 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
- DGIZ je poduzelo naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika
- time bi se zahtijevao nerazmjern napor. U takvom slučaju mora postojati javno obavještavanje ili slična mjera kojom se ispitanici obavještavaju na jednako djelotvoran način

Ispitanik ima pravo podnijeti pritužbu nadzornom tijelu (Agencija za zaštitu osobnih podataka) u slučaju incidenta koji se tiče njegovih osobnih podataka ili ako smatra da DGIZ krši njegova prava definirana Općom uredbom o zaštiti podataka.

XVI. ZAVRŠNE ODREDBE

Ovaj Pravilnik stupa na snagu danom donošenja, a primjenjuje se od 25. svibnja 2018. godine.

Predsjedništvo DGIZ-a