PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA

PROFIL KLETT d.o.o.

Sadržaj

***

1. UVOD

Počevši od 25. svibnja 2018. godine u svim zemljama članicama Europske unije primjenjuje se Uredba (EU) 2016/679 Europskog parlamenta i Vijeća 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)**.

Opća uredba o zaštiti podataka zahtijeva višu razinu pažnje i povećanu kontrolu postupanja kao i načina obrade osobnih podataka, a koja je znatno viša od dosadašnje legislative. Nova pravila uvode upravne novčane kazne koje se mogu kretati u iznosu do 20 000 000 EUR, ili do 4 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome koji iznos je viši.

2. SVRHA PRAVILNIKA O ZAŠTITI OSOBNIH PODATAKA

Pravilnik o zaštiti osobnih podataka predstavlja sveobuhvatna pravila o glavnim obvezama svih zaposlenika i suradnika Profil Klett d.o.o., kao i posrednih i neposrednih dobavljača roba i usluga, a kojih se navedene osobe moraju pridržavati kako bi bili u skladu s Općom uredbom o zaštiti podataka. Pojedinci, obveznici pridržavanja navedenih pravila – dalje u tekstu navedeni su kao: **Korisnici;** dok se društvo Profil Klett d.o.o. dalje u tekstu označuje kao: **Organizacija.** Ovaj Pravilnik o zaštiti osobnih podataka dostupan je na oglasnoj ploči društva.

Korištenje dokumenata, informacija, osobnih podataka, sustava te servisa organizacije koje nije u skladu s pravilima uređenima ovim Pravilnikom može predstavljati razlog za pokretanje disciplinskog, kaznenog ili postupka za naknadu nastale štete organizaciji.

3. DEFINICIJE

Vlasnik procesa: označava osobu imenovanu od ovlaštene osobe u Organizaciji, a koja je unutar određenog okvira odgovorna pratiti i osiguravati usklađenost obrade osobnih podataka s Uredbom za zaštitu osobnih podataka. Svaki vlasnik procesa može u skladu sa svojim ovlastima imenovati drugog vlasnika procesa, ovisno o potrebama i upravljačkoj ulozi koju ima unutar svoje specifične funkcije i odjela. Takvo imenovanje mora naznačiti zadaće za koje je zadužena delegirana osoba.

Savjetnik: označava osobu / funkciju čija je osnovna funkcija pružanje savjeta i podrške vezane za pitanja usklađenosti s Uredbom za zaštitu osobnih podataka.

Korisnik: označava osobu koja je kao zaposlenik ili suradnik Organizacije u obavljanju svojih radnih zadataka uključena u bilo koji postupak u vezi sa obradom osobnih podataka.

Ispitanik: označava fizičku (i gdje je posebno predviđeno – pravnu) osobu, čiji se osobni podaci obrađuju od Organizacije, odnosno nekog njenog tijela.

„Osobni podaci": označavaju 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.

Posebne kategorije osobnih podataka: označavaju osobne podatke o rasnom ili etničkom porijeklu, političkim stavovima, religijskim ili filozofskim uvjerenjima ili sindikalnom članstvu kao i obradu genetskih i biometričkih podataka s ciljem jednoznačne identifikacije fizičke osobe, podatke povezane sa zdravljem ili seksualnim životom ili seksualnom orijentacijom pojedinca te podatke vezane za kaznene ili prekršajne postupke.

Obrada: označava 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, uključujući provedbu logičkih, matematičkih i drugih postupaka s osobnim podacima ili skupovima osobnih podataka.

Izrada profila: označava 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, kreditnom sposobnošću, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca.

Privola za obradu: 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. To bi moglo obuhvaćati označivanje polja kvačicom pri posjetu internetskim stranicama, izjavu ili

ponašanje koje jasno pokazuje da ispitanik prihvaća predloženu obradu svojih osobnih podataka. Šutnja, unaprijed kvačicom označeno polje ili manjak aktivnosti stoga se ne bi smjeli smatrati privolom.

Izvršitelj obrade: označava subjekt (društvo ili pojedinca, upravno ili drugo tijelo) koje obrađuje osobne podatke u ime voditelja obrade. Izvršitelji obrade su subjekti izvan Organizacije koji obrađuju podatke u ime potonjeg. Subjekti Organizacije također mogu imati ulogu izvršitelja obrade u slučaju kada provode radnju obrade u ime klijenta ili drugog subjekta.

Platforma: označava automatizirani alat koji omogućava subjektima Organizacije da ispune zahtjeve Opće uredbe o zaštiti podataka te uključuje, ali se ne ograničava stvaranje i ažuriranje Registra podataka, prijave i revizije, procjenu utjecaja na privatnost te obavijest o povredi osobnih podataka.

Podizvršitelj: označava subjekt (društvo ili pojedinca) kojeg je izvršitelj obrade postavio da u ime voditelja obrade provodi obradu osobnih podataka, a kojeg nadzire izvršitelj obrade. Pod izvršitelji su subjekti izvan Organizacije koji obrađuju podatke u ime klijenata Organizacije.

Voditelj obrade: označava subjekt (društvo ili pojedinca, upravno ili drugo tijelo) koji sam ili zajedno s drugima određuje ciljeve i obrade osobnih podataka.

Povreda osobnih podataka: označava 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.

Regulatorno tijelo: označava nacionalno nadzorno tijelo za zaštitu osobnih podataka koje je nadležno za određeni predmet. Moguće je da su različita Regulatorna tijela nadležna za predmete vezane za subjekte Organizacije, ovisno o specifičnostima svakog slučaja.

Dobavljač: označava treću stranu koja pristupa osobnim podacima koje obrađuje Organizacija / subjekt Organizacije kao voditelj ili izvršitelj obrade, ovisno o slučaju. Može uključivati, na primjer, trećeg pružatelja usluga ili poslovnu stranku.

Subjekti Organizacije: ovisno o kontekstu, zajedno društva Organizacije koja djeluju u EU, koji mogu biti voditelji ili izvršitelji određene obrade osobnih podataka, ovisno o slučaju.

Ovaj Pravilnik o zaštiti osobnih podataka strukturiran je u sljedeće odjeljke:

- *Pravila za adekvatnu obradu osobnih podataka* - **Odjeljak 1**;
- *Pravila za adekvatnu pohranu dokumenata društva* - **Odjeljak 2**;
- *Pravila za adekvatnu uporabu informacija, sustava i usluga* - **Odjeljak 3**;
- *Pravila za adekvatnu klasifikaciju i upravljanje informacijama Organizacije* - **Odjeljak 4**;

4. ODJELJAK 1 - PRAVILA ZA ADEKVATNU OBRADU OSOBNIH PODATAKA

4.1 OBRADA OSOBNIH PODATAKA

4.1.1 Opća načela obrade osobnih podataka

Osobni podaci smiju se obrađivati, uz određene iznimke, u svrhe naznačene u informaciji o privatnosti dane određenom ispitaniku. Osobni podaci:

- moraju se obrađivati na zakonit, pravilan i transparentan način;
- moraju se prikupljati i evidentirati u određenu, eksplicitnu i legitimnu svrhu te upotrebljavati u postupcima obrade koji su kompatibilni s tom svrhom;
- moraju biti precizni i, tamo gdje je to potrebno, ažurirani;
- moraju biti adekvatni, relevantni te ih ne smije biti više no što je potrebno za svrhu u koju su prikupljeni i obrađeni;
- moraju biti pohranjeni u obliku koji omogućava identifikaciju ispitanika na period ne duži nego što je to potrebno za svrhu u koju su prikupljeni i obrađeni; i
- moraju se obrađivati na način koji jamči odgovarajuću sigurnost, uključujući zaštitu odgovarajućim tehničkim i organizacijskim mjerama od neovlaštene ili nezakonite obrade, od gubitka, uništenja ili slučajnog oštećenja.

Opća uredba o zaštiti podataka zahtijeva da Ispitanik bude pravilno obaviješten o obradi svojih podataka kao što je propisano u članku 13. Opće uredbe o zaštiti podataka. Ispitanik mora dati svoju slobodnu, informiranu i jednoznačnu privolu za obradu svojih osobnih podataka ako će se ti osobni podaci obrađivati u druge svrhe osim u svrhu provedbe ugovora s Ispitanikom.

Svakom Ispitaniku mora se pružiti mogućnost kontaktirati voditelja obrade, odnosno odgovornu osobu.

Organizacija je odredila odgovornu osobu unutar svoje organizacije kojoj je povjeren nadzor nad pridržavanjem propisa o zaštiti podataka: „Službenika za zaštitu podataka".

Svi zaposlenici Organizacije su obvezni pridržavati se pravila ovog Pravilnika o zaštiti osobnih podataka. U vrijeme trajanja ugovora o radu/suradnji, svaki zaposlenik ili suradnik mora dobiti – pored informacije o privatnosti koja prikazuje modalitete obrade njegovih osobnih podataka – i ovaj Pravilnik o zaštiti osobnih podataka kao dio ugovornih dokumenata kojima je obvezan te ih mora posebno prihvatiti i izjaviti da ih je analizirao i razumio uvjete. Svrha ovog Pravilnika o zaštiti osobnih podataka jest obavijestiti sve korisnike o njihovim obvezama pri obradi osobnih podataka u ime Organizacije.

Organizacija će informirati zaposlenike s obzirom na obveze proizašle iz Uredbe i ovog Pravilnika o zaštiti osobnih podataka kako bi se osiguralo potpuno razumijevanje i znanje o obvezama vezanim za privatnost osobnih podataka.

Svaki zaposlenik mora barem jednom godišnje proći edukaciju Organizacije o zaštiti osobnih podataka

4.1.2 Uvjeti za obradu osobnih podataka u ime Voditelja obrade

Ukoliko provodi obradu podataka u ime Voditelja obrade, Organizacija mora biti od strane Voditelja obrade imenovana Izvršiteljem obrade. U skladu s Općom uredbom o zaštiti podataka radnje obrade koje provodi Izvršitelj moraju biti uređene ugovorom između Voditelja obrade i Izvršitelja kojim će se ugovoriti predmet i trajanje obrade, priroda i svrha obrade, vrsta osobnih podataka i kategorije ispitanika i obveze i prava Voditelja obrade. Predmetnim ugovorom potrebno je utvrditi da Organizacija kao Izvršitelj:

a) obrađuje osobne podatke samo prema jasnim i dokumentiranim uputama od Voditelja;

b) osigura da su se osobe koje su ovlaštene obrađivati osobne podatke obvezale na povjerljivost;

c) poduzme sve prikladne sigurnosne mjere;

d) ako ju je Voditelj obrade ovlastio za podizvršenje obrade, u ugovoru s podizvršiteljem obrade nametne iste obveze zaštite podataka iznesene u ugovoru s Voditeljem;

e) uzimajući u obzir prirodu obrade, pomaže Voditelju obrade koristeći prikladne tehničke i organizacijske mjere, koliko je to moguće, da ispuni Voditeljevu obvezu odgovora na zahtjeve za ispunjavanjem ispitanikovih prava;

f) pomaže Voditelju u osiguranju pridržavanja obveza iz čl. 32.-36. Opće uredbe o zaštiti podataka (sigurnost obrade, obveza obavješćivanja u slučaju povrede osobnih podataka, procjena utjecaja na zaštitu osobnih podataka, prenosivosti), uzimajući u obzir prirodu obrade te informacije koje su dostupne Izvršitelju obrade;

g) na zahtjev Voditelja obrade briše ili vrati sve osobne podatke Voditelju obrade nakon završetka pružanja usluga;

h) učini dostupnim Voditelju obrade i nadležnom regulatornom tijelu za privatnost sve podatke potrebne da bi se pokazalo pridržavanje zakona o privatnosti podataka.

Svaki korisnik koji u kontekstu svojih zadaća obrađuje osobne podatke u ime Voditelja obrade treba se pobrinuti da njegova radnja ne izlazi izvan okvira iznesenih u aktu kojim je imenovan izvršitelj obrade.

U slučaju da izvršitelj obrade prekrši odredbe Opće uredbu za zaštitu osobnih podataka, utvrđujući svrhe i sredstva obrade, smatrati će se Voditeljem obrade u smislu obrade sa svim odgovornostima koje proizlaze iz toga.

4.2 INFORMACIJE O OSOBNIM PODACIMA

Svaki ispitanik mora od Voditelja obrade dobiti sve informacije vezane za obradu njegovih osobnih podataka koje zahtijeva Opća uredba za zaštitu podataka. Takve informacije o privatnosti moraju se predočiti u trenutku prikupljanja osobnih podataka. Ako su osobni podaci nabavljeni od treće strane, informacije o privatnosti trebaju se predati:

a) unutar razumnog roka od trenutka nabave osobnih podataka, no u svakom slučaju najkasnije unutar mjesec dana od prikupljanja, uzimajući u obzir posebne okolnosti pod kojima se obrađuju osobni podaci;

b) u slučaju da su osobni podaci namijenjeni komunikaciji s ispitanikom, najkasnije prilikom prvog mogućeg kontakta, ili;

c) ako je komunikacija zamišljena s drugim primateljem, najkasnije prilikom prve komunikacije, odnosno prikupljanja osobnih podataka.

Informacija o privatnosti mora sadržavati određene informacije određene Općom uredbom o zaštiti podataka, uključujući, između ostalog, svrhe u koje se osobni podaci obrađuju, detalje o izvršitelju naloga, mogućnost ispitanika da iskoristi svoja prava iz Opće uredbe o zaštiti podataka, rok čuvanja podataka te mogućnost ulaganja prigovora nadležnom regulatornom tijelu za privatnost.

Isključivo Voditelj obrade mora dati ispitanicima informacije o privatnosti dok Izvršitelj obrade mora obraditi osobne podatke u ime Voditelja obrade prema uputama Voditelja obrade i samo u svrhe koje je Voditelj obrade naznačio u pismenom imenovanju Izvršitelja obrade.

Kada nastupa kao voditelji obrade, Organizacija mora predati informacije o privatnosti ispitanicima.

4.3 PRIVOLA ISPITANIKA

Privola ispitanika potrebna je za obradu osobnih podataka u svim slučajevima, osim u niže definiranim slučajevima prema člancima 6. i 9. Opće uredbe o zaštiti podataka.

Obrada osobnih podataka koji ne predstavljaju posebne kategorije osobnih podataka dopuštena je bez izražene privole ispitanika, ako postoji neki od sljedećih uvjeta:

- kada je obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;
- obrada je nužna radi poštovanja pravnih obveza voditelja obrade;
- obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe;
- obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;
- 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.

Osim gore navedenog, obrada posebnih kategorija osobnih podataka dopuštena je bez izričite privole ispitanika, u sljedećim slučajevima:

- obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava voditelja obrade ili ispitanika u području radnog prava i prava socijalne sigurnosti i socijalne zaštite (uključujući kolektivne ugovore);
- obrada je potrebna za zaštitu života ili zdravlja ispitanika ili drugog pojedinca kada je ispitanik fizički ili pravno spriječen da da privolu;
- obrada je provedena u odnosu na njihove legitimne aktivnosti, s odgovarajućim jamstvima;
- obrada potrebna u svrhe preventivne medicine, medicinskih dijagnoza, upravljanja zdravstvom ili zdravstvenim uslugama, pod uvjetom da osobne podatke obrađuju zdravstveni djelatnici na osnovu posebnih propisa i pravila nadležnih tijela;
- obrada je nužna u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, 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 se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik;
- obrada je potrebna iz razloga značajnog javnog interesa.

Za svaku obradu osobnih podataka u svrhe koje nisu povezane s provedbom ugovora ili zakona te u svim slučajevima kada se provodi obrada osobnih podataka u svrhe koje nisu povezane s posebnim ugovorom na koje

se pravilnik o privatnosti odnosi: mora se zahtijevati izričita i odvojena privola od ispitanika (npr. za marketing, u promidžbene svrhe, izradu profila, itd.).

U odnosu na usluge pružene na mrežnim stranicama, aplikacijama, itd., mora se pribaviti ili potvrda da ispitanik nije mlađi od 16 godina ili manje ukoliko je tako određeno primjenjivim propisom u Republici Hrvatskoj, ili odobrenje roditelja/skrbnika u odnosu na usluge pružene maloljetnicima.

Izričita privola ispitanika mora dana biti papirnato ili elektronički tako da postoji odgovarajući nedvojben dokaz da je privola dana.

4.4 PRAVA ISPITANIKA

Ispitanici mogu zatražiti izvršenje svojih prava na način da u e-mail poruci pošalju zahtjev za izvršenje nekog od svojih prava osobi za kontakt koju je Organizacija za to odredila.

Svi zahtjevi ispitanika trebaju biti proslijeđeni Službeniku za zaštitu podataka u Organizaciji:

a) Isto tako, ako je zahtjev ispitanika naslovljen na treću stranu (npr. na dobavljača informacijske tehnologije ili na marketinšku agenciju) koja obrađuje osobne podatke ispitanika u ime Organizacije, ta treća strana mora odmah proslijediti taj zahtjev osobi koja je unutar Organizacije odgovorna za taj ugovor koja će onda pak obavijestiti Službenika za zaštitu podataka. Gornje obveze (obavješćivanja Voditelja) moraju biti uključene u ugovore između Organizacije/voditelja i treće strane/izvršitelja. Službenik za zaštitu podataka mora provjeriti identitet ispitanika koji je podnio zahtjev, te usporediti podatke sadržane u zahtjevu s podacima koje Organizacija već ima.

b) Ako se pronađu nepodudarnosti, mora se kontaktirati ispitanik putem dostupnih podataka o kontaktu te zatražiti od ispitanika da pošalje identifikacijske podatke.

c) Nakon utvrđivanja identiteta ispitanika mora se;

   i) odmah zabilježiti takav zahtjev ispitanika kako bi se osigurala koordinacija i uključivanje drugih odjela Organizacije koji mogu biti mjerodavni - ovisno o zahtjevu, a kako bi se omogućilo identificiranje osobnih podataka koji su predmetom zahtjeva te zajamčilo da će se zahtjev provesti (npr. u slučaju zahtjeva za zaborav). Provedba zahtjeva je potrebna u odnosu na sve računalne sustave i dokumente Organizacije i dobavljača. Službenik za zaštitu podataka mora osigurati da je pridržavanje zahtjeva ispitanika uredno zabilježeno.

   ii) Odmah pisano (pisanim putem ili e-mailom) odgovoriti ispitaniku **unutar 30 kalendarskih dana od ispitanikovog zahtjeva.**

Ako je zahtjev posebno kompleksan, Službenik za zaštitu podataka mora:

   i) tamo gdje je to primjenjivo, **unutar 30 kalendarskih dana** od zahtjeva, pisano ispitaniku objasniti razloge zbog kojih je potrebno produljenje roka za odgovor.

   ii) U svakom slučaju, unutar 60 kalendarskih dana od obavijesti o produljenju pisano odgovoriti ispitaniku.

Ne mogu se naplatiti troškovi ispunjenja zahtjeva ispitanika, osim u slučajevima kad je ispitanikov zahtjev očito neosnovan ili pretjeran tj. repetitivan u slučaju kada ispitanik zatraži dodatne primjerke u odnosu na one predane na prvi zahtjev.

4.4.1 Pravo pristupa osobnim podacima

Ispitanici imaju pravo ishoditi potvrdu o tome jesu li njihovi osobni podaci u postupku obrade te, ako je to slučaj, imaju pravu dobiti pristup svojim osobnim podacima kao i informacijama o sljedećim činjenicama:

a) podrijetlo osobnih podataka;

b) svrhe obrade;

c) kategorije predmetnih osobnih podataka;

d) gdje je moguće, predviđenom razdoblju pohrane osobnih podataka ili, ako to nije moguće, kriterijima koji se koriste u svrhu određivanja tog razdoblja;

e) postojanju prava na zahtjev za ispravljanjem ili brisanjem osobnih podataka ili ograničenjem obrade osobnih podatka koji se tiču ispitanika ili na prigovor takvoj obradi (prema postupcima opisanima u ovome paragrafu);

f) o postojanju automatskog odlučivanja, uključujući izrade profila i, u tom slučaju, primijenjenoj logici i predviđenim posljedicama takve obrade za ispitanika;

g) o primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni ili će biti otkriveni (u slučaju prijenosa osobnih podataka), posebice primateljima u trećim zemljama (ili međunarodnim organizacijama) i, ako je to slučaj, o postojanju odgovarajućih mjera zaštite tog prijenosa;

h) pravu na ulaganje prigovora nadležnom regulatornom tijelu;

i) pravu na ispravljanje, objedinjavanje i prenosivost;

4.4.2 Pravo na brisanje („Pravo na zaborav“)

Ispitanici imaju pravo na brisanje osobnih podataka koji se odnose na njih kada:

a) osobni podaci više nisu potrebni za svrhe u koje su prikupljeni;

b) ispitanici povuku svoju privolu na osnovu koje se provodi obrada te gdje nema druge pravne osnove za obradu;

c) se ispitanici protive obradi (vidi odjeljak 8.6) - ispitanik uloži prigovor na obradu, te ne postoje jači legitimni razlozi za obradu;

d) su osobni podaci nezakonito obrađivani;

e) osobni podaci moraju biti obrisani kako bi se ispunila zakonska obveza; i

f) su osobni podaci prikupljeni u vezi ponude usluga informacijskog društva - nuđenja usluga informacijskog društva izravno djetetu.

Kada nastupa kao izvršitelj obrade, Organizacija mora pomoći voditeljima obrade odgovarajućim tehničkim i organizacijskim mjerama za ispunjenje gornjih obveza, a mjere se moraju precizno opisati u ugovorima kojima se stupa u odnos s klijentima.

4.4.3 Pravo na ograničavanje obrade

Ispitanici mogu ishoditi ograničenje obrade osobnih podataka koji se odnose na njih, što rezultira time da se podaci na ograničeno razdoblje ne mogu koristiti u sljedećim situacijama:

a) kada ispitanik osporava točnost osobnih podataka, i to na razdoblje potrebno Organizaciji da provjeri točnost takvih podataka;

b) kada je obrada nezakonita te se ispitanici protive brisanju osobnih podataka te zahtijevaju ograničenje njihove uporabe;

c) kada voditelj obrade više ne treba osobne podatke za potrebe obrade, ali ih ispitanik traži radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva u nekom odvojenom postupku;

d) kada se ispitanici usprotive obradi, dok se od Organizacije čeka potvrda nadilaze li legitimni razlozi Organizacije razloge ispitanika.

U gornjim slučajevima, kada nastupaju kao voditelji obrade, subjekti Organizacije smiju osobne podatke ispitanika obrađivati samo u svrhe pohrane, u suradnji sa Službenikom za zaštitu podataka. i svim drugim relevantnim službama uključenima u tu svrhu.

U tim okolnosti, osim pohrane, Organizacija može obrađivati ispitanikove podatke – u očekivanju ograničenja obrade – samo u sljedećim okolnostima:

a) kada su ispitanici dali svoju privolu;

b) radi ostvarivanja ili obrane pravnih zahtjeva ili zaštitu prava druge fizičke ili pravne osobe;

c) kako bi se zajamčila zaštita prava Organizacije;

d) relevantnih razloga javnog interesa.

Kada nastupa kao Izvršitelj obrade, Organizacija mora pomoći Voditeljima obrade odgovarajućim tehničkim i organizacijskim mjerama za ispunjenje gornjih obveza. Ovo se mora urediti ugovorima u koje se stupa s klijentima.

4.4.4 Pravo na prenosivost podataka

Ispitanik ima pravo zaprimiti osobne podatke koji se odnose na njega, a koje je pružio Organizaciji, u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade bez ometanja od Organizacije ako je:

a) obrada provedena automatiziranim sredstvima

b) obrada zasnovana na privoli ispitanika ili temeljem legitimnog interesa - ugovora čija je ispitanik strana; i

c) one podatke koji su predmetom zahtjeva za prijenosom dao ili generirao sam ispitanik (isključujući informacije koje je Organizacija izvela ili zaključila na temelju informacija koje je dao isti ispitanik).

Ispitanik može također zatražiti primjerak obrađenih podataka pod uvjetom da to ne krši prava i slobode ostalih ispitanika. Takve podatke vlasnik procesa mora elektronički predati ispitaniku koji postavlja zahtjev putem e-poruke, ili pisano u drugim slučajevima, a detalje o trećim stranama mora prekriti ili izbrisati.

Kada nastupa kao izvršitelj obrade, Organizacija mora pomoći voditeljima obrade odgovarajućim tehničkim i organizacijskim mjerama za ispunjenje gornjih obveza.

Kada nastupa kao Voditelj obrade, Organizacija mora implementirati odgovarajuće postupke kako bi se osiguralo ispunjenje gornjih uvjeta.

Kada nastupa kao Izvršitelj obrade, Organizacija mora pomoći voditeljima obrade odgovarajućim tehničkim i organizacijskim mjerama za ispunjenje gornjih obveza. Ovo se mora urediti ugovorima u koje se stupa s voditeljima obrade.

4.4.5 Pravo na prigovor

Ispitanik ima pravo prigovoriti obradi osobnih podataka koji se odnose na njega kada te podatke Organizacija obrađuje, između ostaloga, u izravne marketinške svrhe, uključujući izradu profila.

4.4.6 Pravo na ispravljanje i objedinjavanje

Ispitanici imaju pravo na ispravljanje netočnih osobnih podataka ili objedinjavanje nepotpunih osobnih podataka. Nakon što se podaci isprave, vlasnik će procesa e-mail porukom ili pisanim putem poslati potvrdu ispitaniku koji je podnio zahtjev, a detalji o trećim stranama moraju biti prekriveni ili izbrisani.

Kada nastupa kao izvršitelj obrade, Organizacija mora pomoći voditeljima obrade odgovarajućim tehničkim i organizacijskim mjerama za ispunjenje gornjih obveza. Ovo se mora urediti ugovorima u koje se stupa s klijentima. Službenik za zaštitu podataka je odgovoran za uključenje informacijsko-tehnološkog odjela i ostalih relevantnih odjela u procjenu tehničkih i organizacijskih mjera predviđenih u ugovoru s klijentima.

4.4.7 Pravo da se na ispitanika ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi

Ispitanici imaju pravo da se na njih ne odnosi odluka koja se isključivo temelji na automatiziranoj obradi tj. bez ljudske intervencije, uključujući i izradu profila, osim u slučajevima kada:

a) je to potrebno za svrhe sklapanja ili ispunjenja ugovora između ispitanika i voditelja obrade;

b) se temelji na eksplicitnoj privoli ispitanika.

Gornji scenarij predviđen je, na primjer ako je tijekom postupka zaposlenja Organizacija zadala automatsku provjeru i odabir kandidata koji su stoga isključeni isključivo temeljeno na automatiziranoj odluci.

Kada nastupa kao Voditelj obrade, Organizacija mora implementirati odgovarajuće postupke kako bi se osiguralo ispunjenje gornjih uvjeta.

Kada nastupa kao Izvršitelj obrade, Organizacija moraju pomoći voditeljima obrade odgovarajućim tehničkim i organizacijskim mjerama za ispunjenje gornjih obveza. Ovo se mora urediti ugovorima u koje se stupa s klijentima. Službenik za zaštitu podataka je odgovoran za uključenje informacijsko-tehnološkog odjela i ostalih relevantnih odjela u procjenu tehničkih i organizacijskih mjera predviđenih u ugovoru s klijentima.

4.5 UPRAVLJANJE OSOBNIM PODACIMA

Osobni podaci ne mogu se otkriti trećoj strani ako ispitanik nije dao svoju privolu ili ako ne postoji druga pravna osnova za svrhe prijenosa podataka, na primjer - ako se ona odnosi na treću stranu koja obrađuje osobne podatke u ime Organizacije i čije su radnje potrebne za provedbu ugovora s kupcem (npr. informacijsko-tehnološke usluge) ili za pružanje usluga kupcu (npr. daljnje praćenje zahtjeva kupca).

Kao općenito pravilo, osim u slučaju posebnih iznimki u skladu s mjerodavnim pravima, osobni podaci ne mogu se prenijeti izvan Europskog gospodarskog prostora osim ako se s primateljem podataka ne provedu aranžmani iz Opće uredbe o zaštiti podataka koji odobravaju takve prijenose, kao na primjer tzv. Standardne ugovorne klauzule EU-a za prijenose podataka.

4.6 ROK ČUVANJA / POHRANE PODATAKA

Osobni podaci moraju se obraditi unutar razdoblja koje je potrebno za određenu svrhe obrade, o čemu se treba obavijestiti ispitanika u informaciji o privatnosti koju treba predati ispitaniku na koga se ti podaci odnose.

U odnosu na svaku kategoriju osobnih podataka, Organizacija kao voditelj obrade primjenjuje pravila određena u informacijama danim ispitanicima, kao i pravila određena ovim Pravilnikom. Nakon proteka roka za čuvanje podataka osobni se podaci moraju izbrisati i/ili anonimizirati.

Voditelj obrade mora:

a) odrediti rok čuvanja podataka vezan za svaku zasebnu kategoriju osobnih podataka;

b) osigurati uredno bilježenje roka čuvanja podataka u registru podataka na kojemu su pohranjeni podaci, zajedno s povezanom dokumentacijom;

c) uključiti u postupak Službenika za zaštitu podataka kako bi se usvojile odgovarajuće mjere u svrhu sprječavanja da se podaci čiji je rok pohrane istekao koriste u druge svrhe osim ispunjenja zakonskih obveza;

d) osigurati brisanje tih podataka nakon isteka relevantnog razdoblja čuvanja podataka.

O provođenju gornjih radnji mora postajati mogućnost dokazivanja njihova izvršenja u dokumentiranom obliku.

Kada nastupa kao Izvršitelj obrade, Organizacija mora odmah uništiti ili vratiti sve osobne podatke obrađene u ime Voditelja obrade nakon isteka sporazuma s tim voditeljem obrade, osim ako mjerodavno pravo ne nalaže pohranu tih podataka.

4.7 UGOVORNI AKTI – SMJERNICE ZA IMENOVANJE TREĆE STRANE IZVRŠITELJEM OBRADE

4.7.1 Imenovanje Izvršiteljem obrade

Kada dobavljač pristupa osobnim podacima koje obrađuje Organizacija, Organizacija mora osigurati da je ta strana prikladna za obradu osobnih podataka u ime Organizacije u skladu s primjenjivim propisima tako da se:

a) osigura da dobavljač prema pravilima Organizacije, bilo kao dio postupka kvalifikacije dobavljača, prije ulaženja u ikakav odnos s dobavljačem ili nakon ulaska u poslovni odnos, ispuni upitnik za provjeru, tzv. „check listu“ (elektronički ili na papiru) s informacijama o društvu, uključujući i sve informacije vezane za neku treću stranu koju taj dobavljač koristi, a da ima pristup podacima – tzv. podizvršitelji obrade. Odjel nabave ili ured odgovoran za ugovorni odnos moraju trećoj strani predati spomenuti upitnik za provjeru.

b) provedu daljnje provjere prema odluci Organizacije u suradnji s odjelom nadležnim za nabavu i Službenikom za zaštitu podataka. Ugovor s dobavljačem ne može se sklopiti ako gore navedene provjere pokažu da nije dovoljno zajamčeno pridržavanje propisa iz područja zaštite osobnih podataka, bilo iz tehničkih, organizacijskih ili drugih razloga.

U svakom slučaju, svaki takav sporazum o obradi osobnih podataka mora prethodno odobriti Službenik za zaštitu podataka, koji također treba komunicirati s odjelom nadležnim za nabavu kako bi ishodio primjerak predloška sporazuma kojim se osigurava valjano postupanje s podacima koje je prikupio Voditelj obrade, odnosno Organizacija.

Ured odgovoran za ugovorni odnos s dobavljačem (Odjel nabave) mora Službeniku za zaštitu podataka dati primjerak potpisanog sporazuma o obradi osobnih podataka u svrhe arhiviranja.

Imenovanje izvršiteljem obrade je neophodno primjerice prilikom sklapanja ugovora s informacijsko-tehnološkim savjetnicima, pružateljima informacijsko-tehnoloških usluga, trgovcima, dobavljačima kao što su to dobavljači financijskih usluga, pružatelji usluga, marketinške agencije, itd.

4.7.2 Imenovanje podizvršiteljem obrade

Kada Organizacija nastupa kao Izvršitelj obrade, kako bi postavila drugog izvršitelja obrade (tj. podizvršitelja), mora potvrditi da je taj podizvršitelj podoban za obradu osobnih podataka u ime Organizacije, ali i u ime relevantnog voditelja obrade. U tu svrhu, moraju se dodatno poduzeti i sljedeće radnje:

a) Vlasnik procesa mora prije odobravanja provedbe sporazuma s podizvršiteljem provjeriti je li postavljanje tog podizvršitelja odobrio klijent - voditelj obrade općenitim odobrenjem sadržanim u sporazumu između Organizacije i Voditelja obrade (npr. sporazum sadrži izričito odobrenje za postavljanje određene kategorije podizvršitelja obrade) te u slučaju da ne postoji općenito odobrenje, posebno se odobrenje mora ishoditi od Voditelja obrade;

b) U slučaju da je podizvršitelj obrade uredno odobren od Voditelja obrade u skladu s točkom a), odjel nabave ili ured odgovoran za ugovorni odnos mora imenovati tog podizvršitelja, a koje imenovanje će biti evidentirano u sporazumu između Organizacije i podizvršitelja, a koji sadrži iste obveze prikazane u sporazumu između Organizacije i Voditelja obrade. Svaku izmjenu tog predloška mora odobriti Službenik za zaštitu podataka sukladno gore navedenoj točki a).

Tijekom provjera koje provodi Organizacija mora se pridati posebna pažnja radnjama koje provode podizvršitelji obrade: ukoliko se utvrdi da podizvršitelj ne ispunjava svoje obveze zaštite osobnih podataka, Organizacija odgovara Voditelju obrade za obveze podizvršitelja obrade.

4.8 OSOBE ZADUŽENE ZA NADZOR NAD PRIDRŽAVANJEVM PROPISA O ZAŠTITI OSOBNIH PODATAKA – VLASNIK PROCESA I SLUŽBENIK ZA ZAŠTITU OSOBNIH PODATAKA

Iako Organizacija u trenutku donošena ovog Pravilnika nije zakonski obvezna postaviti službenika za zaštitu osobnih podataka jer prema člancima 37.-39. Opće uredbe o zaštiti podataka:

a) nije tijelo javne vlasti ni javnopravno tijelo;

b) osnovne radnje Organizacije ne sastoje se od obrade podataka koji prema svojoj prirodi, opsegu i/ili svrsi zahtijevaju redovito i sustavno praćenje ispitanika na velikoj skali; i

c) osnovne radnje Organizacije ne sastoje se od obrade na velikoj skali posebnih kategorija osobnih podataka sukladno članku 9 Opće uredbe o zaštiti podataka i osobnih podataka vezanih za kaznenu osuđivanost i djela na koja se odnosi članak 10 Opće uredbe o zaštiti podataka;

Organizacija je imenovala Službenika za zaštitu podataka u cilju što kvalitetnijeg izvršenja svih obveza Organizacije u vezi sa zaštitom podataka.

Kako bi se pratilo pridržavanje Opće uredbe o zaštiti podataka, svaki vlasnik procesa unutar Organizacije na odgovarajući je način upućen o tome kako postupati u pitanjima zaštite osobnih podataka. U situacijama gdje je to potrebno, vlasnik procesa treba se savjetovati sa Službenikom za zaštitu podataka, voditeljem pravnog odjela a po potrebi i uputi svojih internih funkcija unutar Organizacije i sa regulatornim tijelom.

Službenik za zaštitu podataka Organizacije mora se brzo i odgovarajuće uključiti u sva pitanja koja se tiču zaštite osobnih podataka. Službenik za zaštitu podataka je, između ostaloga, zadužen za obavljanje sljedećih zadataka:

a) obavještavanje i savjetovanje u odnosu na obveze koje proizlaze iz Opće uredbe o zaštiti osobnih podataka kao i iz drugih odredbi koje se odnose na obradu osobnih podataka;

b) podrška Organizaciji u zadaćama praćenja i pridržavanja primjenjivih propisa koji reguliraju zaštitu osobnih podataka kako bi se izbjegle povrede te posljedični rizici za subjekte Organizacije;

c) povećanje svjesnosti o obvezama vezanim za privatnost i provedba edukacija u vezi sa zaštitom osobnih podataka;

d) davanje mišljenja, ako tako zatraži Organizacija, vezano za izradu procjene utjecaja na zaštitu osobnih podataka;

e) suradnja s klijentima i Organizacijom u svrhu osiguravanja pridržavanja načela tehničke i integrirane zaštite privatnosti;

f) suradnja s nadležnim regulatornim tijelom za zaštitu osobnih podataka;

g) izvršavanje uloge nadležne funkcije za kontakt s nadležnim regulatornim tijelom za zaštitu osobnih podataka i za kontakt s klijentima za sva pitanja u vezi obrade osobnih podataka, uključujući prethodne konzultacije kako je propisano člankom 36. Opće uredbe o zaštiti podataka;

h) podnošenje izvještaja upravi Organizacije o statusu pridržavanja Opće urede o zaštiti podataka te dostava relevantnih informacija, dokumenata te novosti vezanih za pridržavanje Uredbe (uključujući informacije o zahtjevima ili istragama nadležnog tijela za privatnost.

Službenik za zaštitu podataka i pojedini vlasnik procesa moraju biti uključeni u implementaciju svih postupaka vezanih za obradu osobnih podataka kako bi se (i) osiguralo da se Organizacija pridržava obveza određenih primjenjivim propisima i (ii) izbjegao rizik povrede osobnih podataka.

U slučaju da je vlasnik procesa upoznat s povredom primjenjivih pravila o zaštiti osobnih podataka, takvoj povredi mora odmah po saznanju obavijestiti nadređenu osobu u Organizaciji i Službenika za zaštitu osobnih podataka.

Vlasnik procesa zajedno sa Službenikom za zaštitu podataka i voditeljem pravnog odjela predložit će plan korektivnih radnji potrebnih radi usklađenja s pravilima o zaštiti osobnih podataka, koji će se implementirati unutar Organizacije.

Vlasnik procesa mora sačuvati svu komunikaciju s nadležnim regulatornim tijelom za zaštitu osobnih podataka.

4.9 PRIDRŽAVANJE NAČELA TEHIČKE I INTEGRIRANE ZAŠTITE PRIVATNOSTI (Data protection by design and by default)

Svi subjekti unutar Organizacije koji započinju neku novu aktivnost i/ili namjeravaju razviti novi proizvod ili uslugu koji uključuju obradu osobnih podataka moraju slijediti sljedeća načela:

a) Tehnička zaštita privatnosti: svaka aktivnost, proizvod i usluga moraju se razvijati tako da se zaštita osobnih podataka uzima u obzir već od faze dizajna (početne faze razvoja);

b) Integrirana zaštita osobnih podataka: svaka aktivnost, proizvod i usluga mora implementirati mjere kako bi se osiguralo da se obrađuju samo oni osobni podaci koji su potrebni za predmetnu svrhu obrade, što se procjenjuje posebno u odnosu na količinu prikupljenih osobnih podataka, na raspon njihove obrade, na razdoblje pohrane i na mogućnost pristupa tim podacima.

Vlasnik procesa uz savjetovanje sa Službenikom za zaštitu podataka mora procijeniti je li potrebno:

a) provesti procjenu utjecaja na privatnost; i

b) ako je potrebno, uključiti osoblje iz drugih odjela u procjenu utjecaja na zaštitu osobnih podataka, pritom osiguravajući da se redovni sastanci održavaju tijekom razvoja proizvoda/usluge, u svrhu provođenja sljedećih aktivnosti:

   i) analize rizika vezanih za obradu osobnih podataka koji proizlaze iz novog proizvoda/usluge;

   ii) izrade plana aktivnosti prema kojemu je potrebno implementirati korektivne mjere kako bi se u potpunosti otklonili rizici ili, ako to nije moguće, barem minimizirali;

   iii) izvršenja kontrole li novi proizvod ili usluga razvijen u skladu s planom aktivnosti.

c) po završetku radnji navedenih pod a), Vlasnik procesa mora poslati Službeniku za zaštitu podataka izvještaj u kojem će ukratko opisati na koji način su se riješila pitanja vezana za zaštitu osobnih podataka koja su se pojavila tijekom radnje opisane pod a).

Opisani postupak mora se poštivati u odnosu na sve promjene ili ažuriranja postojećih proizvoda, usluga ili radnji koji pri izvršenju dovode do promjene u količini ili vrsti obrađenih osobnih podataka ili do postupka za obradu osobnih podataka.

Zabranjeno je razvijati ili provoditi radnje povezane s bilo kojim novim proizvodom, uslugom alatom ili tehničkom aplikacijom koji su usmjereni prema kupcima ili zaposlenicima ili koji na drugi način dovode do obrade osobnih podataka, a da se pritom ne prati postupak prikazan u ovom odjeljku.

Vlasnik procesa mora uredno dokumentirati i pokrenuti gornji postupak te osigurati da korisnici i odjeli koji će biti uključeni mogu lako pristupiti platformi na kojoj su dokumentirani postupci i procjene od strane korisnika kako bi dali svoj doprinos i dovršili svoje zadaće.

4.10 IZVRŠENJE PROCJENE UTJECAJA NA PRIVATNOST

Ako tijekom ili nakon analize iz odjeljka 4.9 c), ili u nekim drugim okolnostima vlasnik procesa u suradnji sa Službenikom za zaštitu podataka procijeni da je potrebno izvršiti procjenu utjecaja na privatnost (PUP) u skladu s člankom 35 Uredbe, Procjena utjecaja na privatnost će se izvršiti prema sljedećim kriterijima (navedeni primjerice):

Primjeri situacija koje zahtijevaju obradu	Mogući relevantni kriteriji
Društvo koje sustavno prati radnje svojih zaposlenika, uključujući i praćenje radnih mjesta zaposlenika, aktivnost na internet itd.	- sustavno praćenje - podaci vezani za ranjive ispitanike
Obrada podataka prikupljenih na društvenim mrežama – javni podaci o aktivnosti na društvenim medijima za stvaranje profila.	- evaluacija ili bodovanje - obrada podataka na velikoj skali - Matching or combining of datasets.
Institucija koja na nacionalnoj razini stvara kreditni rejting ili bazu podataka o prijevarama	- evaluacija ili bodovanje - automatizirano odlučivanje s pravnim ili slično značajnim učinkom - spriječava se ispitanik da iskoristi pravo, koristi uslugu ili ugovor a right or using a service or a contract
Pohrana u svrhe arhiviranja pseudonimiziranih osobnih osjetljivih podataka vezano za ispitanike u istraživačkim projektima ili kliničkim studijama	- osjetljivi podaci - podaci vezani za ranjive ispitanike - sprječava ispitanika da iskoristi pravo, koristi uslugu ili ugovor

Kada nastupa kao Izvršitelj obrade, Organizacija, na traženje Voditelja obrade, mora pomoći Voditelju obrade pri vršenju PUP-a i pritom uzeti u obzir prirodu obrade i informacije dostupne izvršitelju.

4.11 UPRAVLJANJE I PRAĆENJE E-MAIL ADRESE NAMIJENJENE ZA KOMUNIKACIJU VEZANU ZA PITANJA PRIVATNOSTI

Zaposlenici i savjetnici Organizacije sva pitanja i zahtjeve koji se odnose na obradu njihovih podataka ili bilo što drugo povezano s privatnosti podataka trebaju dostavljati na sljedeću e-mail adresu:

privatnost@profil-klett.hr

Službenik za zaštitu podataka prati navedenu e-mail adresu kako bi osigurao da se dolazna pošta stalno analizira te da se brzo obradi ili proslijedi nadležnim odjelima.

4.12 PRAĆENJE I IZVJEŠTAVANJE

Svaki vlasnik procesa mora periodično provjeravati aktivnosti vezane za obradu podataka koje provodi Organizacija.

Vlasnik procesa, u svim hitnim slučajevima (kao primjerice u slučaju povrede osobnih podataka – tzv. „Data breach“ situacije) mora poslati Službeniku za zaštitu podataka i voditelju pravnog odjela izvještaj u kojem će navesti između ostalog: (i) sve situacije gdje se dogodila povreda pri obradi osobnih podataka i povezane korektivne mjere, (ii) opisati predmetne značajne rizike ili probleme pri obradi osobnih podataka, (iii) navesti sve provedene procjene utjecaja na privatnost te one preporučene, i (iv) navesti eventualne nove projekte i opisati njihovu usklađenost s načelima tehničke i integrirane zaštite podataka.

4.13 BILJEŽENJE RADNJI OBRADE PODATAKA

Organizacija mora formirati bazu podataka o radnjama obrade podataka i redovno je ažurirati. Radnje obrade koje provodi Organizacija kao Voditelj obrade moraju biti odvojene od onih radnji koje Organizacija provodi kao Izvršitelj obrade u ime klijenta. U tu svrhu svaki vlasnik procesa kojeg je odredila Organizacije mora biti zadužen za stvaranje, ispunjavanje i održavanje dviju različitih baza o obradi podataka koje spadaju pod područje odgovornosti pojedinog vlasnika procesa:

a) Bilješka o radnjama obrade kao Voditelja obrade:

Bilješka o radnjama obrade Organizacije koja nastupa kao Voditelji obrade mora sadržavati sljedeće informacije:

i) ime i podatke o kontaktu Voditelja obrade (tj. Organizacije) i, gdje je to primjenjivo, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka, ako je imenovan;

ii) svrhu obrade;

iii) opis kategorija ispitanika i kategorija osobnih podataka;

iv) kategorije primatelja kojima se daju ili moraju biti dani osobni podaci, uključujući primatelje iz treće zemlje;

v) gdje je to primjenjivo, prijenose osobnih podataka u treću zemlju s naznakom treće zemlje te dokumentacijom vezanom za odgovarajuća jamstva;

vi) rokove za brisanje raznih kategorija osobnih podataka; i

vii) općeniti opis usvojenih sigurnosnih tehničkih i organizacijskih mjera.

b) Bilješka o radnjama obrade kao Izvršitelja obrade:

Bilješka o radnjama obrade subjekata Organizacije koji nastupaju kao izvršitelji obrade mora sadržavati sljedeće informacije:

i) ime i podaci o kontaktu izvršitelja obrade (tj. Organizacije) te svakog voditelja obrade u čije ime izvršitelj obrade djeluje i, gdje je to primjenjivo, predstavnika voditelja ili izvršitelja obrade i službenika za zaštitu podataka, ako je imenovan;

ii) kategorije obrade provedene u ime svakog voditelja obrade;

iii) gdje je to primjenjivo, prijenose osobnih podataka u treću zemlju s naznakom treće zemlje i dokumentacijom vezanom za prikladna jamstva;

iv) općeniti opis usvojenih sigurnosnih tehničkih i organizacijskih mjera.

Predmetni vlasnik procesa odgovoran je za ažuriranje navedenih baza podataka.

5. ODJELJAK 2 - PRAVILA ZA ODGOVARAJUĆU POHRANU DOKUMENATA DRUŠTVA

5.1 POHRANA

Organizacija mora osigurati da se svi korisnici pridržavaju sljedećih pravila vezanih za sigurnost i zaštitu podataka u Organizaciji:

a) ladice u stolu, ormarići, ostali spremnici i uredi u kojima se nalaze dokumenti koji sadrže povjerljive podatke ili osobne podatke korištene za radnje Organizacije moraju biti zaključani;

b) dokumenti koji sadrže osobne podatke ne smiju se ostaviti na stolu, posebice u slučaju odsustva s posla, već se moraju držati u ladicama u stolu i arhivima koji moraju biti zaključani;

c) pristup arhivima gdje se drže osobni podaci mora biti ograničen samo na zaposlenike čiji je pristup opravdan njihovim radnim zadatkom;

d) dokumenti uklonjeni iz arhiva ili kabineta moraju se pohraniti čim je njihova potrebna uporaba gotova, a arhivi ili kabineti moraju biti zaključani;

e) zabranjeno je koristiti USB-memorijske stick-ove, memorijske kartice, vanjske tvrde diskove, uređaje, laptope, računala i uređaje za pohranu podataka osim ako ih informacijsko-tehnološki odjel predmetnih subjekata Organizacije posebno odobrio ili nabavio;

f) nije dopušteno prenositi podatke sadržane unutar ili na bilo koji način povezane s radnim zadatkom na privatne USB-memorijske stick-ove, memorijske kartice, vanjske tvrde diskove, uređaje ili računala, privatne račune e-pošte ili bilo koje račune osim onog zadanog od predmetnog subjekta Organizacije, na internetske platforme za spremanje podataka (npr. Dropbox) i općenito na bilo koji uređaj, platforma ili račun koji ne dolaze od subjekata Organizacije;

g) zabranjeno je spremiti bilo koji dokument, datoteku ili sadržaj na računalo društva ili uređaj dan od Organizacije za provedbu radnog zadatka, već se oni smiju spremiti samo u mrežne datoteke;

h) dokumenti koji sadrže povjerljive informacije ili osobne podatke o društvima Organizacije moraju se što prije ukloniti iz printera;

i) dokumenti, elektronički uređaji i uređaji za pohranu podataka ne smiju se ostaviti u sobama za sastanke te mjestima koja se nalaze izvan neposredne kontrole predmetnog korisnika;

j) dokumenti, informacije ili osobni podaci povezani s radnim zadatkom koji provode subjekti Organizacije ne smiju se fotografirati, snimati video uređajem ili općenito snimati ni na koji način;

k) mora se posebno voditi računa o tome da se izbjegne da gore nabrojani dokumenti, elektronički uređaji i uređaji za pohranu podataka postanu dostupni osobama koje u tu svrhu nisu dobile izričito odobrenje ili da se isti ostavljaju na nedozvoljenim mjestima u uredima ili na putu, na javnim mjestima ili drugim lokacijama dostupnima javnosti;

Službenik za zaštitu podataka mora pratiti pridržavanje gore opisanih obveza te pisano obavijestiti Upravu Organizacije u slučaju bilo kakve povrede. Uprava i Službenik za zaštitu podataka moraju zajedno s odjelom ljudskih resursa koordinirati svaku disciplinsku mjeru te s voditeljem pravnog odjela procijeniti svaki daljnji postupak.

Organizacija mora osigurati da arhivima ne mogu pristupiti neovlaštene osobe izvan relevantnog odjela. U slučaju odsustva s posla, imenovana osoba mora odrediti zamjenu koja ima pravo pristupa arhiviranim podacima.

6. ODJELJAK 3 – PRAVILA ZA ODGOVARAJUĆU UPORABU INFORMACIJA, SUSTAVA I USLUGA ORGANIZACIJE

6.1 DOPUŠTENA UPORABA

6.1.1 Svrha

Organizacija mora osigurati da svi korisnici slijede dolje navedena pravila vezana za informacijsku sigurnosti unutar Organizacije.

6.1.2 Tehnološki uređaji

Svi su korisnici odgovorni su za upravljanje i čuvanje tehničkih uređaja koji im je povjerila Organizacija za provedbu radnih zadataka. Takvi uređaji uključuju računala i/ili prijenosne uređaje poput laptopa, pametnih mobitela, tableta, tokena ili vanjskih memorija. Korisnici moraju:

a) osigurati da se prijenosni uređaji uvijek čuvaju na zaštićenom mjestu (npr. tijekom putovanja, u uredu izvan radnog vremena ili izvan ureda) te se pobrinuti da nisu izloženi daljnjim rizicima kao što je to ostavljanje uređaja u automobilu bez nadzora;

b) uvijek zaključati (npr. pritiskom na tipke Ctrl+Alt+Del) ili ugasiti računalo prije nego što ga se ostavi bez nadzora;

c) ugasiti svoje računalo na kraju svakog radnog dana;

d) suzdržati se od pokušaja uklanjanja, deinstalacije, onesposobljavanja, kršenja ili zaobilaženja mjera implementirane za zaštitu uređaja;

e) suzdržati se od spajanja svojih uređaja na mreže ili sustave koji nisu sigurni i/ili pouzdani;

f) izbjegavati spajanje bilo kojeg osobnog uređaja i uređaja treće strane, uključujući mobilne uređaje i vanjske memorije na uređaje i mreže Organizacije;

g) suzdržati se od pokušaja instalacije aplikacija ili softvera na uređaje društva. Samo služba za podršku u Organizaciji ima odobrenje instalirati softver na uređaje Organizacije.

6.1.3 Korisnički računi

Većina korisnika Organizacije mora imati pristup – unutar granica koje su potrebne za provedbu njihovog radnog zadatka – sustavima i uslugama i stoga i osobnim podacima jednog ili više subjekata Organizacije. Pristup računalnim sustavima dopušten je samo s jedinstvenim identitetom i lozinkom. Korisnički računi postavljeni su tako da svaki korisnik može imati pristup samo informacijama za provedbu svog radnog zadatka te se slijedom toga gore navedene vjerodajnice moraju adekvatno zaštititi. Konkretno, korisnici se moraju:

a) suzdržati od dijeljenja, komuniciranja ili provođenja ikoje radnje koja može dovesti do toga da treća strana nabavi njihove vjerodajnice, uključujući i članove obitelji ili njima bliske osobe;

b) u slučaju sumnje da su im vjerodajnice kompromitirane, smjesta promijeniti PIN i lozinku;

c) suzdržavati od pristupa ili pokušaja pristupa informacijama, sustavima i uslugama Organizacije za pristup kojima nemaju odobrenje;

d) suzdržati od korištenja računa drugih korisnika ili provođenja drugih radnji povezanih s računom koji im ne pripada;

e) suzdržati od ponovnog korištenja ili kopiranja njihovih vjerodajnica za račun (npr. korisničkog identiteta i lozinki) kako bi stvorili druge, posebice osobne račune, kao i od spremanja ili kopiranja njihovih vjerodajnica na uređaje, dokumente i druga pomagala;

f) suzdržati od korištenja iste lozinke sa svog osobnog računa za njihov račun pri društvu;

g) suzdržati od korištenja javnih računala za pristup informacijama, sustavima i uslugama subjekata Organizacije;

h) pobrinuti da su sve lozinke i PIN-ovi u skladu sa zahtjevima lozinki Organizacije, kao što je to definirano u donjim paragrafima.

Organizacija je usvojila sustave obavještavanja koji (i) sprečavaju nedopušten pristup podacima za koji korisnik nema odobrenje i (ii) prijavljuju sve sumnjive uporabe uređaja nadležnom odjelu.

6.1.4 Korisničke lozinke

Korisničke lozinke za sustave Organizacije moraju slijediti prikladan format koji je određen posebnom odlukom Organizacije koja je obvezujuća za sve korisnike u Organizaciji.

6.1.5 Lozinka/PIN za mobilne uređaje

Lozinke i PIN-ovi za mobilne uređaje (npr. pametni telefon, i tablet) moraju slijediti uvjete određene posebnom odlukom Organizacije koja je obvezujuća za sve korisnike u Organizaciji.

Elektronička komunikacija

Poslovne aktivnosti Organizacije zahtijevaju sposobnost efikasne komunikacije s ljudima, zaposlenicima, klijentima i poslovnim partnerima. Elektronički kanali komunikacije poput e-mailova i instant poruka olakšavaju dnevni tijek komunikacija unutar, ali izvan organizacije. Pri elektroničkom komuniciranju informacija korisnici moraju:

a) zaštititi informacije prema njihovoj klasifikaciji;

b) suzdržati se od slanja dokumenata, informacija ili osobnih podataka e-porukom ili drugim komunikacijskim sredstvima osim ako:

i) nisu adekvatno zaštićene koristeći kriptografski sustav Organizacije i;

ii) ne postoji ugovor o povjerljivosti s predmetnom trećom stranom.

c) suzdržavati se od slanja informacija, dokumenata i osobnih podataka vezano za radni zadatak iz bilo kojeg razloga, uključujući i rad na daljinu, na račune e-pošte ili račune koji im nije zadala Organizacija. Pristup na daljinu može se zatražiti i odobriti pismenim putem slijedom određenog zahtjeva;

d) suzdržavati se od automatiziranih sustava prosljeđivanja/slanja informacija koje se tiču radnih zadataka izvan Organizacije;

e) suzdržavati se od slanja, pokušaja nabave ili pristupa neprikladnom materijalu ili materijalu koji bi mogao biti prijeteći ili zastrašujući prema druge osobama ili ih zlostavljati.

Obratiti pažnju pri primitku priloga, e-mail poruka i poveznica koje nisu zatražene, i od poznatih i od nepoznatih izvora. U slučaju sumnjivih e-poruka, nije dopušteno , otvarati ili skidati priloge te nipošto nije dopušteno slijediti poveznice. Internet, društvene mreže i mediji

Organizacija mora osigurati da se svi korisnici pridržavaju uputa Organizacije i primjenjivih pravila vezanih za korištenje interneta, društvenih mreža i medija koji bi trebali regulirati uvjete za pristup i korištenje društvenih medija (poput Facebooka, Twittera, YouTubea, itd.) putem radnih uređaja i mreža.

Korisnicima pri navedenom korištenju nije dozvoljeno:

a) pokušati pristupiti stranicama i sadržajima koji sadrže neprikladan materijal poput kockanja ili pornografskih stranica kao i stranica koje promiču nasilna ili diskriminatorna ponašanja;

b) izdati ili objaviti diskriminatorne izjave, objaviti informacije ili sudjelovati u radnjama koje bi mogle oklevetati ili naštetiti ugledu Organizacije, osobama i trećim stranama koje surađuju s Organizacijom. To uključuje ponašanja na internetu i/ili na društvenim mrežama i medijima i izvan radnog vremena;

c) koristiti unutarnje ili vanjske društvene mreže i forume na neodgovoran način te kršeći primjenjive propise i/ili obveze Organizacije;

d) dijeliti informacije, dokumente i osobne podatke vezane za kupce, zaposlenike ili dobavljače subjekata, uključujući i povjerljive informacije subjekata na internetu, na društvenim mrežama ili medijima osim ako to nije dopušteno posebnom odlukom Organizacije ili nekim primjenjivim pravilnikom Organizacije;

e) koristiti korisnički račun Organizacije da bi se registrirali na društvene mreže i/ili vanjske forume ako to nije dopušteno posebnom odlukom ili primjenjivim pravilnikom Organizacije;

f) namjerno objavljivati, slati ili primati, stavljati na internet/skidati s interneta, nabavljati, spremiti ili dijeliti bilo koji sadržaj ili materijal koji krši, neprimjereno koristi ili na drugi način povrjeđuje prava na intelektualno vlasništvo, privatnost i povjerljivost bilo kojeg pojedinca, skupine ili subjekta, uključujući i Organizaciju.

Ako postoje sumnje u buduće ponašanje ili u način na koji se druge osobe trebaju ponašati na internetu i društvenim medijima, potrebno je obavijestiti Službenika za zaštitu podataka.

6.1.6 Osobna uporaba informacijsko-tehnoloških sustava društva

i) Subjekti Organizacije moraju osigurati da se svi korisnici pridržavaju posebnih odluka i pravilnika Organizacije koji trebaju regulirati uvjete za osobnu uporabu sustava i usluga Organizacije.

6.1.7 Upravljanje povjerljivim i/ili osjetljivim informacijama

Organizacija često upravlja i obrađuje informacije osjetljive ili povjerljive prirode. To između ostalog uključuje i:

a) informacije o pojedincu koje su predmetom zakona i propisa o privatnosti;

b) osjetljive komercijalne i financijske informacije koje bi mogle dovesti do kazni ako se njima ne upravlja na prikladan način;

c) materijal zaštićen intelektualnim vlasništvom koji predstavlja značajno ulaganje Organizacije.

Upravljanje i obrada povjerljivih i/ili osjetljivih informacija mora se provoditi uz pridržavanje sljedećih pravila:

a) ne koristiti informacije koje su povjerljive ili na bilo koji način povezane s radnim zadatkom, iz bilo kojeg razloga koji nije povezan s tim radnim zadatkom;

b) upravljati svim informacijama, u elektroničkom i papirnatom obliku, u skladu s odredbama ovog Pravilnika;

c) odnositi se prema informacijama, dokumentima i datotekama povezanima s radnim zadacima koji još nisu klasificirani kao povjerljivi s maksimalnom revnošću i pažnjom;

d) pohranjivati dokumente u skladu s odredbama ovog Pravilnika;

e) ne otkrivati povjerljive informacije (npr. omogućavajući da se vidi računalni zaslon) ili razgovarati o njima na javnim mjestima;

f) pobrinuti se da su informacije ispravno spremljene. U tu je svrhu potrebno spremiti dokumente na mrežu društva radije nego putem sredstava dodijeljenih za osobnu upotrebu kao što je e-mail društvo ili tvrdi disk dodijeljenog računala.

Ako postoje sumnje oko primjenjivih rokova pohrane, potrebno je kontaktirati Službenika za zaštitu podataka ili vlasnika procesa.

6.1.8 Prijava povrede osobnih podataka („Data breach“)

U slučaju povrede osobnih podataka, sigurnosnog incidenta, kršenja primjenjivih propisa i/ili ovog Pravilnika, ili iz bilo kojeg drugog razloga koji je izazvao povredu osobnih podataka, korisnici moraju odmah obavijestiti direktno Službenika za zaštitu podataka ili tako da pošalju e-poruku na adresu e-pošte koju je Organizacija dodijelila u tu svrhu. Korisnik mora opisati okolnosti pod kojima je došlo do povrede osobnih podataka uključujući, gdje je to moguće, kategorije i približan broj ispitanika u pitanju i kategorije i približan broj bilježaka o osobnim podacima u pitanju. Primjerice, povreda osobnih podataka uključuje sljedeće slučajeve:

a) gubitak ili krađu dokumenata koji sadrže osobne podatke ili gubitak ili krađu osobnih uređaja ili uređaja Organizacije (npr. mobilnih uređaja, računala, tablet, itd.);

b) neovlašteni unutarnji ili vanjski pristup mreži (npr. hakiranje) Organizacije ili neko drugo kršenje IT sustava koji bi mogli uzrokovati gubitak, kompromitiranje, pristup ili otkrivanje osobnih podataka ili informacija;

c) instalacija malicioznog softvera ili virusa skinutih na uređaje dodijeljenih od Organizacije;

d) sumnjivi e-mailovi ili telefonski pozivi u kojima se traži od korisnika da daju informacije;

6.2 bilo kakva povreda obveznih sigurnosnih provjera informacija koja može dovesti do gubitka ili kompromitiranja informacija.SIGURNOSNI SUSTAVI ZA E-PORUKE

Organizacija se mora pobrinuti da se svi korisnici pridržavaju sljedećih pravila i uputa:

a) Sustav e-pošte jedino je dostupan unutar mreže društva putem uređaja izravno povezanih s tom mrežom ili preko VPN veza odobrenih od ovlaštenih osoba u informacijsko-tehnološkom odjelu.

b) Korisnici opremljeni korporativnim pametnim mobitelima mogu slati i primati e-mail poruke, a da nisu povezani s korporativnom mrežom.

Sustav e-pošte opremljen je sigurnosnim mjerama usmjerenima na čuvanje integriteta sustava poput antivirusnog softvera i softvera protiv neželjene pošte („anti-spam software“).Software protiv neželjene pošte provodi između ostalog sljedeće operacije:

a) uspoređuje adrese porijekla poruke s popisom koji sadrži popis nepoznatih pošiljatelja, a poruke koje dolaze od nepoznatih izvora se uklanjaju.

b) čita riječi (zamišljene kao nizovi znakova, a ne značenja) u porukama i uspoređuje ih s popisom “zabranjenih” riječi. Bodovi su dodijeljeni svakom nizu “zabranjenih” znakova koje je softver identificirao. Ukupni bodovi dodijeljeni tekstu poruke određuju mora li se poruka isporučiti ili ukloniti.

Softver protiv neželjene pošte čita označitelja poruke, a ne značenja.Antivirusni softver analizira sadržaj priloga poruka te ako identificira maliciozne kodove (program ili skup uputa koji mogu uzrokovati štetu računalu) pokušava ih ukloniti; ako nije moguće ukloniti virus, prilog se briše.

Uporaba takvih softvera ima isključivu svrhu očuvanja korporativnih sustava Organizacije.

Sigurnosna kopija poslužitelja e-pošte te podataka sačuvanih na njemu (npr. sadržaj „osobnih sandučića pošte“, a ne „osobnih direktorija“) stvara se svaki dan.

6.3 SIGURNOSNI SUSTAVI NA INTERNETU

Organizacija se mora pobrinuti da se svi korisnici pridržavaju sljedećih pravila i uputa:

a) Pristup internetu dopušten je korisnicima koji su za to ovlašteni od ovlaštenog voditelja Organizacije samo unutar granica pristupnog profila koji im je omogućen te jedino kako bi izvršili svoj radni zadatak te uvijek u skladu s unutarnjim postupcima i mjerodavnim zakonima.

b) U svrhu očuvanja integriteta sustava pristup internetu je opremljen sigurnosnim sustavima poput proxy-poslužitelja, softvera koji filtrira sadržaj te vatrozida.

Moguće je implementirati filtere kako bi se blokirao pristup korisnicima na potencijalno opasne stranice.

Proxy-poslužitelj osigurava (i) praćenje aktivnosti korisnika (proxy-dnevnici), ne kako bi se nadzirala njihova aktivnost, već kako bi se mogle pratiti prijetnje s interneta u slučaju neispravnosti i (ii) blokiranje pristupa stranicama čiji sadržaj se ne smatra korisnim za radni zadatak (stranice sa sadržajem vezanim za npr. seks, oružje, nasilje, itd).

Informacije o korištenju interneta (porijeklo i destinacija – proxy-dnevnik) moraju biti zabilježeni te ih se mora čuvati unutar razdoblja od 24 mjeseca.

Ovaj Pravilnik stupa na snagu dana 25. svibnja 2018. godine.

Direktor

Dalibor Greganić

REFERENCE:

1. Uredba (EU) 2016/679 Europskog parlamenta i Vijeća 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)**
2. Smjernice o prenosivosti podataka (WP Članak 29 od 05.04.2017.- Guidelines on the portability of data regarding the Working Party under Article 29 of 5 April 2017);
3. Smjernice o službenicima za zaštitu podataka (WP Članak 29 od 05.04.2017 - Guidelines on the data protection officers of the Working Party under Article 29 of 5 April 2017);
4. Smjernice o Glavnom nadzornom tijelu (WP Članak 29 od 05.04.2017 - Guidelines on the Lead Supervisory Authority of the Working Party under Article 29 of 5 April 2017);
5. Smjernice o Procjeni utjecaja na privatnost (WP Članak 29 od 05.04.2017- Guidelines on the data protection impact assessment (DPIA) and determining whether processing is likely to result in "high risk" for the purposes of Regulation no. 2016/679 of the Working Party under Article 29 of 5 April 2017 as last revised and adopted on 4 October 2017).

***