RELAXINO, uslužno trgovacki obrt
vl. Andreja Milas
Kumiciceva 2, 10 000 Zagreb
OIB: 55498825593

Pravilnik o sigurnosti osobnih podataka 1

Datum
25.05.2018

Uvodne odredbe

Ovim Pravilnikom se utvrđuje djelotvoran, odgovoran i transparentan okvir za osiguravanje usklađenosti s Općom uredbom o zaštiti osobnih podataka.

Ovaj Pravilnik primjenjuje se na sve organizacijske dijelove RELAXINO, uslužno trgovački obrt (u daljnjem tekstu VODITELJ OBRADE) te na sve zaposlenike, uključujući honorarne djelatnike i privremene radnike jednako kao i na sve vanjske suradnike koji djeluju u ime voditelja obrade.

Izjava o politici

Voditelj obrade posvećen je osiguranju sigurnosti podataka, u skladu sa svim zakonima, regulativama te najvišim standardima etičnog poslovanja.

Ovj pravilnik definira očekivano ophođenje zaposlenika voditelja obrade i njegovih vanjskih suradnika koji se bave prikupljanjem, upotrebom, čuvanjem, prijenosom, objavljivanjem ili uništavanjem bilo kakvih osobnih podataka koji pripadaju zaposlenicima i poslovnim partnerima voditelja obrade.

Svaki organizacijski dio voditelja obrade provesti će ovdje utvrđene fizičke, tehničke i organizacijske mjere kako bi osigurali sigurnost osobnih podataka. To uključuje prevenciju gubitka ili oštećenja podataka, nedopušten pristup, mijenjanje ili obradu podataka ili bilo koji drugi rizik kojemu su podaci izloženi od ljudskog ili prirodnog utjecaja.

Fizičke mjere zaštite

Voditelj obrade propisuje sljedeće mjere fizičke zaštite:

Tehičke mjere zaštite

Voditelj obrade propisuje sljedeće mjere tehničke zaštite:

ANTIVIRUSNA ZAŠTITA
Ovdje opisana pravila odnose se na poslužitelje, radne stanice i infrastrukturu u RELAXINO, uslužno trgovački obrt, uključujući prijenosna računala i tablete koji mogu biti korišteni izvan organizacije.

- Sva računala i uređaji koji pristupaju mreži RELAXINO, uslužno trgovački obrt moraju imati instaliranu antivirusnu zaštitu u skladu s najvišim standardima zaštite.
- Svi poslužitelji i radne stanice u vlasništvu RELAXINO, uslužno trgovački obrt ili trajno korišteni uređaji, moraju imati antivirusni program. Ovo pravilo se odnosi i na prijenosna računala koja se redovito povezuju s mrežom RELAXINO, uslužno trgovački obrt.
- Računala koja rade u mreži drugih organizacija mogu biti izuzeta od prethodnog pravila ako to zahtijevaju sigurnosna pravila druge organizacije, pod uvjetom da su ta računala također zaštićena.
- Svi instalirani antivirusni programi trebaju imati uključeno automatsko ažuriranje.
- Svi uređaji gostiju, posjetitelja i ostala privatna infrastruktura nad kojom RELAXINO, uslužno trgovački obrt nema nadzor mogu se spojiti samo na izdvojenu, za takve potrebe predviđenu internetsku mrežu. Nije dopušteno spajanje na glavnu mrežu RELAXINO, uslužno trgovački obrt.

KORIŠTENJE LOZINKI

- Sustavi koji obrađuju osobne podatke trebaju biti zaštićeni kontrolom pristupa koji se temelji na lozinki.
- Lozinke moraju biti sastavljene od kombinacije slova, brojeva i posebnih znakova (interpunkcijskih oznaka i simbola).
- Lozinke moraju imati kombinaciju velikih i malih slova.
- Lozinke ne bi trebale sadržavati očiti slijed znakova na tipkovnici (npr qwertz ili 12345)
- Lozinke ne bi trebale sadržavati podatke kao što su osobni podaci o sebi, članovima obitelji, kućnim ljubimcima, vašoj djeci, rođendanima, adresama, telefonskim brojevima, lokacijama i sl.
- Ne preporuča se korištenje iste lozinke za pristup različitim sustavima.
- Voditelji nisu ovlašteni tražiti, prikupljati i pohranjivati lozinke zaposlenika.
- Dozvoljeno je korištenje zajedničke lozinke za više operatera, ako je to poslovno opravdano.
- Strogo je zabranjeno dijeljenje lozinki. Lozinke se ne smiju otkrivati ili javno prikazivati.
- Zabranjeno je slanje lozinki elektroničkom poštom.
- Uvijek kada se lozinka smatra kompromitiranom, odmah se mora promijeniti.

Organizacijske mjere zaštite

Voditelj obrade propisuje sljedeće organizacijske mjere zaštite:

KORIŠTENJE INFORMATIČKE OPREME

- Sva informatička infrastruktura može se koristiti isključivo u poslovnim aktivnostima za koje je namijenjena
- Svaki korisnik je odgovoran za očuvanje i ispravnu upotrebu informatičke infrastrukture koja mu je dana na korištenje
- Sva informatička infrastruktura mora biti na mjestima s kontroliranim pristupom.
- Aktivna radna površina i prijenosna računala moraju biti osigurana ukoliko nisu pod nadzorom. Kada je god moguće, spomenuto pravilo mora se provoditi automatski.
- Pristup infrastrukturi nije dozvoljen neovlaštenim osobama. Dodjeljivanje pristupa informatičkoj infrastrukturi i računalnim mrežama mora se obaviti putem odobrenih i prihvaćenih postupaka za upravljanje uslugama informatičke infrastrukture i nadziranim upravljanjem pristupom.
- Korisnici se moraju prema infrastrukturi, koja im je povjerena na korištenje, odnositi s punom pažnjom, te s njom pažljivo rukovati te izbjegavati nepravilno korištenje.
- Posebna se pažnja mora posvetiti zaštiti prijenosnih računala, tableta, pametnih telefona i drugih prijenosnih uređaja od krađe ili gubitka. Također, u obzir treba uzeti druge rizike oštećenja infrastrukture te oštećenja koji mogu rezultirati povredom ili gubitkom podataka kao što su ekstremne temperature, magnetska polja ili padovi.
- Prilikom putovanja (avionom) prijenosna oprema poput prijenosnih računala, tableta ili pametnih telefona, mora ostati u posjedu korisnika kao ručna prtljaga
- Uvijek kada je moguće, neophodno je koristiti tehnologiju šifriranja i brisanja u slučaju gubitka ili krađe prijenosne infrastrukture.
- Gubitak, krađa, oštećenje, neovlašteno korištenje ili drugi incidenti moraju se, što prije od trenutka spoznaje, prijaviti voditelju informatičkog odjela.
- Zbrinjavanje imovine koja se više ne koristi mora se izvršiti u skladu s posebnim postupcima zbrinjavanja informatičkog otpada, uzimajući u obzir zaštitu svih informacija koji su predmet takvog oblika obrade. Imovina koja pohranjuje povjerljive podatke mora biti uništena u prisustvu člana tima za informacijsku sigurnost. Sredstva za čuvanje osjetljivih informacija moraju se prije odlaganja u potpunosti izbrisati u nazočnosti člana tima za informacijsku sigurnost

KORIŠTENJE VLASTITIH UREĐAJA

RELAXINO, uslužno trgovački obrt daje svojim zaposlenicima mogućnost kupnje i korištenja vlastitih pametnih telefona, tableta i laptopa po izboru, u poslovne svrhe društva. Istovremeno, RELAXINO, uslužno trgovački obrt zadržava pravo oduzimanja ove povlastice svima ili pojedincima ako se korisnici ne pridržavaju pravila i postupaka navedenih u nastavku.

RELAXINO, uslužno trgovački obrt definira prihvatljivu poslovnu uporabu kao uporabu u svrhe koje izravno ili neizravno podupiru poslovanje voditelja obrade.

RELAXINO, uslužno trgovački obrt definira prihvatljivu osobnu upotrebu u radnom vremenu zaposlenika ili vanjskog suradnika kao razumnu i ograničenu osobnu komunikaciju.

Zabranjuje se korištenje vlastite opreme:
• u svrhu kreiranja video ili zvučnih zapisa i fotografija u prostorijama voditelja obrade, ili na drugim mjestima u trenutku obavljanja poslovnih aktivnosti vezanih uz poslovanje voditelja obrade.
• radi pohrane ili prijenosa nedopuštenog materijala, povjerljivog materijala, osobnih podataka ili bilo kakvog materijala u vlasništvu voditelja obrade bez izričite suglasnosti voditelja odjela na koji se takvi materijali odnose
• radi pohrane ili prijenosa podataka koji pripadaju drugoj organizaciji
• za zlostavljanje drugih
• za vanjske poslovne aktivnosti.

RELAXINO, uslužno trgovački obrt ima politiku nulte tolerancije za slanje SMS poruka i e-pošte tijekom vožnje. Dopušten je razgovor tijekom vožnje samo korištenjem Hands-free uređaja.

Sigurnost korištenja osobnih informacijskih i komunikacijskih uređaja:

Kako bi se spriječio neovlašteni pristup podacima u uređaju i ostalim podacima kojima uređaj ima pristup, uređaj mora biti zaštićen lozinkom. Ukoliko postoji opcija kriptiranja uređaja, uređaj mora biti kriptiran. Pristup mreži s uređaja također mora biti zaštićen lozinkom s isključenom opcijom automatskog prepoznavanja mreže.

Nakon 5 neuspjelih pokušaja pristupa uređaju, isti mora ostati zaključan, a za ponovni pristup uređaju, mora se kontaktirati voditelj informatičkog odjela.

Uređaji koji su u vlasništvu zaposlenika i koriste se isključivo za privatne potrebe ne smiju se spajati na računalnu mrežu RELAXINO, uslužno trgovački obrt.

Gubitak ili krađa uređaja mora se prijaviti nadležnoj osobi voditelja obrade, najkasnije 24 sata od spoznaje o gubitku ili krađi. Zaposlenici su odgovori za obavješćivanje mobilnog operatera o krađi ili gubitku odmah nakon gubitka ili krađe uređaja.

Očekuje se da će svaki zaposlenik u svakom trenutku koristiti svoje uređaje na etičan način u skladu s pravilima tvrtke i etičkim kodeksom.

Zaposlenik preuzima punu odgovornost za rizike djelomičnog ili potpunog gubitka podataka pohranjenih na uređaju zbog nepravilnog korištenja ili grešaka koje uređaj čine neupotrebljivim.

Mrežna sigurnost

Voditelj obrade propisuje sljedeće mrežne mjere zaštite:

Pravila korištenja interneta i elektroničke pošte odnose se na sve korisnike interneta u RELAXINO, uslužno trgovački obrt, uključujući i privremene korisnike (gosti, posjetitelji, vanjski suradnici) koji imaju privremeni pristup internetu te partnere s ograničenim ili neograničenim vremenom pristupa internetu. Pravilnik zahtjeva i pretpostavlja usklađenost svih korisnika interneta s propisanom politikom.

KORIŠTENJE INTERNETA

- Za sve korisnike interneta dopušten je ograničen pristup.
- Strogo je zabranjen pristup pornografskim web stranicama i svim drugim rizičnim stranicama.
- Pristup internetu uglavnom je predviđen za poslovnu namjenu.
- Pristup internetu u osobne svrhe je dopušten uz uvjet da se ne utječe na produktivnost rada.
- Obeshrabruje se korištenje interneta za osobne svrhe tijekom radnog vremena.
- Pristup internetu kontrolira se pomoću vatrozida.
- Pri pristupanju internetu, korisnici se moraju ponašati u skladu s pravilima koja osiguravaju ugled.
- Potrebno je poduzeti razumne mjere za otkrivanje i sprečavanje napada na servere i radne stanice.

KORIŠTENJE ELEKTRONIČKE POŠTE

- Sve dodijeljene adrese elektroničke pošte i mjesta za pohranu pošte moraju se koristiti isključivo u poslovne svrhe.
- Povremeno korištenje osobne e-mail adrese na internetu za osobnu namjenu može biti dopušteno ako korištenje ne uzrokuje vidljivu potrošnju resursa i ne utječe na produktivnost rada.
- Strogo je zabranjeno korištenje resursa organizacije za neovlašteno oglašavanje, neželjenu elektroničku poštu, političke kampanje i drugo korištenje koje nije povezano s poslovanjem RELAXINO, uslužno trgovački obrt.
- Ni na koji način se resursi i adrese elektroničke pošte ne smiju koristiti za otkrivanje povjerljivih ili osjetljivih informacija koje posjeduje RELAXINO, uslužno trgovački obrt, osim u slučaju otkrivanja podataka ovlaštenim osobama i na autorizirane adrese elektroničke pošte.
- Korištenje resursa i adresa elektroničke pošte RELAXINO, uslužno trgovački obrt za širenje poruka koje se smatraju uvredljivima, rasističkim ili na bilo koji način protivnih zakonu i etici, apsolutno se zabranjuju.
- Elektronička pošta koristi se samo u mjeri koja je potrebna za obavljanje poslovnih zadaća. Kada korisnik i Voditelj obrade prekinu poslovni odnos, elektronička pošta mora biti deaktivirana.
- Korisnici moraju imati privatni identitet da bi pristupili vlastitoj elektroničkoj pošti i resursima za pohranu elektroničke pošte osim u posebnim slučajevima kada pristupaju elektroničkoj pošti dodijeljenoj grupi djelatnika.
- Privatnost nije zajamčena. Ukoliko se pojave posebni zahtjevi povjerljivosti, vjerodostojnosti i integriteta, omogućiti će se korištenje elektronički potpisanih poruka.

POLITIKA UDALJENIH PRISTUPA
Politika udaljenih pristupa definira uvjete za siguran daljinski pristup unutarnjim resursima organizacije.

- Da bi pristupili internim resursima RELAXINO, uslužno trgovački obrt s udaljenih lokacija, korisnici moraju imati potrebna autorizacijska prava. Pristup zaposlenika s udaljenih lokacija može zatražiti samo njemu nadređena osoba, odobrava ga direktor, a omogućava voditelj informatičkog odjela ili djelatnik informatičkog odjela po nalogu voditelja informatičkog odjela.
- Pristup s udaljenih lokacija mora biti omogućen samo sigurnim kanalima uz međusobnu provjeru autentičnosti između poslužitelja i klijenta. I poslužitelj i klijent moraju prepoznati međusobno pouzdane certifikate.
- Nije dozvoljen pristup povjerljivim informacijama s udaljenih lokacija. Iznimka od ovog pravila može se odobriti samo u slučajevima u kojima je to strogo potrebno.
- Korisnici se ne smiju povezivati s javnih računala osim ako se radi o pristupu javnom sadržaju (npr. web stranicama).

Ostale mjere sigurnosti

Voditelj obrade propisuje ostale sigurnosne mjere kako sljedi:

POSTUPAK POVJERAVANJA POSLOVA IZVRŠITELJU OBRADE (OUTSOURCING)

Postupak izdvajanja poslova definira zahtjeve koji su potrebni kako bi se smanjili rizici povezani s povjeravanjem poslova obrade podataka drugim izvršiteljima obrade.

- Prije izdvajanja poslova pružanja bilo kojih usluga, funkcija ili procesa, mora se obaviti procjena rizika izdvajanja poslova, ocijeniti utjecaj na obradu podataka te financijske učinke.
- Kada je god moguće, treba objaviti natječaj za odabir između više pružatelja usluga.
- Pružatelj usluge trebao bi biti odabran nakon procjene njegovog ugleda, iskustva u vrsti tražene usluge, ponudama i jamstvima.
- Ugovori o pružanju usluga i definirane razine usluga moraju sadržavati i odredbe o zaštiti osobnih podataka.
- Izvršitelj obrade mora dobiti odobrenje RELAXINO, uslužno trgovački obrt ako namjerava angažirati treću stranu (podugovaratelja) na poslovima pružanja ugovorene usluge, funkcije ili procesa.

Završne odredbe

Svi djelatnici koji obrađuju osobne podatke moraju biti upoznati sa ovim pravilnikom i izvršavati njegove odredbe.
Ovaj pravilnik sadrži povjerljive informacije i njegov sadržaj ne smije se otkrivati neovlaštenim osobama.
Pravilnik stupa na snagu s danom donošenja.