10000 Zagreb, Kuzminečka 49, za projektiranje IS-a, unutarnju i vanjsku trgovinu
tel 385 **99 255 2765**, e-mail **ipos@ipos.hr** http **www.ipos.hr**
transakcijski račun **HR13 2340 0091 1101 6266 7** kod PBZ Zagreb, OIB **81491680659**

Trgovačko društvo na temelju Opće uredbe o zaštiti osobnih podataka donosi sljedeći

PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA

1. Podloga pravilnika

Ovim Pravilnikom se propisuje način usklađivanja odgovarajućih tehničkih i organizacijskih mjera kako bi se osiguralo i moglo dokazati da se obrada provodi u skladu s Uredbom Europske unije 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinca u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), Službeni list Europske unije, L 119, 4. svibnja 2016. (dalje: Uredba).

2. Podaci voditelja obrade osobnih podataka

Odgovorna osoba za obradu osobnih podataka istodobno je voditelj i izvršitelj obrade

Kemil Kujundžić, direktor
Telefon: 099 255 2765
E-mail: ipos@ipos.hr

3. Zakonitost obrade

Voditelj obrade osobnih podataka zakonito obrađuje osobne podatke na temelju sljedećih zakonitih osnova obrade:

- zakonske obveze voditelja obrade
- legitimnog interesa voditelja obrade ili treće strane
- nužnost radi izvršenja ugovora u kojoj je ispitanik stranka

4. Kategorije osobnih podataka

Voditelj obrade obrađuje sljedeće kategorije osobnih podataka:

- osobne podatke zaposlenika
- osobne podatke djelatnika poslovnih partnera

5. Mjesta gdje se nalaze osobni podaci ispitanika

Ipos više ne koristi papirnatu dokumentaciju.

Od stare arhivske dokumentacije postoje samo stare arhive završnih obračuna i obračuna plaća u kojima se nalaze djelomični podaci zaposlenika.

Najveći dio podataka je u digitalnom obliku na glavnom računalu.

Osobni podaci ispitanika u glavnom računalu se manjim dijelom nalaze u bazi programa Microsoft Outlook tj. Microsoft Office 365 i to samo podaci djelatnika poslovnih partnera sa kojima se vrši korespondecnija vezi poslovanja tvrtke Ipos.
Podaci iz MS Outlooka se istodobno kao kopija nalaze i u oblaku Microsofta.

Svi ostali podaci se nalaze u knjigovodstvenom programu Ipos knjigovodstvo i to u kadrovskoj evidenciji (matični karton radnika), obračunu plaća (podaci o plaći, doprinosima, porezima), bazi poslovnih suradnika (popis djelatnika poslovnih partnera).

Ograničeni dio osobnih podataka naših klijenata koji su istodobno i korisnici našeg programa Ipos knjigovodstvo se nalazi na webu, također u zaštićenom dijelu na serverima tvrtke Avalon doo (ime, prezime, email), a koji su potrebni da bi se korisnici služili dodatnim alatima.

Podaci za pristup na web (korisničko ime i lozinka) su anonimizirani tj. korisničko ime i lozinka su slučajni podaci i ne mogu se povezati sa imenom i prezimenom.

Svi podaci koji se nalaze na glavnom računalu svakodnevno se arhiviraju na dva eksterna diska od kojih se jedan periodično pohranjuje na drugoj fizičkoj lokaciji.

Podaci se prilikom arhiviranja kriptiraju sa AES kriptografskim algoritmom u CBC (Cipher-block chaining) modu i koristi se slučajno generirani ključ sa definiranom veličinom od 256 bitova.

Kripto ključ je dalje kriptiran sa AES-256 koristeći se sa SHA-256 hash-om lozinke kao ključem. Lozinka sama po sebi nigdje nije spremljena na disk ili u arhivu, hash lozinke se koristi kao verifikacija. Sa ovakvom dvostrukom sigurnosti podaci su zaštićeni od bilo kakvog neautoriziranog pristupa i bez lozinke nitko, pa niti vlasnik, ne može do podataka.

6. Svrha obrade

1. Osobni podaci zaposlenika društva

Voditelj obrade obrađuje osobne podatke zaposlenika društva u svrhu nužnog zadovoljenja zakonskih obaveza kao što su zaključivanje ugovora o radu, vođenje kadrovske evidencije radnika prema odredbi čl. 5. Zakona o radu (ZR) NN 93/14.

Pri tome se poštuje odredba čl. 29. ZR prema kojoj se osobni podaci radnika smiju prikupljati, obrađivati, koristiti i dostavljati trećim osobama samo ako je to zakonom dopušteno ili ako je to potrebno radi ostvarivanja prava i obveza iz radnog odnosa, odnosno u vezi s radnim odnosom.

S obzirom na to da je trgovačko društvo kao poslodavac obvezno obraditi nekoliko kategorija podataka o svojim zaposlenicima: obračun obveznih doprinosa zbog zdravstvenog i mirovinskog osiguranja, obračuna plaće, poreza i prireza u skladu s Uredbom, HZMO, HZZO i Porezna uprava su primatelji osobnih podataka kojima, prema odredbi čl. 4. st. 1. t. 6. Uredbe, voditelji ili izvršitelj obrade prenose osobne podatke zaposlenika.

Podaci o zaposlenicima, obračunima plaće, čuvaju se trajno prema zakonskoj obvezi.

2. Osobni podaci djelatnika poslovnih partnera

Voditelj obrade obrađuje osobne podatke poslovnih partnera (dobavljača, ponuđača usluga, kupaca i potencijalnih kupaca) radi izvršenja osnovne djelatnosti i općenito komunikacije sa djelatnicima poslovnih partnera sa kojima ima poslovni odnos.

Osobni podaci djelatnika poslovnih partnera čuvaju se dok postoji poslovni odnos sa partnerom.

7. Osobni podaci koji se obrađuju

Voditelj obrade ima obvezu obrade samo onih osobnih podataka koji su nužni za svaku posebnu svrhu obrade, odnosno podataka koji moraju biti primjereni i relevantni za svrhu.

1. U svrhu osobnih podataka zaposlenika

Voditelj obrade u svrhu osobnih podataka zaposlenika društva obrađuje sve podatke koje je obavezan prikupljati prema Zakonu o radu, radi obaveza prema HZMO-u, HZZO-u, radi obračuna plaće, kao što su: ime i prezime, adresu, OIB, datum rođenja, općina rođenja, državljanstvo, broj djece, obiteljsko stanje, zanimanje kvalifikacija, završena škola, datum zapošljavanja, prethodni staž, broj radnje knjižice, osobni broj osiguranika, broj tekućeg računa, broj žiro računa, član sindikata, invalidnost i dr. zakonom propisani podaci.

2. U svrhu osobnih podataka djelatnika poslovnih partnera

Voditelj obrade u svrhu osobnih podataka djelatnika poslovnih partnera obrađuje sljedeće osobne podatke radi uspostave poslovnih komunikacija sa partnerima:

- ime i prezime
- firma
- titula
- funkcija
- zanimanje
- telefon
- e-Mail

8. Organizacijske i tehničke mjere

Voditelj obrade obrađuje osobne podatke na način koji jamči sigurnost osobnih podataka, tako da su zaštićeni od neovlaštenog pristupa, nezakonite obrade, slučajnoga gubitka, uništenja ili oštećenja.

Voditelj obrade sve navedeno provodi sljedećim organizacijskim i tehničkim mjerama:

1. Zaštita sustava od internih i eksternih rizika

Interno djelatnici Iposa savjesno pristupaju osobnim podacima ispitanika.

Eksterni rizici su u pravilu napadi preko interneta, a gdje su računala višestruka zaštićena vatrozidima na routeru, računalu, Norton Internet Security.

2. Zaštita od neovlaštenog pristupa

Svi uređaji su zaštićeni dužim alfanumeričkim lozinkama, pristup računalu i pristup programu sa podacima.

Same arhive su kreirane pogramom firme Acronis i istodobno kriptirane AES 256 bitnom enkripcijom i lozinkom tako da i slučaju krađe uređaja sa podacima oni nikome neće biti čitljivi.

3. Zaštita podataka u fizičkom obliku

Računala su u štićenom uredu pod alarmom koji je povezan 24-satnom zaštitarskom službom tvrtke APUS.

4. Periodička obuka osoblja

Konstantno se prate informacije i promjene kako u sigurnosti u infomatičkom svijetu tako i u propisima preko časopisa RRIF i na internetu.

9. Prava ispitanika

Svaka informacija i komunikacija u vezi s obradom osobnih podataka ispitaniku je lako dostupna i razumljiva jer se prilikom informiranja ispitanika služi jasnim i jednostavnim jezikom. Ispitanik je upoznat s identitetom voditelja obrade i svrhama obrade na internetskim stranicama voditelja obrade.

Voditelj obrade upoznat će ispitanika s rizicima, pravilima, zaštitnim mjerama i pravima u vezi s obradom osobnih podataka i načinom ostvarenja svojih prava u vezi s obradom putem internetske stranice voditelja obrade https://www.IPOS.hr.

1. Pravo na transparentnost (informacije koje treba dati ispitaniku)

Člankom. 13. Uredbe voditelj obrade će ispitaniku pružiti sljedeće informacije:

a. Identitet i kontaktne podatke voditelja obrade

Nalaze se u samom pravilniku na internetu.

b. Kontaktne podatke službenika za zaštitu podataka

Ista osoba kao voditelj obrade.

c. Svrhe obrade radi kojih se upotrebljavaju osobni podaci kao i pravnu osnovu za obradu

- zakonske obveze voditelja obrade
- legitimni interes voditelja obrade ili treće strane
- nužnosti radi izvršenja ugovora u kojoj je ispitanik stranka

d. Legitimni interes voditelja obrade

Voditelj obrade mora posjedovati osobne podatke o djelatnicima svojih poslovnih partnera radi ostvarivanja djelatnosti sa kojom se bavi tj. radi ostvarivanja kontakata i pružanje podrške korisnicima.

2. Pravo na pristup podatcima

Ispitanik ima pravo od voditelja obrade zahtijevati:

- izdavanje potvrde o svrsi obrade, kategorijama osobnih podataka, primateljima, razdoblju pohrane i
- informacije o pravu na traženje ispravka ili brisanja, o pravu na pritužbu nadzornom tijelu, o posrednom izvoru iz kojeg voditelj prikuplja osobne podatke

Voditelj obrade će ispitaniku na njegov zahtjev predati presliku osobnih podataka koje obrađuje, bez naplate troškova za prvu presliku.

3. Pravo na ispravak

Prema odredbi čl. 16. Uredbe, ispitanik ima pravo bez nepotrebnog odgađanja ishoditi od voditelja obrade ispravak netočnih osobnih podataka koji se na njega odnose, dopuniti nepotpune osobne podatke, davanjem dodatne izjave.

4. Pravo na zaborav (brisanje osobnih podataka)

Ispitanik može zatražiti brisanje svojih podataka bez navođenja posebnih razloga, ali će voditelj obrade upozoriti ispitanika da u tom slučaju više neće moći ostvarivati svoja prava kao korisnik programa Ipos knjigovodstvo

5. Pravo na ograničenje obrade

Voditelj obrade koristi samo najosnovnije podatke ispitanika (ime, prezime, funkcija, telefon, mail), ograničenje tih podataka je isti slučaj kao i brisanje osobnih podataka.

6. Pravo na prenosivost podataka

Voditelj obrade će na zahtjev ispitanika ispitaniku proslijediti njegove podatke u digitalnom obliku.

7. Pravo na prigovor

Pravo na prigovor se u pravilu koristi kada prodavatelj prvi puta kontaktira ispitanika radi nuđenja robe/usluge tzv. izravni marketing.

Ipos se ne koristi takvim sistemom pronalaženja kupaca, nego oglašavanjem tako da prvi kontakt ostvaruje kupac na svoju inicijativu.

8. Pravo protivljenja odluci na temelju profila (Automatizirano pojedinačno donošenje odluka, uključujući izradu profila).

Ipos ne koristi profile kupaca.

10. Poštivanje načela obrade osobnih podataka

1. Zakonitost

Obrada je nužna radi izvršavanja zakonitih obaveza društva, radi nužnosti obrade za izvršavanje ugovora u kojem je ispitanik stranka, radi legitimnih interesa voditelja obrade.

2. Poštenje i transparentnost

Svi djelatnici društva svoje osobne podatke u kadrovskoj evidenciji mogu dobiti u elektronskom obliku, pristup podacima drugih osoba je ograničen samo osobama kojima ti podaci trebaju radi obrade.

Osobni podaci djelatnika poslovnih partnera su manje više podaci koji su javno dostupni kao kontakt podaci tih partnera (ime prezime, funkcija, zanimanje, telefon, mail) i koriste se u redovnoj komunikaciji mailom od i prema poslovnom partneru.
To su podaci niskog rizika jer se uostalom nalaze i u javnim dokumentima samih poslovnih partnera.

3. Ograničavanje svrhe

Svi osobni podaci se koriste samo u svrhu zakonske obrade (zaposlenika društva) i djelatnosti tvrtke (poslovni partneri).

4. Smanjenje količine osobnih podataka

Osobni podaci djelatnika se prikupljaju samo prema zakonskoj osnovi, a podaci poslovnih partnera samo najosnovniji navedeni ranije.

5. Ažurnost i točnost

Svaki novi podatak ili promjena postojećeg odmah po saznanju se unosi programski u računalo u program Ipos knjigovodstvo. Istodobno se svaka takva promjena evidentira u Evidenciji aktivnosti obrade.

6. Ograničenje pohrane

Osobni podaci djelatnika društva se prema zakonu čuvaju trajno.

Osobni podaci djelatnika poslovnih partnera se čuvaju dok god postoji poslovni odnos ili potreba za kontaktom.

7. Cjelovitost i povjerljivost

Svi podaci se nalaze u štićenom uredu pod alarmom koji je povezan 24-satnom zaštitarskom službom tvrtke APUS.

Računala na kojima se nalaze podaci su zaštićena Norton Internet Security poslovnim programom za zaštitu koji ima trajnu pretplatu i uvijek je svježe ažuran protiv napada izvana na računalo.

Uvijek je aktivan vatrozid protim vanjskih upada u računalo.

Operativni sistem Windows 10 je uvijek ažuran najnovijim sigurnosnim zakrpama.

Sve lozinke koje se koriste u firmi Ipos su pohranjene u program 1Password svjetski renomirane tvrtke Agile bits čije usluge koriste CNN, The New York Times, BBC i dr., koristi se snažna, višekratna enkripcija, autentifikacija s više faktora pruža dodatni sloj zaštite u firmi.

1Password odgovara najstrožim industrijskim standardima za povjerljivost podataka, integritet i dostupnost podataka.

Same arhive su kreirane pogramom firme Acronis i istodobno kriptirane AES 256 bitnom enkripcijom i lozinkom tako da i slučaju krađe uređaja sa podacima oni nikome neće biti čitljivi.

8. Pouzdanost

Ipos je informatička tvrtka, podaci koda programa našeg proizvoda su od ključne važnosti te nam je zaštita podataka na prvom mjestu, samim time istu vrstu zaštite primjenjujemo i na ostale podatke, uključujujući osobne podatke pojedinaca.

11. Evidencija aktivnosti obrade

Voditelj obrade svaku promjenu osobnog podatka unosi u Evidenciju aktivnosti obrade, uz primjenu svih ostalih kriterija postavljenih načelima obrade osobnih podataka.

Voditelj obrade koristi automatsku rutinu unutar knjigovodstvenog programa Ipos knjigovodstvo prema kojoj se svaka promjena osobnih podataka zaposlenika ili osobnih podataka djelatnika poslovnih partnera automatski ažurira (datum, vrijeme, osoba koja je napravila izmjenu).

Ista rutina bilježi i sve ostale aktivnosti osobe/korisnika programa od ulaska u program do izlaska iz programa.

Upisivanje podataka u Evidenciju aktivnosti obrade (dalje Evidencija) provodi voditelj obrade Kemil Kujundžić.

Evidencija se vodi elektronski.

Temeljni podaci svake evidencije:

1. naziv evidencije
2. voditelj evidencije (Ipos doo)
3. svrhu obrade
4. pravni temelj uspostave evidencije
5. kategorije osoba
6. vrste podataka
7. način prikupljanja i čuvanja
8. vremensko razdoblje čuvanja i uporabe
9. naziv korisnika zbirke
10. naznaku unošenja/iznošenja iz RH s naznakom države i organizacije
11. naznaka poduzetih mjera zaštite osobnih podataka

12. Procjena rizika

Rizik za gubitak ili otkrivanje podataka o djelatnicima poslovnih partnera (kupci, dobavljači) je nizak jer se ti podaci manje više nalaze javno objavljeni na internet stranicama istih poslovnih partnera, a telefoni i mailovi su zapravo kontakt podaci samog poduzetnika.

Interni rizik se svodi samo na ljudski faktor ako bi netko od zaposlenika društva neovlašteno prenio podatke trećoj strani.

Eksterni rizik je rizik od prodora neželjenih osoba preko interneta do glavnog računala ili presretanjem emailova sa eventualnim osjetljivim informacijama.

Fizički rizik je provala u prostorije ureda i otuđenje opreme sa podacima.

Sva tri rizika su svedena na minimum jer u uredu rade osobe od povjerenja, kao informatička tvrtka imamo postavljenu visoku razinu zaštite, a ured je pod alarmom i povezan sa 24h sa zaštitarskom službom.

Arhive podataka u uredu i dodatnoj lokaciji su kriptirane AES 256 bitnom enkripcijom.

13. Izvješćivanje o povredi osobnih podataka

Prema odredbi čl. 33. st. 1. Uredbe u slučaju povrede osobnih podataka voditelj obrade će najkasnije 72 sata nakon saznanja o to povredi, izvjestiti nadzorno tijelo tj. Agenciju za zaštitu osobnih podataka, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca.

Prema odredbi čl. 34. st.1. i 2. Uredbe, u slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade će bez nepotrebnog odgađanja obavjestiti ispitanika o povredi osobnih podataka, s tim da se obavješćivanjem ispitanika opisuje priroda povrede osobnih podataka uporabom jasnog i jednostavnog jezika te ono sadržava barem: ime i kontaktne podatke službenika za zaštitu podataka ili druge osobe od koje se može dobiti još informacija o učinjenoj povredi osobnih podataka, opis posljedica povrede osobnih podataka, te opis mjera koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka, uključujući, prema potrebi, mjere umanjivanja njezinih mogućih štetnih posljedica.

14. Završne odredbe

Pravilnik se može mijenjati i dopunjavati na jednak način i prema jednakom postupku u skladu s kojim je donesen.

Pravilnik stupa na snagu i primjenjuje se od dana njegove objave na na internetskoj stranici voditelja obrade www.ipos.hr.

Zakonski zastupnik trgovačkog društva:

direktor

Kujundžić Kemil, dipl.ing.