Na temelju uredbe Europske unije o zaštiti osobnih podataka General Data Protection Regulation (GDPR) 2016/679 europskog parlamenta i vijeća (u daljnjem tekstu: GDPR) te Zakonu o zaštiti osobnih podataka (NN 106/2012) (u daljnjem tekstu ZZOP) uprava poduzeća eBurza Grupa d.o.o. (u daljnjem tekstu: Uprava) na svojoj sjednici održanoj 29.01.2018. donosi sljedeći

Pravilnik o zaštiti, nadzoru nad prikupljanjem, obradi i korištenju osobnih podataka

I. Opće odredbe

Članak 1. Danom donošenja ovog pravilnika, prestaju važiti sve odluke i prakse koje su važile do donošenja ovog pravilnika. Pravilnik propisuje: 1. Dodjelu prava korištenja osobnih podataka zaposlenicima poduzeća 2. Način autentifikacije i autorizacije djelatnika za rad s osobnim podacima 3. Procedure i sustav pohrane podataka na siguran način 4. Način prometovanja osobnim podacima unutar i izvan poduzeća 5. Obradu i dostavu osobnih podataka u poslovanju 6. Čuvanje i vođenje evidencije osobnih podataka u poslovanju

Članak 2. Pojedini izrazi imaju sljedeće značenje: • „osobni podaci" znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca;

• „obrada" znači 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, usklaĊivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje; • „sustav pohrane" znači svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi; • „voditelj obrade" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice; • „izvršitelj obrade" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade; • „primatelj" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana. Međutim, tijela javne vlasti koja mogu primiti osobne podatke u okviru odreĊene istrage u skladu s pravom Unije ili države članice ne smatraju se primateljima; obrada tih podataka koju obavljaju ta tijela javne vlasti mora biti u skladu s primjenjivim pravilima o zaštiti podataka prema svrhama obrade; • „treća strana" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade ni osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade; • „biometrijski podaci" znači osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrĊuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci; • „pravo na pristup" (autorizacija i autentifikacija) – način na koje se odabrane zaposlenike identificira za odabrani djelokrug odgovornosti te način na koji im se odobrava

pristup informacijama • „izvor osobnih podataka“ – bilo koja institucija, pravna ili fizička osoba koja dostavlja osobne podatke

II. Dodjela prava na pristup osobnim podacima i informacijama

Članak 3.

Pravo na pristup osobnim podacima posjeduju isključivo odabrani zaposlenici poduzeća što se smatra autentifikacijom s pridodjeljenim korisničkim imenom i zaporkom što se smatra autorizacijom.

Odabir zaposlenika iz stavka 1 donosi Uprava poduzeća.

III. Način autentifikacije i autorizacije djelatnika

Članak 4.

Pravo na pristup osobnim podacima i informacijama dodjeljuje se odabranim zaposlenicima na razini odjela.

Dohvat autorizacije je sljedeći: a) Zaposlenici odjela Uprave imaju neograničeno pravo pristupa svim osobnim podacima u unutarnjem i vanjskom poslovanju poduzeća. b) Zaposlenici odjela Marketing imaju ograničeno pravo pristupa osobnim podacima koju su bitni za redovno poslovanje i poslovne procese kojima poduzeće ostvaruje ispunjenje planiranih ciljeva dnevnog poslovanja. c) Zaposlenici odjela Informatičkih tehnologija imaju ograničeno pravo pristupa osobnim podacima koji su bitni za ispunjenje privremenih i projektnih zadataka d) Zaposlenici odjela Prodaje imaju ograničeno pravo pristupa osobnim podacima prema odluci Uprave poduzeća isključivo u svrhe ispunjenja projektnih ciljeva prodaje.

Način i model ograničavanja pristupa određuje uprava poduzeća i izvješćuje zaposlenike elektroničkim dopisom, a provodi odjel Informatičkih tehnologija.

Pri osnivanju novih odjela ili zatvaranja te prenamjene postojećih, sukladno će se izmijeniti i pravila autentifikacije i autorizacije djelatnika.

IV. Procedure i mjesta za skladištenje podataka na siguran način

Članak 5.

Prava na pristup osobnim podacima i informacijama poduzeća čuvaju se u tabličnom obliku s popisom imena i prezimena, OIB-a i naziva odjela zaposlenika.

Tablica s popisom odabranih zaposlenika čuva se u kriptiranom obliku na vanjskom disku (NAS) koji se nalazi u zaštićenoj lokalnoj mreži u prostorijama sjedišta poduzeća. Tablica je dostupna za izmjene i obradu isključivo zaposlenicima iz članka 3.

Osobni podaci zaposlenika čuvaju se u elektroničkom obliku u za to propisanoj elektroničkoj mapi kojoj pristup imaju samo zaposlenici odabrani prema članku 3.

Osobni podaci i druge informacije dobivene iz izvora osobnih podataka čuvaju se u mapi dobavljača ili naručitelja, odnosno voditelja obrade, kojoj pristup imaju isključivo zaposlenici iz članka 3.

Elektronička mapa za privremenu ili trajnu pohranu osobnih podataka može biti uspostavljena u lokalnoj mreži poduzeća, na udaljenom računalu, serveru ili mjestu za pohranu podataka davatelja usluga masovnog skladištenja podataka koji općim uvjetima poslovanja odgovaraju za sigurnost osobnih podataka, a usklađeni su s važećim propisima.

V. Način prometovanja osobnim podacima unutar poduzeća

Članak 6.

Svi osobni podaci koji se koriste u svrhu obrade plaće zaposlenika, vođenje evidencije radnog vremena, godišnjih odmora i svih dnevnih aktivnosti firme tajni su, a dostupni su odabranim zaposlenicima iz članka 3. Obrada, uvid i upravljanje osobnim podacima zaposlenika što se ne odnosi na zakonom propisano nužno korištenje, a za unutarnje potrebe poduzeća, dozvoljeno je isključivo uz pisani pristanak zaposlenika.

Na računalima poduzeća zaposlenicima nije dozvoljeno čuvanje ili distribucija osobnih podataka kao ni osobnih podataka drugih zaposlenika ili podataka poduzeća već se takvi podaci moraju pohraniti na sigurno mjesto prema članku 5.

Na računalima poduzeća dozvoljena je isključivo obrada osobnih podataka.

VI. Način prometovanja osobnim podacima izvan poduzeća

Članak 7.

Osobni podaci ne smiju se iznositi, davati na uvid ili distribuirati izvan poduzeća uz iznimku službenog institucionalnog naloga službenoj osobi ili poslovnog naloga voditelja obrade, odnosno naručitelja.

Po primitku originala službenog institucionalnog naloga, osobni podaci se smiju dostavljati izvan poduzeća isključivo u pisanom obliku naslovljeni na instituciju koja je zatražila uvid u osobne podatke i to preporučenom pošiljkom s povratnicom.

Uvid u osobne podatke smije izdati nadležni zaposlenik iz članka 10. uz predočenje naloga nadležnog suda, propisano identificiranoj službenoj osobi.

Uvid u osobne podatke smije izdati nadležni zaposlenik iz članka 10. uz pisano i potpisano službeno odobrenje voditelja obrade, odnosno naručitelja, u slučaju da je poduzeće eBurza Grupa d.o.o. suobraditelj osobnih podataka s trećima. U tom slučaju voditelj obrade mora poslovnim nalogom jasno istaknuti da daje pravo poduzeću eBurza Grupa d.o.o. dati osobne podatke na uvid i daljnju obradu trećima s precizno obrazloženim razlogom te nazivom i OIB-om treće strane (sukladno članku 28 st.2, GDPR).

VII. Obrada i dostava osobnih podataka u poslovanju

Članak 8.

Poslovni proces obrade osobnih podatka u poduzeću eBurza Grupa d.o.o. naziva se personalizacija. Personalizacija uključuje aplikaciju imena, prezimena, identifikacijskog broja, biometrijskog sadržaja, štapićastog (ili drugog grafičkog) koda, fotografije, magnetnog zapisa i drugih podatka na različite medije ovisno o tehnologiji koju naručuje naručitelj, a jedinstveno i specifično identificira osobu.

Naručitelj se smatra svakom institucijom, pravnom ili fizičkom osobom koja naručuje projekt personalizacije, a smatra se voditeljem obrade jer određuje svrhe i sredstva obrade osobnih podataka.

eBurza Grupa d.o.o., pri zaprimanju osobnih podataka potrebnih za izvršavanje projekata personalizacije u ulozi je primatelja i izvršitelja osobnih podataka jer se poduzeću otkrivaju osobni podaci, a zaduženo je za obradu i aplikaciju istih u svrhu izvršavanja poslovnih zadataka.

Svaki naručitelj, odnosno, voditelj obrade, dužan je pismenim putem izvjestiti poduzeće eBurza Grupa d.o.o. o usklađenosti vlastith poslovnih procesa o zaštiti, nadzoru nad prikupljanjem, obradi i korištenju osobnih podatka. Svaki naručitelj, odnosno, voditelj obrade u obavezi je potpisati elektronički dokument službenog očitovanja, odnosno, izjavu koju mora potpisanu od strane voditelja obrade vratiti poduzeću eBurza Grupa d.o.o. čime jamči sigurnost u prometu osobnim podacima te da je sa svoje strane poduzeo sve tehničke, kadrovske i organizacijske mjere zaštite osobnih podataka.

Svaki naručitelj, odnosno voditelj obrade, dužan je dostaviti samo nužno potrebne podatke na obradu i personalizaciju (sukladno članku 25. st.2 GDPR). Podaci se dostavljaju pismenim putem ili elektroničkim putem. Ukoliko se podaci šalju pismenim putem, isti moraju biti dostavljeni u zatvorenoj pošiljci s povratnicom. Ukoliko se podaci šalju elektroničkim putem, moraju biti dostavljeni u tabličnom obliku, sažeti nekim od aplikacija za sažimanje podataka i zaštićeni zaporkom što nazivamo set za obradu. Set se imenuje nazivom poslovnog zadatka i datumom dostave (prema uputi djelomične pseudonimizacije, sukladno članku 25. st.1 i članku 32. st.1a, GDPR). Naručitelj, odnosno, voditelj obrade, dostavlja zaporku na način kojeg utvrđuje nadležni zaposlenik iz članka 3., o čemu će spomenuti nadležni zaposlenik izvjestiti naručitelja, odnosno, voditelja obrade.

VIII. Čuvanje i evidencija osobnih podataka u poslovanju

Članak 9.

Osobni podaci dostavljeni na obradu i aplikaciju u procesu personalizacije po uspješno izvršenim poslovnim zadacima se uništavaju i ne čuvaju se (sukladno članku 17., st.1a i članku 28. st.3g, GDPR).

Nadležni zaposlenik iz članka 3. će po primitku obavljene dostave personaliziranog materijala ili po završetku projekta obrisati, odnosno, uništiti sve osobne podatke koji su bili predmet obrade, a pogotovo za podatke iz članka 8., stavka 1.

U slučaju pogreške pri obradi osobnih podataka, a nakon završetka projekta ili poslovnog zadatka, voditelj obrade će ponovno dostaviti navedene podatke na ispravak ili daljnju i dodatnu obradu prema članku 8., stavku 5. (sukladno članku 19. GDPR).

Osobni podaci zaposlenika čuvaju se trajno, odnosno, prema utvrđenim pravilima koje nalaže zakon.

IX. Službenica /službenik za zaštitu osobnih podataka

Članak 10.

Sukladno ZZOP, članak 18a, Uprava poduzeća eBurza Grupa d.o.o., iako nije u obvezi, imenuje službenika za zaštitu osobnih podataka u pisanom obliku. Po imenovanju, poduzeće eBurza Grupa d.o.o. će na svojim internetskim stranicama javno objaviti kontakt podatke te ime i prezime odabrane osobe.

Službenik za zaštitu osobnih podataka ne može biti osoba protiv koje se vodi postupak zbog povrede službene dužnosti, radne obveze ili kojoj je izrečena mjera povrede etičkog kodeksa i drugih pravila poslovne etike i načela dobrog poslovnog ponašanja.

Službenik za zaštitu osobnih podataka je dužan nadzirati zakonitost obrade osobnih podataka, voditi sve evidencije o obradi, prometu te opravdanom iznošenju i davanju na uvid osobnih podataka prema članku 9. te izvješavati i upozoravati voditelje obrade, odnosno, naručitelje o primjeni i provođenju obrade osobnih podataka na siguran način (sukladno članku 33., st.2 i članku 39. GDPR)

X. Prijelazne i završne odredbe

Članak 11.

Ovaj pravilnik stupa na snagu danom donošenja, a objavit će se na internetskim stranicama poduzeća eBurza Grupa d.o.o. radi dostupnosti javnosti u skladu s odredbama Zakona o pravu na pristup informacijama („Narodne Novine“, broj 25/13, i 85/15).

U Zagrebu 29.01. 2018. godine

Uprava poduzeća eBurza Grupa d.o.o.

Alen Šimec, direktor M.P.

_____ (potpis)