



## **Politika zaštite osobnih podataka**



## Sadržaj

|  |   |
|--|---|
| <b>Svrha dokumenta</b> .....                         | 3 |
| <b>Prikupljanje i obrada osobnih podataka</b> .....  | 3 |
| <b>Prava ispitanika</b> .....                        | 3 |
| <b>Evidencija, čuvanje i postupanje</b> .....        | 4 |
| <b>Minimizacija i zaštita osobnih podataka</b> ..... | 4 |
| <b>Upravljanje incidentima</b> .....                 | 5 |
| <b>Certifikacija</b> .....                           | 5 |
| <b>Odgovornosti</b> .....                            | 5 |
| Odgovornost Uprave .....                             | 5 |
| Odgovornost zaposlenika .....                        | 5 |
| Odgovornost Službenika za zaštitu podataka .....     | 6 |
| Odgovornost Sektora informatičke tehnologije .....   | 6 |
| Odgovornost Sektora pravnih i općih poslova .....    | 6 |
| Odgovornost za održavanje ovog dokumenta .....       | 6 |

## **Politika zaštite osobnih podataka**

### **Svrha dokumenta**

Ovom Politikom Uprava društva Imex banka d.d. (dalje u tekstu: Društvo) određuje stav Društva prema osobnim podacima, definira pravila postupanja i dodjeljuje odgovornosti u postupcima obrade osobnih podataka koje Društvo provodi, sukladno odredbama Opće uredbe o zaštiti podataka 2016/679 (dalje u tekstu: Uredba).

Osobni podaci koje Društvo prikuplja i obrađuje u svom radu smatraju se povjerljivim te se s njima mora postupati s posebnom pažnjom i obrađivati ih isključivo u svrhe za koje su prikupljeni.

### **Prikupljanje i obrada osobnih podataka**

Prilikom obrade osobnih podataka Društvo postupa po načelima zakonitosti, transparentnosti i poštenosti, načelu ograničavanja svrhe i pohrane podataka, smanjenju količine podataka, točnosti, cjelovitosti i povjerljivosti podataka, te načelu pouzdanosti.

Društvo prikuplja osobne podatke isključivo na temelju jasno određene i dokumentirane pravne osnove kao što je izvršenje zakonskih obveza, izvršenje ugovornih obveza, zaštita legitimnih interesa Društva, zaštita ključnih interesa ispitanika, privola ispitanika.

Prilikom prikupljanja osobnih podataka, ispitanicima se mora pružiti jasna informacija o razlogu prikupljanja, pravnoj osnovi i vremenskom razdoblju trajanja obrade, pravima koje ispitanik ima u predmetnoj obradi, eventualnim trećim osobama kojima će se podaci prosljeđivati, te informacije o Društvu i kontakt podatke Službenika za zaštitu podataka.

Ovisno od svrhe obrade, dozvoljeno je prikupljati i obrađivati samo one podatke koji su nužni te je zabranjeno svako suvišno prikupljanje osobnih podataka.

Ako se podaci prikupljaju od djece, neophodno je uspostaviti posebne mehanizme koji će osigurati da su djeca dovoljno stara kako bi razumjela posljedice davanja informacija. Svakom prikupljanju i obradi informacija maloljetnika mora se pristupati sa posebnom pažnjom, te se pri tome mora voditi najvišim etičkim načelima.

### **Prava ispitanika**

Na zahtjev, Društvo ispitanicima mora pružiti informacije o obradi njihovih osobnih podataka i omogućiti im pravo na pristup podacima, pravo na ispravak netočnih i nadopunu nepotpunih osobnih podataka, te pravo na povlačenje prethodno dane suglasnosti za obradu.

Na zahtjev ispitanika (povlačenje privole), osobni podaci koji su dani na temelju privole moraju se obrisati iz svih informacijskih sustava Društva i informacijskih sustava trećih strana kojima je Društvo omogućilo obradu ovih podataka.

Ukoliko je primjenjivo, Društvo mora ispitaniku ispuniti i pravo na brisanje podataka, ograničenje obrade, pravo na prenosivost osobnih podataka i pravo prigovora na odluke koje su donesene isključivo automatskom obradom podataka.

### **Evidencija, čuvanje i postupanje**

Društvo je dužno uspostaviti i održavati evidenciju aktivnosti obrada osobnih podataka i osobnih podataka koji se obrađuju, te osigurati da za predmetnu obradu postoji odgovarajuća pravna osnova sukladno Uredbi te da se obrađuju isključivo podaci koji su nužni za ostvarenje svrhe obrade.

Podaci za koje ne postoji pravna osnova daljnje obrade i pohrane moraju se bez odlaganja obrisati na siguran način.

Osobni podaci se u treće zemlje smiju prenositi isključivo uz prethodnu izričitu privolu ispitanika, u svrhe izvršavanja ugovora u kojem je ispitanik stranka, te u drugim slučajevima propisanim Uredbom, uz obavezno poduzimanje odgovarajućih pravnih i tehničkih mjera zaštite.

### **Tehnička i integrirana zaštita podataka**

Kod izgradnje informacijskih sustava i dizajna poslovnih procesa koji na bilo koji način mogu utjecati na sigurnost osobnih podataka ili ostvarivanje prava na privatnost ispitanika, Društvo će provoditi procjenu učinka na zaštitu podataka te osigurati primjerene zaštitne mjere. Ukoliko se ustanovi da zaštitne mjere koje može implementirati nisu dovoljne, prije obrade Društvo će se savjetovati s nadzornim tijelom. Svi novi procesi i informacijski sustavi u Društvu moraju se dizajnirati tako da ispunjavaju sve zahtjeve ove Politike.

### **Minimizacija i zaštita osobnih podataka**

Društvo će osobne podatke prikupljati i pohranjivati isključivo u mjeri u kojoj je to potrebno. Prilikom pohrane podataka, osobni će se podaci pohranjivati na najmanjem mogućem broju mjesta na kojima moraju biti adekvatno zaštićeni. Pristup osobnim podacima smije biti omogućen isključivo na temelju poslovne potrebe.

Zabranjeno je koristiti osobne podatke u svrhe razvoja ili testiranja IT sustava. Osobne podatke za koje procjena rizika ukaže da narušavanjem njihove povjerljivosti može doći do značajnog utjecaja na prava i slobode pojedinca, potrebno je štiti enkripcijom, pseudonimizacijom ili anonimizacijom gdje god je to moguće.

### **Upravljanje incidentima**

Društvo mora uspostaviti i održavati procedure odgovora na incidente vezane uz narušavanje sigurnosti osobnih podataka, interno i kod trećih strana kojima je Društvo ustupilo ili od kojih je primilo osobne podatke. Društvo mora uspostaviti i održavati strukturu odgovornosti za izvještavanje o incidentima vezanim uz sigurnost osobnih podataka.

Društvo mora uspostaviti i održavati mjere za detekciju neovlaštenog pristupa osobnim podacima i curenja osobnih podataka iz informacijskog sustava. U slučaju narušavanja sigurnosti osobnih podataka koje može negativno utjecati na prava i slobode ispitanika, Društvo će bez odlaganja, a najkasnije u roku od 72 sata po otkrivanju incidenta, o tome izvijestiti nadzorno tijelo. U slučaju curenja osobnih podataka i visokog rizika za prava i slobode ispitanika, Društvo će o tome obavijestiti i ispitanike čiji su podaci kompromitirani.

### **Certifikacija**

Svoj sustav upravljanja osobnim podacima, Društvo će uspostaviti i održavati sukladno primjenjivim standardima iz područja zaštite privatnosti i informacijske sigurnosti (poput ISO 27001), a usklađenost će dokazivati odgovarajućom certifikacijom kada je to moguće.

### **Odgovornosti**

#### **Odgovornost Uprave**

Uprava Društva dužna je imenovati Službenika za zaštitu podataka.

Uprava pruža podršku Službeniku za zaštitu podataka i ostalim osobama/organizacijskim jedinicama, osiguravajući im potrebne resurse za provedbu mjera zaštite osobnih podataka, stjecanje i održavanje stručnog znanja te ostalih aktivnosti koje su neophodne za održavanje mjera i načela koje definira ova Politika.

#### **Odgovornost zaposlenika**

Postupanje po mjerama i načelima definiranim ovom Politikom obvezno je za sve zaposlenike Društva i treće strane koje u okviru poslovne suradnje obrađuju osobne podatke po nalogu Društva.

#### Odgovornost Službenika za zaštitu podataka

Službenika za zaštitu podataka imenuje Uprava kojoj je izravno odgovoran za svoj rad.

Službenik za zaštitu podataka odgovoran je za savjetovanje u uspostavi i održavanju sustavnog upravljanja osobnim podacima i njihovom sigurnošću, na način usklađen s primjenjivom zakonskom regulativom, etičkim načelima i najboljim svjetskim praksama.

Službenik za zaštitu podataka odgovoran je posebno za:

- Informiranje i savjetovanje Društva ili trećih strana o obvezama iz Uredbe
- Praćenje usklađenosti poslovanja Društva s Uredbom
- Praćenje poštovanja Uredbe i internih politika i ostale regulative vezane uz zaštitu osobnih podataka
- Uspostavu i održavanje evidencije aktivnosti obrade osobnih podataka
- Dodjelu odgovornosti za zaštitu osobnih podataka zaposlenicima i trećim stranama uključenima u postupke obrade osobnih podataka
- Podizanje svijesti o važnosti zaštite osobnih podataka i održavanje edukacija o pravilnom postupanju u postupcima obrade osobnih podataka
- Savjetovanje kod provedbe postupka procjene učinka na zaštitu podataka
- Suradnja s nadzornim tijelom
- Nadziranje procesa upravljanja rizikom u obradama osobnih podataka

#### Odgovornost Sektora informatičke tehnologije

Sektor informatičke tehnologije je odgovoran za operativnu uspostavu i održavanje tehničkih kontrola potrebnih za usklađivanje sa zahtjevima ove Politike, a posebice mjera za:

- Identifikaciju i zaštitu osobnih podataka
- Sposobnost otkrivanja povrede osobnih podataka
- Uspostavu mehanizama za ispunjavanje prava ispitanika

#### Odgovornost Sektora pravnih i općih poslova

Sektor pravnih i općih poslova odgovoran je za upoznavanje svih zaposlenika s ovom Politikom i drugim internim aktima kojima je regulirana zaštita osobnih podataka.

#### Odgovornost za održavanje ovog dokumenta

Ova se Politika revidira nakon svake izmjene u pravnom okruženju ili okruženju rizika koje bi moglo imati učinak na njezinu provedbu. Za održavanje ove Politike zadužen je Službenik za zaštitu podataka.