

U skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Uredba), te Zakonom o provedbi Opće uredbe o zaštiti podataka Uprava J&t banke d.d. usvojila je **Pravilnik o zaštiti osobnih podataka** s ciljem usklađenja s odredbama Uredbe i Zakona.

## PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA

### SVRHA I CILJ

Pravilnik o zaštiti osobnih podataka je krovni akt J&T banke d.d. kojem je svrha uspostava zaštite osobnih podataka u skladu s odredbama Opće uredbe o zaštiti podataka (Uredba) i Zakona o provedbi Opće uredbe o zaštiti podataka (Zakon).

Cilj je osiguravanje pravne sigurnosti i transparentnosti u smislu obrade osobnih podataka i aktivnosti obrade osobnih podataka klijenata Banke, radnika Banke i svih ostalih osoba čiji se osobni podaci obrađuju, te propisivanje osnove i svrhe obrada, kategorija osoba čiji se podaci obrađuju, prava pojedinaca, mjera zaštite i sl.

### POJMOVI I SKRAĆENICE

Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Uredba)

Zakon o provedbi Opće uredbe o zaštiti podataka (Zakon)

J&T banka d.d. (Banka)

Europska unija (Unija)

Agencija za zaštitu osobnih podataka (Agencija)

### PODRUČJE PRIMJENE

Pojmovi u smislu ovoga Pravilnika imaju jednako značenje kao pojmovi korišteni u Uredbi:

Osobni podaci, Ispitanik, Obrada, Ograničavanje obrade, Izrada profila, Pseudonimizacija, Voditelj obrade, Izvršitelj obrade, Primatelj, Privola, Povreda osobnih podataka, Genetski podaci, Biometrijski podaci, Podaci koji se odnose na zdravlje, Nadzorno tijelo te ostali korišteni pojmovi iz Uredbe.

### Načela obrade osobnih podataka

Osobni podaci u Banci obrađuju se na način da se Banka kao voditelj obrade, u svim svojim organizacijskim jedinicama, striktno pridržava sljedećih načela:

- (a) **zakonitost, poštenost i transparentnost;** voditelj obrade obrađuje podatke prema svim važećim zakonskim odredbama, štiteći sva potrebna prava ispitanika; voditelj obrade će ispitaniku pružiti sve dodatne informacije neophodne za osiguravanje poštene i transparentne obrade uzimajući u obzir posebne okolnosti i kontekst obrade osobnih podataka; voditelj obrade ne izvršava profiliranje ispitanika ni automatizirano donošenje odluka
- (b) **ograničenje svrhe;** podaci će biti prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama; ali je moguća daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe
- (c)  **smanjenje količine podataka;** podaci će biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe za koje se obrađuju

- (d) **točnost**; podaci moraju biti točni i prema potrebi ažurni; Banka će poduzeti razumne mjere radi osiguravanja da se osobni podaci koji nisu točni, bez odlaganja izbrišu ili isprave
- (e) **ograničenje pohrane**; podaci moraju biti čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju; na dulja razdoblja čuvanja su moguća samo ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe uz provedbu primjerenih mjera zaštite propisanih Uredbom, **cjelovitost i povjerljivost**; podaci će biti obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera. Navedene mjere primjenjuju se u svim organizacijskim jedinicama Banke. Obaveza je da su osobni podaci u poslovnicama i u „back office“ prostorijama Banke pohranjeni u zaključanim ormarima. Obaveza je provođenja politike čistih radnih stolova u cijeloj Banci, a mjesta u ili na kojima su sadržani osobni podaci ne smiju biti ostavljena nezaključanima i bez odgovarajućeg nadzora. Svi zaposlenici Banke potpisali su izjavu o povjerljivosti kojom se obvezuju na poštivanje načela cjelovitosti i povjerljivosti obrade osobnih podataka.

### **Zakonitost obrade**

Banka je u svom poslovanju uspostavila mehanizme kojima provodi obradu osobnih podataka kao zakonitu i to samo ako je ispunjeno najmanje jedno od sljedećega:

- (a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha; privola je 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; ispitanik ima pravo u svakom trenutku povući svoju privolu
- (b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora
- (c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade; primjerice obrada u skladu sa Zakonom o sprječavanju pranja novca i financiranja terorizma ili obrada kroz video-nadzor u skladu s Zakonom o zaštiti novčarskih institucija
- (d) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe; primjerice, otkrivanje od strane nadležnih tijela podataka jednog roditelja drugomu u svrhu uzdržavanja djeteta
- (e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade
- (f) 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. Primjerice, unapređenja procesa.

### **Obrada posebnih kategorija osobnih podataka**

Banka ne vrši obradu osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obradu genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca.

Navedeno se ne primjenjuje samo ako je ispunjeno jedno od sljedećeg:

- (a) ispitanik je dao izričitu privolu za obradu tih osobnih podataka za jednu ili više određenih svrha;
- (b) obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava voditelja obrade ili ispitanika u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti u mjeri u kojoj je to odobreno u okviru prava Unije ili prava Republike Hrvatske;
- (c) obrada je nužna za zaštitu životno važnih interesa ispitanika ili drugog pojedinca;
- (d) obrada se provodi u sklopu legitimnih aktivnosti s odgovarajućim zaštitnim mjerama;
- (e) obrada se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik;
- (f) obrada je nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva ili kad god sudovi djeluju u sudbenom svojstvu;
- (g) obrada je nužna za potrebe značajnog javnog interesa na temelju prava Unije ili prava države Republike Hrvatske;

(h) obrada je nužna u svrhu preventivne medicine ili medicine rada radi procjene radne sposobnosti zaposlenika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi ili tretmana ili upravljanja zdravstvenim ili socijalnim sustavima i uslugama;

(i) obrada je nužna u svrhu javnog interesa u području javnog zdravlja;

(j) obrada je nužna u svrhu arhiviranja u javnom interesu, u svrhu znanstvenog ili povijesnog istraživanja ili u statističke svrhe.

Prema odredbama Zakona, u okviru obrade osobnih podataka u svrhu proizvodnje službene statistike u skladu s posebnim propisima iz područja službene statistike, tijela koja proizvode službenu statistiku nisu dužna osigurati ispitanicima pravo pristupa osobnim podacima, pravo na ispravak osobnih podataka, pravo na ograničenje obrade osobnih podataka niti pravo na prigovor na obradu osobnih podataka, i to radi osiguravanja uvjeta nužnih za ostvarivanje svrhe službene statistike u mjeri u kojoj je vjerojatno da bi se takvim pravima moglo onemogućiti ili ozbiljno ugroziti postizanje tih svrha te kada su takva odstupanja od prava prijeko potrebna za postizanje tih svrha.

Tijela nadležna za proizvodnju službene statistike dužna su primjenjivati tehničke i organizacijske mjere zaštite podataka prikupljenih za potrebe službene statistike.

Banka kao voditelj obrade osobnih podataka prilikom prijenosa osobnih podataka tijelima nadležnima za službenu statistiku nije dužna obavještavati ispitanike o prijenosu osobnih podataka u statističke svrhe.

Obrada osobnih podataka u statističke svrhe smatra se podudarnom svrsi za koju su podaci prikupljeni, pod uvjetom da se poduzmu odgovarajuće zaštitne mjere.

Osobni podaci obrađeni u statističke svrhe ne smiju omogućiti identifikaciju osobe na koju se podaci odnose.

### **Prava ispitanika**

Banka je u svom poslovanju uspostavila mehanizme kroz koje su zadovoljena sva prava ispitanika u skladu s Uredbom. Proces ostvarivanja prava ispitanika odvija se dostavom zahtjeva kroz sljedeće kanale: primarno službenik za zaštitu osobnih podataka ili poslovnica. Ukoliko se zahtjev dostavlja kroz poslovnicu, nužna je istovremena obavijest iz poslovnice prema službeniku za zaštitu osobnih podataka. Službenik za zaštitu osobnih podataka zadužen je za daljnju koordinaciju sa nadležnim organizacijskim jedinicama Banke vezano uz obradu zahtjeva kao i distribuciju zahtjeva te za nadzor provedbe.

### **Transparentne informacije, komunikacija i modaliteti za ostvarivanje prava ispitanika**

Banka kao voditelj obrade poduzima potrebne mjere kako bi se ispitaniku pružile sve informacije iz članaka 13. i 14. Uredbe i omogućilo ostvarivanje prava ispitanika na pristup, prava na ispravak, prava na brisanje, prava na ograničenje obrade, obveza izvješćivanja, prava na prenosivost podataka, prava na prigovor i obavješćivanje ispitanika o povredi osobnih podataka.

Banka kao voditelj obrade ispitaniku pruža informacije o poduzetim radnjama za ostvarivanja prava ispitanika u svakom navedenom slučaju u roku od mjesec dana od zaprimanja zahtjeva. Taj se rok može prema potrebi produljiti za dodatna dva mjeseca, uzimajući u obzir složenost i broj zahtjeva. Voditelj obrade obavješćuje ispitanika o svakom takvom produljenju u roku od mjesec dana od zaprimanja zahtjeva, zajedno s razlozima odgađanja. Ako ispitanik podnese zahtjev elektroničkim putem, informacije se pružaju elektroničkim putem ako je to moguće, osim ako ispitanik zatraži drugačije.

Ako Banka kao voditelj obrade ne postupi po zahtjevu ispitanika, voditelj obrade bez odgađanja i najkasnije jedan mjesec od primitka zahtjeva izvješćuje ispitanika o razlozima zbog kojih nije postupio i o mogućnosti podnošenja pritužbe nadzornom tijelu i traženja pravnog lijeka.

Svaki ispitanik koji smatra da mu je povrijeđeno neko pravo zajamčeno Zakonom i Uredbom, može Agenciji podnijeti zahtjev za utvrđivanje povrede prava.

### **Informacije koje treba dostaviti ako se osobni podaci prikupljaju od ispitanika**

Ako su osobni podaci koji se odnose na ispitanika prikupljeni od ispitanika, Banka kao voditelj obrade u trenutku prikupljanja osobnih podataka ispitaniku pruža sljedeće informacije:

(a) identitet i kontaktne podatke voditelja obrade i, ako je primjenjivo, predstavnika voditelja obrade;

- (b) kontaktne podatke službenika za zaštitu podataka, ako je primjenjivo;
- (c) svrhe obrade radi kojih se upotrebljavaju osobni podaci kao i pravnu osnovu za obradu;
- (d) ako je primjenjivo, legitimne interese voditelja obrade ili treće strane;
- (e) primatelje ili kategorije primatelja osobnih podataka, ako ih ima; i
- (f) ako je primjenjivo, činjenicu da voditelja obrade namjerava osobne podatke prenijeti trećoj zemlji ili međunarodnoj organizaciji.

Osim gornjih informacija, voditelj obrade u trenutku kada se osobni podaci prikupljaju pruža ispitaniku sljedeće dodatne informacije potrebne kako bi se osigurala poštena i transparentna obrada:

- (a) razdoblje u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterije kojima se utvrdilo to razdoblje;
- (b) postojanje prava da se od voditelja obrade zatraži pristup osobnim podacima i ispravak ili brisanje osobnih podataka ili ograničavanje obrade koji se odnose na ispitanika ili prava na ulaganje prigovora na obradu takvih te prava na prenosivost podataka;
- (c) ako je primjenjivo, postojanje prava da se u bilo kojem trenutku povuče privolu, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije nego što je ona povučena;
- (d) pravo na podnošenje prigovora nadzornom tijelu;
- (e) informaciju o tome je li pružanje osobnih podataka zakonska ili ugovorna obveza ili uvjet nužan za sklapanje ugovora te ima li ispitanik obvezu pružanja osobnih podataka i koje su moguće posljedice ako se takvi podaci ne pruže;

Ako osobni podaci nisu dobiveni od ispitanika, uz navedene informacije pridodaje se izvor osobnih podataka.

### **Pravo ispitanika na pristup**

Ispitanik ima pravo dobiti od voditelja obrade potvrdu obrađuju li se osobni podaci koji se odnose na njega te ako se takvi osobni podaci obrađuju, pristup osobnim podacima i informacije, među ostalim, o obrađenim osobnim podacima, o svrsi obrade, roku pohrane, iznošenju u treće zemlje.

### **Pravo na ispravak**

Ispitanik ima pravo zahtijevati ispravak netočnih osobnih podataka koji se na njega odnose, a uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave.

### **Pravo na brisanje („pravo na zaborav“)**

Ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja te voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako je ispunjen jedan od sljedećih uvjeta:

- (a) osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni;
- (b) ispitanik povuče privolu na kojoj se obrada temelji i ako ne postoji druga pravna osnova za obradu;
- (c) ispitanik uloži prigovor na obradu u skladu s člankom 21. Uredbe;
- (d) osobni podaci nezakonito su obrađeni;
- (e) osobni podaci moraju se brisati radi poštovanja pravne obveze iz prava Unije ili prava Republike Hrvatske;

### **Pravo na ograničenje obrade**

Banka će osobne podatke ispitanika koristiti isključivo za svrhu za koju su prikupljeni. U slučaju nastajanja poslovne potrebe za korištenjem osobnih podataka u bilo koju drugu svrhu, od one inicijalno predviđene, ispitanik će o tome biti pravovremeno obaviješten, a po potrebi će biti zatražena i privola.

O potrebi korištenja osobnih podataka za drugu svrhu od one za koju su inicijalno prikupljeni, potrebno je informirati službenika za zaštitu osobnih podataka, koji takvu promjenu mora u pisanom obliku dozvoliti.

Ispitanik ima pravo od voditelja obrade ishoditi ograničenje obrade kada osporava točnost osobnih podataka, kada je obrada nezakonita ili kada voditelj obrade više ne treba osobne podatke za potrebe obrade.

### **Obveza izvješćivanja u vezi s ispravkom ili brisanjem osobnih podataka ili ograničenjem obrade**

Voditelj obrade priopćuje svaki ispravak ili brisanje osobnih podataka ili ograničenje obrade svakom primatelju kojem su otkriveni osobni podaci, osim ako se to pokaže nemogućim ili zahtijeva nerazmjerni napor. Voditelj obrade obavješćuje ispitanika o tim primateljima ako to ispitanik zatraži.

### **Pravo na prenosivost podataka**

Ispitanik ima pravo zaprimiti osobne podatke koji se odnose na njega, a koje je pružio voditelju obrade u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade bez ometanja od strane voditelja obrade kojem su osobni podaci pruženi, ako se obrada provodi automatiziranim putem i temelji na privoli ili ugovoru. Banka je uspostavila mehanizam u kojem se ispitaniku pružaju podaci u strojno čitljivom formatu i dostavljaju mailom.

### **Pravo na prigovor**

Ispitanik ima pravo na temelju svoje posebne situacije uložiti prigovor na obradu osobnih podataka koji se odnose na njega; tada voditelj obrade ne smije više obrađivati osobne podatke ispitanika osim ako dokaže da njegovi legitimni razlozi za obradu nadilaze interese ispitanika te radi zaštite pravnih zahtjeva; ujedno, ako se ispitanik protivi obradi za potrebe izravnog marketinga, osobni podaci više se ne smiju obrađivati. Banka ne provodi aktivnosti izravnog marketinga.

### **Automatizirano pojedinačno donošenje odluka, uključujući izradu profila**

Ispitanik ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu, osim ako je takva odluka potrebna za sklapanje ili izvršenje ugovora između ispitanika i voditelja obrade podataka, ako je dopuštena pravom Unije ili pravom Republike Hrvatske ili temeljena na izričitoj privoli ispitanika. Banka ne donosi odluke na temelju automatiziranog donošenja odluka niti izrađuje profile.

### **Ograničenja**

Zaštita osobnih podataka nije apsolutno pravo već pravo koje treba balansirati s drugim pravima. Stoga, na temelju prava Unije ili prava Republike Hrvatske voditelj ili izvršitelj obrade mogu ograničiti opseg prava ispitanika ako se takvim ograničenjem poštuje bit temeljnih prava i sloboda te ono predstavlja nužnu i razmjernu mjeru u demokratskom društvu za zaštitu značajnih vrijednosti poput nacionalne sigurnosti, obrane, javne sigurnosti, drugih važnih ciljeva od općeg javnog interesa Unije ili države članice, zaštite neovisnosti pravosuđa i sl.

Svaka takva zakonodavna mjera sadrži posebne odredbe o svrhama obrade ili kategorijama obrade, kategorijama osobnih podataka, opsegu uvedenih ograničenja, zaštitnim mjerama za sprečavanje zlorabe, specifikaciji voditelja obrade ili kategorija voditelja obrade i ostalim aspektima kako bi se zaštitila prava pojedinaca.

## **VODITELJ OBRAD E I IZVRŠITELJ OBRAD E**

### **Obveze voditelja i izvršitelja obrade**

Uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade te njezinu rizičnost, voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s Uredbom. Te se mjere prema potrebi preispituju i ažuriraju.

## **Tehnička i integrirana zaštita podataka**

Banka je implementirala metodologije i procese koji osiguravaju da su pitanja privatnosti i zaštite osobnih podataka adekvatno adresirana prilikom inicijalnog dizajna i arhitekture sustava koji obrađuju osobne podatke (*engl. Privacy by design*).

Konfiguracija sustava koji obrađuje osobne podatke mora biti postavljena na način da su mjere vezane uz privatnost i zaštitu osobnih podataka inicijalno omogućene s ciljem osiguravanja maksimalne privatnosti za ispitanika (*engl. Privacy by default*).

Za svaki sustav koji obrađuje osobne podatke osigurati će se pisani zapis koji će potvrditi da su prilikom dizajna sustava adresirane kontrole vezane uz privatnost i zaštitu osobnih podataka te da su sve relevantne postavke inicijalno omogućene. Eventualno isključenje kontrola koje osiguravaju privatnost i zaštitu osobnih podataka biti će dokumentirane i adekvatno obrazložene. Službenik za zaštitu osobnih podataka mora biti upoznat s prethodno navedenim zapisima te iste mora odobriti zajedno sa voditeljem Službe informacijske sigurnosti.

## **Izvršitelj obrade**

Ako se obrada provodi u ime voditelja obrade, voditelj obrade koristi se jedino izvršiteljima obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu sa zahtjevima iz ove Uredbe i da se njome osigurava zaštita prava ispitanika.

Izvršitelj obrade ne smije angažirati drugog izvršitelja obrade bez prethodnog posebnog ili općeg pisanog odobrenja voditelja obrade. U slučaju općeg pisanog odobrenja, izvršitelj obrade obavješćuje voditelja obrade o svim planiranim izmjenama u vezi s dodavanjem ili zamjenom drugih izvršitelja obrade kako bi time voditelju obrade omogućio da uloži prigovor na takve izmjene.

Obrada koju provodi izvršitelj obrade uređuje se ugovorom, kojim se izvršitelja obrade obvezuje prema voditelju obrade, te se u njemu moraju navesti predmet i trajanje obrade, prirodu i svrhu obrade, vrstu osobnih podataka i kategoriju ispitanika te obveze i prava voditelja obrade. Ugovorom se osobito određuje da izvršitelj obrade mora među ostalim postupati prema uputama voditelja obrade, da fizičke osobe koje obrađuju osobne podatke su dužne čuvati povjerljivost istih te da će postupiti u skladu s odredbama Uredbe.

## **Evidencija aktivnosti obrade**

Voditelj obrade vodi evidenciju aktivnosti obrade za koje je odgovoran. Ta evidencija sadržava sve sljedeće informacije:

- ime i kontaktne podatke voditelja obrade i, ako je primjenjivo, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka;
- svrhu obrade;
- opis kategorija ispitanika i kategorija osobnih podataka;
- kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije;
- ovlaštene osobe koje imaju pristup podacima;
- ako je primjenjivo, prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije te, u slučaju prijenosa iz članka 49. stavka 1. drugog podstavka, dokumentaciju o odgovarajućim zaštitnim mjerama;
- ako je to moguće, predviđene rokove za brisanje različitih kategorija podataka;
- ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 32. stavka 1.
- osnovu obrade: zakonski okvir, legitimni interes, privola

Svaki izvršitelj obrade i predstavnik izvršitelja obrade, vodi evidenciju svih kategorija aktivnosti obrade koje se obavljaju za voditelja obrade, koja sadržava:

- ime i kontaktne podatke jednog ili više izvršitelja obrade i svakog voditelja obrade u čije ime izvršitelj obrade djeluje te, ako je primjenjivo, predstavnika voditelja obrade ili izvršitelja obrade te službenika za zaštitu podataka;
- kategorije obrade koje se obavljaju u ime svakog voditelja obrade;

- ako je primjenjivo, prijenos osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije te dokumentaciju o odgovarajućim zaštitnim mjerama;
- ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera

Evidenciju vodi i ažurira službenik za zaštitu osobnih podataka, prema podacima dostavljenim iz ovlaštenih organizacijskih jedinica Banke. Evidencija mora biti u pisanom obliku, uključujući elektronički oblik.

## **SIGURNOST OSOBNIH PODATAKA**

### **Sigurnost obrade**

Uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi:

- (a) pseudonimizaciju i enkripciju osobnih podataka;
- (b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;
- (c) sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta;
- (d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

### **Izješćivanje nadzornog tijela o povredi osobnih podataka**

Ako je vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode ispitanika, voditelj obrade mora izvijestiti bez odgađanja nadzorno tijelo o povredi osobnih podataka (najkasnije u roku od 72 sata od saznanja o povredi). Nadzorno tijelo je Agencija za zaštitu osobnih podataka. Navedeno izješćivanje treba sadržati opis povrede uz informacije o ispitanicima i osobnim podacima, opis vjerojatnih posljedica povrede, opis mjera koje su poduzete ili predložene za rješavanje povrede te kontakt točku voditelja. Ukoliko se dogodi propust vezan uz zaštitu osobnih podataka, svi radnici Banke dužni su o istome odmah izvijestiti službenika za zaštitu osobnih podataka.

### **Obavješćivanje ispitanika o povredi osobnih podataka**

Ako je vjerojatno da će povreda prouzročiti visok rizik za prava i slobode ispitanika, voditelj obrade je dužan informirati ispitanika o povredi osobnih podataka. Iznimno, neće biti potrebno ako je voditelj obrade primijenio zaštitne mjere kojima je spriječio korištenje povrijeđenih osobnih podataka, poduzeo naknadne mjere zaštite zbog kojih nije vjerojatan visok rizik ili ako je kontaktiranje svakog ispitanika predstavljalo nerazmjernan napor, pri čemu je onda nužno ispitanike obavijestiti sredstvima javnog priopćavanja ili na drugi djelotvoran način

## **PROCJENA UČINKA NA ZAŠTITU PODATAKA I PRETHODNO SAVJETOVANJE**

### **Procjena učinka na zaštitu podataka**

Ako je vjerojatno da će neka vrsta obrade prouzročiti visok rizik za prava i slobode ispitanika, tada je voditelj obrade dužan provesti procjenu učinka. Provođenje procjene učinka je nužno ako se sustavno i opsežno procjenjuju osobni aspekti pojedinaca temeljem automatizirane obrade (profiliranje) /što Banka ne provodi/, ako se opsežno obrađuju posebne kategorije osobnih podataka ili podaci kaznenim djelima ili osudama (tu ne spada obrada politički izloženih osoba ili obrada doznaka o bolovanju od strane Banke) te ako se sustavno prati javno dostupno područje u velikoj mjeri (tu ne spada video nadzor dijela vanjskog prostora ispred Banke).

Procjena učinka treba sadržavati opis postupaka obrade i njezine svrhe, procjenu nužnosti i proporcionalnosti, procjenu rizičnosti te opis mjera kojima se umanjuje rizičnost obrade.

Ako bi se procjenom učinka na zaštitu podataka pokazalo da bi, u slučaju da voditelj obrade ne donese mjere za ublažavanje rizika, obrada dovela do visokog rizika, tada je voditelj obrade dužan kontaktirati nadzorno tijelo i dostaviti mu među ostalima informacije o svrsi i sredstvima obrade, zaštitnim mjerama, provedenoj procjeni učinka itd.

Banka trenutno ne provodi sustavnu i opsežnu procjenu osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila, i na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili na sličan način značajno utječu na pojedinca; ne provodi opsežnu obradu posebnih kategorija osobnih podataka; ne provodi sustavno praćenje javno dostupnog područja u velikoj mjeri, pa stoga nema potrebe za procjenom učinka rizika.

## **SLUŽBENIK ZA ZAŠTITU PODATAKA**

### **Imenovanje službenika za zaštitu podataka**

Voditelj obrade je imenovao službenika za zaštitu osobnih podataka. Službenik je imenovan na temelju stručnih kvalifikacija, te sposobnosti izvršavanja zadaća:

(a) informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz Uredbe te drugim odredbama Unije ili prava Republike Hrvatske;

(b) praćenje poštovanja Uredbe te drugih odredaba Unije ili prava Republike Hrvatske o zaštiti podataka i politika voditelja obrade ili izvršitelja obrade u odnosu na zaštitu osobnih podataka, uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade te povezane revizije;

(c) pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja;

(d) suradnja s nadzornim tijelom;

(e) djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, te savjetovanje, prema potrebi, o svim drugim pitanjima;

(f) provođenje odredbi iz ovog Pravilnika

Službenik za zaštitu podataka pri obavljanju svojih zadaća vodi računa o riziku povezanom s postupcima obrade i uzima u obzir prirodu, opseg, kontekst i svrhe obrade. Službenik za zaštitu podataka odgovorna je osoba za sudjelovanje i uključenje u svim procesima i svim pitanjima u svezi zaštite osobnih podataka. U kontekstu potrebe za ostvarivanjem prava ispitanika, dostupni kontakti službenika za zaštitu podataka su:

Službenik za zaštitu osobnih podataka, Aleja kralja Zvonimira 1, 42000 Varaždin; Tel: 042 659-443;

Faks: 042 659-331; e-mail: [zastita.osobnih.podataka@jtbanka.hr](mailto:zastita.osobnih.podataka@jtbanka.hr)

Ovaj Pravilnik se primjenjuje od 25.05.2018.