

## Opći uvjeti poslovanja Zagrebačke banke d.d. za korištenje direktnih kanala od strane potrošača

Izdavatelj ovih Općih uvjeta poslovanja Zagrebačke banke d.d. za korištenje direktnih kanala od strane potrošača (dalje u tekstu: Opći uvjeti poslovanja) jest Zagrebačka banka d.d., Trg bana Josipa Jelačića 10, 10000 Zagreb, Republika Hrvatska (dalje u tekstu: Banka), SWIFT oznaka: ZABHR2X, upisana u sudski registar kod Trgovačkog suda u Zagrebu rješenjem broj Tt-95/1-2 od 17. 3. 1995., MBS 080000014, OIB 92963223473, [zaba@unicreditgroup.zaba.hr](mailto:zaba@unicreditgroup.zaba.hr), Internetska stranica Banke: [www.zaba.hr](http://www.zaba.hr).

Banka posluje na temelju odobrenja za rad Hrvatske narodne banke koja je nadležno tijelo za nadzor nad poslovanjem Banke, izuzev u dijelu pružanja usluga povjerenja koje su regulirane Uredbom (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257/73 28. 8. 2014. – dalje u tekstu: Uredba (EU) br. 910/2014), u pogledu kojih usluga je za nadzor poslovanja Banke nadležno središnje tijelo državne uprave nadležno za poslove gospodarstva.

### 1. PODRUČJE PRIMJENE

1.1. Ovi Opći uvjeti poslovanja uređuju uvjete korištenja direktnih kanala od strane fizičke osobe potrošača (dalje u tekstu: Korisnik) te dopunjuju posebne pogodbe ugovora o korištenju pojedinih direktnih kanala sklopljenih između Banke i Korisnika i sastavni su dio svakog od tih ugovora.

1.2. Ovi Opći uvjeti poslovanja primjenjuju se zajedno s Izvatom iz Odluke o tarifi naknada za usluge Banke po transakcijskim računima fizičkih osoba i usluga platnog prometa te direktnih kanala.

1.3. Ako je Korisnik zaključio s Bankom Ugovor o pružanju usluga povjerenja za kvalificirani osobni potpisni certifikat, ovi Opći uvjeti poslovanja primjenjuju se zajedno s tim ugovorom.

### 2. POJMOVNIK

2.1. Pojedini pojmovi upotrijebljeni u ovim Općim uvjetima poslovanja imaju sljedeće značenje:

**Aktivacijski ključ i Identifikacijski ključ** su osobni tajni identifikacijski brojevi koje Banka dodjeljuje Korisniku kao Personalizirane sigurnosne vjerodajnice, a služe za aktivaciju pojedinog Direktnog kanala i/ili pojedine usluge koja je Korisniku dostupna putem pojedinog Direktnog kanala ili za aktivaciju pojedinog sredstva za autentifikaciju i autorizaciju, nakon čega se više ne mogu upotrebljavati.

**Autorizacija** znači postupak kojim Korisnik putem ugovorenog Direktnog kanala daje suglasnost za izvršenje jedne ili više platnih ili drugih financijskih ili nefinancijskih transakcija ili kojim ugovara jednu ili više bankovnih ili nebankovnih usluga ili potvrđuje prihvata dokumenta.

**Biometrijska autentifikacija** jest autentifikacija Korisnika koju Banka provodi prilikom pristupa Korisnika *On-line* bankarstvu putem mobilne aplikacije (m-zaba) i/ili m-tokenu, a temelji se na primjeni dvaju međusobno nezavisnih elemenata, od kojih jedan element predstavlja svojstvo Korisnika (npr. otisak prsta ili prepoznavanje lica), a drugi element predstavlja sredstvo za autentifikaciju i autorizaciju koje je Banka dodijelila Korisniku (npr. m-token).

- **Autentifikacija otiskom prsta (engl. *Touch ID*)** predstavlja metodu autentifikacije pomoću biometrije, otiska prsta koji je Korisnik pohranio u mobilni uređaj kojim se koristi za pristup *On-line* bankarstvu putem mobilne aplikacije (m-zaba) i/ili m-tokenu pri čemu mobilni uređaj uspoređuje otisak prsta koji je prethodno pohranjen u taj Pametni uređaj s otiskom prsta kojim se pristupa m-zabi/m-tokenu. Banka se oslanja na tako provedenu biometrijsku autentifikaciju putem mobilnog uređaja te se Korisnik smatra autentificiranim ako mobilni uređaj potvrdi podudarnost otiska prsta prethodno pohranjenog u mobilni uređaj s otiskom prsta kojim se pristupa m-zabi /m-tokenu.
- **Autentifikacija prepoznavanjem lica (engl. *Face recognition*)** predstavlja metodu autentifikacije pomoću biometrije koja se temelji na prepoznavanju lica čije je biometrijske karakteristike Korisnik pohranio u mobilni uređaj kojim se koristi za pristup *On-line* bankarstvu putem mobilne aplikacije (m-zaba) i/ili m-tokenu, pri čemu taj mobilni uređaj uspoređuje crte lica prethodno pohranjene u mobilni uređaj s crtama lica koje mobilni uređaj učitava prilikom pristupa m-zabi/m-tokenu. Banka se oslanja na tako provedenu biometrijsku autentifikaciju putem mobilnog uređaja te se Korisnik smatra autentificiranim ako mobilni uređaj potvrdi podudarnost biometrijskih značajki lica prethodno pohranjenih u mobilni uređaj s biometrijskim značajkama lica kojima se pristupa m-zabi/m-tokenu.

**Direktni kanali** – označuju sve oblike daljinske komunikacije Korisnika s Bankom bez istodobne fizičke prisutnosti Korisnika i zaposlenika Banke koji omogućuju ugovaranje i korištenje pojedinim bankovnim i/ili nebankovnim uslugama i/ili obavljanje drugih transakcija koje Banka omogući Korisniku te razmjenu informacija između Banke i Korisnika putem elektroničkih načina komuniciranja (primjerice: *On-line* bankarstvo).

**Dubinska analiza** – obuhvaća mjere koje Banka sukladno Mjerodavnim propisima poduzima prilikom uspostave poslovnog odnosa s Korisnikom računa te periodično tijekom trajanja poslovnog odnosa, a koje primjerice uključuju:

- utvrđivanje i provjeru identiteta Korisnika računa
- prikupljanje podataka o namjeni i predviđenoj prirodi poslovnoga odnosa te drugih podataka u skladu s Mjerodavnim propisima
- stalno praćenje poslovnog odnosa, uključujući i kontrolu transakcija koje Korisnik računa obavlja.

**Elektronička platna transakcija** jest platna transakcija (kreditni transfer) koja je inicirana i izvršena upotrebom elektroničke platforme ili uređaja kao što su primjerice računalo ili mobilni uređaj.

**Elektronički potpis, Kvalificirani elektronički potpis** – imaju značenje kako im je određeno u članku 5. gdje su definirani svi pojmovi u vezi s Elektroničkim potpisom i Kvalificiranim elektroničkim potpisom.

**e-poslovnica** – predstavlja uslugu koja Korisniku omogućuje da nakon provedene autentifikacije, putem telefona, *chata*, videopoziva ili Verificirane e-adrese obavlja određene transakcije i/ili prima od Banke određene informacije. Komunikacija putem e-poslovnice provodi se isključivo na hrvatskome jeziku s punoljetnim i poslovno sposobnim korisnicima sa statusom rezidenta Republike Hrvatske.

**Identifikacija i Autentifikacija** označuju postupke koji Banci omogućuju provjeru identiteta Korisnika prilikom korištenja pojedinim Direktnim kanalom i provjeru valjanosti primjene sredstva za autentifikaciju i autorizaciju, uključujući provjeru upotrebe Korisnikovih Personaliziranih sigurnosnih vjerodajnica.

**Jednokratne lozinke / kodovi** – niz brojeva koji su generirani u m-zaba aplikaciji ili putem m-tokena, a koji mogu služiti za verifikaciju broja mobitela Korisnika, registraciju za pristup određenim uslugama ili funkcionalnostima, Identifikaciju i/ili Autentifikaciju Korisnika za korištenje pojedinim uslugama ili za drugu svrhu koju je Banka odredila (primjerice OTP – *One Time Password*).

**Kontakt centar** – centar kojem se Korisnik može obratiti s upitom, zahtjevom i/ili prigovorom u vezi s korištenjem Direktnim kanalima na broj telefona ili kontaktnu adresu koja je Korisnicima dostupna putem Internetske stranice Banke.

**Korisnik** je fizička osoba, potrošač, koja ugovara korištenje Direktnim kanalom i koristi se Direktnim kanalom izvan područja svoje poslovne djelatnosti ili slobodnog zanimanja.

**Mjerodavni propisi** označuje svaki propis, smjernicu, uputu, preporuku, standard, tumačenje propisa i mišljenje, tijela koje je nadležno za nadzor nad poslovanjem banaka ili nekog drugog ovlaštenog tijela, koje Banka primjenjuje i u mjeri u kojoj ih primjenjuje u poslovanju uključujući sve njihove izmjene i dopune.

**Mobilni token** (dalje u tekstu: **m-token**) jest platni instrument, sredstvo za autentifikaciju Korisnika i Autorizaciju koje Korisnik instalira na mobilni uređaj u okviru m-zaba aplikacije, a koje generira Jednokratne lozinke ograničenog trajanja kojima se Korisnik autentificira prilikom korištenja pojedinim Direktnim kanalima i/ili pojedinim drugim bankovnim ili nebankovnim uslugama, odnosno kojim autorizira Elektroničke platne transakcije te druge financijske i nefinancijske transakcije.

**m-PIN** – osobni tajni identifikacijski broj koji definira, odnosno određuje sam Korisnik, poznat isključivo njemu, a upotrebljava se za autentifikaciju Korisnika prilikom pristupa *On-line* bankarstvu putem mobilne aplikacije (m-zaba) ili m-tokenu.

**m-zaba aplikacija** – aplikacija za mobilni uređaj koja objedinjuje više različitih funkcionalnosti i/ili usluga koje Banka čini dostupnima putem aplikacije, primjerice mogućnosti ugovaranja pojedinih bankovnih i nebankovnih usluga i dr. Banka prema svojoj diskrecijskoj ocjeni odlučuje koje će usluge i funkcionalnosti biti dostupne u aplikaciji.

**On-line bankarstvo** su Direktni kanali putem kojih Banka omogućuje Korisniku korištenje pojedinim uslugama putem interneta (*On-line* bankarstvo putem interneta (e-zaba)) ili mobilne aplikacije koju je Korisnik prethodno instalirao na svojem mobilnom uređaju (*On-line* bankarstvo putem mobilne aplikacije (m-zaba)).

- **On-line bankarstvo putem interneta** ili **e-zaba** jest usluga koja Korisniku omogućuje da putem interneta te pomoću m-tokena obavlja Elektroničke platne transakcije i/ili druge financijske ili nefinancijske transakcije koje mu omogući Banka, sklapa pojedine ugovore u elektroničkom obliku, prati stanja i izmjena stanja po računima otvorenim u Banci, podnosi zahtjeve te prima od Banke obavijesti i dokumentaciju u elektroničkom obliku.
- **On-line bankarstvo putem mobilne aplikacije** ili **m-zaba** jest usluga koja Korisniku omogućuje da putem mobilne aplikacije obavlja Elektroničke platne transakcije i/ili druge financijske ili nefinancijske transakcije koje mu omogući Banka, sklapa pojedine ugovore u elektroničkom obliku, prati stanja i promjene stanja po računima otvorenim u Banci, podnosi

zahtjeve te prima od Banke obavijesti i dokumentaciju u elektroničkom obliku.

**Personalizirane sigurnosne vjerodajnice** – personalizirana sigurnosna obilježja koja Banka daje Korisniku u svrhu autentifikacije (primjerice: m-PIN, Jednokratne lozinke, Identifikacijski ključ, Aktivacijski ključ, Lozinka za pristup kvalificiranom certifikatu za elektronički potpis i sve druge lozinke i kodovi koje je Banka dostavila/odredila Korisniku u svrhu Identifikacije i/ili Autentifikacije.

**Pouzdana autentifikacija** jest postupak provjere identiteta Korisnika ili valjanosti upotrebe platnog instrumenta, uključujući provjeru upotrebe Personaliziranih sigurnosnih vjerodajnica Korisnika na osnovi uporabe bar dvaju elemenata koji su međusobno neovisni, od kojih je jedan uvijek platni instrument (npr. m-token), a drugi element može biti Autentifikacija otiskom prsta (engl. *Touch ID*), Autentifikacija prepoznavanjem lica (engl. *Face recognition*), m-PIN ili druga Personalizirana sigurnosna vjerodajnica u skladu s ovim Općim uvjetima poslovanja.

**Pretinac za digitalne dokumente** je Direktni kanal u kojem je Korisniku omogućeno da putem interneta putem poveznice koju mu Banka dostavi te pomoću m-tokena za pojedine proizvode i usluge podnosi zahtjeve, dostavi potrebnu dokumentaciju, sklapa ugovore u elektroničkom obliku te primi od Banke pripadajuću dokumentaciju u elektroničkom obliku.

**Sankcije** – označuju gospodarske, financijske, trgovinske ili druge mjere ograničenja koje Banka primjenjuje u poslovanju koje, među ostalim, uključuju potpun ili djelomičan prekid gospodarskih odnosa, zabranu pružanja pojedinih ili svih usluga, ograničenja raspolaganja imovinom te druga slična ograničenja određena:

- (i) pravnim aktima Ujedinjenih naroda ili drugih međunarodnih organizacija koji obvezuju Republiku Hrvatsku, ili
- (ii) propisima Republike Hrvatske ili odlukama Vlade Republike Hrvatske ili drugih nadležnih tijela Republike Hrvatske, ili
- (iii) propisima Europske unije ili odlukama Vijeća Europske unije, Europske komisije ili drugih nadležnih tijela Europske unije, ili
- (iv) propisima Sjedinjenih Američkih Država (SAD) ili odlukama državnih tijela SAD-a, uključujući Ured za kontrolu strane imovine američkog Ministarstva financija (OFAC), ili
- (v) propisima Ujedinjenog Kraljevstva (UK) ili odlukama državnih tijela UK-a, uključujući Ured za provedbu financijskih sankcija (*Office of Financial Sanctions Implementation* – OFSI), ili
- (vi) propisima ili odlukama državnih tijela bilo koje druge države na čijem području Banka i/ili bilo koja druga članica grupe kreditnih institucija kojoj pripada Banka pruža usluge, bilo

neposredno ili posredstvom svojih podružnica, predstavništva ili zastupnika.

**Sankcionirana država** – svaka država ili područje koje je pod Sankcijama ili protiv čije su vlade ili druge vladajuće strukture odnosno tijela izvršne vlasti usmjerene Sankcije; lista država i područja protiv kojih je uveden opsežan paket zabrana i država protiv kojih je uveden uži paket zabrana dostupna je na Internetskim stranicama Banke.

**Sankcionirana osoba** – označuje bilo koju fizičku ili pravnu osobu, međunarodnu organizaciju ili subjekt bez pravne osobnosti protiv kojih su usmjerene Sankcije, odnosno pravni subjekt koji je u vlasništvu jedne ili više sankcioniranih osoba ili kojeg kontrolira jedna ili više sankcioniranih osoba navedenih na sankcijskim listama.

- **Osoba povezana sa sankcioniranom državom** – je pojedinac koji zakonito boravi u Republici Hrvatskoj odnosno državi u kojoj posluje Banka, odnosno u bilo kojoj drugoj državi unutar EU-a ili Europskog gospodarskog prostora (EGP), SAD-a, UK-a, Australije i Kanade s ekvivalentnim programom sankcija, a koji je po državljanstvu povezan sa sankcioniranom državom ili područjem.

**Ugovor o korištenju direktnim kanalom** jest svaki ugovor o korištenju Direktnim kanalom koji je sklopljen između Banke i Korisnika, neovisno o njegovu nazivu i obliku u kojem je sklopljen.

Pojmovi „Usluga informiranja o računu“, „Usluga iniciranja plaćanja“, „Pružatelj usluge informiranja o računu ili AISP“ i „Pružatelj usluge iniciranja plaćanja ili PISP“ imaju isto značenje kao i u Općim uvjetima poslovanja Zagrebačke banke d.d. po transakcijskim računima potrošača.

### 3. OPĆE ODREDBE

3.1. Odluku o uspostavi poslovnog odnosa s Korisnikom Banka donosi prema slobodnoj procjeni, u skladu sa svojom poslovnom strategijom i pristupom utemeljenim na riziku, bez obveze davanja obavijesti i obrazloženja.

3.2. Banka poslovni odnos uspostavlja i održava pod pretpostavkom urednog ispunjavanja obveza koje proizlaze iz Mjerodavnih propisa i ugovora kao što su primjerice, ali ne isključivo:

- podmirivanje obveza prema Banci sredstvima koja potječu iz zakonitih izvora
- pravovremena i potpuna dostava dokumentacije i podataka koji su Banci potrebni u svrhu ispunjavanja svih obveza sukladno Mjerodavnim propisima i Sankcijama (osobito podaci i dokumentacija potrebna Banci za provođenje Dubinske analize).

3.3. Banka, među ostalim, može odbiti uspostavljanje ili održavanje poslovnog odnosa ili ograničiti pružanje bilo koje usluge ako smatra da bi uspostava, odnosno

održavanje poslovnog odnosa ili pružanje određene usluge dovelo do neprihvatljivog rizika za Banku, odnosno ako bi bilo u suprotnosti s Mjerodavnim propisima i/ili Sankcijama.

3.4. Banka može odbiti uspostavu poslovnog odnosa sa Sankcioniranim osobama i ograničiti postojeći poslovni odnos Osobama povezanim sa sankcioniranim državom zbog pridržavanja Sankcija te im stoga određeni proizvodi i/ili usluge neće biti omogućeni.

3.5. Korisnik se obvezuje za korištenje pojedinim Direktnim kanalima osigurati o svojem trošku odgovarajuću računalnu (strojnu i programsku) ili mobilnu opremu te komunikacijsku vezu s Bankom. Tehnički zahtjevi koje je potrebno ispuniti za korištenje pojedinim Direktnim kanalima navedeni su na Internetskim stranicama Banke [www.zaba.hr](http://www.zaba.hr) i/ili su dostupni u poslovnoj mreži Banke.

3.6. Podaci, obavijesti, izvodi, ugovori i druga dokumentacija (npr. ugovori) u elektroničkom obliku koju Banka dostavi Korisniku putem Direktnih kanala jednakovrijedni su kao i papirnata dokumentacija. Banka će Korisniku omogućiti uvid u predmetne podatke i dokumentaciju putem Direktnog kanala onoliko dugo koliko je to potrebno s obzirom na njihovu namjenu.

3.7. Podaci i dokumentacija koju Banka dostavlja Korisniku putem Direktnog kanala ili e-maila smatraju se uredno dostavljenim u trenutku u kojem je Banka podatak ili dokument učinila Korisniku dostupnim putem tog Direktnog kanala, odnosno poslala putem e-maila.

3.8. Uspostavom telefonske, audio, video ili *chat*-komunikacije s Bankom Korisnik je upoznat s time da Banka može snimati i pohranjivati sadržaj predmetne komunikacije te se audiozapisom, odnosno pohranjenom pisanom/*chat* ili videokomunikacijom Banka može koristiti:

- kao dokazom o tome koje je podatke Korisnik zadao u svrhu izvršenja naloga, provođenja druge financijske ili nefinancijske transakcije i/ili ugovaranja/aktivacije usluge
- kao dokazom da se Korisnik usuglasio s provođenjem naloga, provođenjem druge financijske ili nefinancijske transakcije odnosno ugovaranjem/aktivacijom usluge
- u svrhu prijave okolnosti koje u skladu s ovim Općim uvjetima poslovanja predstavljaju osnovu za ograničenje pristupa Direktnim kanalima
- u svrhu upravljanja kvalitetom usluge te rješavanja Korisnikova prigovora u vezi s korištenjem Direktnim kanalima i sredstvima za autentifikaciju i autorizaciju, odnosno rješavanja spora između Korisnika i Banke.

## 4. UGOVARANJE I KORIŠTENJE DIREKTNIM KANALIMA

Banka određuje način i uvjete ugovaranja i korištenja Direktnim kanalima. Banka samostalno određuje koje će usluge pružati putem Direktnih kanala i putem kojeg Direktnog kanala. Informacije o uslugama i funkcionalnostima pojedinog Direktnog kanala sadržane su u ovim Općim uvjetima poslovanja i/ili u Ugovoru o korištenju Direktnim kanalom.

Korištenje pojedinim Direktnim kanalom Korisnik i Banka ugovaraju na neki od sljedećih načina:

- (i) sklapanjem Ugovora u poslovnici
- (ii) sklapanjem ugovora putem Direktnog kanala putem kojeg to Banka omogući (primjerice m-zaba aplikacija).

### 4.1. On-line bankarstvo

4.1.1. Za korištenje m-zaba aplikacijom i *On-line* bankarstvom putem mobilne aplikacije (m-zaba) te m-tokenom potrebno je s internetske stranice u vlasništvu trećih osoba (npr. AppStore ili Play Store) instalirati m-zaba aplikaciju na mobilni uređaj. Sve nadogradnje m-zaba aplikacije Banka će učiniti dostupnima Korisniku putem navedenih internetskih stranica u vlasništvu trećih osoba. Korisnik je upoznat s time da internetske stranice s kojih je moguće instalirati m-zaba aplikaciju ne pripadaju Banci te je suglasan da Banka ne odgovara za mogućnost i uvjete korištenja predmetnim internetskim stranicama, kao ni za uvjete pod kojima se m-zaba aplikacija može instalirati na mobilni uređaj. Korisnik snosi sve naknade i troškove povezane s instaliranjem i uporabom m-zaba aplikacije i svim njezinim nadogradnjama.

4.1.2. Mogućnost pristupa *On-line* bankarstvu, kao i mogućnost korištenja pojedinim uslugama koje su dostupne putem *On-line* bankarstva može ovisiti o operativnom sustavu i uvjetima uporabe operativnog sustava ili pojedinih funkcionalnosti operativnog sustava koji je instaliran na računalu, odnosno mobilnom ili drugom uređaju kojim se Korisnik koristi za pristup *On-line* bankarstvu.

4.1.3. Preduvjet za ugovaranje, odnosno aktiviranje i korištenje *On-line* bankarstvom jest da Korisnik u Banci ima otvoren i aktiviran tekući račun u eurima ili žiroračun u eurima.

4.1.4. Korisnik se obvezuje za aktivaciju i korištenje *On-line* bankarstvom putem mobilne aplikacije (m-zaba) i/ili m-tokena:

- u poslovnici Banke preuzeti Aktivacijski ključ i Identifikacijski ključ putem dvaju različitih kanala komunikacije (primjerice: SMS porukom ili putem Verificirane e-adrese) te odrediti m-PIN kojim će se koristiti za autentifikaciju prilikom pristupa m-zabi, odnosno m-tokenu ili
- prilikom ugovaranja *On-line* bankarstva putem mobilne aplikacije (m-zaba) putem m-zaba aplikacije odrediti m-PIN-a kojim će se koristiti za



autentifikaciju prilikom pristupa m-zabi, odnosno m-tokenu.

4.1.5. Korisnik za aktivaciju i korištenje *On-line* bankarstvom putem interneta (e-zaba) treba aktivirati m-token na način opisan u prethodnom stavku ovog članka ovih Općih uvjeta poslovanja.

4.1.6. Korisniku koji nije primio ili je zaboravio ili izgubio dodijeljeni Aktivacijski i/ili Identifikacijski ključ ili je zaboravio m-PIN kojim pristupa *On-line* bankarstvu putem mobilne aplikacije (m-zaba) ili m-tokenu Banka će ponovo dodijeliti Aktivacijski i Identifikacijski ključ te omogućiti određivanje novog m-PIN-a i na temelju njegova zahtjeva koji je predao Banci u poslovnici ili putem Direktnog kanala kojim je to omogućeno.

4.1.7. U slučajevima krađe uređaja na kojem je instalirano *On-line* bankarstvo putem mobilne aplikacije (m-zaba)/ m-token, gubitka, ili zaključavanja *On-line* bankarstva putem mobilne aplikacije (m-zaba) ili m-tokena Banka će Korisniku na temelju njegova zahtjeva predanog Banci u poslovnici ili Kontakt centru ili putem Direktnog kanala kojim je to omogućeno izdati novi Identifikacijski ključ i Aktivacijski ključ.

## **4.2. Ugovaranje ili aktiviranje *On-line* bankarstva ili m-tokena putem opunomoćenika**

4.2.1. Korisnik može samo specijalnom punomoći na kojoj je njegov potpis javnobilježnički ovjeren opunomoćiti jednu ili više osoba za ugovaranje i/ili aktivaciju usluga *On-line* bankarstva ili m-tokena.

4.2.2. U specijalnoj punomoći za aktivaciju *On-line* bankarstva putem interneta (e-zaba) ili *On-line* bankarstva putem mobilne aplikacije (m-zaba) i/ili m-tokena potrebno je među ostalim navesti sljedeće:

- (i) broj mobitela Korisnika na koji će Banka Korisniku poslati Aktivacijski ključ za aktivaciju
- (ii) izričito ovlaštenje opunomoćeniku da u svrhu ugovaranja i/ili aktivacije *On-line* bankarstva putem interneta (e-zaba) ili *On-line* bankarstva putem mobilne aplikacije (m-zaba) i/ili m-tokena u poslovnici Banke u ime i za račun Korisnika preuzme Identifikacijski ključ.

## **5. UPORABA ELEKTRONIČKOG POTPISA**

Banka Korisniku može omogućiti sklapanje i potpisivanje ugovora za određenu uslugu putem Direktnog kanala Elektroničkim potpisom ili Kvalificiranim elektroničkim potpisom.

### **5.1. Pojmovi u vezi s Elektroničkim potpisom i Kvalificiranim elektroničkim potpisom**

Pojedini pojmovi u vezi s Elektroničkim potpisom i Kvalificiranim elektroničkim potpisom upotrijebljeni u ovim Općim uvjetima poslovanja imaju sljedeće značenje:

**Certifikat za elektronički potpis** jest elektronička potvrda koja povezuje podatke za validaciju

elektroničkog potpisa s određenim Korisnikom i potvrđuje identitet tog Korisnika.

**Elektronički potpis** jest skup podataka u elektroničkom obliku koji je pridružen ili logički povezan s drugim podacima u elektroničkom obliku i kojima se Korisnik koristi za potpisivanje ugovora, naloga ili drugih naloga i dokumenata u elektroničkom obliku, putem Direktnih kanala.

**Korisnik certifikata** jest Korisnik kojem je Banka izdala Kvalificirani certifikat za elektronički potpis u skladu s Ugovorom o pružanju usluga povjerenja za kvalificirani osobni potpisni certifikat.

**Kvalificirani certifikat za elektronički potpis** ili **Kvalificirani certifikat** jest certifikat za elektronički potpis koji Banka u svojstvu kvalificiranog pružatelja usluga povjerenja izdaje Korisniku certifikata i koji ispunjava sve zahtjeve koji su Mjerodavnim propisima određeni za kvalificirane certifikate za elektronički potpis. Korištenje i upravljanje Kvalificiranim certifikatom regulirano je Općim pravilima pružanja kvalificirane usluge povjerenja te Pravilnikom o postupcima certificiranja kvalificiranih certifikata za elektroničke potpise i pečate.

**Kvalificirani elektronički potpis** jest napredan elektronički potpis koji je izrađen pomoću kvalificiranog sredstava za izradu elektroničkog potpisa i temelji se na Kvalificiranom certifikatu za elektronički potpis koji je Banka izdala Korisniku certifikata.

**Lozinka za pristup kvalificiranom certifikatu** označuje određeni izraz ili niz brojeva ili slova koje je Korisnik certifikata odabrao za pristup svojem udaljenom Kvalificiranom certifikatu putem određenog direktnog kanala.

**Ugovor o pružanju usluga povjerenja za kvalificirani osobni potpisni certifikat** jest ugovor sklopljen između Banke i Korisnika certifikata kojim se uređuju prava, obveze i odgovornosti Banke i Korisnika certifikata u vezi s izdavanjem, korištenjem, zaštitom, opozivom i prestankom valjanosti kvalificiranog certifikata.

### **5.2. Ugovaranje i uporaba Kvalificiranog elektroničkog potpisa**

5.2.1. Banka, kao pružatelj usluga povjerenja, putem Direktnog kanala omogućuje sklapanje i potpisivanje Ugovora o pružanju usluga povjerenja za kvalificirani osobni potpisni certifikat na temelju kojeg Korisniku izdaje Kvalificirani osobni potpisni certifikat kojim se Korisnik može koristiti za potpisivanje određenih ugovora s Bankom na kanalima na kojima Banka omogući takav način ugovaranja usluga.

5.2.2. Korisnik koji s Bankom sklopi Ugovor o pružanju usluga povjerenja za kvalificirani osobni potpisni certifikat obvezuje se pravodobno obnoviti izdani Kvalificirani certifikat nakon isteka roka njegove valjanosti ako se i dalje namjerava njime koristiti. Obnova Kvalificiranog certifikata provodi se u skladu s Ugovorom o pružanju usluga povjerenja za kvalificirani

osobni potpisni certifikat i njegovim sastavnim dijelovima.

5.2.3. Ako je rok valjanosti Ugovora o pružanju usluga povjerenja za kvalificirani osobni potpisni certifikat kraći od razdoblja valjanosti Kvalificiranog certifikata, Korisnik se obvezuje s Bankom sklopiti novi Ugovor o pružanju usluga povjerenja za kvalificirani osobni potpisni certifikat.

## **6. AUTENTIFIKACIJA KORISNIKA**

### **6.1. Autentifikacija za pristup *On-line* bankarstvu**

6.1.1. Korisnik koji je ugovorio *On-line* bankarstvo putem interneta (e-zaba) prilikom pristupa e-zabi pouzdano se autentificira unosom u za to predviđena polja na ekranskom sučelju e-zabe serijskog broja m-tokena koji mu je izdala Banka te unosom OTP-a koji je generirao m-token, sve nakon što je Korisnik u m-token unio u za to predviđeno polje m-zaba aplikacije m-PIN ili se prilikom pristupa m-tokenu autentificirao Autentifikacijom otiskom prsta ili Autentifikacijom prepoznavanjem lica.

6.1.2. Korisnik koji je ugovorio *On-line* bankarstvo putem mobilne aplikacije (m-zaba) prilikom pristupa m-zabi može se autentificirati:

- unosom u za to predviđeno polje m-zaba aplikacije m-PIN-a ili
- Autentifikacijom otiskom prsta ili Autentifikacijom prepoznavanjem lica.

### **6.2. Autentifikacija m-tokenom**

6.2.1. Korisnik koji se kao sredstvom za autentifikaciju i autorizaciju koristi m-tokenom prilikom pristupa m-tokenu pouzdano se autentificira na neki od sljedećih načina:

- unosom u m-token m-PIN-a koji je odabrao za pristup m-zabi odnosno m-tokenu
- Autentifikacijom otiskom prsta ili Autentifikacijom prepoznavanjem lica.

6.2.2. Iznimno od navedenog, Korisnik koji pristupa m-tokenu iz *On-line* bankarstva putem mobilne aplikacije (m-zaba) može se koristiti m-tokenom bez dodatnog unosa m-PIN-a ako se prilikom pristupa *On-line* bankarstvu putem mobilne aplikacije (m-zaba) pouzdano autentificirao unosom m-PIN-a ili Biometrijskom autentifikacijom.

### **6.3. Autentifikacija biometrijom**

6.3.1. Primjena Biometrijske autentifikacije dobrovoljna je te ne isključuje i ne ograničava mogućnost Pouzdane autentifikacije Korisnika m-PIN-om koji je Korisnik odabrao za pristup m-zabi i/ili m-tokenu. Korištenje pojedinim uslugama koje su dostupne putem m-zabe i/ili m-tokena Banka može onemogućiti ili ograničiti u slučaju Biometrijske autentifikacije Korisnika te njihovu uporabu uvjetovati Pouzdanom autentifikacijom Korisnika unosom m-PIN-a.

6.3.2. Aktiviranjem i primjenom opcije Biometrijske autentifikacije Korisnik potvrđuje da je upoznat i suglasan s time da Banka ne pruža uslugu autentifikacije biometrijom, nego da se koristi autentifikacijom biometrijom koju omogućuje mobilni uređaj te da stoga Banka ne odgovara za nemogućnost ili ograničenu mogućnost primjene autentifikacije biometrijom ni za rezultat takve autentifikacije, neovisno o tome odgovaraju li otisak prsta ili biometrijske značajke lica pomoću kojih se Korisnik identificira prilikom pristupa m-zabi i/ili m-tokenu ili ne odgovaraju otisku prsta ili biometrijskim značajkama lica koje je Korisnik prethodno pohranio u mobilni uređaj kojim se koristi za pristup m-zabi.

6.3.3. Banka nema pristup podacima ni kontrolu nad podacima koje je Korisnik u svrhu Biometrijske autentifikacije pohranio u mobilni uređaj kojim se koristi za pristup m-zabi i/ili m-tokenu.

6.3.4. Korisnik može onemogućiti Biometrijsku autentifikaciju tako da promijeni odabrane opcije u m-zaba aplikaciji koje omogućuju Biometrijsku autentifikaciju.

6.3.5. Korisnik se obvezuje u mobilni uređaj kojim se koristi za pristup m-zabi i/ili m-tokenu pohraniti isključivo biometrijske značajke svojeg lica odnosno otisak svojeg prsta. Korisnik je suglasan da je u slučaju aktivirane opcije Biometrijske autentifikacije Banka izvršila autentifikaciju Korisnika u trenutku kada mobilni uređaj kojim se pristupa m-zabi/m-tokenu pozitivno potvrdi korištenje biometrijskim značajkama (npr. otisak prsta ili značajke lica) pohranjenim u tom mobilnom uređaju.

6.3.6. Korisnik je upoznat i suglasan s time da Banka u slučaju autentifikacije Korisnika nekom od metoda Biometrijske autentifikacije može prema svojoj diskrecijskoj ocijeni za izvršenje Elektroničke platne transakcije ili obavljanja bilo koje druge radnje u sklopu m-zabe njezino poduzimanje uvjetovati unosom m-PIN-a.

### **6.4. Autentifikacija pri korištenju uslugama Pružatelja usluga informiranja o računu (AISP) i Pružatelja usluga iniciranja plaćanja PISP**

6.4.1. Korisnik koji je ugovorio korištenje e-zabom ili m-zabom može:

- a) posredstvom bilo kojeg Pružatelja usluge informiranja o računu (AISP) primiti informacije o stanju i prometima po jednom ili više računa otvorenih u Banci te
- b) posredstvom Pružatelja usluge iniciranja plaćanja (PISP) inicirati naloge za plaćanje na teret jednog ili više računa otvorenih u Banci.

6.4.2. Nakon što se Korisnik s mrežnih stranica AISP-a odnosno PISP-a preusmjeri na mrežne stranice Banke, Banka provodi Pouzdanu autentifikaciju Korisnika:

- (i) koji putem mrežnih stranica AISP-a daje AISP-u suglasnost za pristup informacijama o jednom ili više transakcijskih računa te

stanju i prometu po jednom ili više transakcijskih računa otvorenih u Banci na način da:

- Korisnik na mrežnim stranicama Banke unese u za to predviđena polja serijski broj m-tokena i OTP
- prilikom pristupa m-zabi unese m-PIN za prijavu u m-zabu ili se prijavi Autentifikacijom otiskom prsta ili Autentifikacijom prepoznavanjem lica

(ii) koji putem mrežnih stranica PISP-a zadaje i podnosi na izvršenje nalog za plaćanje koji se treba izvršiti po transakcijskom računu otvorenom u Banci na način da ili:

- Korisnik na mrežnim stranicama Banke
  - a. unese serijski broj m-tokena i MAC ako je u prethodnom koraku na mrežnim stranicama PISP-a uz iznos plaćanja unio i IBAN platitelja ili
  - b. unese serijski broj m-tokena i OTP ako u prethodnom koraku na mrežnim stranicama PISP-a nije unio i IBAN platitelja
- ili Korisnik prilikom pristupa m-zabi unese m-PIN za prijavu u m-zabu ili se prijavi Autentifikacijom otiskom prsta ili Autentifikacijom prepoznavanjem lica.

## **7. AUTORIZACIJA TRANSAKCIJA, SKLAPANJE UGOVORA I POTVRDA PRIHVATA DOKUMENTA**

7.1. Suglasnost (Autorizaciju) za izvršenje financijske i/ili nefinancijske transakcije odnosno ugovaranje bankarske ili nebankarske usluge te potvrdu prihvata dokumenta daje se na neki od sljedećih načina:

(i) potpisivanjem naloga, ugovora ili drugog dokumenta Elektroničkim potpisom, uporabom m-tokena uporabom MAC (*Message Authentication Code*)/APPLI2 u postupku Autorizacije naloga te potpisivanja ugovora i prihvata dokumenata putem *On-line* bankarstva (e-zaba ili m-zaba) ili na mrežnoj stranici Banke pri čemu Korisnik:

- i. u slučaju korištenja e-zabom u m-token unese niz znamenaka s ekranskog sučelja e-zabe (*challenge*) ili preuzimanjem i unosom podataka u m-token na drugi način koji je Banka omogućila Korisniku (npr. očitanjem QR koda s dokumenta koji treba autorizirati ili potpisati), nakon čega m-token automatski generira jedinstveni niz znamenaka (*response*) koje je potrebno unijeti u polje MAC na ekranskom sučelju e-zabe čime se nalog odnosno ugovor smatraju potpisanim elektroničkim potpisom, odnosno

- ii. u slučaju korištenja m-zabom odabire opciju za potvrđivanje pri čemu se MAC generira automatski nakon što se Korisnik prilikom pristupa m-zabi autentificirao na ugovoreni način.

(ii) davanjem suglasnosti za izvršenje financijske ili nefinancijske transakcije, ugovaranjem bankovne ili nebankovne usluge te potvrdom prihvata dokumenata putem *chat*-kontakta u okviru usluge e-poslovnica.

(iii) potpisivanjem ugovora ili drugog dokumenta u elektroničkom obliku Kvalificiranim elektroničkim potpisom koji se automatski kreira nakon što Korisnik certifikata u odgovarajuće polje na ekranskom sučelju *On-line* bankarstva kojim pristupa svojem Kvalificiranom certifikatu unese Lozinku za pristup kvalificiranom certifikatu te prema potrebi izvrši drugu radnju kojom *On-line* bankarstvo uvjetuje sklapanje ugovora, odnosno potpis dokumenta Kvalificiranim elektroničkim potpisom.

7.2. Nalog za izvršenje financijske ili nefinancijske transakcije, ugovaranje bankarske ili nebankarske usluge te potvrda prihvata dokumenta za koje je suglasnost dana na neki od načina opisanih u ovoj glavi Općih uvjeta poslovanja smatra se autoriziranim, odnosno prihvaćenim od strane Korisnika. U slučaju ugovaranja bankarske ili nebankarske usluge za koje je potrebno potpisivanje ugovorne dokumentacije ugovor je sklopljen nakon što ga potvrde i potpišu i Banka i Korisnik.

7.3. Korisnik se obvezuje tijekom zadavanja naloga odnosno provođenja druge financijske ili nefinancijske transakcije ili ugovaranja/aktivacije usluge telefonskim ili audioputem pažljivo poslušati podatke sa zadanog naloga, odnosno podatke za provođenje druge financijske ili nefinancijske transakcije, ili ugovaranja/aktivacije usluge koje ponavlja zaposlenik Banke, a Korisnikova potvrda tih podataka, odnosno suglasnost osnova je za provedbu naloga, odnosno provođenje transakcije, ugovaranje/aktivaciju usluge.

7.4. U slučaju nemogućnosti provedbe transakcije u iznosu koji je Korisnik odredio Banka može Korisniku ponuditi izvršenje transakcije u iznosu koji je najbliži iznosu neizvršene transakcije.

7.5. Banka može odrediti maksimalni broj izvršenja Elektroničkih platnih transakcija i/ili maksimalni iznos Elektroničkih platnih transakcija koje se dnevno mogu provesti pojedinim Direktnim kanalima, o čemu će obavijestiti Korisnika putem Direktnog kanala na koji se ograničenje odnosi i/ili putem Internetskih stranica Banke. Tako određena ograničenja primjenjivat će se i u provedbi Elektroničkih platnih transakcija i ostalih financijskih i/ili nefinancijskih transakcija koje su prije inicirane, a čije je izvršenje zadano za datum nakon početka primjene ograničenja.

## **8. ONEMOGUĆIVANJE PRISTUPA DIREKTNIM KANALIMA I KVALIFICIRANOM CERTIFIKATU**

8.1. Svaki gubitak, krađu, saznanje o zlouporabi ili sumnju na zlouporabu sredstva za autentifikaciju i autorizaciju, mobilnog uređaja (u slučaju korištenja m-zabom ili m-tokenom), Kvalificiranog certifikata ili Personaliziranih sigurnosnih vjerodajnica, saznanje ili sumnju da je neovlaštena osoba saznala njegove Personalizirane sigurnosne vjerodajnice te saznanje ili sumnju da je neovlaštena osoba imala pristup ugovorenom Direktnom kanalu Korisnik mora odmah prijaviti u poslovnicu Banke ili dežurnoj službi Banke na telefonske brojeve koji su objavljeni na Internetskim stranicama Banke i pritom zatražiti blokadu pristupa Direktnom kanalu.

8.2. Korisnik je također obavezan samostalno i bez odgode odmah promijeniti odabrani m-PIN ili Lozinku za pristup kvalificiranom certifikatu ako ima saznanje ili sumnju da ih je saznala neovlaštena osoba.

8.3. U slučaju saznanja ili sumnje na bilo koju od prethodno navedenih okolnosti Korisnik se mora odmah prestati koristiti Direktnim kanalom.

8.4. Banka je ovlaštena prema opravdanoj i razumnoj procjeni i bez prijave Korisnika onemogućiti pristup pojedinim ili svim Direktnim kanalima, onemogućiti upotrebu sredstva za autentifikaciju ili autorizaciju ili onemogućiti korištenje pojedinim ili svim uslugama koje su dostupne putem nekog Direktnog kanala, smanjiti ili ograničiti limite za izvršenje platnih i drugih financijskih i/ili nefinancijskih transakcija, odnosno onemogućiti pristup Kvalificiranom certifikatu:

- 1) u slučaju sumnje na neovlaštenu uporabu ili zlouporabu sredstva za autentifikaciju i autorizaciju, mobilnog uređaja na kojem je instalirana m-zaba aplikacija, Personaliziranih sigurnosnih vjerodajnica ili Kvalificiranog certifikata
- 2) u slučaju da je prilikom korištenja m-tokenom ili prilikom pristupa m-zabi odnosno prilikom provođenja Pouzdane autentifikacije Korisnika koji je s mrežnih stranica AISP-a ili PISP-a preusmjeren na mrežne stranice Banke pripadajuća Personalizirana sigurnosna vjerodajnica više puta uzastopno pogrešno unesena
- 3) u slučaju sumnje da se Direktni kanal upotrebljava za prijevaru ili zlouporabu
- 4) ako je Korisnik prilikom ugovaranja Direktnog kanala dao Banci pogrešne ili neistinite podatke
- 5) ako se Korisnik ne pridržava ugovornih odredbi i uvjeta korištenja pojedinim Direktnim kanalom i ne izvršava svoje obveze iz Ugovora o korištenju direktnim kanalima i ovih Općih uvjeta poslovanja
- 6) ako Korisnik postupa protivno Mjerodavnim propisima
- 7) u slučajevima više sile, tehničkih poteškoća i drugih neočekivanih događaja.

8.5. Banka može umjesto onemogućivanja pristupa Direktnom kanalu Korisniku privremeno onemogućiti korištenje jednom ili većim brojem usluga ili funkcionalnosti koje su dostupne putem tog Direktnog kanala ili Autorizaciju pojedinih ili svih vrsta transakcija uvjetovati dodatnim radnjama koje Korisnik mora poduzeti, kojima se prema procjeni Banke umanjuje rizik od izvršenja neautorizirane transakcije ili obavljanja neke druge neovlaštene radnje na štetu Korisnika.

8.6. Banka će pravodobno unaprijed obavijestiti Korisnika o namjeravanom onemogućivanju pristupa Direktnom kanalu i/ili nemogućnosti korištenja pojedinom uslugom Direktnog kanala te razlozima takva postupanja, osim ako je davanje obavijesti u suprotnosti s objektivno opravdanim sigurnosnim razlozima ili protivno zakonu.

8.7. Obavijest o nemogućnosti korištenja Direktnim kanalom ili pojedinom uslugom koja je dostupna putem Direktnog kanala Banka upućuje Korisniku putem istog Direktnog kanala ili na drugi odgovarajući način.

8.8. Banka nije obvezna unaprijed obavijestiti Korisnika o onemogućavanju pristupa Direktnom kanalu u sljedećim slučajevima:

- 1) u slučaju višekratnog pogrešnog unosa Personaliziranih sigurnosnih vjerodajnica
- 2) u slučaju sumnje da se Direktni kanal upotrebljava za prijevaru ili zlouporabu ili da je postupanje Korisnika protivno Mjerodavnim propisima
- 3) ako je Korisnik prilikom ugovaranja Direktnog kanala dao Banci pogrešne ili neistinite podatke
- 4) ako se Korisnik ne pridržava ugovornih odredbi i uvjeta korištenja Direktnim kanalom
- 5) u slučajevima više sile, tehničkih poteškoća i drugih neočekivanih događaja.

8.9. Banka može, uz prethodnu najavu, privremeno onemogućiti korištenje ugovorenim Direktnim kanalima u slučaju promjena opsega usluga koje su dostupne putem određenog Direktnog kanala te zbog promjena i nadogradnji u informacijskom sustavu Banke, uključujući sustav njezine informacijske sigurnosti. Obavijest o privremenoj nemogućnosti korištenja Direktnim kanalom zbog navedenih razloga Banka šalje Korisniku putem tog Direktnog kanala ili na drugi odgovarajući način i/ili čini dostupnom objavom na Internetskim stranicama Banke.

## **9. NAKNADE I TROŠKOVI**

9.1. Za ugovaranje i korištenje Direktnim kanalom Banka obračunava i naplaćuje naknadu u skladu s Izvatkom iz Odluke o tarifi naknada za usluge Banke po transakcijskim računima fizičkih osoba i usluga platnog prometa te direktnih kanala važećom na dan obračuna naknade.



9.2. Banka je ovlaštena dospjele naknade i troškove naplatiti s računa Korisnika koji se vode u Banci u nacionalnoj valuti.

## 10. OBVEZE KORISNIKA

10.1. Korisnik se obvezuje:

- 1) uredno ispunjavati sve svoje obveze iz Ugovora o korištenju Direktnim kanalom te ovih Općih uvjeta poslovanja
- 2) brižno čuvati dodijeljeno sredstvo za autentifikaciju i autorizaciju tako da spriječi njegov gubitak, krađu ili zlouporabu
- 3) brižno čuvati vlastite uređaje kojima se koristi za pristup pojedinim Direktnim kanalima, poput računala ili mobilnog uređaja, tako da spriječi njihov gubitak, krađu ili zlouporabu
- 4) zapamtiti dodijeljenu ili odabranu Personaliziranu sigurnosnu vjerodajnicu
- 5) poduzeti sve razumne mjere zaštite dodijeljenih ili odabranih Personaliziranih sigurnosnih vjerodajnica tako da spriječi njihov gubitak, krađu, zlouporabu ili neovlašteno otkrivanje. Primjerice, neće se smatrati da je Korisnik poduzeo potrebne razumne mjere zaštite tajnosti odabranog m-PIN-a ili Lozinke za pristup Kvalificiranom certifikatu ako za m-PIN ili lozinku za pristup Kvalificiranom certifikatu odabere kombinaciju brojeva, slova ili znakova koja se može lako utvrditi, kao što su primjerice ime ili prezime Korisnika ili članova njegove obitelji, datum rođenja Korisnika ili neprekinuti niz istih ili uzastopnih brojeva, slova ili znakova.
- 6) da Personalizirane sigurnosne vjerodajnice neće zapisati na sredstvu za autentifikaciju i autorizaciju, osobnim ispravama, osobnom računalu ili mobilnom uređaju, papiru, ili bilo kojem drugom mediju niti ih učiniti dostupnima / priopćiti drugim osobama ili na bilo koji način omogućiti drugoj osobi da ih sazna, uključujući Banku i njezine zaposlenike. Korisnik je upoznat s time da Banka i njezini zaposlenici ni u kojem slučaju neće tražiti podatke o njegovim Personaliziranim sigurnosnim vjerodajnicama.
- 7) da Personalizirane sigurnosne vjerodajnice neće prosljeđivati elektroničkom poštom te da neće otvarati, prosljeđivati i odgovarati na poruke elektroničke pošte (e-mailove) koje stvaraju privid da potječu od Banke. Korisnik je upoznat s time da će mu svaka poruka poslana e-poštom koja potječe od Banke biti upućena isključivo sa službene e-adrese Banke koja završava s @unicreditgroup.zaba.hr.
- 8) prije davanja Personaliziranih sigurnosnih vjerodajnica u svrhu pouzdane autentifikacije Korisnika koju Banka provodi prilikom pružanja usluga koje je Korisnik zatražio od Banke posredstvom AISP-a odnosno PISP-a provjeriti klikom na ikonu lokota u/pokraj adresnog polja u internetskom pregledniku nalazi li se na Internetskim stranicama Banke, a u slučaju da se ne nalazi na Internetskim stranicama Banke, bez odgađanja prestati s korištenjem uslugom i o tome obavijestiti Banku.
- 9) pristupati e-zabi isključivo izravno s Internetske stranice Banke <https://www.zaba.hr/ebank/gradjani/Prijava>, a ne putem linkova iz drugih internetskih stranica poruka poslanih e-poštom te prilikom pristupa e-zabi i tijekom korištenja e-zabom klikom na ikonu lokota u/pokraj adresnog polja u internetskom pregledniku provjeriti nalazi li se na Internetskim stranicama Banke, a u slučaju da se prilikom pristupa e-zabi i/ili korištenja e-zabom ne nalazi na Internetskim stranicama Banke, bez odgađanja prestati s korištenjem e-zabom.
- 10) odmah obavijestiti Banku o nastanku svake okolnosti koja u skladu s Općim uvjetima poslovanja predstavlja osnovu za blokadu pristupa ugovorenom Direktnom kanalu i zatražiti od Banke blokadu pristupa Direktnom kanalu
- 11) u slučaju nepravilnosti u radu ili netipičnog rada Direktnog kanala odmah prestati s njegovom uporabom i o uočenim nepravilnostima ili netipičnom radu bez odgađanja obavijestiti Banku
- 12) redovito, a osobito prije korištenja Direktnim kanalom pregledavati obavijesti i provjeravati postojanje novih obavijesti koje mu Banka učini dostupnima putem Internetskih stranica Banke [www.zaba.hr](http://www.zaba.hr) i/ili dostavi putem ugovorenog Direktnog kanala, e-pošte, na kućnu adresu ili na drugi ugovoreni način primanja obavijesti te postupati u skladu s njima
- 13) Banku odmah obavijestiti o promjenama svih podataka koji su nužni za ispravno i sigurno funkcioniranje pojedinih Direktnih kanala ili za primanje obavijesti od Banke kao što su primjerice broj mobitela za korištenje m-zabom, m-tokenom ili za dostavu SMS poruka, promjena osobnih ili kontaktnih podataka Korisnika
- 14) redovito nadograđivati m-zaba aplikaciju svim nadogradnjama koje Banka učini dostupnima
- 15) da neće mijenjati ili dekompilirati ni omogućiti drugim osobama da mijenjaju ili dekompiliraju m-zaba aplikaciju koju je instalirao na mobilni uređaj
- 16) pridržavati se svih sigurnosnih mjera zaštite i korištenja računalom odnosno mobilnim uređajem kojim se koristi za pristup Direktnom kanalu o kojima ga Banka obavijesti putem svojih internetskih stranica ili ugovorenog Direktnog kanala, uključujući:
  - za pristup Direktnim kanalima koristiti se isključivo odgovarajućom računalnom i/ili mobilnom (strojnom i programskom) te komunikacijskom opremom koja je određena u tehničkim

zahtjevima pojedinog Direktnog kanala i usklađena s preporučenom konfiguracijom objavljenom na Internetskoj stranici Banke [www.zaba.hr](http://www.zaba.hr) i/ili u poslovnica Banke te koja ima instalirane i ažurirane u skladu sa svim posljednjim dostupnim nadogradnjama proizvođača operativni sustav, internetski preglednik, antivirusnu zaštitu i vatrozid

- redovito, a osobito prije korištenja Direktnim kanalom provjeriti postojanje virusa i drugih malicioznih programa na računalu odnosno mobilnom uređaju kojim se koristi za pristup Direktnom kanalu te u slučaju njihova postojanja upotrebljavati Direktni kanal tek nakon što su oni uklonjeni nekim od pouzdanih programa za uklanjanje virusa i malicioznih programa
  - voditi računa o internetskim stranicama koje se posjećuju s uređaja kojima pristupa Direktnim kanalima jer pristup nekim stranicama uključuje povećani rizik od zaraze računala odnosno mobilnog uređaja malicioznim programima
  - ne otvarati poruke elektroničke pošte (e-mailove) te privitke i poveznice (linkove) iz sumnjivih poruka ili poruka koje ne očekuje.
- 17) zaštititi pristup računalu odnosno mobilnom uređaju povjerljivom lozinkom te za predmetnu lozinku odabrati kombinaciju slova, brojeva i znakova koja se ne može lako otkriti, primjerice tako da za lozinku ne odabire svoje ime ili niz istih ili uzastopnih brojeva, slova ili znakova
- 18) redovito mijenjati m-PIN i lozinku gdje je to moguće
- 19) Banku bez odgađanja obavijestiti o prijavi nadležnom tijelu krađe ili zlouporabe sredstva za autentifikaciju i autorizaciju, mobilnog uređaja (u slučaju korištenja m-zabom i/ili m-tokenom) ili Personaliziranih sigurnosnih vjerodajnica te saznanje ili sumnju da je neovlaštena osoba imala pristup ugovorenom Direktnom kanalu
- 20) ako je u slučaju zlouporabe ili sumnje na zlouporabu Direktnog kanala kao oštećena osoba pokrenuo odgovarajuće postupke pred mjerodavnim tijelima, upoznati Banku s tijekom i ishodom tih postupaka
- 21) Korisnik je obavezan za vrijeme trajanja Ugovora dostaviti Banci, u obliku i na način koje odredi Banka, sve podatke i dokumentaciju koju Banka zatraži od Korisnika u svrhu provedbe Dubinske analize Korisnika u skladu s Mjerodavnim propisima i/ili Sankcijama.

10.2. Korisnik je suglasan da se nepridržavanje bilo koje od obveza iz ovog članka ovih Općih uvjeta poslovanja smatra njegovom krajnjom nepažnjom u korištenju Direktnim kanalom te da u tom slučaju odgovara za svu time nastalu štetu.

10.3. Korisnik u cijelosti odgovara za sve transakcije koje su izvršene i ugovore koji su sklopljeni zlouporabom Kvalificiranog certifikata od strane treće osobe prije prijave Banci okolnosti koja predstavlja osnovu za blokadu pristupa Kvalificiranom certifikatu, kao i za svu time nastalu štetu.

## **11. ISKLJUČENJE ODGOVORNOSTI BANKE**

11.1. Banka ne odgovara za štetu koja Korisniku nastane zbog:

- 1) nefunkcioniranja ili nepravilnog rada računala, mobilnog telefona ili drugog uređaja koji nije u vlasništvu Banke, a upotrebljava se za pristup Direktnom kanalu ili nefunkcioniranja ili nepravilnog rada aplikativnog rješenja instaliranog na tom uređaju
- 2) zahvata Korisnika ili druge neovlaštene osobe na dodijeljenom sredstvu za autentifikaciju i autorizaciju
- 3) postupanja ili propusta osobe koja Korisniku i/ili Banci pruža usluge pokretne i/ili nepokretne telekomunikacije
- 4) postupanja ili propusta AISP-a i/ili PISP-a
- 5) više sile pod kojom se smatraju rat, nemiri, terorističko djelovanje, prirodna katastrofa, epidemija, štrajk, prestanak isporuke električne energije, smetnje u telekomunikacijskom i ostalom prometu, greške nastale u prijenosu podataka telekomunikacijskim mrežama, odluke i djelovanja tijela vlasti, kao i sve druge slične okolnosti čiji se nastanak ne može pripisati Banci, odnosno koje su izvan kontrole Banke, a zbog kojih je onemogućeno korištenje Direktnim kanalom
- 6) gubitka ili uništenja podataka i opreme Korisnika te zbog nebankarskih troškova uzrokovanih instaliranjem i upotrebom Direktnih kanala
- 7) zlouporabe Kvalificiranog certifikata od strane treće osobe prije telefonske prijave Banci okolnosti koja predstavlja osnovu za blokadu pristupa Kvalificiranom certifikatu.

11.2. Banka ne odgovara za točnost podataka koje Korisniku putem Direktnih kanala dostavljaju druge pravne ili fizičke osobe (npr. u slučaju ugovaranja, korištenja ili pristupa uslugama trećih osoba koje su dostupne u m-zaba aplikaciji).

## **12. PRIGOVORI, PRITUŽBE I ALTERNATIVNO RJEŠAVANJE POTROŠAČKIH SPOROVA**

12.1. Prigovori u vezi s korištenjem Direktnih kanala mogu se podnijeti Banci pismenim putem na neki od sljedećih načina:

- osobno u najbližoj poslovnici Banke
- e-mailom: zaba@unicreditgroup.zaba.hr
- putem internetske stranice: www.zaba.hr
- poštom: Zagrebačka banka d.d. Kontakt centar, Samoborska 145, 10090 Zagreb.

12.2. Korisnik koji je s Bankom *On-line* ugovorio uslugu ima pravo u svrhu izvansudskog alternativnog rješavanja sporova podnijeti svoju pritužbu putem platforme za *On-line* rješavanje sporova (platforma za ORS). Poveznica na platformu za ORS jest: <https://ec.europa.eu/consumers/odr/main>.

Prigovor minimalno treba sadržavati:

- osobne podatke klijenta (ime i prezime fizičke osobe)
- detaljan opis događaja/situacije ili okolnosti koje su izazvale nezadovoljstvo te dokaz osnovanosti prigovora
- adresu za dostavu odgovora.

Banka ne odgovara na anonimne prigovore.

Korisnik može uputiti i pritužbu Hrvatskoj narodnoj banci. U svim sporovima između Korisnika i Banke nastalim u vezi s ugovornim odnosom o korištenju Direktnim kanalom i/ili ugovorom koji je sklopljen između Korisnika i Banke korištenjem Direktnog kanala Korisnik može podnijeti prijedlog za mirenje Centru za mirenje pri Hrvatskoj gospodarskoj komori (Rooseveltov trg 2, 10000 Zagreb, <http://www.hgk.hr/centar-za-mirenje/o-centru-za-mirenje>) ili Centru za mirenje pri Hrvatskoj udruzi za mirenje (Teslina 1/I, 10000 Zagreb, <https://hrvatskaudrugazamirenje.wordpress.com>), kao i bilo kojem drugom tijelu nadležnom za alternativno rješavanje potrošačkih sporova. Banka će sudjelovati u postupku koji bi se vodio na osnovi takva prijedloga za mirenje.

Na uredno zaprimljen prigovor Banka će odgovoriti Korisniku u roku 15 (petnaest) dana od dana primitka prigovora, izuzev kada se prigovor odnosi na bilo koju od usluga platnog prometa kojom se Korisnik koristi ili kojom se može koristiti putem nekog od Direktnih kanala, u kojem slučaju će na primljeni prigovor Banka odgovoriti u roku od 10 (deset) dana od dana njegova primitka, a u skladu s Općim uvjetima poslovanja Zagrebačke banke d.d. po transakcijskim računima potrošača. Kad rješavanje prigovora može trajati dulje od očekivanog zbog razloga koji su izvan kontrole Banke, Banka će unutar prethodno navedenog roka obavijestiti Korisnika o razlozima odgode te o okvirnom vremenu u kojem može očekivati konačan odgovor Banke.

Prigovore koji se odnose na usluge koje pružaju AISP i/ili PISP, a koji proizlaze iz ugovornog odnosa Korisnika i tih pružatelja platnih usluga, uključujući, ali ne ograničavajući se na suglasnosti koje Korisnik daje navedenim pružateljima platnih usluga, Korisnik upućuje isključivo njima, pod uvjetima i na načine koje su međusobno ugovorili. Ako je riječ o prigovorima povezanim s Autorizacijom i izvršenjem platnih

transakcija iniciranih putem PISP-a, oni se upućuju Banci na jednak način kao i kad je riječ o prigovorima povezanim s platnim transakcijama iniciranim putem Direktnih kanala Banke.

Prigovore koji su povezani s uporabom uređaja ili operativnih sustava koji su instalirani na uređaju kojim se Korisnik koristi za pristup e-zabi ili m-zabi Korisnik upućuje proizvođaču uređaja ili operativnog sustava koji je instaliran na uređaju.

### 13. TRAJANJE I PRESTANAK UGOVORA

Ugovor o korištenju Direktnim kanalom sklapa se na neodređeno vrijeme, a prestaje:

- otkazom
- smrću Korisnika ili
- zatvaranjem (otkazom/deaktivacijom) tekućeg računa u eurima ili žiroračuna u eurima na temelju kojeg se naplaćuje naknada za Direktni kanal.

#### 13.1. Otkaz Ugovora o korištenju direktnim kanalom

13.1.1. Korisnik može jednostrano otkazati Ugovor o korištenju direktnim kanalom:

- pisanim putem u poslovnici Banke, ili
- putem Direktnog kanala kojim je to omogućeno, ili
- dostavom potpisanog zahtjeva za otkaz Ugovora o korištenju direktnim kanalom od strane Korisnika putem pošte:
  - na adresu Banke: Zagrebačka banka d.d. Kontakt centar, Samoborska cesta 145, 10090 Zagreb ili
  - na adresu poslovnice: adrese poslovnica dostupne su na Internetskoj stranici Banke [www.zaba.hr](http://www.zaba.hr).

13.1.2. Zahtjev dostavljen poštom treba biti ovjeren od:

- nadležnog domaćeg tijela (javnog bilježnika) – za zahtjeve poslane poštom iz RH, odnosno
- stranog nadležnog tijela, ovlaštene osobe diplomatskog ili konzularnog predstavništva – za zahtjeve poslane poštom iz inozemstva.

13.1.3. Dan primitka otkaznog pisma / zahtjeva za otkaz je dan kada je on zaprimljen u Banku te se ugovor otkazuje na isti dan u sljedećem mjesecu, a ako je otkaz zaprimljen 31., a sljedeći mjesec ima 30 dana (ili u veljači 28./29.), tada se ugovor otkazuje zadnjeg dana u sljedećem mjesecu.

13.1.4. Banka može jednostrano otkazati Ugovor o korištenju direktnim kanalom uz otkazni rok od dva mjeseca. Dan dostave otkaznog pisma Korisniku jest dan slanja otkaznog pisma Korisniku putem ugovorenog Direktnog kanala ako on omogućuje razmjenu obavijesti između Korisnika i Banke ili dan slanja otkaznog pisma pošiljkom na adresu koju je Korisnik prethodno prijavio Banci kao adresu za

dostavu pisanih obavijesti, a u slučaju nepostojanja takve adrese Korisnika dan slanja otkaznog pisma na adresu koju je Korisnik prijavio Banci kao adresu svojeg prebivališta ili boravišta.

### **13.2. Raskid Ugovora o korištenju direktnim kanalom**

13.2.1. Banka u sljedećim slučajevima ima pravo raskinuti Ugovor o korištenju direktnim kanalom s učinkom od dana slanja obavijesti o raskidu putem ugovorenog Direktnog kanala ako on omogućuje razmjenu obavijesti između Korisnika i Banke ili slanjem obavijesti o raskidu pošiljkom na adresu koju je Korisnik prethodno prijavio Banci kao adresu za dostavu pismenih obavijesti, a u slučaju nepostojanja takve adrese Korisnika, slanjem na adresu koju je Korisnik prijavio Banci kao adresu svojeg prebivališta ili boravišta:

- ako Korisnik krši odredbe Ugovora o korištenju direktnim kanalom ili ovih Općih uvjeta poslovanja
- ako je Korisnik prilikom sklapanja Ugovora dostavio Banci pogrešne ili neistinite osobne podatke ili druge podatke odlučujuće za pravilno i zakonito pružanje ugovorene usluge
- ako Korisnik postupa suprotno Mjerodavnim propisima
- ako Banka utvrdi ili posumnja na mogućnost povrede odredaba Zakona o sprečavanju pranja novca i financiranja terorizma i njegovih provedbenih propisa i/ili Sankcija ili Banka utvrdi da je Korisnik računa Sankcionirana osoba
- ako Korisnik, na zahtjev Banke, ne dostavi tražene podatke i dokumentaciju potrebnu za uspostavu i nastavak zasnovanog ugovornog odnosa u skladu s Mjerodavnim propisima
- ako Korisnik ne ispuni ili zakasni s ispunjenjem bilo koje novčane obveze po bilo kojem poslovnom odnosu s Bankom i/ili ako nastanu druge okolnosti ili ako prijeti nastanak drugih okolnosti za koje Banka može razumno pretpostaviti da povećavaju rizik da Korisnik neće uredno ispunjavati obveze prema Banci po osnovi Ugovora.

13.2.2. S danom prestanka valjanosti Ugovora o korištenju direktnim kanalom Banka onemogućuje korištenje Direktnim kanalom i obračunava sve nepodmirene obveze Korisnika u skladu s Izvatkom iz Odluke o tarifi naknada za usluge Banke po transakcijskim računima fizičkih osoba i usluga platnog prometa te direktnih kanala.

13.2.3. U slučaju raskida Ugovora sve naknade koje Banka obračunava za korištenje raskinutim ili deaktiviranim Direktnim kanalom, a naplaćuju se periodično u skladu s Izvatkom iz Odluke o tarifi naknada za usluge Banke po transakcijskim računima fizičkih osoba i usluga platnog prometa te Direktnih kanala, naplatit će se razmjerno vremenu trajanja Ugovora.

### **13.3. Raskid ugovora sklopljenog na daljinu**

Korisnik može, ne navodeći za to razloge i bez plaćanja naknada raskinuti Ugovor o korištenju direktnim kanalom sklopljen izvan poslovnih prostorija Banke u roku od 14 radnih dana od dana sklapanja.

### **14. ZAVRŠNE ODREDBE**

14.1. Ugovor o korištenju direktnim kanalom sklapa se na hrvatskome jeziku i komunikacija za vrijeme trajanja ugovornog odnosa obavlja se na hrvatskome jeziku.

14.2. Za sve sporove koji proizlaze iz ugovornog odnosa uređenog ovim Općim uvjetima poslovanja nadležan je stvarno nadležni sud sa sjedištem u mjestu prebivališta Korisnika.

14.3. Banka može tijekom trajanja ugovornog odnosa izmijeniti i/ili dopuniti bilo koju odredbu ovih Općih uvjeta poslovanja kada za to postoje objektivni razlozi koji to opravdavaju (npr. promjene ili dopune poslovnih procesa proizašlih iz tehničko-tehnoloških razloga, donošenje ili promjene mjerodavnih propisa i/ili Sankcija, promjena tržišnih uvjeta).

Banka će obavijestiti Korisnika Direktnog kanala o izmjenama ovih Općih uvjeta poslovanja i Izvatka iz Odluke o tarifi naknada za usluge Banke po transakcijskim računima fizičkih osoba i usluga platnog prometa te direktnih kanala dva mjeseca prije njihova stupanja na snagu putem ugovorenog i aktiviranog Direktnog kanala ili drugim ugovorenim kanalima komunikacije ako Korisnik nema aktiviran Direktni kanal. Izmjene i dopune Banka će dva mjeseca prije njihova stupanja na snagu učiniti dostupnima Korisnicima u poslovnicama Banke i na Internetskoj stranici Banke [www.zaba.hr](http://www.zaba.hr).

14.4. Smatra se da je Korisnik suglasan s izmjenama i dopunama ovih Općih uvjeta poslovanja i Izvatka iz Odluke o tarifi naknada za usluge Banke po transakcijskim računima fizičkih osoba i usluga platnog prometa te direktnih kanala ako do dana njihova stupanja na snagu:

- pisanim putem na neki od načina određen člankom 13. ovih Općih uvjeta poslovanja ne obavijesti Banku da ih ne prihvaća. Banka će primanjem takve obavijesti smatrati da je Korisnik jednostrano otkazao Ugovor o korištenju direktnim kanalom, odnosno da je deaktivirao pojedinu uslugu Direktnog kanala ugovorenu Ugovorom o transakcijskom poslovanju u odnosu na koju ne prihvaća izmjene, i to s datumom stupanja na snagu predloženih izmjena, osim ako Korisnik ne navede drugi datum stupanja na snagu otkaza, odnosno deaktivacije. Datum otkaza ili deaktivacije ne može biti kasniji od datuma na koji bi predložene izmjene stupile na snagu. U slučaju da je kao datum otkaza ili deaktivacije naveden raniji datum od datuma primanja obavijesti od strane Banke, otkaz odnosno deaktivacija u odnosu na Banku ima pravni učinak i stupa na snagu prvoga idućeg radnog dana od dana kada je Banka primila obavijest.



- ako u skladu s člankom ovih Općih uvjeta poslovanja ne otkáže ili deaktivira korištenje ugovorenim Direktnim kanalom.

14.5. U slučaju da Korisnik otkazuje Ugovor o korištenju direktnim kanalom ili deaktivira uslugu Direktnog kanala ugovorenu Ugovorom o transakcijskom poslovanju zato što nije suglasan s predloženim izmjenama i dopunama, otkaz ima pravo provesti bez naknade.

14.6. S danom stupanja na snagu ovih Općih uvjeta poslovanja prestaju vrijediti dosadašnji Opći uvjeti poslovanja Banke za korištenje Direktnih kanala od strane potrošača od 1. siječnja 2023.

14.7. Ovi Opći uvjeti poslovanja stupaju na snagu i primjenjuju se od 15. veljače 2024.