



HRVATSKA POŠTANSKA BANKA

Hrvatska poštanska banka, dioničko društvo
Jurišićeva 4, HR-10000 Zagreb

Na temelju članka 13. Statuta Hrvatske poštanske banke, dioničko društvo dana 09. ožujka 2021. godine Uprava Banke donosi sljedeće

OPĆE UVJETE POSLOVANJA HRVATSKE POŠTANSKE BANKE, DIONIČKO DRUŠTVO ZA KORIŠTENJE USLUGA IZRAVNOG BANKARSTVA ZA POSLOVNE SUBJEKTE

Izdavatelj ovih Općih uvjeta poslovanja Hrvatske poštanske banke, dioničko društvo za korištenje usluga izravnog bankarstva za poslovne subjekte (u daljnjem tekstu: Opći uvjeti poslovanja) je Hrvatska poštanska banka, dioničko društvo, Jurišićeva 4, 10000 Zagreb, Republika Hrvatska (u daljnjem tekstu: Banka), SWIFT oznaka: HPBZHR2X, upisana u sudski registar kod Trgovačkog suda u Zagrebu pod brojem MBS: 080010698, OIB: 87939104217, hpb@hpb.hr.

Tijelo nadležno za nadzor: Hrvatska narodna banka.

Banka ima odobrenje za rad Hrvatske narodne banke te se nalazi na popisu kreditnih institucija objavljenom na internetskoj stranici Hrvatske narodne banke www.hnb.hr.

1. PODRUČJE PRIMJENE

- 1.1. Ovi Opći uvjeti poslovanja reguliraju prava, obveze, način i uvjete korištenja usluga izravnog bankarstva od strane poslovnog subjekta (u daljnjem tekstu: Korisnik) i fizičke osobe ovlaštene za korištenje usluga izravnog bankarstva u ime i za račun Korisnika (u daljnjem tekstu: Ovlašteni Korisnik).
- 1.2. Ovi Opći uvjeti poslovanja primjenjuju se zajedno s Općim uvjetima poslovanja Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanje platnih usluga za poslovne subjekte, Odlukom o naknadama i drugim troškovima Hrvatske poštanske banke, dioničko društvo, za usluge u poslovanju (u daljnjem tekstu: Odluka o naknadama), pojedinačnim korisničkim Uputama za usluge izravnog bankarstva (u daljnjem tekstu: Uputa) te njihovim izmjenama i dopunama donesenima za vrijeme trajanja ugovornog odnosa između Banke i Korisnika. U odnosu na Opće uvjete poslovanja Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanje platnih usluga za poslovne subjekte, ovi Opći uvjeti poslovanja smatraju se posebnima i imaju prednost u primjeni. Oni reguliraju prava i obveze korisnika Usluga izravnog bankarstva te prava i obveze Banke u pružanju Usluga izravnog bankarstva. Oni zajedno s Pristupnicom čine ugovor (u daljnjem tekstu: Ugovor), a Ugovor, Opći uvjeti poslovanja Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanje platnih usluga za poslovne subjekte, Ugovor o otvaranju i vođenju transakcijskog računa i obavljanju platnih usluga i Odluka o naknadama sastavni su dijelovi Okvirnog ugovora o platnim uslugama.

Ovi Opći uvjeti poslovanja zajedno s Općim uvjetima poslovanja Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanje platnih usluga za poslovne subjekte koji se primjenjuju na ugovorni odnos između Banke i Korisnika dostupni su na internetskoj stranici Banke www.hpb.hr.

2. UVODNE ODREDBE

Pojedini pojmovi korišteni u ovim Općim uvjetima poslovanja imaju sljedeće značenje:

- 2.1. **Administrator ovlaštenja** – Ovlašteni korisnik kojega je Korisnik ovlastio da u ime i za račun Korisnika dodjeljuje, ukida i mijenja ovlaštenja za sebe i ostale Ovlaštene korisnike. Administrator ovlaštenja dodjeljuje, ukida ili mijenja dozvole uvida za pojedine funkcionalnosti dostupne u on-line bankarstvu kao i ovlaštenja po računima. Administratoru ovlaštenja omogućeno je upravljanje ovlastima odnosno dozvolama uvida za sljedeće funkcionalnosti: Poslovne račune, Izvode, Kredite, Depozite, Vrijednosne papire, Akreditive, Garancije, Kartice, HPB Invest, Pain 002 i Camt 053.
- 2.2. **Akti Banke** - u smislu odredbi ovih Općih uvjeta poslovanja jesu svi dokumenti i odluke što ih po propisanoj proceduri donose ovlaštena tijela Banke i koja su Korisniku dostupna putem pojedinih distributivnih kanala, a uređuju prava, ovlasti i obveze Korisnika i svih ostalih osoba koje preuzimaju prava i obveze prema Banci kao i Banke same (primjerice: Posebni opći uvjeti, Odluke o naknadama i tome sl.).
- 2.3. **Aktivacijski kod** - osobni identifikacijski brojevi koje Banka dodjeljuje Ovlaštenom korisniku, a koristi se u procesu registracije Ovlaštenog korisnika za korištenje pojedine usluge izravnog bankarstva ili aktiviranja pojedinih Sredstava za identifikaciju/autentifikaciju.
- 2.4. **Autorizacija** - suglasnost Korisnika odnosno Krajnjeg korisnika za izvršenje naloga za plaćanje.
- 2.5. **Banka** - Hrvatska poštanska banka, dioničko društvo, Jurišićeva 4, 10000 Zagreb, Republika Hrvatska, kao izdavatelj ovih Općih uvjeta poslovanja.
- 2.6. **Biometrijska autentifikacija** – autentifikacija utemeljena na biometrijskom svojstvu Ovlaštenog korisnika pohranjenom u Uređaju koji Ovlašteni korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju za usluge izravnog bankarstva koja se može koristiti u kombinaciji sa Sredstvom za identifikaciju/autentifikaciju koje je Banka dodijelila Korisniku (primjerice tokenom, mTokenom ili drugim Sredstvom koje Banka stavi Korisniku na raspolaganje). Metode biometrijske autentifikacije mogu biti metoda autentifikacije otiskom prsta kojeg je Korisnik pohranio u uređaju koji Korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju i/ili pri provođenju platne transakcije te metoda autentifikacija prepoznavanjem lica čija su svojstva pohranjena u uređaju koji Korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju i/ili pri provođenju platne transakcije.
- 2.7. **Certifikat** - potvrda u elektroničkom obliku, izdana od strane Banke, s ograničenim rokom važenja, pohranjena na pametnoj kartici ili USB uređaju, koja povezuje podatke za verifikaciju elektroničkog potpisa s Ovlaštenim korisnikom kojem je Banka dodijelila predmetnu pametnu karticu ili USB uređaj te potvrđuje njegov identitet.
- 2.8. **Dnevni limit** - predstavlja sigurnosni mehanizam koji omogućuje određivanje maksimalnog iznosa sredstava, unutar raspoloživog stanja na računu, kojim Ovlašteni korisnik može raspolagati u jednom danu putem usluga izravnog bankarstva.
- 2.9. **Inicijalni PIN** - osobni identifikacijski broj kojeg Banka dodjeljuje Ovlaštenom korisniku koji kao Sredstvo za identifikaciju/autentifikaciju koristi token ili drugo Sredstvo za identifikaciju/autentifikaciju za čije je inicijalno korištenje potreban unos inicijalnog PIN-a, poznat je isključivo Ovlaštenom korisniku i služi za njegovu inicijalnu autentifikaciju.

- 2.10. **Instant kreditni transfer** (u daljnjem tekstu: instant nalog) – platna usluga kojom se platna transakcija izvršava po nalogu platitelja na teret njegovog transakcijskog računa, a sredstva su raspoloživa primatelju na transakcijskom računu druge banke u zemlji u roku od nekoliko sekundi (do 10 (deset) sekundi). Usluga je dostupna 24 (dvadesetčetiri) sata dnevno sve kalendarske dane u godini i primjenjuje se isključivo kod izvršenja nacionalnih platnih transakcija u kunama zadanih u korist računa u drugim bankama.
- 2.11. **Personalizirane sigurnosne vjerodajnice** - personalizirana obilježja u obliku niza brojeva ili znakova koja Banka daje Korisniku ili Ovlaštenom korisniku u svrhu aktivacije usluga ili uređaja ili lozinki i kodova koji su poznati samo Korisniku ili Ovlaštenom korisniku. Personalizirane sigurnosne vjerodajnice obuhvaćaju, ali nisu ograničena na, identifikacijski kod, aktivacijski kod, korisnički broj, personaliziranu sigurnosnu riječ, PIN-ove koje je Ovlašteni korisnik odredio za korištenje mobilne aplikacije, tokena, mTokena, lozinku za pristup kvalificiranom elektroničkom certifikatu te sve kodove koje generiraju identifikacijski/autentifikacijski Uređaji.
- 2.12. **Jednokratna lozinka (OTP – One time password)** – je kriptografski kod generiran pomoću tokena/mTokena, primjenjiv samo jedanput i s ograničenim vremenom valjanosti, koji se može koristiti u postupku autentifikacije ili potvrde drugih radnji koje Ovlašteni korisnik inicira putem usluge internetskog/mobilnog bankarstva. Postupak generiranja OTP koda Banka naziva još i APPLI1, a kod se generira odabirom odgovarajuće funkcije tokena/mTokena koja će generirati navedenu vrstu koda uz primjenu PIN-a.
- 2.13. **Kanali izravnog bankarstva** - sredstva daljinske komunikacije koja omogućavaju korištenje bankovnih i drugih financijskih i nefinancijskih usluga korištenjem elektroničkih načina komuniciranja, bez istodobne fizičke nazočnosti Ovlaštenog korisnika i zaposlenika Banke na istom mjestu.
- 2.14. **Korisnik** - Poslovni subjekt kojem je Banka odobrila korištenje jedne ili više Usluga izravnog bankarstva. Korisnikom može postati Poslovni subjekt koji u Banci ima otvoren Račun.
- 2.15. **Kreditni transfer** – platna usluga kojom se transakcijski račun primatelja plaćanja odobrava za platnu transakciju ili niz platnih transakcija na teret platiteljevog transakcijskog računa od strane pružatelja platne usluge kod kojeg se vodi platiteljev transakcijski račun, na osnovi naloga za plaćanje kojeg zadaje platitelj.
- 2.16. **MAC (Message authentication code)** - je kriptografski kod generiran pomoću tokena/mTokena koji se može koristiti u postupku autorizacije određenih vrsta platnih transakcija ili potvrde drugih radnji koje Ovlašteni korisnik inicira putem usluge internetskog/mobilnog bankarstva. Postupak generiranja MAC koda Banka naziva još i APPLI2, a kod se generira odabirom odgovarajuće funkcije tokena/mTokena koja će generirati navedenu vrstu koda uz primjenu niza znamenki koje su korisniku pri korištenju usluge internetskog/mobilnog bankarstva prikazane kao podatak za unos ili upit za potvrdom. Generirani kod predstavlja kod za potvrdu koji Ovlašteni korisnik može koristiti u postupku autorizacije platne transakcije ili potvrde drugih radnji koje je inicirao putem usluge internetskog/mobilnog bankarstva.
- 2.17. **MDS (Multiple Data Signature)** - je kriptografski kod generiran pomoću tokena/mTokena koji se može koristiti u postupku autorizacije platne transakcije ili potvrde drugih radnji koje Ovlašteni korisnik inicira putem usluge internetskog/mobilnog bankarstva. Postupak generiranja MDS koda Banka naziva još i APPLI3, a kod se generira odabirom odgovarajuće funkcije tokena/mTokena koja će generirati navedenu vrstu koda uz primjenu dvaju nizova znamenki koje su korisniku pri korištenju usluge internetskog/mobilnog bankarstva prikazane kao podaci za unos ili kao obavijest koju je potrebno potvrditi. Nizovi znamenki za unos su tako odabrani da ujedno za Ovlaštenog korisnika predstavljaju najbližu tehnički ostvarivu reprezentaciju obavijesti

o iznosu platne transakcije i primatelju plaćanja. Generirani kod predstavlja kod za potvrdu koju Ovlašteni korisnik može koristiti u postupku autorizacije platne transakcije ili potvrde drugih radnji koje je inicirao putem usluge internetskog/mobilnog bankarstva.

- 2.18. **Nalozi za plaćanje** – instrukcija platitelja ili primatelja plaćanja Banci kojom se traži izvršenje platne transakcije.
- 2.19. **Okvirni ugovor** - Okvirni ugovor o platnim uslugama čine ovi Opći uvjeti poslovanja zajedno s Pristupnicom, Opći uvjeti poslovanja Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanju platnih usluga za poslovne subjekte, Ugovor o otvaranju i vođenju transakcijskog računa i Odluka o naknadama i drugim troškovima Hrvatske poštanske banke d.d. za usluge u poslovanju, Odluka o visini kamatnih stopa i Terminski plan izvršenja platnih transakcija poslovnih subjekata.
- 2.20. **Ovlašteni korisnik** - fizička osoba koja je ovlaštena od strane Korisnika i u njegovo ime i za njegov račun koristiti uslugu izravnog bankarstva ovisno o dobivenim ovlaštenjima. Vrste ovlaštenja i moguće kombinacije vrsta ovlaštenja koje Korisnik može dodijeliti Ovlaštenim korisnicima navedene su u obrascima za ugovaranje i/ili korištenje usluga izravnog bankarstva. Ovlaštenom korisniku moguće je dodijeliti sljedeća ovlaštenja po računima za usluge internetskog i mobilnog bankarstva: pregled, unos, izvršavanje ili samostalno potpisivanje platnih naloga.
- 2.21. **Ovlašteni korisnik s pravom potpisivanja platnih naloga** - ovlašten je za potpisivanje platnih naloga te na izvršavanje registracije i deregistracije PIR-a vezanog uz broj transakcijskog računa za kojeg je ovlašten.
- 2.22. **Pametna kartica/USB uređaj** - certificirani kriptografski uređaj za sigurnu pohranu certifikata koji služi za identifikaciju Ovlaštenog korisnika za pojedinog Korisnika, pristup i korištenje usluge internetskog bankarstva ovisno o danim ovlaštenjima.
- 2.23. **PIN** - osobni tajni identifikacijski broj Ovlaštenog korisnika, koji je poznat isključivo Ovlaštenom korisniku te se koristi za identifikaciju Ovlaštenog korisnika za pristup tokenu, mTokenu, mobilnom bankarstvu, pametnoj kartici, USB uređaju ili drugom Sredstvu za identifikaciju/autentifikaciju koje se može koristiti nakon ispravnog unosa PIN-a.
- 2.24. **Posredni identifikator računa** - dalje u tekstu: PIR) – broj mobitela, e mail adresa ili osobni identifikacijski broj (OIB) Korisnika koji Ovlašteni korisnik s pravom potpisa platnih naloga povezuje s IBAN-om transakcijskog računa Korisnika, koji Banka, temeljem suglasnosti Ovlaštenog korisnika, dostavlja u RPIR, u svrhu iniciranja platnih transakcija u korist transakcijskog računa. PIR jedinstveno identificira predmetni IBAN sve dok je u RPIR-u uz njega povezan.
- 2.25. **Podnositelj Pristupnice** - Korisnik koji predajom potpisane Pristupnice od Banke traži mogućnost korištenja usluga izravnog bankarstva za poslovne subjekte.
- 2.26. **Poslovni subjekt** - pravna osoba, tijelo državne vlasti, tijelo državne uprave, jedinica lokalne ili područne samouprave te njihova tijela, udruga i društvo (sportsko, kulturno, dobrotvorno i sl.) te fizička osoba (nepotrošač) koja djeluje unutar područja svoje registrirane gospodarske djelatnosti ili slobodnog zanimanja i s Bankom zaključuje Okvirni ugovor.
- 2.27. **Potpisnik** - Ovlašteni korisnik koji posjeduje Uređaj koji koristi kao Sredstvo za identifikaciju/autentifikaciju kojim se potpisuju i autoriziraju nalozi za plaćanje u ime i za račun Korisnika. Potpisnik može biti lijevi, desni ili samostalni, a ovlaštenje mu je moguće dodijeliti po pojedinom računu. Ovlašteni korisnici s ovlaštenjem za potpisivanje platnih naloga mogu obavljati registraciju i deregistraciju određenog posrednog identifikatora računa (PIR) uz određeni broj transakcijskog računa (IBAN) u Registar posrednih identifikatora računa (RPIR).

- 2.28. **Pouzdana autentifikacija** – jest autentifikacija na osnovi uporabe dvaju ili više elemenata koji pripadaju u kategoriju znanja (nešto što samo korisnik zna), posjedovanje (nešto što korisnik posjeduje) i svojstvenosti (nešto što korisnik jest) koji su međusobno neovisni, što znači da povreda jednog ne umanjuje pouzdanost drugih i koja je osmišljena na takav način da štiti povjerljivost autentifikacijskih podataka, pri čemu najmanje dva od navedenih elemenata moraju pripadati različitoj kategoriji.
- 2.29. **Pristupnica** – pisani zahtjev za korištenje usluga izravnog bankarstva za poslovne subjekte.
- 2.30. **Provjereni primatelj** – primatelj kreditnog transfera za kojeg je dopušteno ne primjenjivati pouzdanu autentifikaciju prilikom autorizacije transakcije. Korisnik on-line bankarstva sam stvara i mijenja popis provjerenih primatelja. Dodavanje na popis je moguće prilikom prvog iniciranja plaćanja prema određenom primatelju, a dodavanje ili uklanjanje određenog primatelja s popisa je moguće unutar odgovarajućeg izbornika aplikacije. Svako dodavanje ili mijenjanje liste provjerenih pouzdanih primatelja Korisnik mora potvrditi pouzdanom autentifikacijom.
- 2.31. **Pružatelj usluge informiranja o računu (AISP - Account Information Service Provider)** je pružatelj platnih usluga koji obavlja djelatnost informiranja o računu.
- 2.32. **Pružatelj usluge iniciranja plaćanja (PISP - Payment Initiation Service Provider)** je pružatelj platnih usluga koji obavlja djelatnost iniciranja plaćanja.
- 2.33. **Račun** - svaki transakcijski račun Korisnika otvoren u Banci, a koji se koristi za izvršavanje platnih transakcija u domaćoj i stranoj valuti kao i u druge svrhe vezane uz platno-prometne usluge.
- 2.34. **Raspoloživo stanje na transakcijskom računu** - iznos pozitivnog stanja u valuti terećenja uvećan za neiskorišteni iznos odobrenog prekoračenja po računu u valuti terećenja umanjeno za ranije predane naloge za plaćanje u valuti terećenja koji čekaju izvršenje na zadani datum ili neproknjižena sredstva (npr. nalozi poslani u klirinške sustave, kartične transakcije)
- 2.35. **Registar posrednih identifikatora računa (dalje u tekstu: RPIR)** - je sustav koji sudionicima RPIR-a omogućuje povezivanje određenih posrednih identifikatora računa korisnika platnih usluga u platnoj transakciji s njihovim IBAN-om u svrhu korištenja jedne ili više platnih usluga bez potrebe da korisnici platnih usluga prethodno znaju informaciju o IBAN-u drugog korisnika platnih usluga, odnosno IBAN se automatski popunjava podacima iz RPIR-a. Nacionalnim registrom upravlja Financijska agencija (FINA) u koji se, putem Banke kao sudionika RPIR-a, registrira od strane Ovlaštenog korisnika s ovlaštenjem potpisivanja platnih naloga, određeni PIR uz određeni broj transakcijskog računa (IBAN). RPIR potom omogućava drugom korisniku platne usluge čiji je pružatelj platne usluge također sudionik RPIR-a, da prilikom iniciranja platne transakcije dohvati iz RPIR-a podatak o broju transakcijskog računa primatelja plaćanja (IBAN) putem podatka primatelja plaćanja koji je registriran u RPIR-u kao PIR povezan uz određeni transakcijski račun. Banka obavlja registraciju IBAN-a vezanog uz PIR kako je definirao Ovlašteni korisnik s ovlaštenjem potpisivanja platnih naloga, odjavu PIR-a pridruženog uz IBAN iz RPIR-a, dohvat podataka iz RPIR-a za potrebe iniciranja platne transakcije, dohvat deaktiviranih parova PIR-IBAN od drugog korisnika RPIR-a te pretraživanje podataka svojih korisnika platnih usluga. RPIR je usklađen sa standardima SPL-a (engl. Standardised Proxy Lookup) – jedinstvenom europskom bazom koju razvija Europsko platno vijeće (engl. European Payments Council) u svrhu interoperabilnosti na razini EU-a, odnosno mogućnost da se korištenjem baze mogu zadavati plaćanja u korist bilo kojeg primatelja plaćanja na području Europske unije. Na zahtjev Korisnika registrirani par PIR-IBAN bit će dostupan pružateljima platnih usluga unutar SEPA područja kroz SPL bazu nakon što Europsko platno vijeće dovrši razvoj funkcionalnosti.

- 2.36. **Sankcije (međunarodne mjere ograničavanja)** - su instrument diplomatske ili gospodarske prirode kojima se nastoji promijeniti aktivnosti ili politike poput kršenja međunarodnog prava ili ljudskih prava, ili politike koje ne poštuju vladavinu prava ili demokratska načela i utječu na poslovanje financijskih institucija i njihovih klijenata postavljanjem ograničenja, i kontrolom kretanja roba, usluga i sredstava obustavom izvršenja usluga i kontrolom kretanja roba, usluga i sredstava.
- Sankcije su zabrane nametnute organizacijama, fizičkim osobama i njihovim tvrtkama, kao i proizvodi i usluge navedeni u propisima Vijeća Europe, rezolucijama Vijeća sigurnosti, Ujedinjenih naroda, i u slučaju sankcija SAD-a, propisa OFAC-a kao i bilo koje sankcije koje nalažu tijela vlasti određenih zemalja i ograničavajuće odredbe s međunarodnom ili regionalnom snagom koje izdaju tijela vlasti drugih zemalja.
- Popis najvažnijih institucija koje propisuju sankcijske mjere uključuje: Ujedinjene narode, Europsku uniju, Ured za nadzor strane imovine Ministarstva financija SAD-a (Office of Foreign Assets Control – OFAC), Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske. Sankcije koje primjenjuju Sjedinjene Američke Države su sankcije, zabrane i mjere ograničavanja koje je izdao predsjednik Sjedinjenih Američkih Država i objavio Ured za kontrolu strane imovine američkog Ministarstva financija (OFAC). Te sankcije se odnose na sve fizičke i pravne osobe koje imaju američki status, kao i financijske transakcije denominirane u USD.
- 2.37. **Sigurnosna riječ** - Riječ koju određuje Ovlašteni korisnik prema vlastitom odabiru prilikom popunjavanja Pristupnice, a koja služi za identifikaciju Korisnika prilikom deblokade tokena.
- 2.38. **SMS usluga** - usluga koja omogućuje Korisnicima da putem mobilnog uređaja od Banke primaju poruke s informacijama.
- 2.39. **Softver banke** - aplikativno rješenje koje se koristi za pružanje Usluga izravnog bankarstva, poput mobilne aplikacije ili web aplikacije. Isti se instalira na računalo Korisnika/Ovlaštenog korisnika ili mobilni (višenamjenski) uređaj.
- 2.40. **Sredstva za identifikaciju/autentifikaciju** - tehničko sredstvo i/ili aplikativno rješenje koje omogućava identifikaciju Korisnika prilikom korištenja pojedine usluge izravnog bankarstva i autorizaciju naloga za plaćanje i drugih vrsta naloga koje je Korisnik zadao korištenjem pojedine usluge izravnog bankarstva. Sredstvo za identifikaciju/autentifikaciju može biti različito, ovisno o usluzi izravnog bankarstva (na primjer, token, mToken, pametna kartica, USB uređaj i druga Sredstva za identifikaciju/autentifikaciju koje Banka stavi korisniku, odnosno Ovlaštenom korisniku na raspolaganje).
- 2.41. **Šifra za otključavanje** - je alfanumerički set znakova koji se koristi za otključavanje pametne kartice ili USB uređaja u slučaju kad se isti zaključaju usred uzastopnog unosa pogrešnog PIN-a.
- 2.42. **Token/mToken** - kriptografski uređaj/aplikacija, inicijaliziran pridruženim ključem i zaštićen lozinkom koji putem kriptografskih algoritama služi za identifikaciju Ovlaštenog korisnika za pojedinog Korisnika (kontrola pristupa), ovisno o danim ovlaštenjima, autorizaciju transakcija i potpisivanje naloga, generira jednokratne lozinke ograničenog trajanja koje identificiraju Korisnika usluge izravnog bankarstva i/ili drugih usluga čije korištenje Banka omogući Korisniku.
- 2.43. **Unositelj** - Ovlašteni korisnik koji posjeduje Uređaj koji koristi kao Sredstvo za identifikaciju/autentifikaciju kojim se unose nalozi za plaćanje, a ovlaštenje mu je moguće dodijeliti po pojedinom računu.
- 2.44. **Uređaj** - predstavlja token, pametnu karticu, USB uređaj, mToken ili sličan kriptografski uređaj na kojem se generiraju korisnički kriptografski ključevi i na kojem se pohranjuju certifikati koji identificiraju Korisnika. Uređaji u vlasništvu Banke su token, pametna kartica, USB uređaj, mToken ili sličan kriptografski uređaj kojim se potpisuju i

autoriziraju nalozi za plaćanje u ime i za račun Korisnika. Uređaji koji nisu u vlasništvu Banke su računalo i mobilni uređaj (višenamjenski uređaj) na koji se instalira aplikacija.

- 2.45. **Usluga informiranja o transakcijskom računu** - online elektronička usluga kojom se pružaju konsolidirane informacije o jednom ili više transakcijskih računa za plaćanje koje korisnik platnih usluga ima kod drugog pružatelja platnih usluga ili kod više pružatelja platnih usluga.
- 2.46. **Usluga iniciranja plaćanja** - usluga zadavanja naloga za plaćanje na zahtjev korisnika platnih usluga s njegova transakcijskog računa koji vodi drugi pružatelj platnih usluga.
- 2.47. **Usluge izravnog bankarstva** - skup usluga Banke koji čine usluga internetskog i mobilnog bankarstva Banke i SMS usluga (u daljnjem tekstu: Usluge).
- 2.48. **Politika zaštite osobnih podataka** - temeljni akt koji opisuje svrhu i ciljeve prikupljanja, obrade i upravljanja osobnim podacima, a osigurava adekvatnu razinu zaštite podataka u skladu s Općom uredbom o zaštiti podataka i svim ostalim vezanim zakonskim propisima.

Svi pojmovi koji nisu posebno definirani ovim Općim uvjetima poslovanja imaju značenje kako je to utvrđeno Općim uvjetima Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanje platnih usluga za poslovne subjekte, a ukoliko nisu definirani niti njima, imaju značenje kako je to utvrđeno Zakonom o platnom prometu

3. OPSEG USLUGE

- 3.1. Informacije o ponudi Usluga dostupne su u poslovnoj mreži i na internetskoj stranici Banke (www.hpb.hr).
- 3.2. Za svaku ugovorenu Uslugu, Banka će omogućiti Korisniku uvid u informacije i obavljanje transakcija u opsegu i na način naveden u Ugovoru i/ili Uputi za korištenje Usluga za poslovne subjekte. Uputa je dostupna na internetskoj stranici Banke www.hpb.hr. Banka ima pravo izmjene Uputa, a Korisnik je dužan po istima postupati.
- 3.3. Banka pridržava pravo izmjene opsega i sadržaja Usluga, Uputa za korištenje usluge i Uputa za korištenje Uređaja koji se koristi kao Sredstvo za identifikaciju/autentifikaciju. Sve izmjene bit će Korisniku dostupne na prikladan način u poslovnoj mreži Banke i na internetskim stranicama Banke www.hpb.hr prije stupanja izmjena Uputa na snagu. Smatrat će se da je Korisnik prihvatio izmjene usluga ukoliko ugovorenu Uslugu ne otkáže pisanim putem do dana stupanja izmjena na snagu. Zaprimanjem pisane obavijesti Korisnika o neprihvatanju izmjena Usluga koje se mogu obavljati korištenjem ugovorene Usluge smatra se da je Korisnik otkazao korištenje Usluge. Korisnik nema pravo zahtijevati naknadu štete u slučaju izmjene opsega i sadržaja Usluge.
- 3.4. Korištenjem internetskog i mobilnog bankarstva omogućuju se sljedeće usluge:
 - izvršenje i pregled platnih transakcija;
 - pregled stanja, prometa po računima i izvoda;
 - razmjena obavijesti između Korisnika i Banke;
 - registracija i deregistracija PIR-a vezanog uz transakcijski račun u RPIR-u;
 - obavljanje ostalih usluga
- 3.5. Banka je ovlaštena uvoditi nove i mijenjati postojeće obrasce koji se koriste za ugovaranje ili korištenje pojedine Usluge te će ih objaviti na internetskoj stranici Banke www.hpb.hr.
- 3.6. Korisnik se obvezuje koristiti Usluge na ugovoreni način u svim odnosima za koje je predviđena sukladno Okvirnom ugovoru i uputama za korištenje pojedine Usluge.

4. UGOVARANJE USLUGE

- 4.1. Za ugovaranje Usluge, Korisnik mora zadovoljiti sljedeće uvjete:
- Korisnik Usluge može postati onaj poslovni subjekt koji u Banci ima otvoren račun za plaćanje ili iznimno onaj poslovni subjekt koji u Banci nema otvoren račun za plaćanje, ali je korisnik nekog drugog proizvoda ili usluge za koju je omogućeno korištenje Usluga;
 - Korisnik mora Banci dostaviti pravilno popunjenu i potpisanu Pristupnicu za korištenje Usluge u poslovnu mrežu Banke ili poštom na adresu Hrvatske poštanske banke, dioničko društvo, Direkcija izravnog bankarstva, Jurišićeva 4, 10 000 Zagreb;
 - Zakonski zastupnik Korisnika svojim potpisom mora jamčiti za davanje ovlaštenja Ovlaštenim korisnicima na vlastitu odgovornost i ujedno Ovlaštenim korisnicima s pravom potpisivanja platnih naloga, davanje ovlaštenja za ugovaranje dodatnih usluga putem Usluge. Ovlašteni korisnik s pravom potpisivanja platnih naloga obavlja registraciju i deregistraciju PIR-a vezanog uz određeni broj transakcijskog računa.
- 4.2. Korisnik može ugovoriti jednu ili više Usluga.
- 4.3. Ugovor o korištenju Usluge sklapa se između Banke i Korisnika, na neodređeno vrijeme.
- 4.4. Korisnik svojim potpisom na Pristupnici prihvaća Opće uvjete poslovanja i ostale akte koji se primjenjuju zajedno s njima, ugovara korištenje Usluge i potvrđuje točnost podataka naznačenih na Pristupnici.
- 4.5. Trenutkom sklapanja Ugovora smatra se trenutak odobrenja Pristupnice od strane Banke.
- 4.6. Korisnik u Pristupnici odabire način dostave Uređaja kojeg će koristiti kao Sredstvo za identifikaciju/autentifikaciju.
- 4.7. Korisnik u Pristupnici mora odrediti jednog ili više Ovlaštenih korisnika, koji će u njegovo ime koristiti ugovorenu Uslugu.
- 4.8. Korisnik mora svakom Ovlaštenom korisniku usluge internetskog i mobilnog bankarstva odabrati jednu vrstu ovlaštenja, između onih koje mu ponudi Banka.
- 4.9. Za pojedinog Ovlaštenog korisnika moguće je odabrati različite vrste ovlaštenja. Odabir, izmjena i opoziv ovlaštenja Ovlaštenih korisnika temelji se na dostavi ispravno popunjenih obrazaca Banke predviđenih za pojedinu uslugu, koje Korisnik dostavi Banci na predviđen način za pojedinu uslugu. Alternativno, Administrator ovlaštenja može unutar internetskog bankarstva samostalno odabrati, mijenjati ili opozvati ovlaštenja Ovlaštenih korisnika. Svaki odabir, izmjena ili opoziv ovlaštenja je neopoziv nalog za daljnje postupanje Banke.
- 4.10. Korisnik Usluga izravnog bankarstva može pojedinom ili svim Ovlaštenim korisnicima odrediti dnevni limit raspolaganja novčanim sredstvima u odnosu na pojedini transakcijski račun, do kojeg isti mogu obavljati platne transakcije putem Usluga. Iznos odobrenog limita je promjenjiv i može se naknadno smanjiti, povećati ili ukinuti sukladno pisanom zahtjevu Korisnika.
- 4.11. Korisnik je upoznat s činjenicom da je Banka ovlaštena samostalno uvoditi nove vrste ovlaštenja, mijenjati opseg ili ukidati pojedine vrste ovlaštenja koje Korisnik odabire Ovlaštenim korisnicima te je s istim suglasan.

- 4.12. Sva dokumentacija, uključivo i sve bančine obrasce koje Korisnik dostavi Banci u vezi s ugovaranjem, korištenjem ili opozivom korištenja Usluge moraju biti potpisani od strane zakonskog zastupnika Korisnika.
- 4.13. Korisnik se uslugom internetskog ili mobilnog bankarstva može koristiti najkasnije od prvog sljedećeg radnog dana nakon što potpiše svu propisanu dokumentaciju, preuzme sve potrebne podatke, Uređaje i/ili Sredstva za identifikaciju/autentifikaciju, koja su nužna za korištenje usluge.
- 4.14. Korisnik odnosno Ovlašteni korisnik je dužan koristiti Usluge izravnog bankarstva u skladu s propisima o sprječavanju pranja novca i financiranja terorizma, međunarodnim mjerama ograničavanja odnosno sankcijama koje primjenjuju Sjedinjene Američke Države i Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske i/ili drugih prisilnih propisa, te na zahtjev Banke, u obliku i na način koji odredi Banka, dostaviti podatke i dokumentaciju potrebnu za uspostavu Usluga izravnog bankarstva te za nastavak i praćenje zasnovanoga ugovornog odnosa u skladu s odredbama navedenih propisa o sprječavanju pranja novca i financiranja terorizma, međunarodnim mjerama ograničavanja i/ili drugih prisilnih propisa odnosno sankcijama koje primjenjuju Sjedinjene Američke Države i Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske.
- 4.15. Banka, sukladno uvjetima svoje poslovne politike, zadržava pravo odbiti Pristupnicu odnosno odlučuje o odobrenju ili odbijanju pružanja Usluge, bez obaveze da Podnositelju Pristupnice obrazloži svoju odluku.

5. KORIŠTENJE USLUGE

- 5.1. Korisnik koristi Usluge pomoću mobilnog uređaja, računala te Uređaja kojeg koristi kao Sredstvo za identifikaciju/autentifikaciju.
- 5.2. Korisnik usluzi internetskog/mobilnog bankarstva pristupa pomoću Uređaja koji su nužni za identifikaciju/autentifikaciju. Po odobrenju Pristupnice Banka Korisniku uručuje Uređaje nužne za identifikaciju/autentifikaciju ili ih šalje poštom na adresu za korespondenciju navedenu na Pristupnici. PIN šalje poštom na adresu za korespondenciju Ovlaštenog korisnika navedenu na Pristupnici odvojeno od Uređaja.
- 5.3. Ovlaštenom korisniku koji kao Uređaj koristi mToken ili je zatražio aktivaciju mobilnog bankarstva Banka će u roku od 2 (dva) radna dana od dana ugovaranja njegovog korištenja poslati na ugovoreni broj mobilnog (višenamjenskog) uređaja SMS poruku s poveznicom s koje Ovlašteni korisnik može instalirati mToken ili aplikaciju za mobilno bankarstvo na mobilni (višenamjenski) uređaj. Također, Banka će Ovlaštenom korisniku, dostaviti aktivacijski kod kojim može aktivirati mToken i/ili mobilno bankarstvo. Korisnik potvrđuje da je upoznat s time da se mToken ili aplikacija mobilnog bankarstva instalira na mobilni (višenamjenski) uređaj s internetskih stranica koje ne pripadaju Banci te je suglasan da Banka ne odgovara za mogućnosti i uvjete korištenja predmetnih internetskih stranica, kao ni za uvjete pod kojima se mToken ili aplikacija mobilnog bankarstva može instalirati. Ovlašteni korisnik je obvezan odmah nakon aktivacije mTokena ili mobilnog bankarstva, a prije prve prijave u internetsko ili mobilno bankarstvo odabrati i potvrditi PIN ili odabrati metodu biometrijske autentifikacije kojim će se nadalje identificirati pri korištenju mTokena ili mobilnog bankarstva. Korisnik odnosno Ovlašteni Korisnik snosi sve naknade i troškove povezane s instaliranjem i korištenjem aplikacije.
- 5.4. Aktivacijski kod za mToken ili mobilno bankarstvo šalje se Ovlaštenom korisniku iz sigurnosnih razloga u dva dijela putem dva odvojena kanala, SMS-om na mobilni (višenamjenski) uređaj i e-mailom na e-mail Korisnika.
- 5.5. Aktivacijski kod za mToken ili mobilno bankarstvo vrijedi 15 (petnaest) dana od dana izdavanja koda. Nakon isteka navedenog roka, iz sigurnosnih razloga, neiskorišteni

aktivacijski kod prestaje vrijediti. Korisnik može zatražiti izdavanje novog koda bez naknade.

- 5.6. Korisnik se uslugom internetskog ili mobilnog bankarstva može koristiti najkasnije od prvog sljedećeg radnog dana nakon što preuzme sve potrebne podatke i/ili Sredstva za identifikaciju/autentifikaciju, koja su nužna za korištenje usluge.
- 5.7. Prilikom prvog korištenja usluge internetskog ili mobilnog bankarstva, Korisnik/Ovlašteni korisnik je obavezan promijeniti PIN na način propisan kratkom uputom za korištenje tokena, unutar same aplikacije kod spajanja putem mobilnog (višenamjenskog) uređaja, pametne kartice ili USB uređaja. Upute za korištenje Uređaja koji se koriste kao Sredstva za identifikaciju/autentifikaciju dostupne su na internetskim stranicama Banke www.hpb.hr.
- 5.8. Uređaji koji se koriste kao Sredstva za identifikaciju/autentifikaciju osiguravaju autorizirani pristup servisu te dodatno digitalno potpisivanje financijskih transakcija.
- 5.9. Za korištenje Usluge izravnog bankarstva Korisnik sam osigurava minimalne tehničke uvjete, uključujući računalo i pristup internetu te mobilni (višenamjenski) uređaj kako je navedeno u Uputi za korištenje pojedine usluge izravnog bankarstva koja je dostupna na internetskim stranicama Banke. Korisnik se potpisom Pristupnice obvezuje postupati u cijelosti u skladu s Uputom za korištenje pojedine usluge izravnog bankarstva.
- 5.10. Ako se Korisnik nalazi u inozemstvu, a zaboravio je PIN za mToken ili mobilno bankarstvo, može zatražiti ponovo izdavanje aktivacijskog koda. U tom slučaju, potpis Korisnika na dokumentu kojim traži ponovo izdavanje aktivacijskog koda, mora biti ovjeren od strane nadležnog tijela sukladno posebnim propisima (primjerice javni bilježnik, sud, konzularna predstavništva RH u inozemstvu), a potrebno ga je dostaviti na e-mail adresu Banke direkcija.izravnog.bankarstva@hpb.hr.
- 5.11. Svi oblici korištenja usluge internetskog i mobilnog bankarstva zadani elektroničkim putem uz primjenu propisane korisničke dokumentacije izjednačeni su s vlastoručnim potpisivanjem od strane Ovlaštenih korisnika.

6. AUTENTIFIKACIJA KORISNIKA

- 6.1. Korisnik koji je ugovorio internetsko bankarstvo prilikom pristupa istome autentificira se na jedan od sljedećih načina:
 - Korisnik koji za pristup internetskom bankarstvu kao Sredstvo za identifikaciju/autorizaciju koristi token identificira se unosom serijskog broja tokena u za to predviđeno polje na ekranskom sučelju kanala, a pouzdano se autentificira jednokratnom lozinkom koju generira token nakon unosa ispravnog PIN-a.
 - Korisnik koji za pristup internetskom bankarstvu kao Sredstvo za identifikaciju/autorizaciju koristi mToken identificira se unosom serijskog broja mTokena u za to predviđeno polje na ekranskom sučelju kanala, a pouzdano se autentificira jednokratnom lozinkom koju generira token nakon unosa ispravnog PIN-a. Iznimno od navedenog, Korisnik može koristiti mToken bez unosa PIN-a tako da se pouzdano autentificira nekom od metoda biometrijske autentifikacije, na način i pod uvjetima definiranim ovim Općim uvjetima poslovanja.
- 6.2. Korisnik koji je ugovorio mobilno bankarstvo prilikom pristupa mobilnom bankarstvu autentificira se na jedan od sljedećih načina:
 - unosom odabranog PIN-a za pristup mobilnom bankarstvu u za to predviđeno polje u aplikaciji mobilnog bankarstva koja je instalirana na mobilnom (višenamjenskom) uređaju Korisnika ili

- jednom od metoda biometrijske autentifikacije, na način i pod uvjetima definiranim ovim Općim uvjetima poslovanja.
- 6.3. Biometrijska autentifikacija se temelji na tehnologiji mobilnog (višenamjenskog) uređaja kojeg Korisnik koristi za pristup internetskom ili mobilnom bankarstvu. Pojedini mobilni (višenamjenski) uređaji ne podržavaju biometrijsku autentifikaciju ili pojedine metode biometrijske autentifikacije.
 - 6.4. Banka nema pristup podacima niti kontrolu nad podacima koje je Korisnik u svrhu biometrijske autentifikacije pohranio u mobilni (višenamjenski) uređaj koji koristi za pristup internetskom ili mobilnom bankarstvu.
 - 6.5. Korisnik potvrđuje da je u mobilni (višenamjenski) uređaj koji koristi za pristup internetskom ili mobilnom bankarstvu pohranio isključivo biometrijske karakteristike svojeg lica odnosno otisak svojeg prsta. Korisnik prihvaća da se u svrhu njegove biometrijske autentifikacije prilikom pristupa internetskom ili mobilnom bankarstvu mogu koristiti biometrijski podaci koji su pohranjeni u mobilnom (višenamjenskom) uređaju koji Korisnik koristi za pristup internetskom ili mobilnom bankarstvu.
 - 6.6. Korištenje biometrijske autentifikacije je dobrovoljno te ne isključuje niti ograničava mogućnost pouzdane autentifikacije Korisnika PIN-om kojeg je odabrao za pristup mobilnom ili internetskom bankarstvu.
 - 6.7. Banka može ograničiti ili onemogućiti korištenje pojedine usluge internetskog ili mobilnog bankarstva u slučaju biometrijske autentifikacije Korisnika te uvjetovati njihovo korištenje pouzdanom autentifikacijom Korisnika PIN-om kojeg je odabrao za pristup internetskom ili mobilnom bankarstvu.
 - 6.8. Kada se na Uređaju koji Korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju na kojem je aktivirana neka od metoda biometrijske autentifikacije prilikom pristupa Korisnika ili bilo koje druge osobe internetskom ili mobilnom bankarstvu pozitivno potvrdi korištenje otiska prsta ili lica čije su karakteristike pohranjene na navedenom Uređaju, koji Korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju, smatra se da je Banka izvršila autentifikaciju Korisnika.
 - 6.9. Aktiviranjem i korištenjem opcije biometrijske autentifikacije Korisnik potvrđuje da je upoznat i suglasan s time da Banka ne pruža uslugu biometrijske autentifikacije, već da koristi biometrijsku autentifikaciju koju omogućava Uređaj koji Korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju koje koristi.
 - 6.10. Banka ne odgovara za nemogućnost ili ograničenu mogućnost korištenja biometrijske autentifikacije, niti za rezultat takve biometrijske autentifikacije, neovisno o tome da li otisak prsta ili karakteristike lica pomoću kojih se Korisnik identificira prilikom pristupa internetskom ili mobilnom bankarstvu odgovaraju ili ne odgovaraju otisku prsta ili karakteristikama lica koje je Korisnik prethodno pohranio u mobilni (višenamjenski) uređaj kojeg koristi kao Sredstvo za identifikaciju/autentifikaciju za pristup internetskom ili mobilnom bankarstvu.
 - 6.11. Korisnik može onemogućiti biometrijsku autentifikaciju tako da na Uređaju koji koristi kao Sredstvo za identifikaciju/autentifikaciju promjeni odabrane metode identifikacije/autentifikacije koje omogućava biometrijska autentifikacija

7. SIGURNOST

7.1. Radi sigurnosti pristupa usluzi internetskog i mobilnog bankarstva te radi obavljanja transakcija Banka će Ovlaštenom korisniku dodijeliti Sredstvo za identifikaciju/autentifikaciju.

7.2. Korisnik i Ovlašteni korisnik obvezuju se:

- S povećanom pažnjom čuvati sva dodijeljena Sredstva za identifikaciju/autentifikaciju, tako da spriječe njihovo oštećenje, gubitak, krađu, neovlaštenu uporabu ili zlouporabu,
- s povećanom pažnjom zaštititi vlastite Uređaje koje koriste za pristup pojedinoj usluzi izravnog bankarstva, poput računala ili mobilnog (višenamjenskog) uređaja, tako da spriječe njihovo oštećenje, gubitak, krađu, neovlaštenu uporabu ili zlouporabu,
- koristiti se dodijeljenim Sredstvima za identifikaciju/autentifikaciju, uključujući i mobilni (višenamjenski) uređaj putem kojeg koristi određenu Uslugu na način uređen ovim Općim uvjetima poslovanja, Uputom za korištenje usluga izravnog bankarstva za poslovne subjekte i relevantnom uputom za korištenje Uređaja kojeg koristi kao Sredstvo za identifikaciju/autentifikaciju,
- redovito provjeravati postojanje novih obavijesti i postupati u skladu s obavijestima koje im Banka učini dostupnima putem ugovorene Usluge i/ili internetskoj stranici Banke www.hpb.hr,
- pridržavati se svih sigurnosnih mjera zaštite i korištenja računala, odnosno mobilnog uređaja kojeg koriste za pristup usluzi izravnog bankarstva, uključujući:
 - zaštititi pristup računalu i mobilnom (višenamjenskom) uređaju povjerljivom zaporkom ili biometrijskom autentifikacijom,
 - odabrati za zaporku takvu kombinaciju brojeva, velikih i malih slova te posebnih znakova koje se ne može lako otkriti, primjerice loše bi bilo odabrati uzastopni niz brojeva, datum rođenja Ovlaštenog korisnika ili ime/prezime Ovlaštenog korisnika. Također je bitno redovito periodički mijenjati zaporku,
 - zaštititi tajnost odabrane zaporke kako bi se spriječilo njezino otkrivanje ili neovlašteno korištenje (ne zapisivati zaporku!),
 - ne otvarati elektroničku poštu i privitke pristigle od nepoznatih i/ili sumnjivih pošiljatelja te ne otvarati poveznice iz takvih poruka,
 - pribavljati informatičku opremu i programske aplikacije iz provjerenih i sigurnih izvora,
 - spajati računalo i mobilni (višenamjenski) uređaj samo na sigurne i provjerene WI-FI mreže
 - instalirati i redovito ažurirati antivirusne programe i definicije i skenirati sve aplikacije na računalu kojeg koriste za pristup Uslugama antivirusnim programom kojeg Ovlašteni korisnik posjeduje na računalu,
 - redovito ažurirati sigurnosne dodatke i programske definicije vezane za operativni sustav mobilnog (višenamjenskog) uređaja i/ili računala.
 - pravodobno obnavljati certifikat pohranjen na dodijeljenom Uređaju kojeg koristi kao Sredstvo za identifikaciju/autentifikaciju,
 - nakon prestanka korištenja Uređaja kojeg koristi kao Sredstvo za identifikaciju/autentifikaciju, isti je potrebno ukloniti iz računala,
 - u roku od najkasnije 90 (devedeset) dana od dana ugovaranja usluge preuzeti Uređaj za autorizaciju
 - pravodobno pristupati zamjeni Uređaja za autorizaciju i

- za svo vrijeme važenja odredaba ovog Ugovora omogućiti da najmanje jedan Ovlašteni korisnik u svakom trenutku posjeduje Uređaj koji zadovoljava tehničke preduvjete nužne za Sredstva za identifikaciju/autentifikaciju;
- 7.3. Korisnik je dužan čuvati tajnost svih PIN-ova i drugih personaliziranih sigurnosnih vjerodajnica kao i tajnost svih podataka vezanih uz korištenje Usluge izravnog bankarstva te voditi brigu da Sredstvo za identifikaciju /autentifikaciju ne dospije u ruke trećoj, neovlaštenoj osobi i prihvaća potpunu odgovornost za sve obveze nastale njihovim korištenjem. Štetu nastalu nepridržavanjem ovih odredbi u cijelosti snosi Korisnik.
- 7.4. Korisnik ne smije neovlašteno raditi preinake na Uređajima koje koristi kao Sredstva za identifikaciju/autorizaciju, softveru Banke ili mobilnom (višenamjenskom) uređaju (na primjer root, jailbreak) te snosi svu štetu nastalu nepridržavanjem ovih odredbi.
- 7.5. Korisnik odgovara za način uporabe Sredstava za identifikaciju/autentifikaciju, kao i za sve posljedice koje za njega mogu iz toga proizaći ukoliko se istima ne koristi u skladu s ovim Općim uvjetima poslovanja. Korisnik snosi svu štetu nastalu nepridržavanjem ovih odredbi.
- 7.6. Korisnik je dužan za pristup usluzi internetskog bankarstva koristiti samo ona računala koja imaju instaliranu antivirusnu zaštitu.
- 7.7. Banka ne snosi odgovornost u slučaju da se Korisnik ne može koristiti Uslugom zbog okolnosti na koje Banka ne može utjecati i okolnosti navedenih u točki 15.3 do 15.12. ovih Općih uvjeta poslovanja.
- 7.8. U slučaju da prilikom korištenja usluge internetskog bankarstva adresa Banke ne započinje <https://ibps.hpb.hr/HPB.iBank.IBPS.Web/> korisnik se ne nalazi na internetskim stranicama Banke te u tom slučaju mora bez odgađanja prestati s korištenjem usluge. Korisnik je dužan prije započinjanja s korištenjem usluge internetskog bankarstva provjeriti nalazi li se na internetskim stranicama Banke.
- 7.9. Na internetskim stranicama Banke ili putem Usluga Korisniku su dostupna upozorenja i informacije o sigurnom korištenju Usluge.
- 7.10. Ako Korisnik primijeti sumnjivu aktivnost ili smatra da je netko neautorizirano pristupio njegovom Računu, dužan je to odmah prijaviti na besplatan broj telefona Banke 0800 472 472 (za pozive iz inozemstva +385 1 4890 365) ili putem elektroničke pošte na adresu hpb@hpb.hr. Nakon poduzetih radnji, Banka će Korisniku poslati pisani dopis o učinjenome, sukladno svojim internim aktima.

8. RASPOLAGANJE SREDSTVIMA

- 8.1. Korisnik raspolaže sredstvima na transakcijskim računima, otvorenim na temelju sklopljenog ugovora s Bankom, do visine raspoloživog stanja na računu.
- 8.2. Ovlašteni korisnik kojem je Korisnik po određenom računu definirao dnevni limit za provođenje platnih transakcija putem usluga izravnog bankarstva, može raspolagati sredstvima po tom računu do iznosa koji je Korisnik odredio.

9. IZVRŠAVANJE PLATNIH TRANSAKCIJA

- 9.1. Ukoliko je Korisnik ugovorio Uslugu koja mu omogućava obavljanje platnih transakcija, Banka će izvršiti nalog za plaćanje kada su ispunjeni svi uvjeti za izvršenje u skladu s Općim uvjetima poslovanja Hrvatske poštanske banke, dioničko društvo za

transakcijske račune i obavljanje platnih usluga za poslovne subjekte i ovim Općim uvjetima poslovanja, važećima u trenutku izvršenja transakcije.

- 9.2. Korisnik mora voditi računa o raspoloživom stanju na transakcijskom računu u Banci, definiranom dnevnom limitu za pojedine ili sve Ovlaštene korisnike te o popunjavanju naloga svim potrebnim elementima. Podaci o obveznim elementima koje mora sadržavati nalog za plaćanje dostupni su Korisnicima u poslovnoj mreži Banke te na internetskim stranicama Banke www.hpb.hr. Korisnik je odgovoran za točnost i potpunost podataka na nalogu za plaćanje.
- 9.3. Suglasnost za izvršenje naloga za plaćanje Korisnik odnosno Ovlašteni korisnik/korisnici daju na jedan od sljedećih načina:
 - Unosom odgovarajuće vrste koda (MAC ili MDS, koji su generirani odgovarajućim postupcima APPLI2 ili APPLI3) za odgovarajuću vrstu postupka suglasnosti, u za to predviđeno polje na ekranskom sučelju, u slučaju kada Ovlašteni korisnik kao Sredstvo za identifikaciju/autentifikaciju koristi token ili mToken.
 - Elektroničkim potpisivanjem naloga za plaćanje u slučaju kada Ovlašteni korisnik kao Sredstvo za identifikaciju/autentifikaciju koristi pametnu karticu ili USB uređaj. Ukoliko je sredstvima po računu ovlašteno raspolagati više osoba u svojstvu Ovlaštenih korisnika, Banka pridržava pravo u svrhu dodatne provjere sigurnosti zahtijevati od Korisnika naknadnu potvrdu autorizirane platne transakcije. Preporuka je da se prilikom autorizacije naloga koriste dva potpisnika.
 - Potvrđivanjem unesenih podataka unosom PIN-a ili korištenjem biometrijske autentifikacije, kod usluge mobilnog bankarstva.
 - Ostalim ugovorenim i/ili zakonski propisanim načinima za pojedine Usluge.
- 9.4. Banka za provođenje platnih transakcija provodi pouzdanu autentifikaciju koja uključuje dinamičko povezivanje elemenata naloga kako bi se minimizirali rizici pogreške ili prijevare. Elementi naloga za dinamičko povezivanje su nizovi znamenki tako odabrani da ujedno za Ovlaštenog korisnika predstavljaju najbližu tehnički ostvarivu reprezentaciju obavijesti o iznosu platne transakcije i primatelju plaćanja.
- 9.5. Platna transakcija za čije je izvršenje Korisnik/Ovlašteni korisnik dao suglasnost na jedan od načina navedenih pod 9.3 smatra se autoriziranom.
- 9.6. Korištenje personaliziranog sigurnosnog obilježja i Sredstva za identifikaciju/autentifikaciju smatra se nedvojbenim dokazom identiteta Korisnika odnosno Ovlaštenog korisnika, osim ako se ne dokaže suprotno u odgovarajućem postupku. Činjenica da je Banka zabilježila korištenje Sredstva za identifikaciju/autentifikaciju kojem se pristupa korištenjem personaliziranog sigurnosnog obilježja, dovoljna je da bi Banka smatrala da je Korisnik odnosno Ovlašteni korisnik autorizirao tu platnu transakciju.
- 9.7. Korisnik je suglasan da se u slučaju izvršenja platne transakcije koja se autorizira sigurnosnim obilježjima, unesena sigurnosna obilježja smatraju nedvojbenim dokazom njegovog identiteta i autorizacije transakcije. Korisnik stoga u cijelosti, bez ograničenja, odgovara za sve troškove, naknade i štetu nastalu kao posljedica njegova prijevarnog postupanja te ukoliko namjerno ili zbog krajnje nepažnje nije postupao sukladno odredbama svih primjenjivih Općih uvjeta.
- 9.8. Nalog za plaćanje zadan putem Usluga koja omogućuje zadavanje naloga za plaćanje, smatra se da je elektronički potpisan, autoriziran i iniciran u ime i za račun Korisnika.
- 9.9. Smatra se da je Banka zaprimila nalog za plaćanje u trenutku kada je Korisnik uredno popunjeni nalog za plaćanje potpisao i poslao na izvršenje putem Usluge. Naloga za bezgotovinsko plaćanje koji se odnose na nacionalne platne transakcije u kunama i eurima i na prekogranične platne transakcije u eurima Banka zaprima do 60

kalendarskih dana unaprijed. Takvi nalozi se evidentiraju u sustavu Banke i izvršavaju na zadani datum izvršenja. Naloge za plaćanje zadane kao instant naloge nije moguće zadati s datumom valute unaprijed, već se isti izvršavaju s tekućim datumom valute.

- 9.10. Ako je račun Korisnika blokiran i/ili raspoloživo stanje na računu nije dostatno za izvršenje plaćanja:
- Kod plaćanja koja se odnose na nacionalne platne transakcije u kunama i eurima i na prekogranične platne transakcije u eurima, Banka će zaprimljene naloge za plaćanje izvršiti u sljedećih 5 (pet) kalendarskih dana ukoliko se naknadno bude osiguralo pokriće na računu ili se račun odblokira.
 - Kod plaćanja koja se odnose na instant naloge, iste neće biti moguće zadati te će Korisnik odmah o tome dobiti informaciju unutar aplikacije internetskog ili mobilnog bankarstva.
- 9.11. Nalog za plaćanje moguće je zadati kao instant nalog pod sljedećim uvjetima:
- da je maksimalan iznos transakcije određen Pravilima HRK SCTInst platne sheme
 - da se odnosi isključivo na nacionalne platne transakcije u kunama zadane u korist računa u drugoj banci,
 - da se zadaje pojedinačno ručnim unosom,
 - da je banka primatelja sudionik HRK SCTInst platne sheme. Popis banaka sudionica HRK SCTInst platne sheme dostupan je na internetskoj stranici <https://www.hub.hr/hr/registri>.
- 9.12. Ako je Korisnik na listi neurednih poslodavaca, a zadaje instant plaćanja koja se odnose na isplatu plaće, Banka će zaprimljene naloge odbiti, a Korisnik će o odbijanju dobiti informaciju kod navedenog naloga unutar aplikacije internetskog ili mobilnog bankarstva.
- 9.13. Po primitku naloga za plaćanje, putem Usluge kojom je isti zadan, Korisniku/Ovlaštenom korisniku dostupna je informacija o uspješnom prijehu naloga. Informacija o uspješnom prijehu naloga za plaćanje ne znači da će nalog biti proveden, već samo da ga je Banka zaprimila.
- 9.14. Banka ispravne naloge za plaćanje izvršava u propisanim ili dogovorenim rokovima za pojedinu vrstu naloga za plaćanje, u skladu sa Terminskim planom izvršenja platnih transakcija za poslovne subjekte važećima u trenutku izvršenja platne transakcije dostupnim na internetskim stranicama www.hpb.hr.
- 9.15. Ako Banka zaprimi nalog za plaćanje iza vremena određenog Terminskim planom izvršenja platnih transakcija poslovnih subjekata kao kraj radnog dana, smatrat će se da je nalog za plaćanje zaprimljen sljedećeg radnog dana.
- 9.16. Korisnik je odgovoran za točnost i potpunost podataka na nalogu za plaćanje.
- 9.17. Banka nije odgovorna za neizvršeno plaćanje ili prijenos, odnosno pogrešno plaćanje ili prijenos napravljen putem Usluge koje je nastalo netočno unesenim podacima od strane Korisnika.
- 9.18. Banka će zaprimljeni nalog za plaćanje izvršavati isključivo u okviru raspoloživog stanja na računu/računima uzimajući u obzir definirane dnevne limite za pojedine ili sve Ovlaštene korisnike.
- 9.19. Banka neće izvršiti neispravno uneseni platni nalog.
- 9.20. U slučaju neizvršenja ili neurednog izvršenja autorizirane platne transakcije greškom Banke, Banka će Korisniku nadoknaditi štetu uključujući naplaćene naknade i pripadajuće kamate.
- 9.21. Korisnik je dužan pratiti ishod financijskih transakcija zaprimljenih putem Usluge.

- 9.22. Korisnik se izvješćuje o svim platnim transakcijama i stanju računa putem Izvatka, koji se dostavlja na način koji je ugovoren prilikom otvaranja transakcijskog računa.
- 9.23. Banka ne odgovara za neizvršenje ili neuredno izvršenje platnih transakcija ili izvršenje neautoriziranih platnih transakcija u sljedećim slučajevima:
- ako je izvršenje neautorizirane transakcije, neizvršenje i/ili neuredno izvršenje platne transakcije posljedica Korisnikove prijave, prijave njegovih Ovlaštenih korisnika, posljedica pogrešnog unosa podataka od strane Ovlaštenog korisnika ili ako Korisnik ili njegov Ovlašteni korisnik ne ispunjavaju obveze iz ovih Općih uvjeta poslovanja i/ili Općih uvjeta poslovanje po transakcijskim računima,
 - ako se nesporno utvrdi da je nalog za plaćanje Korisnika krivotvoren,
 - ako je izvršenje neautorizirane platne transakcije posljedica uporabe ukradenog ili izgubljenog Uređaja koji je bio zlouporabljen.
- 9.24. Korisnik je dužan bez odgađanja obavijestiti Banku o neautoriziranim platnim transakcijama, kao i o sumnji u gubitak, krađu, zlouporabu ili neovlašteno korištenje platnog instrumenta.

10. POSREDNI IDENTIFIKATOR RAČUNA

- 10.1. Korisniku je omogućeno korištenje RPIR-a u postupku iniciranja platnih transakcija, putem *on-line* bankarstva. RPIR-om upravlja FINA. Korisnik može u nacionalnom platnom prometu inicirati platnu transakciju kreditnog transfera u korist određenog primatelja plaćanja posredstvom PIR-a kao jedinstvenog identifikatora računa primatelja plaćanja.
- 10.2. U svrhu iniciranja naloga za plaćanje u korist transakcijskog računa Korisnika, svaki Ovlašteni korisnik s ovlaštenjem potpisa platnih naloga, može povezati broj transakcijskog računa Korisnika (IBAN) s jednim od PIR-ova: broj mobitela, e-mail adresa ili OIB Korisnika. Registracijom para PIR-IBAN ti podaci postaju dostupni FINA-i radi evidentiranja istog u RPIR-u te time i svim pružateljima platnih usluga koji su sudionici RPIR-a, kako bi drugi korisnici koji koriste platne usluge tih pružatelja platnih usluga i imaju podatak o Korisnikovom PIR-u, putem svojeg pružatelja platnih usluga mogli dohvatiti podatak o njegovom IBAN-u i tako kreirati nalog za plaćanje u korist tog transakcijskog računa Korisnika. Uz jedan PIR moguće je vezati samo jedan transakcijski račun. Ovlašteni korisnik povezuje IBAN transakcijskog računa i odabrani PIR (e-mail i/ili broj mobilnog telefona) unosom sigurnosnog koda odnosno davanjem suglasnosti, kada je PIR OIB.
- 10.3. U slučaju kada Korisnik više ne želi koristiti uslugu RPIR-a putem *on-line* bankarstva svaki Ovlašteni korisnik s ovlaštenjem potpisa platnih naloga, može provesti postupak deaktivacije registriranog para PIR-IBAN. Po uspješnoj deregistraciji para PIR-IBAN Banka će provesti deaktivaciju u RPIR-u.
- 10.4. Registrirani par PIR-IBAN u RPIR-u je aktivan 2 (dvije) godine. Prije isteka navedenog razdoblja, Banka će Korisnika najmanje 2 (dva) mjeseca ranije obavijestiti o isteku aktivnosti registriranog para PIR-IBAN. Ukoliko Korisnik želi dalje koristiti uslugu RPIR-a, treba ponovno potvrditi da registrirani PIR pripada predmetnom IBAN-u. Ako Korisnik ne potvrdi svoj par PIR-IBAN u tom postupku, isti će se smatrati poništenim i bit će deregistriran.
- 10.5. U slučaju prestanka Okvirnog Ugovora, registrirani par PIR-IBAN bit će deaktiviran u RPIR-u.

11. USLUGE INICIRANJA PLAĆANJA I INFORMIRANJA O RAČUNU

- 11.1. Korisnik koji ima ugovorenu uslugu izravnog bankarstva može nalog za plaćanje zadati koristeći usluge pružatelja usluge iniciranja plaćanja (PISP) i/ili se koristiti platnom uslugom informiranja o računu koju pruža ovlašteni pružatelj usluge informiranja o računu (AISP). Za zadavanje naloga iniciranja plaćanja i/ili informiranja o računu Korisnik odnosno, Ovlašteni korisnik mora dati suglasnost pružatelju usluge iniciranja plaćanja (PISP-u) i/ili pružatelju usluge informiranja o računu (AISP-u) koristeći autentifikacijske Uređaje koje koristi za usluge izravnog bankarstva Banke.
- 11.2. Banka provodi pouzdanu autentifikaciju Ovlaštenog korisnika koji putem mrežnih stranica pružatelja usluga informiranja o računu (AISP-a) daje pružatelju usluga informiranja o računu (AISP-u) suglasnost za pristup informacijama o jednom ili više transakcijskih računa otvorenih u Banci. Također, Banka provodi pouzdanu autentifikaciju Ovlaštenog korisnika koji putem mrežnih stranica pružatelja usluga iniciranja plaćanja (PISP-a) zadaje i podnosi na izvršenje nalog za plaćanje koji se treba izvršiti na teret transakcijskog računa otvorenog u Banci. Postupak autentifikacije Banka provodi nakon preusmjeravanja Ovlaštenog korisnika s mrežnih stranica pružatelja usluge informiranja o računu (AISP-a) odnosno pružatelja usluge iniciranja plaćanja (PISP-a) na mrežne stranice Banke.
- 11.3. Banka će sa zaprimljenim nalogima zadanim putem pružatelja usluge iniciranja plaćanja (PISP-a) postupati na isti način kao i s nalogima zadanim izravno od strane platitelja putem usluga izravnog bankarstva Banke uključujući Terminski plan izvršenja platnih transakcija za poslovne subjekte i Odluku Banke o naknadama u poslovanju s poslovnim subjektima, osim u slučaju objektivno opravdanih razloga.
- 11.4. Nakon primitka naloga za plaćanje od pružatelja usluge iniciranja plaćanja Banka će dati ili učiniti raspoloživim pružatelju usluge iniciranja plaćanja sve informacije o iniciranju i sve informacije u vezi s izvršenjem platne transakcije koje su joj dostupne dok se sve ostale informacije o Korisniku platnih usluga, dobivene pri pružanju usluge iniciranja plaćanja, pružaju samo primatelju plaćanja i samo uz izričitu suglasnost Korisnika platnih usluga.
- 11.5. Banka neće diskriminirati zahtjeve za davanje podataka koji su zaprimljeni od pružatelja usluga informiranja o računu, osim ako za to postoji objektivni razlog.
- 11.6. Pružatelji platne usluge iniciranja plaćanja i platne usluge informiranja o računu smiju pružati navedene usluge samo uz izričitu suglasnost Korisnika odnosno, Ovlaštenog korisnika danu pružatelju usluge iniciranja plaćanja i/ili pružatelju usluge informiranja o računu te su dužni osigurati da personalizirane sigurnosne vjerodajnice Korisnika nisu dostupne drugim osobama.
- 11.7. Platna transakcija koja se provodi putem pružatelja usluge iniciranja plaćanja (PISP-a) je autorizirana:
 - Ako je Ovlašteni korisnik dao suglasnost pružatelju usluge iniciranja plaćanja (PISP-u) da se posredstvom pružatelja usluge iniciranja plaćanja izvrši platna transakcija ili
 - Ako je Ovlašteni korisnik dao suglasnost pružatelju usluge iniciranja plaćanja (PISP-u) da se posredstvom pružatelja usluge iniciranja plaćanja izvrši niz platnih transakcija čiji je dio ta platna transakcija.
- 11.8. U slučaju iniciranja platne transakcije preko pružatelja usluge iniciranja plaćanja (PISP-a), Ovlašteni korisnik radi iniciranja platne transakcije daje izričitu suglasnost pružatelju usluge iniciranja plaćanja.
- 11.9. Korisnik i Ovlašteni korisnik može opozvati suglasnost koju je dao pružatelju usluge iniciranja plaćanja (PISP-u) za izvršenje platne transakcije ili niza platnih transakcija.

Oblik i postupak opoziva suglasnosti uređuje se ugovorom između Korisnika i pružatelja usluge iniciranja plaćanja (PISP-a).

- 11.10. U slučaju odbijanja izvršenja naloga za plaćanje iniciranih putem pružatelja usluge iniciranja plaćanja (PISP-a) Banka će o istome obavijestiti Korisnika putem pružatelja usluge iniciranja plaćanja (PISP-a).
- 11.11. Pružatelji platne usluge iniciranja plaćanja i platne usluge informiranja o računu dužni su proslijediti personalizirane sigurnosne vjerodajnice sigurnim i efikasnim kanalima.
- 11.12. Pružatelj platne usluge informiranja o računu smije pristupati samo informacijama i platnim transakcijama povezanim s računom za plaćanje za koji je Ovlašteni korisnik dao suglasnost.
- 11.13. Ako je nakon davanja suglasnosti pružatelju usluge informiranja o računu (AISP-u) i/ili pružatelju usluge iniciranja plaćanja (PISP-u) Korisnik raskinuo s Bankom uslugu internetskog ili mobilnog bankarstva, automatizmom se opoziva i suglasnost za korištenje usluge informiranja o računu i/ili iniciranja plaćanja.
- 11.14. Pružatelj platne usluge informiranja o računu dužan je upotrebljavati podatke, pristupati im te ih pohranjivati isključivo u svrhu pružanja usluga informiranja o računu koju je Ovlašteni korisnik izričito zatražio, sukladno pravilima o zaštiti podataka te ne smije zahtijevati osjetljive podatke o računima za plaćanje. Naziv Korisnika i broj računa ne smatraju se osjetljivim podacima u odnosu na uslugu informiranja o računu.
- 11.15. U slučaju neovlaštenog pristupa računu za plaćanje od strane pružatelja platne usluge informiranja o računu (AISP-a) ili iniciranja plaćanja (PISP-a) s ciljem prijevare, uključujući neovlašteno iniciranje platne transakcije, Banka smije uskratiti pristup računu za plaćanje na temelju dokazanih i objektivno opravdanih razloga o čemu će pravovremeno obavijestiti Korisnika osim ako je to u suprotnosti s objektivno opravdanim sigurnosnim razlozima ili protivno propisima. Banka će o navedenom incidentu odmah dostaviti obavijest i Hrvatskoj narodnoj banci. Obavijest Hrvatskoj narodnoj banci treba sadržavati sve relevantne pojedinosti o slučaju i razloge uskraćivanja pristupa računu za plaćanje.
- 11.16. Banka će ponovno omogućiti pristup računu za plaćanje odmah nakon što prestanu postojati razlozi za uskraćivanje pristupa.

12. OPOZIV NALOGA ZA PLAĆANJE

- 12.1. Korisnik može opozvati nalog za plaćanje u opsegu i rokovima sukladnim odredbama Općih uvjeta poslovanja Hrvatske poštanske banke, dioničko društvo, za transakcijske račune i obavljanje platnih usluga za poslovne subjekte.

13. BLOKADA I OTKAZ USLUGE

- 13.1. Nestanak (krađa ili gubitak), zlouporabu Uređaja/Usluge ili sumnju na zlouporabu Korisnik ili Ovlašteni korisnik je dužan odmah prijaviti pozivom na broj telefona 0800 472 472 (za pozive iz inozemstva +385 1 4890 365), u poslovnoj mreži Banke i zatražiti blokadu pristupa Usluzi te istu prijavu i pisano potvrditi na adresu Hrvatske poštanske banke, dioničko društvo, Direkcija digitalnog bankarstva, Jurišićeva 4, 10000 Zagreb, putem elektroničke pošte na adresu kontakt.centar@hpb.hr. Banka će jednako odgovarajuće postupiti bilo po prijavi Korisnika ili Ovlaštenog korisnika.
- 13.2. Banka će onemogućiti Korisniku pristup usluzi internetskog ili mobilnog bankarstva ako posumnja da postoji zlouporaba te će Korisniku poslati pisani dopis o učinjenome,

sukladno svojim internim aktima. Banka će onemogućiti pristup usluzi i/ili raskinuti Ugovor u slučaju da se Korisnik ne pridržava ugovornih odredbi, ovih Općih uvjeta poslovanja i ostalih Akata Banke, bez otkaznog roka. Ukoliko Korisnik procijeni da do zlouporabe nije došlo, može zatražiti deblokadu ili ponovno izdavanje Sredstva za identifikaciju/autentifikaciju u poslovnoj mreži Banke.

- 13.3. Banka će Ovlaštenom korisniku automatski onemogućiti korištenje usluge internetskog bankarstva ili mobilnog bankarstva ako prilikom prijave unese netočne korisničke podatke 3 (tri) ili 6 (šest) puta ovisno o Sredstvu za identifikaciju/autentifikaciju neovisno da li je usluzi pristupio izravno putem Usluge izravnog bankarstva Banke ili posredstvom pružatelja usluge iniciranja plaćanja (PISP), odnosno pružatelja usluge informiranja o računu (AISP). U tom slučaju pristup usluzi Korisnik ili Ovlašteni korisnik može zatražiti osobno u Regionalnom/poduzetničkom centru za gospodarstvo Banke ili pozivom na broj 0800 472 472 (iz inozemstva +385 1 4890 365).
- 13.4. Banka će Korisniku automatski onemogućiti korištenje usluge internetskog bankarstva putem pametne kartice ili USB uređaja ako prilikom prijave 5 (pet) puta unese netočne korisničke podatke. U tom slučaju pristup usluzi Korisnik ili Ovlašteni korisnik mora zatražiti osobno u Regionalnom/poduzetničkom centru za gospodarstvo Banke ili pozivom na broj 0800 472 472 (iz inozemstva +385 1 4890 365).
- 13.5. U slučaju da Korisnik ili Ovlašteni korisnik, ne obnovi pravodobno certifikat pohranjen na Uređaju dodijeljenom Ovlaštenom korisniku, Banka će tom Ovlaštenom korisniku privremeno do obnove postojećeg ili izdavanja novog certifikata onemogućiti pristup ugovorenoj Usluzi.
- 13.6. Banka nije dužna Korisnika odnosno Ovlaštenog korisnika obavijestiti o nemogućnosti korištenja pojedine Usluge u slučaju neispravnog unosa korisničkih podataka ili protoka roka važenja certifikata pohranjenih na Uređajima. Obavijest o nemogućnosti korištenja pojedine Usluge dostupna je kroz odgovarajuću Uslugu.
- 13.7. Banka je prema vlastitoj procjeni ovlaštena i bez prijave Korisnika, odnosno Ovlaštenog korisnika radi sigurnosti onemogućiti pristup pojedinim Uslugama blokadom Uređaja kojeg Korisnik ili Ovlašteni korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju u slučaju sumnje na neovlašteno korištenje ili zlouporabu Uređaja ili u slučaju sumnje da se Usluga koristi za prijevaru ili zlouporabu. Ako Banka utvrdi ili posumnja na mogućnost kršenja odredbi propisa o sprječavanju pranja novca i financiranja terorizma, međunarodnim mjerama ograničavanja, odnosno sankcija koje primjenjuju Sjedinjene Američke Države i Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske ili u druge svrhe koje su protivne prisilnim propisima, te ako Korisnik ili Ovlašteni korisnik na zahtjev Banke ne dostavi tražene podatke i dokumentaciju potrebnu za nastavak i praćenje zasnovanoga poslovnog odnosa u skladu s odredbama propisa o sprječavanju pranja novca i financiranja terorizma, međunarodnim mjerama ograničavanja, odnosno sankcije koje primjenjuju Sjedinjene Američke Države, Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske i/ili drugih prisilnih propisa.
- 13.8. Sve troškove nastale neovlaštenim korištenjem Uređaja do zaprimanja pisane prijave nestanka snosi Korisnik.
- 13.9. Korisnik snosi sav rizik za moguće neovlašteno korištenje Usluge ukoliko se ne pridržava propisanih mjera sigurnosti.
- 13.10. Na osnovi pisane prijave nestanka Sredstva za identifikaciju, Banka izdaje Korisniku i novo Sredstvo za identifikaciju/autentifikaciju s novim PIN-om te naplaćuje Korisniku naknadu za njegovo izdavanje sukladno Odluci o naknadama.
- 13.11. Korisnik ima pravo jednostrano otkazati korištenje Usluge predajom pisanog zahtjeva osobno u poslovnoj mreži Banke pri čemu se dan i vrijeme odobrenja takvog zahtjeva za zatvaranjem od strane Banke ujedno smatra i trenutkom otkaza Usluge. Otkazivanjem Usluge Korisnik je obavezan vratiti i dodijeljene mu Uređaje koje koristi

kao Sredstva za identifikaciju/autentifikaciju u Regionalnom/poduzetničkom centru za gospodarstvo Banke, osobno ili preporučenom pošiljkom na adresu Banke, osim ako je ujedno Korisnik i druge usluge za koju koristi iste Uređaje kao Sredstva za identifikaciju/autentifikaciju.

- 13.12. Sve transakcije zadane unaprijed putem Usluge, koje do datuma otkaza nisu opozvane, biti će izvršene u slučaju da je račun aktivan.
- 13.13. Banka će Korisniku onemogućiti korištenje Usluge u slučaju da Korisnik zatvori sve Račune u Banci te u slučaju prestanka postojanja Korisnika, odnosno u slučaju smrti ako se radi o Korisniku - fizičkoj osobi koja djeluje u okviru svoje gospodarske djelatnosti ili slobodnog zanimanja. Korisnik ovlašćuje Banku da bez ikakve daljnje suglasnosti i obavijesti može trošak nastao korištenjem Usluge naplatiti bez intervencije suda sa svih njegovih računa koji se vode u Banci.
- 13.14. Banka može pisanim putem jednostrano otkazati Usluge bez ostavljanja otkaznog roka i s trenutnim učinkom. Usluge se u navedenom slučaju smatraju otkazane istekom otkaznog roka od 15 (petnaest) dana, računajući od dana slanja obavijesti o otkazu Usluge Korisniku preporučenom poštom na adresu sjedišta Korisnika odnosno drugu adresu za korespondenciju koju je Korisnik prijavio Banci, neovisno o tome da li je i kada je Korisnik preuzeo otkazno pismo.
- 13.15. Banka ima pravo jednostrano otkazati Usluge bez ostavljanja otkaznog roka i s trenutnim učinkom na način opisan u prethodnoj točki:
 - Ako je Korisnik ili Ovlašteni korisnik prilikom sklapanja Usluge dao Banci neistinite ili pogrešne podatke,
 - Ako Korisnik ne ispunjava uvjete za korištenje ugovorene Usluge,
 - Ako se korisnik ili Ovlašteni korisnik ne pridržava Ugovora, Općih uvjeta poslovanja, Korisničke upute, pojedinačnih uputa za korištenje Uređaja koje koristi kao Sredstva za identifikaciju/autentifikaciju ili ostalih akata koji se primjenjuju zajedno s ovim Općim uvjetima poslovanja,
 - Ako Korisnik ili Ovlašteni korisnik postupa protivno prisilnim propisima koji se primjenjuju na pravni odnos između Banke i Korisnika, uključujući propise koji se odnose na sprječavanje pranja novca i financiranje terorizma, obavljanje platnog prometa i elektroničko poslovanje
 - Ako Banka utvrdi ili posumnja na mogućnost prijave ili zlouporabe,
 - Ako Banka utvrdi ili posumnja na mogućnost kršenja odredbi propisa o sprječavanju pranja novca i financiranja terorizma, međunarodnim mjerama ograničavanja odnosno sankcija koje primjenjuju Sjedinjene Američke Države, Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske i/ili drugih prisilnih propisa,
 - Ako Banka utvrdi da je Klijent fizička ili pravna osoba za koju su propisane sankcijske mjere ograničavanja poslovanja ili koja krši propisane sankcijske mjere
 - Ako je protiv Klijenta poduzeta istražna radnja ili postupak radi primjene međunarodnih sankcija od strane nadležnih Tijela sukladno odredbama Zakona o međunarodnim mjerama ograničavanja
 - Ako Banka utvrdi ili posumnja da u poslovnom odnosu s Klijentom postoje indikatori da Klijent svjesno zaobilazi međunarodne sankcijske mjere ograničavanja, sankcije koje primjenjuju Sjedinjene Američke Države ili Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske.
 - Ako Korisnik ili Ovlašteni korisnik na zahtjev Banke ne dostavi tražene podatke i dokumentaciju potrebnu za korištenje Usluge te nastavak i praćenje zasnovanoga ugovornog odnosa u skladu s odredbama navedenih propisa o sprječavanju pranja novca i financiranja terorizma, međunarodnim mjerama ograničavanja, sankcija koje

primjenjuju Sjedinjene Američke Države i Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske i/ili drugih prisilnih propisa.

- Ukoliko Ovlašteni korisnik ni nakon 90 (devedeset) dana od ugovaranja usluge nije preuzeo Uređaj za autorizaciju,
- ukoliko Ovlašteni korisnik ni nakon ponovljenog poziva od strane Banke nije pristupio zamjeni Uređaja za autorizaciju, a niti jedan Ovlašteni korisnik ne posjeduje Uređaj koji zadovoljava tehničke preduvjete nužne za Sredstva za identifikaciju/autentifikaciju.

13.16. S danom prestanka važenja Usluge, Banka onemogućava uporabu ugovorene usluge i obračunava sve nepodmirene obveze Korisnika sukladno Odluci o naknadama i drugim troškovima Banke za usluge u poslovanju, a Korisnik je dužan vratiti dodijeljene mu Uređaje koje je koristio kao Sredstvo za identifikaciju/autentifikaciju, osim ako je korisnik i neke druge usluge za koju koristi iste Uređaje za identifikaciju/autentifikaciju.

14. PRAVA I OBVEZE KORISNIKA

14.1. Korisnik/Ovlašteni korisnik je obvezan čuvati tajnost svih podataka vezanih uz korištenje Usluga te voditi brigu da Uređaj koji se koristi kao Sredstvo za identifikaciju/autentifikaciju ne dospije u ruke trećoj, neovlaštenoj osobi i prihvaća potpunu odgovornost za sve obveze nastale njihovim korištenjem. Ukoliko Korisnik posumnja ili utvrdi da je s PIN-om upoznata druga osoba, dužan ga je promijeniti.

14.2. Korisnik/Ovlašteni korisnik je dužan odmah i neizostavno obavijestiti Banku o gubitku neovlaštenoj upotrebi ili mogućnosti neovlaštene uporabe tajnih podataka i Uređaja na broj 0800 472 472 od 0-24 sata, 7 (sedam) dana u tjednu (iz inozemstva +385 1 4890 365) te pisanu prijavu osobno predati najbližem Regionalnom/poduzetničkom centru za gospodarstvo Banke.

14.3. U slučaju da je Korisnik u svojem Uređaju koji koristi kao Sredstvo za identifikaciju/autentifikaciju aktivirao korištenje biometrijske autentifikacije, Korisnik mora osigurati da su u svakom trenutku u Uređaju koji koristi kao Sredstvo za identifikaciju/autentifikaciju pohranjeni isključivo Korisnikovi biometrijski podaci jer će se svaka prijava putem bilo koje metode biometrijske autentifikacije smatrati provedenom od strane Korisnika kao i svi eventualno provedeni nalozi nakon takve prijave te Korisnik prihvaća potpunu odgovornost za sve tako nastale obveze.

14.4. Korisnik se obvezuje da će koristiti Usluge u skladu s Uputom za uslugu koju ima aktiviranu. Pri popunjavanju naloga, Korisnik mora voditi računa o raspoloživom iznosu sredstava na računu u Banci, uključujući dnevni limit i dozvoljeno prekoračenje. Korisnik je odgovoran za točnost svih podataka na platnim nalogima te snosi rizik unosa netočnih podataka.

14.5. U slučaju provođenja neautorizirane transakcije od strane Korisnika, ako Korisnik smatra da je žrtva kaznenog djela, Korisnik je dužan isto odmah prijaviti Banci i Ministarstvu unutarnjih poslova/Državnom odvjetništvu Republike Hrvatske.

14.6. Korisnik prihvaća da Usluge, ovisno o njihovoj vrsti uključuju prijenos podataka putem telekomunikacijskih veza (internet, e-mail, telefon, GSM uređaj) te su stoga povezani s rizicima koji su uobičajeni za korištenje navedenih načina komunikacije. Banka jamči korisniku da je komunikacija putem internetskog i mobilnog bankarstva kriptirana.

14.7. Korisnik, odnosno Ovlašteni korisnik obvezuju se:

- sve transakcije zadati u skladu s Općim uvjetima poslovanja Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanje platnih usluga za poslovne subjekte te zakonskim i podzakonskim aktima,

- prijaviti promjenu svih osobnih ili drugih podataka neophodnih za korištenje Usluge ili koji mogu utjecati na korištenje Usluge podnošenjem potpisanog Zahtjeva za promjenu podataka,
- samostalno brinuti o zatvaranju ili promjeni ovlasti u korištenju Usluge za sve Ovlaštene korisnike.

15. PRAVA I OBVEZE BANKE

- 15.1. Banka za korištenje Usluga primjenjuje tehnološko rješenje koje omogućava sigurnu vezu između Korisnika i računala Banke, a koja predstavlja standard sigurne komunikacije u komercijalnoj primjeni.
- 15.2. Banka omogućuje korisniku raspolaganje sredstvima na svim računima do visine raspoloživih sredstava na Računu.
- 15.3. Banka ne snosi odgovornost u slučaju kada je nalog odbijen u sustavu platnog prometa ili kada ga nije moguće izvršiti točno i na vrijeme, uslijed pogreške Korisnika.
- 15.4. Banka ne snosi odgovornost za neizvršenu transakciju uslijed neispravno ili netočno unesenih podataka od strane Korisnika.
- 15.5. Banka ne preuzima odgovornost za nedostupnost Usluge koje je nastupila kao posljedica tehničkih problema na računalnoj opremi ili mobilnim (višenamjenskom) uređaju, ispada ili smetnji u telekomunikacijskim vezama, nestanka struje ili kao posljedica više sile.
- 15.6. Banka može, uz prethodnu najavu, privremeno onemogućiti korištenje ugovorenih direktnih kanala u slučaju promjena opsega usluga koje su dostupne putem određenog direktnog kanala, promjena i nadogradnji u informacijskom sustavu Banke, uključujući sustav njezine informacijske sigurnosti. Obavijest o privremenoj nemogućnosti korištenja direktnog kanala zbog navedenih razloga Banka dostavlja Korisniku putem istog direktnog kanala, te objavljuje na internetskim stranicama Banke.
- 15.7. Banka ne preuzima odgovornost za štetu nastalu uslijed ne dostave podataka o promjenama osobnih ili drugih podataka neophodnih za sigurno funkcioniranje pojedine Usluge.
- 15.8. Banka ne odgovara za štetu uzrokovanu neopravdanim zahvatima Korisnika ili trećih osoba zbog kojih je došlo do nefunkcioniranja Usluga.
- 15.9. Banka ne odgovara za gubitak ili uništenje podataka na opremi koju Korisnik koristi za pristup Uslugama.
- 15.10. Banka ne odgovara za štetu nastalu prije primitaka Korisnikove prijave gubitka, krađe, neovlaštenog korištenja, zlouporabe ili sumnje na zlouporabu Uređaja, mobilnog (višenamjenskog) uređaja na kojem je instaliran mToken ili mobilno bankarstvo.
- 15.11. Banka ne odgovara za štetu koja Korisniku ili Ovlaštenom korisniku nastane zbog:
 - nepridržavanja Ugovora, Općih uvjeta poslovanja, Korisničke upute, pojedinačnih uputa za korištenje Uređaja koji se koriste kao Sredstva za identifikaciju/autentifikaciju ili ostalih akata koji se primjenjuju zajedno sa ovim Općim uvjetima poslovanja od strane Korisnika ili Ovlaštenog korisnika,
 - nepridržavanja posljednjih sigurnosnih uputa koje je Banka objavila na svojim internetskim stranicama ili koje je dostavila Korisniku ili Ovlaštenom korisniku ugovorenom Uslugom od strane Korisnika ili Ovlaštenog korisnika,
 - prijevare ili drugog protupravnog postupanja od strane trećih osoba na štetu Korisnika ili Ovlaštenog korisnika,

- prestanka važenja certifikata pohranjenog na Uređaju, dodijeljenog Korisniku odnosno Ovlaštenom korisniku,
- ako je izvršenje, neizvršenje i/ili neuredno izvršenje platne transakcije posljedica iznimnih i nepredvidivih okolnosti na koje Banka nije mogla utjecati i čije se posljedice ne bi mogle izbjeći unatoč postupanju s potrebnom pozornošću,
- ako je neizvršenje ili neuredno izvršenje Platne transakcije u odnosu na Korisnika usluga Banke koji je primatelj plaćanja, posljedica postupanja Pružatelja platnih usluga Platitelja,
- odavanja PIN-a, neke druge sigurnosne vjerodajnice ili bilo kojeg drugog povjerljivog podatka trećoj osobi kao i u slučaju prijave ili provođenja naloga putem jedne od metoda biometrijske autentifikacije ako Korisnik u svojem Uređaju koji koristi kao Sredstvo za identifikaciju/autentifikaciju kojim pristupa internetskom ili mobilnom bankarstvu ima pohranjen biometrijski podatak koji se ne odnosi na Korisnika nego na drugu osobu,
- ako je neizvršenje ili neuredno izvršenje posljedica postupanja primatelja plaćanja kod platnih transakcija iniciranih od strane primatelja plaćanja ili preko primatelja plaćanja,
- postupanja ili propusta pružatelja usluge iniciranja plaćanja (PISP-a) i/ili pružatelja usluge informiranja o računu (AISP-a),
- privremene nedostupnosti on-line usluga izravnog bankarstva i/ili djelomične ili potpune nemogućnosti korištenja internetske i/ili mobilne aplikacije za vrijeme planiranih aktivnosti održavanja sustava Banke,
- posljedica tehničkih problema na računalnoj opremi ili mobilnim (višenamjenskom) uređaju, ispada ili smetnji u telekomunikacijskim vezama, nestanka struje ili više sile,
- Banka se također oslobađa odgovornosti za produljenje roka izvršenja ili neizvršenje naloga kojemu je uzrok obveza Banke da primjenjuje i provodi mjere sukladno propisima i međunarodno prihvaćenim obvezama na području sprječavanja pranja novca i financiranja terorizma, međunarodnih mjera ograničavanja, odnosno sankcija koje primjenjuju Sjedinjene Američke Države, Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske i/ili drugih prisilnih propisa, kao i propisima koji Banci nalažu obveze u pogledu provjere informacija koje moraju biti priložene prijenosu novčanih sredstava,
- u drugim slučajevima definiranim ovim Općim uvjetima poslovanja.

15.12. Banka ne odgovara za transakcije koje su učinjene preuzimanjem kontrole nad računalom ili mobilnim (višenamjenskim) uređajem Korisnika ili Ovlaštenog korisnika ili bilo kojem obliku zloupotrebe koja je uzrokovana instaliranim zloćudnim kodom na računalu ili mobilnom (višenamjenskom) uređaju Korisnika ili Ovlaštenog korisnika.

16. ZAŠTITA OSOBNIH PODATAKA I POVJERLJIVIH INFORMACIJA

- 16.1. Načela i pravila obrade osobnih podataka regulirana su Politikom zaštite osobnih podataka Hrvatske poštanske banke, dioničko društvo, javno dostupnoj na internetskoj stranici Banke <https://www.hpb.hr/zastita-osobnih-podataka>.
- 16.2. Banka u svrhu sprječavanja zloupotreba i iz sigurnosnih razloga prilikom korištenja izravnih kanala bankarstva (internetsko i mobilno bankarstvo) prikuplja i obrađuje podatke o IP adresi Uređaja koji se koristi kao Sredstvo za identifikaciju/autentifikaciju s kojega se pristupa izravnom kanalu te podatke o Uređaju (kao što su model Uređaja,

internetski preglednik, operativni sustav, dostupni jedinstveni identifikatori Uređaja i podaci o mobilnoj mreži s koje se pristupa izravnom kanalu).

17. NAKNADE

- 17.1. Za korištenje Usluga, izdavanje Uređaja koji se koriste kao Sredstva za identifikaciju/autentifikaciju, otkaz ili blokadu korištenja Usluge Banka naplaćuje naknade sukladno važećoj Odluci o naknadama.
- 17.2. Za ponovno izdavanje mToken-a, ponovno generiranje PIN-a za pametnu karticu, USB uređaj i token, Banka ne naplaćuje naknadu sukladno Odluci o naknadama.
- 17.3. Korisnik ovlašćuje Banku da bez ikakve daljnje suglasnosti i obavijesti može teretiti njegove Račune za sve troškove nastale korištenjem Usluga uključujući naknade i druge troškove koji mogu nastati uslijed npr. tečajnih razlika i sl.
- 17.4. Naknade su objavljene na internetskoj stranici Banke www.hpb.hr. Banka će Korisniku dostaviti fakturu ili učiniti raspoloživim putem Usluge za protekli period na mjesečnoj osnovi. Korisnik je suglasan da Banka tereti njegove Račune za sve naknade nastale korištenjem Usluga.
- 17.5. U slučaju otkaza Usluge od strane Banke kao i u slučaju otkaza od strane Korisnika, neovisno o uručenju Uređaja koji se koriste kao Sredstva za identifikaciju/autentifikaciju Korisniku/Banci, Korisnik nema pravo na povrat naknada.
- 17.6. Naknade i troškovi koje Banka obračunava Korisniku za korištenje Usluga su promjenjive, a Banka će Korisnika obavijestiti o njihovim promjenama najmanje 15 (petnaest) dana prije stupanja promjena na snagu, objavom na internetskim stranicama Banke www.hpb.hr ili na drugi način koji je ugovoren s Korisnikom. Smatra se da je Korisnik suglasan s promjenama ako do dana početka primjene promijenjene visine naknade ili troškova ne obavijesti Banku pisanim putem da ih ne prihvaća. Zaprimanjem pisane obavijesti Korisnika o neprihvatanju promijenjenih naknada i troškova smatra se da je korisnik otkazao sve Ugovore.

18. NAČIN I SREDSTVA KOMUNIKACIJE

- 18.1. Korisnik je odgovoran za sve kontakt informacije koje je predao Banci, a koje su neophodne za ispravno i sigurno funkcioniranje Usluge i dužan ih je ažurirati i obavijestiti Banku o svakoj njihovoj promjeni.
- 18.2. Banka je dužna Korisniku omogućiti spremanje i/ili tiskanje podataka o provedenim Uslugama tako da bi mu bili dostupni za kasniju uporabu u primjerenom razdoblju s obzirom na namjenu podataka. Banka je dužna Korisniku omogućiti neizmijenjeno reproduciranje spremljenih podataka.
- 18.3. Banka šalje Korisniku sve informacije koje Korisnik može preuzeti u elektroničkom obliku isključivo na zahtjev Korisnika.

19. RJEŠAVANJE PRIGOVORA

- 19.1. Korisnik može podnijeti Banci pisani prigovor ukoliko smatra da se Banka ne pridržava odredbi Ugovora, ovih Općih uvjeta poslovanja te zakona kojim je uređeno pružanje platnih usluga.

- 19.2. Korisnik je na prethodno naveden način dužan obavijestiti Banku o neautoriziranoj, neizvršenoj ili neuredno izvršenoj platnoj transakciji odmah nakon saznanja, a najkasnije u roku od 8 (osam) dana od dana terećenja njegovog računa.
- 19.3. Banka u poslovnim prostorima u kojima obavlja poslovanje s fizičkim i pravnim osobama i na internetskoj stranici Banke osigurava obavijesti o mogućnosti i načinu podnošenja prigovora te postupku rješavanja prigovora. Načela i pravila upravljanja prigovorima koje Korisnici/podnositelji prigovora podnose Banci uređena su Politikom upravljanja prigovorima koja je javno objavljena i dostupna na internetskim stranicama Banke www.hpb.hr.
- 19.4. Korisnik može podnijeti Banci prigovor na jedan od navedenih načina:
- osobno u poslovnoj mreži Banke (Regionalnom centru za stanovništvo) ili Regionalnom/poduzetničkom centru za gospodarstvo,
 - e-mailom: kvalitetausluge@hpb.hr i hpb@hpb.hr,
 - putem internetske stranice: www.hpb.hr, popunjavanjem forme za podnošenje prigovora,
 - poštom: Hrvatska poštanska banka, dioničko društvo, Ured za upravljanje kvalitetom usluge, Jurišićeva 4, 10 000 Zagreb
 - telefaksom: 01/4707 987.
- 19.5. Prigovore koji se odnose na usluge koje pružaju usluge iniciranja plaćanja (PISP) i usluge informiranja o računu (AISP), 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 vezanim za autorizaciju i izvršenje platnih transakcija iniciranih putem pružatelja usluge iniciranja plaćanja (PISP-a), isti se upućuju Banci na isti način kao i kad je riječ o prigovorima vezanim za platne transakcije inicirane korištenjem kanala izravnog bankarstva Banke.
- 19.6. Prigovori koji se odnose na obradu osobnih podataka podnose se službeniku za zaštitu osobnih podataka na e-mail: dpo@hpb.hr i rješavaju se na način uređen Politikom zaštite osobnih podataka Banke objavljenom na internetskoj stranici Banke www.hpb.hr.
- 19.7. Prigovor Banci treba sadržavati slijedeće podatke:
- naziv, adresu i OIB Korisnika,
 - detaljan opis događaja ili okolnosti koje su izazvale nezadovoljstvo, a koje su predmet prigovora te dokaz osnovanosti prigovora.
- 19.8. Banka će odgovoriti Korisniku najkasnije u zakonom propisanom roku od 10 (deset) dana od dana zaprimanja prigovora. Iznimno, u slučajevima kada Banka ne može dati odgovor u roku od 10 (deset) dana od dana zaprimanja, Banka će unutar naprijed navedenog roka dostaviti privremeni odgovor u kojem će obavijestiti Korisnika /podnositelja prigovora o razlozima odgode i kašnjenja odgovora te roku do kojeg će primiti konačan odgovor koji ne može biti duži od 35 (trideset pet) dana od dana zaprimanja prigovora.
- 19.9. Ukoliko Korisnik odnosno Ovlašteni korisnik i/ili Korisnik kao podnositelj prigovora smatra da Banka postupa protivno odredbama Zakona o platnom prometu koje se odnose na obveze informiranja ili na prava i obveze u vezi s pružanjem i korištenjem platnih usluga, Korisnik odnosno Ovlaštena osoba i/ili Korisnik koji je podnio prigovor može uputiti pritužbu protiv Banke Hrvatskoj narodnoj banci.
- 19.10. U svrhu rješavanja prigovora Korisnik/Ovlašteni korisnik je dužan priložiti dokumentaciju koja se tiče transakcije na koju se prigovor odnosi.

20. ZAVRŠNE ODREDBE

- 20.1. Ovi Opći uvjeti poslovanja su objavljeni na internetskoj stranici Banke www.hpb.hr.
- 20.2. Izmjene ovih Općih uvjeta poslovanja Banka će učiniti dostupnima na internetskoj stranici Banke www.hpb.hr najmanje 15 (petnaest) dana prije predloženog datuma početka primjene izmjena. Ako Korisnik nije suglasan s izmjenama, može bez otkaznog roka i bez naknade otkazati korištenje Usluge. Uslugu mora otkazati pisanim putem, najkasnije do predloženog datuma početka primjene izmjena ovih Općih uvjeta poslovanja.
- 20.3. Ovi Opći uvjeti poslovanja sastavljeni su na hrvatskom jeziku i komunikacija za vrijeme njegovog trajanja odvija se na hrvatskom jeziku.
- 20.4. Smatrat će se da je Korisnik prihvatio navedene izmjene ako do predloženog datuma početka primjene izmjena ovih Općih uvjeta poslovanja ne obavijesti Banku da ih ne prihvaća.
- 20.5. Na Ugovor i međusobna prava i obveze Korisnika i Banke primjenjuje se pravo Republike Hrvatske, a za sve sporove koje proizlaze iz Ugovora ili su u vezi s njim ugovara se nadležnost hrvatskih sudova te mjesna nadležnost suda u Zagrebu.
- 20.6. Danom stupanja na snagu ovih Općih uvjeta poslovanja prestaju važiti Opći uvjeti Hrvatske poštanske banke, dioničko društvo za korištenje usluga izravnog bankarstva za poslovne subjekte, od dana 15. prosinca 2020.godine.
- 20.7. Ovi Opći uvjeti poslovanja stupaju na snagu s danom donošenja, a primjenjuju se od 24. ožujka 2021. godine



HRVATSKA POŠTANSKA BANKA

Hrvatska poštanska banka, dioničko društvo
Jurišićeva 4, HR-10000 Zagreb

Na temelju članka 13. Statuta Hrvatske poštanske banke, dioničko društvo dana 09. ožujka 2021. godine Uprava Banke donosi sljedeće

OPĆE UVJETE POSLOVANJA HRVATSKE POŠTANSKE BANKE, DIONIČKO DRUŠTVO ZA KORIŠTENJE USLUGA IZRAVNOG BANKARSTVA ZA POSLOVNE SUBJEKTE

Izdavatelj ovih Općih uvjeta poslovanja Hrvatske poštanske banke, dioničko društvo za korištenje usluga izravnog bankarstva za poslovne subjekte (u daljnjem tekstu: Opći uvjeti poslovanja) je Hrvatska poštanska banka, dioničko društvo, Jurišićeva 4, 10000 Zagreb, Republika Hrvatska (u daljnjem tekstu: Banka), SWIFT oznaka: HPBZHR2X, upisana u sudski registar kod Trgovačkog suda u Zagrebu pod brojem MBS: 080010698, OIB: 87939104217, hpb@hpb.hr.

Tijelo nadležno za nadzor: Hrvatska narodna banka.

Banka ima odobrenje za rad Hrvatske narodne banke te se nalazi na popisu kreditnih institucija objavljenom na internetskoj stranici Hrvatske narodne banke www.hnb.hr.

1. PODRUČJE PRIMJENE

- 1.1. Ovi Opći uvjeti poslovanja reguliraju prava, obveze, način i uvjete korištenja usluga izravnog bankarstva od strane poslovnog subjekta (u daljnjem tekstu: Korisnik) i fizičke osobe ovlaštene za korištenje usluga izravnog bankarstva u ime i za račun Korisnika (u daljnjem tekstu: Ovlašteni Korisnik).
- 1.2. Ovi Opći uvjeti poslovanja primjenjuju se zajedno s Općim uvjetima poslovanja Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanje platnih usluga za poslovne subjekte, Odlukom o naknadama i drugim troškovima Hrvatske poštanske banke, dioničko društvo, za usluge u poslovanju (u daljnjem tekstu: Odluka o naknadama), pojedinačnim korisničkim Uputama za usluge izravnog bankarstva (u daljnjem tekstu: Uputa) te njihovim izmjenama i dopunama donesenima za vrijeme trajanja ugovornog odnosa između Banke i Korisnika. U odnosu na Opće uvjete poslovanja Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanje platnih usluga za poslovne subjekte, ovi Opći uvjeti poslovanja smatraju se posebnima i imaju prednost u primjeni. Oni reguliraju prava i obveze korisnika Usluga izravnog bankarstva te prava i obveze Banke u pružanju Usluga izravnog bankarstva. Oni zajedno s Pristupnicom čine ugovor (u daljnjem tekstu: Ugovor), a Ugovor, Opći uvjeti poslovanja Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanje platnih usluga za poslovne subjekte, Ugovor o otvaranju i vođenju transakcijskog računa i obavljanju platnih usluga i Odluka o naknadama sastavni su dijelovi Okvirnog ugovora o platnim uslugama.

Ovi Opći uvjeti poslovanja zajedno s Općim uvjetima poslovanja Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanje platnih usluga za poslovne subjekte koji se primjenjuju na ugovorni odnos između Banke i Korisnika dostupni su na internetskoj stranici Banke www.hpb.hr.

2. UVODNE ODREDBE

Pojedini pojmovi korišteni u ovim Općim uvjetima poslovanja imaju sljedeće značenje:

- 2.1. **Administrator ovlaštenja** – Ovlašteni korisnik kojega je Korisnik ovlastio da u ime i za račun Korisnika dodjeljuje, ukida i mijenja ovlaštenja za sebe i ostale Ovlaštene korisnike. Administrator ovlaštenja dodjeljuje, ukida ili mijenja dozvole uvida za pojedine funkcionalnosti dostupne u on-line bankarstvu kao i ovlaštenja po računima. Administratoru ovlaštenja omogućeno je upravljanje ovlastima odnosno dozvolama uvida za sljedeće funkcionalnosti: Poslovne račune, Izvode, Kredite, Depozite, Vrijednosne papire, Akreditive, Garancije, Kartice, HPB Invest, Pain 002 i Camt 053.
- 2.2. **Akti Banke** - u smislu odredbi ovih Općih uvjeta poslovanja jesu svi dokumenti i odluke što ih po propisanoj proceduri donose ovlaštena tijela Banke i koja su Korisniku dostupna putem pojedinih distributivnih kanala, a uređuju prava, ovlasti i obveze Korisnika i svih ostalih osoba koje preuzimaju prava i obveze prema Banci kao i Banke same (primjerice: Posebni opći uvjeti, Odluke o naknadama i tome sl.).
- 2.3. **Aktivacijski kod** - osobni identifikacijski brojevi koje Banka dodjeljuje Ovlaštenom korisniku, a koristi se u procesu registracije Ovlaštenog korisnika za korištenje pojedine usluge izravnog bankarstva ili aktiviranja pojedinih Sredstava za identifikaciju/autentifikaciju.
- 2.4. **Autorizacija** - suglasnost Korisnika odnosno Krajnjeg korisnika za izvršenje naloga za plaćanje.
- 2.5. **Banka** - Hrvatska poštanska banka, dioničko društvo, Jurišićeva 4, 10000 Zagreb, Republika Hrvatska, kao izdavatelj ovih Općih uvjeta poslovanja.
- 2.6. **Biometrijska autentifikacija** – autentifikacija utemeljena na biometrijskom svojstvu Ovlaštenog korisnika pohranjenom u Uređaju koji Ovlašteni korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju za usluge izravnog bankarstva koja se može koristiti u kombinaciji sa Sredstvom za identifikaciju/autentifikaciju koje je Banka dodijelila Korisniku (primjerice tokenom, mTokenom ili drugim Sredstvom koje Banka stavi Korisniku na raspolaganje). Metode biometrijske autentifikacije mogu biti metoda autentifikacije otiskom prsta kojeg je Korisnik pohranio u uređaju koji Korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju i/ili pri provođenju platne transakcije te metoda autentifikacija prepoznavanjem lica čija su svojstva pohranjena u uređaju koji Korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju i/ili pri provođenju platne transakcije.
- 2.7. **Certifikat** - potvrda u elektroničkom obliku, izdana od strane Banke, s ograničenim rokom važenja, pohranjena na pametnoj kartici ili USB uređaju, koja povezuje podatke za verifikaciju elektroničkog potpisa s Ovlaštenim korisnikom kojem je Banka dodijelila predmetnu pametnu karticu ili USB uređaj te potvrđuje njegov identitet.
- 2.8. **Dnevni limit** - predstavlja sigurnosni mehanizam koji omogućuje određivanje maksimalnog iznosa sredstava, unutar raspoloživog stanja na računu, kojim Ovlašteni korisnik može raspolagati u jednom danu putem usluga izravnog bankarstva.
- 2.9. **Inicijalni PIN** - osobni identifikacijski broj kojeg Banka dodjeljuje Ovlaštenom korisniku koji kao Sredstvo za identifikaciju/autentifikaciju koristi token ili drugo Sredstvo za identifikaciju/autentifikaciju za čije je inicijalno korištenje potreban unos inicijalnog PIN-a, poznat je isključivo Ovlaštenom korisniku i služi za njegovu inicijalnu autentifikaciju.

- 2.10. **Instant kreditni transfer** (u daljnjem tekstu: instant nalog) – platna usluga kojom se platna transakcija izvršava po nalogu platitelja na teret njegovog transakcijskog računa, a sredstva su raspoloživa primatelju na transakcijskom računu druge banke u zemlji u roku od nekoliko sekundi (do 10 (deset) sekundi). Usluga je dostupna 24 (dvadesetčetiri) sata dnevno sve kalendarske dane u godini i primjenjuje se isključivo kod izvršenja nacionalnih platnih transakcija u kunama zadanih u korist računa u drugim bankama.
- 2.11. **Personalizirane sigurnosne vjerodajnice** - personalizirana obilježja u obliku niza brojeva ili znakova koja Banka daje Korisniku ili Ovlaštenom korisniku u svrhu aktivacije usluga ili uređaja ili lozinki i kodova koji su poznati samo Korisniku ili Ovlaštenom korisniku. Personalizirane sigurnosne vjerodajnice obuhvaćaju, ali nisu ograničena na, identifikacijski kod, aktivacijski kod, korisnički broj, personaliziranu sigurnosnu riječ, PIN-ove koje je Ovlašteni korisnik odredio za korištenje mobilne aplikacije, tokena, mTokena, lozinku za pristup kvalificiranom elektroničkom certifikatu te sve kodove koje generiraju identifikacijski/autentifikacijski Uređaji.
- 2.12. **Jednokratna lozinka (OTP – One time password)** – je kriptografski kod generiran pomoću tokena/mTokena, primjenjiv samo jedanput i s ograničenim vremenom valjanosti, koji se može koristiti u postupku autentifikacije ili potvrde drugih radnji koje Ovlašteni korisnik inicira putem usluge internetskog/mobilnog bankarstva. Postupak generiranja OTP koda Banka naziva još i APPLI1, a kod se generira odabirom odgovarajuće funkcije tokena/mTokena koja će generirati navedenu vrstu koda uz primjenu PIN-a.
- 2.13. **Kanali izravnog bankarstva** - sredstva daljinske komunikacije koja omogućavaju korištenje bankovnih i drugih financijskih i nefinancijskih usluga korištenjem elektroničkih načina komuniciranja, bez istodobne fizičke nazočnosti Ovlaštenog korisnika i zaposlenika Banke na istom mjestu.
- 2.14. **Korisnik** - Poslovni subjekt kojem je Banka odobrila korištenje jedne ili više Usluga izravnog bankarstva. Korisnikom može postati Poslovni subjekt koji u Banci ima otvoren Račun.
- 2.15. **Kreditni transfer** – platna usluga kojom se transakcijski račun primatelja plaćanja odobrava za platnu transakciju ili niz platnih transakcija na teret platiteljevog transakcijskog računa od strane pružatelja platne usluge kod kojeg se vodi platiteljev transakcijski račun, na osnovi naloga za plaćanje kojeg zadaje platitelj.
- 2.16. **MAC (Message authentication code)** - je kriptografski kod generiran pomoću tokena/mTokena koji se može koristiti u postupku autorizacije određenih vrsta platnih transakcija ili potvrde drugih radnji koje Ovlašteni korisnik inicira putem usluge internetskog/mobilnog bankarstva. Postupak generiranja MAC koda Banka naziva još i APPLI2, a kod se generira odabirom odgovarajuće funkcije tokena/mTokena koja će generirati navedenu vrstu koda uz primjenu niza znamenki koje su korisniku pri korištenju usluge internetskog/mobilnog bankarstva prikazane kao podatak za unos ili upit za potvrdom. Generirani kod predstavlja kod za potvrdu koji Ovlašteni korisnik može koristiti u postupku autorizacije platne transakcije ili potvrde drugih radnji koje je inicirao putem usluge internetskog/mobilnog bankarstva.
- 2.17. **MDS (Multiple Data Signature)** - je kriptografski kod generiran pomoću tokena/mTokena koji se može koristiti u postupku autorizacije platne transakcije ili potvrde drugih radnji koje Ovlašteni korisnik inicira putem usluge internetskog/mobilnog bankarstva. Postupak generiranja MDS koda Banka naziva još i APPLI3, a kod se generira odabirom odgovarajuće funkcije tokena/mTokena koja će generirati navedenu vrstu koda uz primjenu dvaju nizova znamenki koje su korisniku pri korištenju usluge internetskog/mobilnog bankarstva prikazane kao podaci za unos ili kao obavijest koju je potrebno potvrditi. Nizovi znamenki za unos su tako odabrani da ujedno za Ovlaštenog korisnika predstavljaju najbližu tehnički ostvarivu reprezentaciju obavijesti

o iznosu platne transakcije i primatelju plaćanja. Generirani kod predstavlja kod za potvrdu koju Ovlašteni korisnik može koristiti u postupku autorizacije platne transakcije ili potvrde drugih radnji koje je inicirao putem usluge internetskog/mobilnog bankarstva.

- 2.18. **Nalozi za plaćanje** – instrukcija platitelja ili primatelja plaćanja Banci kojom se traži izvršenje platne transakcije.
- 2.19. **Okvirni ugovor** - Okvirni ugovor o platnim uslugama čine ovi Opći uvjeti poslovanja zajedno s Pristupnicom, Opći uvjeti poslovanja Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanju platnih usluga za poslovne subjekte, Ugovor o otvaranju i vođenju transakcijskog računa i Odluka o naknadama i drugim troškovima Hrvatske poštanske banke d.d. za usluge u poslovanju, Odluka o visini kamatnih stopa i Terminski plan izvršenja platnih transakcija poslovnih subjekata.
- 2.20. **Ovlašteni korisnik** - fizička osoba koja je ovlaštena od strane Korisnika i u njegovo ime i za njegov račun koristiti uslugu izravnog bankarstva ovisno o dobivenim ovlaštenjima. Vrste ovlaštenja i moguće kombinacije vrsta ovlaštenja koje Korisnik može dodijeliti Ovlaštenim korisnicima navedene su u obrascima za ugovaranje i/ili korištenje usluga izravnog bankarstva. Ovlaštenom korisniku moguće je dodijeliti sljedeća ovlaštenja po računima za usluge internetskog i mobilnog bankarstva: pregled, unos, izvršavanje ili samostalno potpisivanje platnih naloga.
- 2.21. **Ovlašteni korisnik s pravom potpisivanja platnih naloga** - ovlašten je za potpisivanje platnih naloga te na izvršavanje registracije i deregistracije PIR-a vezanog uz broj transakcijskog računa za kojeg je ovlašten.
- 2.22. **Pametna kartica/USB uređaj** - certificirani kriptografski uređaj za sigurnu pohranu certifikata koji služi za identifikaciju Ovlaštenog korisnika za pojedinog Korisnika, pristup i korištenje usluge internetskog bankarstva ovisno o danim ovlaštenjima.
- 2.23. **PIN** - osobni tajni identifikacijski broj Ovlaštenog korisnika, koji je poznat isključivo Ovlaštenom korisniku te se koristi za identifikaciju Ovlaštenog korisnika za pristup tokenu, mTokenu, mobilnom bankarstvu, pametnoj kartici, USB uređaju ili drugom Sredstvu za identifikaciju/autentifikaciju koje se može koristiti nakon ispravnog unosa PIN-a.
- 2.24. **Posredni identifikator računa** - dalje u tekstu: PIR) – broj mobitela, e mail adresa ili osobni identifikacijski broj (OIB) Korisnika koji Ovlašteni korisnik s pravom potpisa platnih naloga povezuje s IBAN-om transakcijskog računa Korisnika, koji Banka, temeljem suglasnosti Ovlaštenog korisnika, dostavlja u RPIR, u svrhu iniciranja platnih transakcija u korist transakcijskog računa. PIR jedinstveno identificira predmetni IBAN sve dok je u RPIR-u uz njega povezan.
- 2.25. **Podnositelj Pristupnice** - Korisnik koji predajom potpisane Pristupnice od Banke traži mogućnost korištenja usluga izravnog bankarstva za poslovne subjekte.
- 2.26. **Poslovni subjekt** - pravna osoba, tijelo državne vlasti, tijelo državne uprave, jedinica lokalne ili područne samouprave te njihova tijela, udruga i društvo (sportsko, kulturno, dobrotvorno i sl.) te fizička osoba (nepotrošač) koja djeluje unutar područja svoje registrirane gospodarske djelatnosti ili slobodnog zanimanja i s Bankom zaključuje Okvirni ugovor.
- 2.27. **Potpisnik** - Ovlašteni korisnik koji posjeduje Uređaj koji koristi kao Sredstvo za identifikaciju/autentifikaciju kojim se potpisuju i autoriziraju nalozi za plaćanje u ime i za račun Korisnika. Potpisnik može biti lijevi, desni ili samostalni, a ovlaštenje mu je moguće dodijeliti po pojedinom računu. Ovlašteni korisnici s ovlaštenjem za potpisivanje platnih naloga mogu obavljati registraciju i deregistraciju određenog posrednog identifikatora računa (PIR) uz određeni broj transakcijskog računa (IBAN) u Registar posrednih identifikatora računa (RPIR).

- 2.28. **Pouzdana autentifikacija** – jest autentifikacija na osnovi uporabe dvaju ili više elemenata koji pripadaju u kategoriju znanja (nešto što samo korisnik zna), posjedovanje (nešto što korisnik posjeduje) i svojstvenosti (nešto što korisnik jest) koji su međusobno neovisni, što znači da povreda jednog ne umanjuje pouzdanost drugih i koja je osmišljena na takav način da štiti povjerljivost autentifikacijskih podataka, pri čemu najmanje dva od navedenih elemenata moraju pripadati različitoj kategoriji.
- 2.29. **Pristupnica** – pisani zahtjev za korištenje usluga izravnog bankarstva za poslovne subjekte.
- 2.30. **Provjereni primatelj** – primatelj kreditnog transfera za kojeg je dopušteno ne primjenjivati pouzdanu autentifikaciju prilikom autorizacije transakcije. Korisnik on-line bankarstva sam stvara i mijenja popis provjerenih primatelja. Dodavanje na popis je moguće prilikom prvog iniciranja plaćanja prema određenom primatelju, a dodavanje ili uklanjanje određenog primatelja s popisa je moguće unutar odgovarajućeg izbornika aplikacije. Svako dodavanje ili mijenjanje liste provjerenih pouzdanih primatelja Korisnik mora potvrditi pouzdanom autentifikacijom.
- 2.31. **Pružatelj usluge informiranja o računu (AISP - Account Information Service Provider)** je pružatelj platnih usluga koji obavlja djelatnost informiranja o računu.
- 2.32. **Pružatelj usluge iniciranja plaćanja (PISP - Payment Initiation Service Provider)** je pružatelj platnih usluga koji obavlja djelatnost iniciranja plaćanja.
- 2.33. **Račun** - svaki transakcijski račun Korisnika otvoren u Banci, a koji se koristi za izvršavanje platnih transakcija u domaćoj i stranoj valuti kao i u druge svrhe vezane uz platno-prometne usluge.
- 2.34. **Raspoloživo stanje na transakcijskom računu** - iznos pozitivnog stanja u valuti terećenja uvećan za neiskorišteni iznos odobrenog prekoračenja po računu u valuti terećenja umanjeno za ranije predane naloge za plaćanje u valuti terećenja koji čekaju izvršenje na zadani datum ili neproknjižena sredstva (npr. nalozi poslani u klirinške sustave, kartične transakcije)
- 2.35. **Registar posrednih identifikatora računa (dalje u tekstu: RPIR)** - je sustav koji sudionicima RPIR-a omogućuje povezivanje određenih posrednih identifikatora računa korisnika platnih usluga u platnoj transakciji s njihovim IBAN-om u svrhu korištenja jedne ili više platnih usluga bez potrebe da korisnici platnih usluga prethodno znaju informaciju o IBAN-u drugog korisnika platnih usluga, odnosno IBAN se automatski popunjava podacima iz RPIR-a. Nacionalnim registrom upravlja Financijska agencija (FINA) u koji se, putem Banke kao sudionika RPIR-a, registrira od strane Ovlaštenog korisnika s ovlaštenjem potpisivanja platnih naloga, određeni PIR uz određeni broj transakcijskog računa (IBAN). RPIR potom omogućava drugom korisniku platne usluge čiji je pružatelj platne usluge također sudionik RPIR-a, da prilikom iniciranja platne transakcije dohvati iz RPIR-a podatak o broju transakcijskog računa primatelja plaćanja (IBAN) putem podatka primatelja plaćanja koji je registriran u RPIR-u kao PIR povezan uz određeni transakcijski račun. Banka obavlja registraciju IBAN-a vezanog uz PIR kako je definirao Ovlašteni korisnik s ovlaštenjem potpisivanja platnih naloga, odjavu PIR-a pridruženog uz IBAN iz RPIR-a, dohvat podataka iz RPIR-a za potrebe iniciranja platne transakcije, dohvat deaktiviranih parova PIR-IBAN od drugog korisnika RPIR-a te pretraživanje podataka svojih korisnika platnih usluga. RPIR je usklađen sa standardima SPL-a (engl. Standardised Proxy Lookup) – jedinstvenom europskom bazom koju razvija Europsko platno vijeće (engl. European Payments Council) u svrhu interoperabilnosti na razini EU-a, odnosno mogućnost da se korištenjem baze mogu zadavati plaćanja u korist bilo kojeg primatelja plaćanja na području Europske unije. Na zahtjev Korisnika registrirani par PIR-IBAN bit će dostupan pružateljima platnih usluga unutar SEPA područja kroz SPL bazu nakon što Europsko platno vijeće dovrši razvoj funkcionalnosti.

- 2.36. **Sankcije (međunarodne mjere ograničavanja)** - su instrument diplomatske ili gospodarske prirode kojima se nastoji promijeniti aktivnosti ili politike poput kršenja međunarodnog prava ili ljudskih prava, ili politike koje ne poštuju vladavinu prava ili demokratska načela i utječu na poslovanje financijskih institucija i njihovih klijenata postavljanjem ograničenja, i kontrolom kretanja roba, usluga i sredstava obustavom izvršenja usluga i kontrolom kretanja roba, usluga i sredstava.
- Sankcije su zabrane nametnute organizacijama, fizičkim osobama i njihovim tvrtkama, kao i proizvodi i usluge navedeni u propisima Vijeća Europe, rezolucijama Vijeća sigurnosti, Ujedinjenih naroda, i u slučaju sankcija SAD-a, propisa OFAC-a kao i bilo koje sankcije koje nalažu tijela vlasti određenih zemalja i ograničavajuće odredbe s međunarodnom ili regionalnom snagom koje izdaju tijela vlasti drugih zemalja.
- Popis najvažnijih institucija koje propisuju sankcijske mjere uključuje: Ujedinjene narode, Europsku uniju, Ured za nadzor strane imovine Ministarstva financija SAD-a (Office of Foreign Assets Control – OFAC), Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske. Sankcije koje primjenjuju Sjedinjene Američke Države su sankcije, zabrane i mjere ograničavanja koje je izdao predsjednik Sjedinjenih Američkih Država i objavio Ured za kontrolu strane imovine američkog Ministarstva financija (OFAC). Te sankcije se odnose na sve fizičke i pravne osobe koje imaju američki status, kao i financijske transakcije denominirane u USD.
- 2.37. **Sigurnosna riječ** - Riječ koju određuje Ovlašteni korisnik prema vlastitom odabiru prilikom popunjavanja Pristupnice, a koja služi za identifikaciju Korisnika prilikom deblokade tokena.
- 2.38. **SMS usluga** - usluga koja omogućuje Korisnicima da putem mobilnog uređaja od Banke primaju poruke s informacijama.
- 2.39. **Softver banke** - aplikativno rješenje koje se koristi za pružanje Usluga izravnog bankarstva, poput mobilne aplikacije ili web aplikacije. Isti se instalira na računalo Korisnika/Ovlaštenog korisnika ili mobilni (višenamjenski) uređaj.
- 2.40. **Sredstva za identifikaciju/autentifikaciju** - tehničko sredstvo i/ili aplikativno rješenje koje omogućava identifikaciju Korisnika prilikom korištenja pojedine usluge izravnog bankarstva i autorizaciju naloga za plaćanje i drugih vrsta naloga koje je Korisnik zadao korištenjem pojedine usluge izravnog bankarstva. Sredstvo za identifikaciju/autentifikaciju može biti različito, ovisno o usluzi izravnog bankarstva (na primjer, token, mToken, pametna kartica, USB uređaj i druga Sredstva za identifikaciju/autentifikaciju koje Banka stavi korisniku, odnosno Ovlaštenom korisniku na raspolaganje).
- 2.41. **Šifra za otključavanje** - je alfanumerički set znakova koji se koristi za otključavanje pametne kartice ili USB uređaja u slučaju kad se isti zaključaju usred uzastopnog unosa pogrešnog PIN-a.
- 2.42. **Token/mToken** - kriptografski uređaj/aplikacija, inicijaliziran pridruženim ključem i zaštićen lozinkom koji putem kriptografskih algoritama služi za identifikaciju Ovlaštenog korisnika za pojedinog Korisnika (kontrola pristupa), ovisno o danim ovlaštenjima, autorizaciju transakcija i potpisivanje naloga, generira jednokratne lozinke ograničenog trajanja koje identificiraju Korisnika usluge izravnog bankarstva i/ili drugih usluga čije korištenje Banka omogući Korisniku.
- 2.43. **Unositelj** - Ovlašteni korisnik koji posjeduje Uređaj koji koristi kao Sredstvo za identifikaciju/autentifikaciju kojim se unose nalozi za plaćanje, a ovlaštenje mu je moguće dodijeliti po pojedinom računu.
- 2.44. **Uređaj** - predstavlja token, pametnu karticu, USB uređaj, mToken ili sličan kriptografski uređaj na kojem se generiraju korisnički kriptografski ključevi i na kojem se pohranjuju certifikati koji identificiraju Korisnika. Uređaji u vlasništvu Banke su token, pametna kartica, USB uređaj, mToken ili sličan kriptografski uređaj kojim se potpisuju i

autoriziraju nalozi za plaćanje u ime i za račun Korisnika. Uređaji koji nisu u vlasništvu Banke su računalo i mobilni uređaj (višenamjenski uređaj) na koji se instalira aplikacija.

- 2.45. **Usluga informiranja o transakcijskom računu** - online elektronička usluga kojom se pružaju konsolidirane informacije o jednom ili više transakcijskih računa za plaćanje koje korisnik platnih usluga ima kod drugog pružatelja platnih usluga ili kod više pružatelja platnih usluga.
- 2.46. **Usluga iniciranja plaćanja** - usluga zadavanja naloga za plaćanje na zahtjev korisnika platnih usluga s njegova transakcijskog računa koji vodi drugi pružatelj platnih usluga.
- 2.47. **Usluge izravnog bankarstva** - skup usluga Banke koji čine usluga internetskog i mobilnog bankarstva Banke i SMS usluga (u daljnjem tekstu: Usluge).
- 2.48. **Politika zaštite osobnih podataka** - temeljni akt koji opisuje svrhu i ciljeve prikupljanja, obrade i upravljanja osobnim podacima, a osigurava adekvatnu razinu zaštite podataka u skladu s Općom uredbom o zaštiti podataka i svim ostalim vezanim zakonskim propisima.

Svi pojmovi koji nisu posebno definirani ovim Općim uvjetima poslovanja imaju značenje kako je to utvrđeno Općim uvjetima Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanje platnih usluga za poslovne subjekte, a ukoliko nisu definirani niti njima, imaju značenje kako je to utvrđeno Zakonom o platnom prometu

3. OPSEG USLUGE

- 3.1. Informacije o ponudi Usluga dostupne su u poslovnoj mreži i na internetskoj stranici Banke (www.hpb.hr).
- 3.2. Za svaku ugovorenu Uslugu, Banka će omogućiti Korisniku uvid u informacije i obavljanje transakcija u opsegu i na način naveden u Ugovoru i/ili Uputi za korištenje Usluga za poslovne subjekte. Uputa je dostupna na internetskoj stranici Banke www.hpb.hr. Banka ima pravo izmjene Uputa, a Korisnik je dužan po istima postupati.
- 3.3. Banka pridržava pravo izmjene opsega i sadržaja Usluga, Uputa za korištenje usluge i Uputa za korištenje Uređaja koji se koristi kao Sredstvo za identifikaciju/autentifikaciju. Sve izmjene bit će Korisniku dostupne na prikladan način u poslovnoj mreži Banke i na internetskim stranicama Banke www.hpb.hr prije stupanja izmjena Uputa na snagu. Smatrat će se da je Korisnik prihvatio izmjene usluga ukoliko ugovorenu Uslugu ne otkáže pisanim putem do dana stupanja izmjena na snagu. Zaprimanjem pisane obavijesti Korisnika o neprihvatanju izmjena Usluga koje se mogu obavljati korištenjem ugovorene Usluge smatra se da je Korisnik otkazao korištenje Usluge. Korisnik nema pravo zahtijevati naknadu štete u slučaju izmjene opsega i sadržaja Usluge.
- 3.4. Korištenjem internetskog i mobilnog bankarstva omogućuju se sljedeće usluge:
 - izvršenje i pregled platnih transakcija;
 - pregled stanja, prometa po računima i izvoda;
 - razmjena obavijesti između Korisnika i Banke;
 - registracija i deregistracija PIR-a vezanog uz transakcijski račun u RPIR-u;
 - obavljanje ostalih usluga
- 3.5. Banka je ovlaštena uvoditi nove i mijenjati postojeće obrasce koji se koriste za ugovaranje ili korištenje pojedine Usluge te će ih objaviti na internetskoj stranici Banke www.hpb.hr.
- 3.6. Korisnik se obvezuje koristiti Usluge na ugovoreni način u svim odnosima za koje je predviđena sukladno Okvirnom ugovoru i uputama za korištenje pojedine Usluge.

4. UGOVARANJE USLUGE

- 4.1. Za ugovaranje Usluge, Korisnik mora zadovoljiti sljedeće uvjete:
- Korisnik Usluge može postati onaj poslovni subjekt koji u Banci ima otvoren račun za plaćanje ili iznimno onaj poslovni subjekt koji u Banci nema otvoren račun za plaćanje, ali je korisnik nekog drugog proizvoda ili usluge za koju je omogućeno korištenje Usluga;
 - Korisnik mora Banci dostaviti pravilno popunjenu i potpisanu Pristupnicu za korištenje Usluge u poslovnu mrežu Banke ili poštom na adresu Hrvatske poštanske banke, dioničko društvo, Direkcija izravnog bankarstva, Jurišićeva 4, 10 000 Zagreb;
 - Zakonski zastupnik Korisnika svojim potpisom mora jamčiti za davanje ovlaštenja Ovlaštenim korisnicima na vlastitu odgovornost i ujedno Ovlaštenim korisnicima s pravom potpisivanja platnih naloga, davanje ovlaštenja za ugovaranje dodatnih usluga putem Usluge. Ovlašteni korisnik s pravom potpisivanja platnih naloga obavlja registraciju i deregistraciju PIR-a vezanog uz određeni broj transakcijskog računa.
- 4.2. Korisnik može ugovoriti jednu ili više Usluga.
- 4.3. Ugovor o korištenju Usluge sklapa se između Banke i Korisnika, na neodređeno vrijeme.
- 4.4. Korisnik svojim potpisom na Pristupnici prihvaća Opće uvjete poslovanja i ostale akte koji se primjenjuju zajedno s njima, ugovara korištenje Usluge i potvrđuje točnost podataka naznačenih na Pristupnici.
- 4.5. Trenutkom sklapanja Ugovora smatra se trenutak odobrenja Pristupnice od strane Banke.
- 4.6. Korisnik u Pristupnici odabire način dostave Uređaja kojeg će koristiti kao Sredstvo za identifikaciju/autentifikaciju.
- 4.7. Korisnik u Pristupnici mora odrediti jednog ili više Ovlaštenih korisnika, koji će u njegovo ime koristiti ugovorenu Uslugu.
- 4.8. Korisnik mora svakom Ovlaštenom korisniku usluge internetskog i mobilnog bankarstva odabrati jednu vrstu ovlaštenja, između onih koje mu ponudi Banka.
- 4.9. Za pojedinog Ovlaštenog korisnika moguće je odabrati različite vrste ovlaštenja. Odabir, izmjena i opoziv ovlaštenja Ovlaštenih korisnika temelji se na dostavi ispravno popunjenih obrazaca Banke predviđenih za pojedinu uslugu, koje Korisnik dostavi Banci na predviđen način za pojedinu uslugu. Alternativno, Administrator ovlaštenja može unutar internetskog bankarstva samostalno odabrati, mijenjati ili opozvati ovlaštenja Ovlaštenih korisnika. Svaki odabir, izmjena ili opoziv ovlaštenja je neopoziv nalog za daljnje postupanje Banke.
- 4.10. Korisnik Usluga izravnog bankarstva može pojedinom ili svim Ovlaštenim korisnicima odrediti dnevni limit raspolaganja novčanim sredstvima u odnosu na pojedini transakcijski račun, do kojeg isti mogu obavljati platne transakcije putem Usluga. Iznos odobrenog limita je promjenjiv i može se naknadno smanjiti, povećati ili ukinuti sukladno pisanom zahtjevu Korisnika.
- 4.11. Korisnik je upoznat s činjenicom da je Banka ovlaštena samostalno uvoditi nove vrste ovlaštenja, mijenjati opseg ili ukidati pojedine vrste ovlaštenja koje Korisnik odabire Ovlaštenim korisnicima te je s istim suglasan.

- 4.12. Sva dokumentacija, uključivo i sve bančine obrasce koje Korisnik dostavi Banci u vezi s ugovaranjem, korištenjem ili opozivom korištenja Usluge moraju biti potpisani od strane zakonskog zastupnika Korisnika.
- 4.13. Korisnik se uslugom internetskog ili mobilnog bankarstva može koristiti najkasnije od prvog sljedećeg radnog dana nakon što potpiše svu propisanu dokumentaciju, preuzme sve potrebne podatke, Uređaje i/ili Sredstva za identifikaciju/autentifikaciju, koja su nužna za korištenje usluge.
- 4.14. Korisnik odnosno Ovlašteni korisnik je dužan koristiti Usluge izravnog bankarstva u skladu s propisima o sprječavanju pranja novca i financiranja terorizma, međunarodnim mjerama ograničavanja odnosno sankcijama koje primjenjuju Sjedinjene Američke Države i Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske i/ili drugih prisilnih propisa, te na zahtjev Banke, u obliku i na način koji odredi Banka, dostaviti podatke i dokumentaciju potrebnu za uspostavu Usluga izravnog bankarstva te za nastavak i praćenje zasnovanoga ugovornog odnosa u skladu s odredbama navedenih propisa o sprječavanju pranja novca i financiranja terorizma, međunarodnim mjerama ograničavanja i/ili drugih prisilnih propisa odnosno sankcijama koje primjenjuju Sjedinjene Američke Države i Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske.
- 4.15. Banka, sukladno uvjetima svoje poslovne politike, zadržava pravo odbiti Pristupnicu odnosno odlučuje o odobrenju ili odbijanju pružanja Usluge, bez obaveze da Podnositelju Pristupnice obrazloži svoju odluku.

5. KORIŠTENJE USLUGE

- 5.1. Korisnik koristi Usluge pomoću mobilnog uređaja, računala te Uređaja kojeg koristi kao Sredstvo za identifikaciju/autentifikaciju.
- 5.2. Korisnik usluzi internetskog/mobilnog bankarstva pristupa pomoću Uređaja koji su nužni za identifikaciju/autentifikaciju. Po odobrenju Pristupnice Banka Korisniku uručuje Uređaje nužne za identifikaciju/autentifikaciju ili ih šalje poštom na adresu za korespondenciju navedenu na Pristupnici. PIN šalje poštom na adresu za korespondenciju Ovlaštenog korisnika navedenu na Pristupnici odvojeno od Uređaja.
- 5.3. Ovlaštenom korisniku koji kao Uređaj koristi mToken ili je zatražio aktivaciju mobilnog bankarstva Banka će u roku od 2 (dva) radna dana od dana ugovaranja njegovog korištenja poslati na ugovoreni broj mobilnog (višenamjenskog) uređaja SMS poruku s poveznicom s koje Ovlašteni korisnik može instalirati mToken ili aplikaciju za mobilno bankarstvo na mobilni (višenamjenski) uređaj. Također, Banka će Ovlaštenom korisniku, dostaviti aktivacijski kod kojim može aktivirati mToken i/ili mobilno bankarstvo. Korisnik potvrđuje da je upoznat s time da se mToken ili aplikacija mobilnog bankarstva instalira na mobilni (višenamjenski) uređaj s internetskih stranica koje ne pripadaju Banci te je suglasan da Banka ne odgovara za mogućnosti i uvjete korištenja predmetnih internetskih stranica, kao ni za uvjete pod kojima se mToken ili aplikacija mobilnog bankarstva može instalirati. Ovlašteni korisnik je obvezan odmah nakon aktivacije mTokena ili mobilnog bankarstva, a prije prve prijave u internetsko ili mobilno bankarstvo odabrati i potvrditi PIN ili odabrati metodu biometrijske autentifikacije kojim će se nadalje identificirati pri korištenju mTokena ili mobilnog bankarstva. Korisnik odnosno Ovlašteni Korisnik snosi sve naknade i troškove povezane s instaliranjem i korištenjem aplikacije.
- 5.4. Aktivacijski kod za mToken ili mobilno bankarstvo šalje se Ovlaštenom korisniku iz sigurnosnih razloga u dva dijela putem dva odvojena kanala, SMS-om na mobilni (višenamjenski) uređaj i e-mailom na e-mail Korisnika.
- 5.5. Aktivacijski kod za mToken ili mobilno bankarstvo vrijedi 15 (petnaest) dana od dana izdavanja koda. Nakon isteka navedenog roka, iz sigurnosnih razloga, neiskorišteni

aktivacijski kod prestaje vrijediti. Korisnik može zatražiti izdavanje novog koda bez naknade.

- 5.6. Korisnik se uslugom internetskog ili mobilnog bankarstva može koristiti najkasnije od prvog sljedećeg radnog dana nakon što preuzme sve potrebne podatke i/ili Sredstva za identifikaciju/autentifikaciju, koja su nužna za korištenje usluge.
- 5.7. Prilikom prvog korištenja usluge internetskog ili mobilnog bankarstva, Korisnik/Ovlašteni korisnik je obavezan promijeniti PIN na način propisan kratkom uputom za korištenje tokena, unutar same aplikacije kod spajanja putem mobilnog (višenamjenskog) uređaja, pametne kartice ili USB uređaja. Upute za korištenje Uređaja koji se koriste kao Sredstva za identifikaciju/autentifikaciju dostupne su na internetskim stranicama Banke www.hpb.hr.
- 5.8. Uređaji koji se koriste kao Sredstva za identifikaciju/autentifikaciju osiguravaju autorizirani pristup servisu te dodatno digitalno potpisivanje financijskih transakcija.
- 5.9. Za korištenje Usluge izravnog bankarstva Korisnik sam osigurava minimalne tehničke uvjete, uključujući računalo i pristup internetu te mobilni (višenamjenski) uređaj kako je navedeno u Uputi za korištenje pojedine usluge izravnog bankarstva koja je dostupna na internetskim stranicama Banke. Korisnik se potpisom Pristupnice obvezuje postupati u cijelosti u skladu s Uputom za korištenje pojedine usluge izravnog bankarstva.
- 5.10. Ako se Korisnik nalazi u inozemstvu, a zaboravio je PIN za mToken ili mobilno bankarstvo, može zatražiti ponovo izdavanje aktivacijskog koda. U tom slučaju, potpis Korisnika na dokumentu kojim traži ponovo izdavanje aktivacijskog koda, mora biti ovjeren od strane nadležnog tijela sukladno posebnim propisima (primjerice javni bilježnik, sud, konzularna predstavništva RH u inozemstvu), a potrebno ga je dostaviti na e-mail adresu Banke direkcija.izravnog.bankarstva@hpb.hr.
- 5.11. Svi oblici korištenja usluge internetskog i mobilnog bankarstva zadani elektroničkim putem uz primjenu propisane korisničke dokumentacije izjednačeni su s vlastoručnim potpisivanjem od strane Ovlaštenih korisnika.

6. AUTENTIFIKACIJA KORISNIKA

- 6.1. Korisnik koji je ugovorio internetsko bankarstvo prilikom pristupa istome autentificira se na jedan od sljedećih načina:
 - Korisnik koji za pristup internetskom bankarstvu kao Sredstvo za identifikaciju/autorizaciju koristi token identificira se unosom serijskog broja tokena u za to predviđeno polje na ekranskom sučelju kanala, a pouzdano se autentificira jednokratnom lozinkom koju generira token nakon unosa ispravnog PIN-a.
 - Korisnik koji za pristup internetskom bankarstvu kao Sredstvo za identifikaciju/autorizaciju koristi mToken identificira se unosom serijskog broja mTokena u za to predviđeno polje na ekranskom sučelju kanala, a pouzdano se autentificira jednokratnom lozinkom koju generira token nakon unosa ispravnog PIN-a. Iznimno od navedenog, Korisnik može koristiti mToken bez unosa PIN-a tako da se pouzdano autentificira nekom od metoda biometrijske autentifikacije, na način i pod uvjetima definiranim ovim Općim uvjetima poslovanja.
- 6.2. Korisnik koji je ugovorio mobilno bankarstvo prilikom pristupa mobilnom bankarstvu autentificira se na jedan od sljedećih načina:
 - unosom odabranog PIN-a za pristup mobilnom bankarstvu u za to predviđeno polje u aplikaciji mobilnog bankarstva koja je instalirana na mobilnom (višenamjenskom) uređaju Korisnika ili

- jednom od metoda biometrijske autentifikacije, na način i pod uvjetima definiranim ovim Općim uvjetima poslovanja.
- 6.3. Biometrijska autentifikacija se temelji na tehnologiji mobilnog (višenamjenskog) uređaja kojeg Korisnik koristi za pristup internetskom ili mobilnom bankarstvu. Pojedini mobilni (višenamjenski) uređaji ne podržavaju biometrijsku autentifikaciju ili pojedine metode biometrijske autentifikacije.
 - 6.4. Banka nema pristup podacima niti kontrolu nad podacima koje je Korisnik u svrhu biometrijske autentifikacije pohranio u mobilni (višenamjenski) uređaj koji koristi za pristup internetskom ili mobilnom bankarstvu.
 - 6.5. Korisnik potvrđuje da je u mobilni (višenamjenski) uređaj koji koristi za pristup internetskom ili mobilnom bankarstvu pohranio isključivo biometrijske karakteristike svojeg lica odnosno otisak svojeg prsta. Korisnik prihvaća da se u svrhu njegove biometrijske autentifikacije prilikom pristupa internetskom ili mobilnom bankarstvu mogu koristiti biometrijski podaci koji su pohranjeni u mobilnom (višenamjenskom) uređaju koji Korisnik koristi za pristup internetskom ili mobilnom bankarstvu.
 - 6.6. Korištenje biometrijske autentifikacije je dobrovoljno te ne isključuje niti ograničava mogućnost pouzdane autentifikacije Korisnika PIN-om kojeg je odabrao za pristup mobilnom ili internetskom bankarstvu.
 - 6.7. Banka može ograničiti ili onemogućiti korištenje pojedine usluge internetskog ili mobilnog bankarstva u slučaju biometrijske autentifikacije Korisnika te uvjetovati njihovo korištenje pouzdanom autentifikacijom Korisnika PIN-om kojeg je odabrao za pristup internetskom ili mobilnom bankarstvu.
 - 6.8. Kada se na Uređaju koji Korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju na kojem je aktivirana neka od metoda biometrijske autentifikacije prilikom pristupa Korisnika ili bilo koje druge osobe internetskom ili mobilnom bankarstvu pozitivno potvrdi korištenje otiska prsta ili lica čije su karakteristike pohranjene na navedenom Uređaju, koji Korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju, smatra se da je Banka izvršila autentifikaciju Korisnika.
 - 6.9. Aktiviranjem i korištenjem opcije biometrijske autentifikacije Korisnik potvrđuje da je upoznat i suglasan s time da Banka ne pruža uslugu biometrijske autentifikacije, već da koristi biometrijsku autentifikaciju koju omogućava Uređaj koji Korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju koje koristi.
 - 6.10. Banka ne odgovara za nemogućnost ili ograničenu mogućnost korištenja biometrijske autentifikacije, niti za rezultat takve biometrijske autentifikacije, neovisno o tome da li otisak prsta ili karakteristike lica pomoću kojih se Korisnik identificira prilikom pristupa internetskom ili mobilnom bankarstvu odgovaraju ili ne odgovaraju otisku prsta ili karakteristikama lica koje je Korisnik prethodno pohranio u mobilni (višenamjenski) uređaj kojeg koristi kao Sredstvo za identifikaciju/autentifikaciju za pristup internetskom ili mobilnom bankarstvu.
 - 6.11. Korisnik može onemogućiti biometrijsku autentifikaciju tako da na Uređaju koji koristi kao Sredstvo za identifikaciju/autentifikaciju promjeni odabrane metode identifikacije/autentifikacije koje omogućava biometrijska autentifikacija

7. SIGURNOST

7.1. Radi sigurnosti pristupa usluzi internetskog i mobilnog bankarstva te radi obavljanja transakcija Banka će Ovlaštenom korisniku dodijeliti Sredstvo za identifikaciju/autentifikaciju.

7.2. Korisnik i Ovlašteni korisnik obvezuju se:

- S povećanom pažnjom čuvati sva dodijeljena Sredstva za identifikaciju/autentifikaciju, tako da spriječe njihovo oštećenje, gubitak, krađu, neovlaštenu uporabu ili zlouporabu,
- s povećanom pažnjom zaštititi vlastite Uređaje koje koriste za pristup pojedinoj usluzi izravnog bankarstva, poput računala ili mobilnog (višenamjenskog) uređaja, tako da spriječe njihovo oštećenje, gubitak, krađu, neovlaštenu uporabu ili zlouporabu,
- koristiti se dodijeljenim Sredstvima za identifikaciju/autentifikaciju, uključujući i mobilni (višenamjenski) uređaj putem kojeg koristi određenu Uslugu na način uređen ovim Općim uvjetima poslovanja, Uputom za korištenje usluga izravnog bankarstva za poslovne subjekte i relevantnom uputom za korištenje Uređaja kojeg koristi kao Sredstvo za identifikaciju/autentifikaciju,
- redovito provjeravati postojanje novih obavijesti i postupati u skladu s obavijestima koje im Banka učini dostupnima putem ugovorene Usluge i/ili internetskoj stranici Banke www.hpb.hr,
- pridržavati se svih sigurnosnih mjera zaštite i korištenja računala, odnosno mobilnog uređaja kojeg koriste za pristup usluzi izravnog bankarstva, uključujući:
 - zaštititi pristup računalu i mobilnom (višenamjenskom) uređaju povjerljivom zaporkom ili biometrijskom autentifikacijom,
 - odabrati za zaporku takvu kombinaciju brojeva, velikih i malih slova te posebnih znakova koje se ne može lako otkriti, primjerice loše bi bilo odabrati uzastopni niz brojeva, datum rođenja Ovlaštenog korisnika ili ime/prezime Ovlaštenog korisnika. Također je bitno redovito periodički mijenjati zaporku,
 - zaštititi tajnost odabrane zaporke kako bi se spriječilo njezino otkrivanje ili neovlašteno korištenje (ne zapisivati zaporku!),
 - ne otvarati elektroničku poštu i privitke pristigle od nepoznatih i/ili sumnjivih pošiljatelja te ne otvarati poveznice iz takvih poruka,
 - pribavljati informatičku opremu i programske aplikacije iz provjerenih i sigurnih izvora,
 - spajati računalo i mobilni (višenamjenski) uređaj samo na sigurne i provjerene WI-FI mreže
 - instalirati i redovito ažurirati antivirusne programe i definicije i skenirati sve aplikacije na računalu kojeg koriste za pristup Uslugama antivirusnim programom kojeg Ovlašteni korisnik posjeduje na računalu,
 - redovito ažurirati sigurnosne dodatke i programske definicije vezane za operativni sustav mobilnog (višenamjenskog) uređaja i/ili računala.
 - pravodobno obnavljati certifikat pohranjen na dodijeljenom Uređaju kojeg koristi kao Sredstvo za identifikaciju/autentifikaciju,
 - nakon prestanka korištenja Uređaja kojeg koristi kao Sredstvo za identifikaciju/autentifikaciju, isti je potrebno ukloniti iz računala,
 - u roku od najkasnije 90 (devedeset) dana od dana ugovaranja usluge preuzeti Uređaj za autorizaciju
 - pravodobno pristupati zamjeni Uređaja za autorizaciju i

- za svo vrijeme važenja odredaba ovog Ugovora omogućiti da najmanje jedan Ovlašteni korisnik u svakom trenutku posjeduje Uređaj koji zadovoljava tehničke preduvjete nužne za Sredstva za identifikaciju/autentifikaciju;
- 7.3. Korisnik je dužan čuvati tajnost svih PIN-ova i drugih personaliziranih sigurnosnih vjerodajnica kao i tajnost svih podataka vezanih uz korištenje Usluge izravnog bankarstva te voditi brigu da Sredstvo za identifikaciju /autentifikaciju ne dospije u ruke trećoj, neovlaštenoj osobi i prihvaća potpunu odgovornost za sve obveze nastale njihovim korištenjem. Štetu nastalu nepridržavanjem ovih odredbi u cijelosti snosi Korisnik.
 - 7.4. Korisnik ne smije neovlašteno raditi preinake na Uređajima koje koristi kao Sredstva za identifikaciju/autorizaciju, softveru Banke ili mobilnom (višenamjenskom) uređaju (na primjer root, jailbreak) te snosi svu štetu nastalu nepridržavanjem ovih odredbi.
 - 7.5. Korisnik odgovara za način uporabe Sredstava za identifikaciju/autentifikaciju, kao i za sve posljedice koje za njega mogu iz toga proizaći ukoliko se istima ne koristi u skladu s ovim Općim uvjetima poslovanja. Korisnik snosi svu štetu nastalu nepridržavanjem ovih odredbi.
 - 7.6. Korisnik je dužan za pristup usluzi internetskog bankarstva koristiti samo ona računala koja imaju instaliranu antivirusnu zaštitu.
 - 7.7. Banka ne snosi odgovornost u slučaju da se Korisnik ne može koristiti Uslugom zbog okolnosti na koje Banka ne može utjecati i okolnosti navedenih u točki 15.3 do 15.12. ovih Općih uvjeta poslovanja.
 - 7.8. U slučaju da prilikom korištenja usluge internetskog bankarstva adresa Banke ne započinje <https://ibps.hpb.hr/HPB.iBank.IBPS.Web/> korisnik se ne nalazi na internetskim stranicama Banke te u tom slučaju mora bez odgađanja prestati s korištenjem usluge. Korisnik je dužan prije započinjanja s korištenjem usluge internetskog bankarstva provjeriti nalazi li se na internetskim stranicama Banke.
 - 7.9. Na internetskim stranicama Banke ili putem Usluga Korisniku su dostupna upozorenja i informacije o sigurnom korištenju Usluge.
 - 7.10. Ako Korisnik primijeti sumnjivu aktivnost ili smatra da je netko neautorizirano pristupio njegovom Računu, dužan je to odmah prijaviti na besplatan broj telefona Banke 0800 472 472 (za pozive iz inozemstva +385 1 4890 365) ili putem elektroničke pošte na adresu hpb@hpb.hr. Nakon poduzetih radnji, Banka će Korisniku poslati pisani dopis o učinjenome, sukladno svojim internim aktima.

8. RASPOLAGANJE SREDSTVIMA

- 8.1. Korisnik raspolaze sredstvima na transakcijskim računima, otvorenim na temelju sklopljenog ugovora s Bankom, do visine raspoloživog stanja na računu.
- 8.2. Ovlašteni korisnik kojem je Korisnik po određenom računu definirao dnevni limit za provođenje platnih transakcija putem usluga izravnog bankarstva, može raspolagati sredstvima po tom računu do iznosa koji je Korisnik odredio.

9. IZVRŠAVANJE PLATNIH TRANSAKCIJA

- 9.1. Ukoliko je Korisnik ugovorio Uslugu koja mu omogućava obavljanje platnih transakcija, Banka će izvršiti nalog za plaćanje kada su ispunjeni svi uvjeti za izvršenje u skladu s Općim uvjetima poslovanja Hrvatske poštanske banke, dioničko društvo za

transakcijske račune i obavljanje platnih usluga za poslovne subjekte i ovim Općim uvjetima poslovanja, važećima u trenutku izvršenja transakcije.

- 9.2. Korisnik mora voditi računa o raspoloživom stanju na transakcijskom računu u Banci, definiranom dnevnom limitu za pojedine ili sve Ovlaštene korisnike te o popunjavanju naloga svim potrebnim elementima. Podaci o obveznim elementima koje mora sadržavati nalog za plaćanje dostupni su Korisnicima u poslovnoj mreži Banke te na internetskim stranicama Banke www.hpb.hr. Korisnik je odgovoran za točnost i potpunost podataka na nalogu za plaćanje.
- 9.3. Suglasnost za izvršenje naloga za plaćanje Korisnik odnosno Ovlašteni korisnik/korisnici daju na jedan od sljedećih načina:
 - Unosom odgovarajuće vrste koda (MAC ili MDS, koji su generirani odgovarajućim postupcima APPLI2 ili APPLI3) za odgovarajuću vrstu postupka suglasnosti, u za to predviđeno polje na ekranskom sučelju, u slučaju kada Ovlašteni korisnik kao Sredstvo za identifikaciju/autentifikaciju koristi token ili mToken.
 - Elektroničkim potpisivanjem naloga za plaćanje u slučaju kada Ovlašteni korisnik kao Sredstvo za identifikaciju/autentifikaciju koristi pametnu karticu ili USB uređaj. Ukoliko je sredstvima po računu ovlašteno raspolagati više osoba u svojstvu Ovlaštenih korisnika, Banka pridržava pravo u svrhu dodatne provjere sigurnosti zahtijevati od Korisnika naknadnu potvrdu autorizirane platne transakcije. Preporuka je da se prilikom autorizacije naloga koriste dva potpisnika.
 - Potvrđivanjem unesenih podataka unosom PIN-a ili korištenjem biometrijske autentifikacije, kod usluge mobilnog bankarstva.
 - Ostalim ugovorenim i/ili zakonski propisanim načinima za pojedine Usluge.
- 9.4. Banka za provođenje platnih transakcija provodi pouzdanu autentifikaciju koja uključuje dinamičko povezivanje elemenata naloga kako bi se minimizirali rizici pogreške ili prijevare. Elementi naloga za dinamičko povezivanje su nizovi znamenki tako odabrani da ujedno za Ovlaštenog korisnika predstavljaju najbližu tehnički ostvarivu reprezentaciju obavijesti o iznosu platne transakcije i primatelju plaćanja.
- 9.5. Platna transakcija za čije je izvršenje Korisnik/Ovlašteni korisnik dao suglasnost na jedan od načina navedenih pod 9.3 smatra se autoriziranom.
- 9.6. Korištenje personaliziranog sigurnosnog obilježja i Sredstva za identifikaciju/autentifikaciju smatra se nedvojbenim dokazom identiteta Korisnika odnosno Ovlaštenog korisnika, osim ako se ne dokaže suprotno u odgovarajućem postupku. Činjenica da je Banka zabilježila korištenje Sredstva za identifikaciju/autentifikaciju kojem se pristupa korištenjem personaliziranog sigurnosnog obilježja, dovoljna je da bi Banka smatrala da je Korisnik odnosno Ovlašteni korisnik autorizirao tu platnu transakciju.
- 9.7. Korisnik je suglasan da se u slučaju izvršenja platne transakcije koja se autorizira sigurnosnim obilježjima, unesena sigurnosna obilježja smatraju nedvojbenim dokazom njegovog identiteta i autorizacije transakcije. Korisnik stoga u cijelosti, bez ograničenja, odgovara za sve troškove, naknade i štetu nastalu kao posljedica njegova prijevarnog postupanja te ukoliko namjerno ili zbog krajnje nepažnje nije postupao sukladno odredbama svih primjenjivih Općih uvjeta.
- 9.8. Nalog za plaćanje zadan putem Usluga koja omogućuje zadavanje naloga za plaćanje, smatra se da je elektronički potpisan, autoriziran i iniciran u ime i za račun Korisnika.
- 9.9. Smatra se da je Banka zaprimila nalog za plaćanje u trenutku kada je Korisnik uredno popunjeni nalog za plaćanje potpisao i poslao na izvršenje putem Usluge. Naloga za bezgotovinsko plaćanje koji se odnose na nacionalne platne transakcije u kunama i eurima i na prekogranične platne transakcije u eurima Banka zaprima do 60

kalendarskih dana unaprijed. Takvi nalozi se evidentiraju u sustavu Banke i izvršavaju na zadani datum izvršenja. Naloge za plaćanje zadane kao instant naloge nije moguće zadati s datumom valute unaprijed, već se isti izvršavaju s tekućim datumom valute.

- 9.10. Ako je račun Korisnika blokiran i/ili raspoloživo stanje na računu nije dostatno za izvršenje plaćanja:
- Kod plaćanja koja se odnose na nacionalne platne transakcije u kunama i eurima i na prekogranične platne transakcije u eurima, Banka će zaprimljene naloge za plaćanje izvršiti u sljedećih 5 (pet) kalendarskih dana ukoliko se naknadno bude osiguralo pokriće na računu ili se račun odblokira.
 - Kod plaćanja koja se odnose na instant naloge, iste neće biti moguće zadati te će Korisnik odmah o tome dobiti informaciju unutar aplikacije internetskog ili mobilnog bankarstva.
- 9.11. Nalog za plaćanje moguće je zadati kao instant nalog pod sljedećim uvjetima:
- da je maksimalan iznos transakcije određen Pravilima HRK SCTInst platne sheme
 - da se odnosi isključivo na nacionalne platne transakcije u kunama zadane u korist računa u drugoj banci,
 - da se zadaje pojedinačno ručnim unosom,
 - da je banka primatelja sudionik HRK SCTInst platne sheme. Popis banaka sudionica HRK SCTInst platne sheme dostupan je na internetskoj stranici <https://www.hub.hr/hr/registri>.
- 9.12. Ako je Korisnik na listi neurednih poslodavaca, a zadaje instant plaćanja koja se odnose na isplatu plaće, Banka će zaprimljene naloge odbiti, a Korisnik će o odbijanju dobiti informaciju kod navedenog naloga unutar aplikacije internetskog ili mobilnog bankarstva.
- 9.13. Po primitku naloga za plaćanje, putem Usluge kojom je isti zadan, Korisniku/Ovlaštenom korisniku dostupna je informacija o uspješnom prijehu naloga. Informacija o uspješnom prijehu naloga za plaćanje ne znači da će nalog biti proveden, već samo da ga je Banka zaprimila.
- 9.14. Banka ispravne naloge za plaćanje izvršava u propisanim ili dogovorenim rokovima za pojedinu vrstu naloga za plaćanje, u skladu sa Terminskim planom izvršenja platnih transakcija za poslovne subjekte važećima u trenutku izvršenja platne transakcije dostupnim na internetskim stranicama www.hpb.hr.
- 9.15. Ako Banka zaprimi nalog za plaćanje iza vremena određenog Terminskim planom izvršenja platnih transakcija poslovnih subjekata kao kraj radnog dana, smatrat će se da je nalog za plaćanje zaprimljen sljedećeg radnog dana.
- 9.16. Korisnik je odgovoran za točnost i potpunost podataka na nalogu za plaćanje.
- 9.17. Banka nije odgovorna za neizvršeno plaćanje ili prijenos, odnosno pogrešno plaćanje ili prijenos napravljen putem Usluge koje je nastalo netočno unesenim podacima od strane Korisnika.
- 9.18. Banka će zaprimljeni nalog za plaćanje izvršavati isključivo u okviru raspoloživog stanja na računu/računima uzimajući u obzir definirane dnevne limite za pojedine ili sve Ovlaštene korisnike.
- 9.19. Banka neće izvršiti neispravno uneseni platni nalog.
- 9.20. U slučaju neizvršenja ili neurednog izvršenja autorizirane platne transakcije greškom Banke, Banka će Korisniku nadoknaditi štetu uključujući naplaćene naknade i pripadajuće kamate.
- 9.21. Korisnik je dužan pratiti ishod financijskih transakcija zaprimljenih putem Usluge.

- 9.22. Korisnik se izvješćuje o svim platnim transakcijama i stanju računa putem Izvatka, koji se dostavlja na način koji je ugovoren prilikom otvaranja transakcijskog računa.
- 9.23. Banka ne odgovara za neizvršenje ili neuredno izvršenje platnih transakcija ili izvršenje neautoriziranih platnih transakcija u sljedećim slučajevima:
- ako je izvršenje neautorizirane transakcije, neizvršenje i/ili neuredno izvršenje platne transakcije posljedica Korisnikove prijave, prijave njegovih Ovlaštenih korisnika, posljedica pogrešnog unosa podataka od strane Ovlaštenog korisnika ili ako Korisnik ili njegov Ovlašteni korisnik ne ispunjavaju obveze iz ovih Općih uvjeta poslovanja i/ili Općih uvjeta poslovanje po transakcijskim računima,
 - ako se nesporno utvrdi da je nalog za plaćanje Korisnika krivotvoren,
 - ako je izvršenje neautorizirane platne transakcije posljedica uporabe ukradenog ili izgubljenog Uređaja koji je bio zlouporabljen.
- 9.24. Korisnik je dužan bez odgađanja obavijestiti Banku o neautoriziranim platnim transakcijama, kao i o sumnji u gubitak, krađu, zlouporabu ili neovlašteno korištenje platnog instrumenta.

10. POSREDNI IDENTIFIKATOR RAČUNA

- 10.1. Korisniku je omogućeno korištenje RPIR-a u postupku iniciranja platnih transakcija, putem *on-line* bankarstva. RPIR-om upravlja FINA. Korisnik može u nacionalnom platnom prometu inicirati platnu transakciju kreditnog transfera u korist određenog primatelja plaćanja posredstvom PIR-a kao jedinstvenog identifikatora računa primatelja plaćanja.
- 10.2. U svrhu iniciranja naloga za plaćanje u korist transakcijskog računa Korisnika, svaki Ovlašteni korisnik s ovlaštenjem potpisa platnih naloga, može povezati broj transakcijskog računa Korisnika (IBAN) s jednim od PIR-ova: broj mobitela, e-mail adresa ili OIB Korisnika. Registracijom para PIR-IBAN ti podaci postaju dostupni FINA-i radi evidentiranja istog u RPIR-u te time i svim pružateljima platnih usluga koji su sudionici RPIR-a, kako bi drugi korisnici koji koriste platne usluge tih pružatelja platnih usluga i imaju podatak o Korisnikovom PIR-u, putem svojeg pružatelja platnih usluga mogli dohvatiti podatak o njegovom IBAN-u i tako kreirati nalog za plaćanje u korist tog transakcijskog računa Korisnika. Uz jedan PIR moguće je vezati samo jedan transakcijski račun. Ovlašteni korisnik povezuje IBAN transakcijskog računa i odabrani PIR (e-mail i/ili broj mobilnog telefona) unosom sigurnosnog koda odnosno davanjem suglasnosti, kada je PIR OIB.
- 10.3. U slučaju kada Korisnik više ne želi koristiti uslugu RPIR-a putem *on-line* bankarstva svaki Ovlašteni korisnik s ovlaštenjem potpisa platnih naloga, može provesti postupak deaktivacije registriranog para PIR-IBAN. Po uspješnoj deregistraciji para PIR-IBAN Banka će provesti deaktivaciju u RPIR-u.
- 10.4. Registrirani par PIR-IBAN u RPIR-u je aktivan 2 (dvije) godine. Prije isteka navedenog razdoblja, Banka će Korisnika najmanje 2 (dva) mjeseca ranije obavijestiti o isteku aktivnosti registriranog para PIR-IBAN. Ukoliko Korisnik želi dalje koristiti uslugu RPIR-a, treba ponovno potvrditi da registrirani PIR pripada predmetnom IBAN-u. Ako Korisnik ne potvrdi svoj par PIR-IBAN u tom postupku, isti će se smatrati poništenim i bit će deregistriran.
- 10.5. U slučaju prestanka Okvirnog Ugovora, registrirani par PIR-IBAN bit će deaktiviran u RPIR-u.

11. USLUGE INICIRANJA PLAĆANJA I INFORMIRANJA O RAČUNU

- 11.1. Korisnik koji ima ugovorenu uslugu izravnog bankarstva može nalog za plaćanje zadati koristeći usluge pružatelja usluge iniciranja plaćanja (PISP) i/ili se koristiti platnom uslugom informiranja o računu koju pruža ovlašteni pružatelj usluge informiranja o računu (AISP). Za zadavanje naloga iniciranja plaćanja i/ili informiranja o računu Korisnik odnosno, Ovlašteni korisnik mora dati suglasnost pružatelju usluge iniciranja plaćanja (PISP-u) i/ili pružatelju usluge informiranja o računu (AISP-u) koristeći autentifikacijske Uređaje koje koristi za usluge izravnog bankarstva Banke.
- 11.2. Banka provodi pouzdanu autentifikaciju Ovlaštenog korisnika koji putem mrežnih stranica pružatelja usluga informiranja o računu (AISP-a) daje pružatelju usluga informiranja o računu (AISP-u) suglasnost za pristup informacijama o jednom ili više transakcijskih računa otvorenih u Banci. Također, Banka provodi pouzdanu autentifikaciju Ovlaštenog korisnika koji putem mrežnih stranica pružatelja usluga iniciranja plaćanja (PISP-a) zadaje i podnosi na izvršenje nalog za plaćanje koji se treba izvršiti na teret transakcijskog računa otvorenog u Banci. Postupak autentifikacije Banka provodi nakon preusmjeravanja Ovlaštenog korisnika s mrežnih stranica pružatelja usluge informiranja o računu (AISP-a) odnosno pružatelja usluge iniciranja plaćanja (PISP-a) na mrežne stranice Banke.
- 11.3. Banka će sa zaprimljenim nalogima zadanim putem pružatelja usluge iniciranja plaćanja (PISP-a) postupati na isti način kao i s nalogima zadanim izravno od strane platitelja putem usluga izravnog bankarstva Banke uključujući Terminski plan izvršenja platnih transakcija za poslovne subjekte i Odluku Banke o naknadama u poslovanju s poslovnim subjektima, osim u slučaju objektivno opravdanih razloga.
- 11.4. Nakon primitka naloga za plaćanje od pružatelja usluge iniciranja plaćanja Banka će dati ili učiniti raspoloživim pružatelju usluge iniciranja plaćanja sve informacije o iniciranju i sve informacije u vezi s izvršenjem platne transakcije koje su joj dostupne dok se sve ostale informacije o Korisniku platnih usluga, dobivene pri pružanju usluge iniciranja plaćanja, pružaju samo primatelju plaćanja i samo uz izričitu suglasnost Korisnika platnih usluga.
- 11.5. Banka neće diskriminirati zahtjeve za davanje podataka koji su zaprimljeni od pružatelja usluga informiranja o računu, osim ako za to postoji objektivni razlog.
- 11.6. Pružatelji platne usluge iniciranja plaćanja i platne usluge informiranja o računu smiju pružati navedene usluge samo uz izričitu suglasnost Korisnika odnosno, Ovlaštenog korisnika danu pružatelju usluge iniciranja plaćanja i/ili pružatelju usluge informiranja o računu te su dužni osigurati da personalizirane sigurnosne vjerodajnice Korisnika nisu dostupne drugim osobama.
- 11.7. Platna transakcija koja se provodi putem pružatelja usluge iniciranja plaćanja (PISP-a) je autorizirana:
 - Ako je Ovlašteni korisnik dao suglasnost pružatelju usluge iniciranja plaćanja (PISP-u) da se posredstvom pružatelja usluge iniciranja plaćanja izvrši platna transakcija ili
 - Ako je Ovlašteni korisnik dao suglasnost pružatelju usluge iniciranja plaćanja (PISP-u) da se posredstvom pružatelja usluge iniciranja plaćanja izvrši niz platnih transakcija čiji je dio ta platna transakcija.
- 11.8. U slučaju iniciranja platne transakcije preko pružatelja usluge iniciranja plaćanja (PISP-a), Ovlašteni korisnik radi iniciranja platne transakcije daje izričitu suglasnost pružatelju usluge iniciranja plaćanja.
- 11.9. Korisnik i Ovlašteni korisnik može opozvati suglasnost koju je dao pružatelju usluge iniciranja plaćanja (PISP-u) za izvršenje platne transakcije ili niza platnih transakcija.

Oblik i postupak opoziva suglasnosti uređuje se ugovorom između Korisnika i pružatelja usluge iniciranja plaćanja (PISP-a).

- 11.10. U slučaju odbijanja izvršenja naloga za plaćanje iniciranih putem pružatelja usluge iniciranja plaćanja (PISP-a) Banka će o istome obavijestiti Korisnika putem pružatelja usluge iniciranja plaćanja (PISP-a).
- 11.11. Pružatelji platne usluge iniciranja plaćanja i platne usluge informiranja o računu dužni su proslijediti personalizirane sigurnosne vjerodajnice sigurnim i efikasnim kanalima.
- 11.12. Pružatelj platne usluge informiranja o računu smije pristupati samo informacijama i platnim transakcijama povezanim s računom za plaćanje za koji je Ovlašteni korisnik dao suglasnost.
- 11.13. Ako je nakon davanja suglasnosti pružatelju usluge informiranja o računu (AISP-u) i/ili pružatelju usluge iniciranja plaćanja (PISP-u) Korisnik raskinuo s Bankom uslugu internetskog ili mobilnog bankarstva, automatizmom se opoziva i suglasnost za korištenje usluge informiranja o računu i/ili iniciranja plaćanja.
- 11.14. Pružatelj platne usluge informiranja o računu dužan je upotrebljavati podatke, pristupati im te ih pohranjivati isključivo u svrhu pružanja usluga informiranja o računu koju je Ovlašteni korisnik izričito zatražio, sukladno pravilima o zaštiti podataka te ne smije zahtijevati osjetljive podatke o računima za plaćanje. Naziv Korisnika i broj računa ne smatraju se osjetljivim podacima u odnosu na uslugu informiranja o računu.
- 11.15. U slučaju neovlaštenog pristupa računu za plaćanje od strane pružatelja platne usluge informiranja o računu (AISP-a) ili iniciranja plaćanja (PISP-a) s ciljem prijevare, uključujući neovlašteno iniciranje platne transakcije, Banka smije uskratiti pristup računu za plaćanje na temelju dokazanih i objektivno opravdanih razloga o čemu će pravovremeno obavijestiti Korisnika osim ako je to u suprotnosti s objektivno opravdanim sigurnosnim razlozima ili protivno propisima. Banka će o navedenom incidentu odmah dostaviti obavijest i Hrvatskoj narodnoj banci. Obavijest Hrvatskoj narodnoj banci treba sadržavati sve relevantne pojedinosti o slučaju i razloge uskraćivanja pristupa računu za plaćanje.
- 11.16. Banka će ponovno omogućiti pristup računu za plaćanje odmah nakon što prestanu postojati razlozi za uskraćivanje pristupa.

12. OPOZIV NALOGA ZA PLAĆANJE

- 12.1. Korisnik može opozvati nalog za plaćanje u opsegu i rokovima sukladnim odredbama Općih uvjeta poslovanja Hrvatske poštanske banke, dioničko društvo, za transakcijske račune i obavljanje platnih usluga za poslovne subjekte.

13. BLOKADA I OTKAZ USLUGE

- 13.1. Nestanak (krađa ili gubitak), zlouporabu Uređaja/Usluge ili sumnju na zlouporabu Korisnik ili Ovlašteni korisnik je dužan odmah prijaviti pozivom na broj telefona 0800 472 472 (za pozive iz inozemstva +385 1 4890 365), u poslovnoj mreži Banke i zatražiti blokadu pristupa Usluzi te istu prijavu i pisano potvrditi na adresu Hrvatske poštanske banke, dioničko društvo, Direkcija digitalnog bankarstva, Jurišićeva 4, 10000 Zagreb, putem elektroničke pošte na adresu kontakt.centar@hpb.hr. Banka će jednako odgovarajuće postupiti bilo po prijavi Korisnika ili Ovlaštenog korisnika.
- 13.2. Banka će onemogućiti Korisniku pristup usluzi internetskog ili mobilnog bankarstva ako posumnja da postoji zlouporaba te će Korisniku poslati pisani dopis o učinjenome,

sukladno svojim internim aktima. Banka će onemogućiti pristup usluzi i/ili raskinuti Ugovor u slučaju da se Korisnik ne pridržava ugovornih odredbi, ovih Općih uvjeta poslovanja i ostalih Akata Banke, bez otkaznog roka. Ukoliko Korisnik procijeni da do zlouporabe nije došlo, može zatražiti deblokadu ili ponovno izdavanje Sredstva za identifikaciju/autentifikaciju u poslovnoj mreži Banke.

- 13.3. Banka će Ovlaštenom korisniku automatski onemogućiti korištenje usluge internetskog bankarstva ili mobilnog bankarstva ako prilikom prijave unese netočne korisničke podatke 3 (tri) ili 6 (šest) puta ovisno o Sredstvu za identifikaciju/autentifikaciju neovisno da li je usluzi pristupio izravno putem Usluge izravnog bankarstva Banke ili posredstvom pružatelja usluge iniciranja plaćanja (PISP), odnosno pružatelja usluge informiranja o računu (AISP). U tom slučaju pristup usluzi Korisnik ili Ovlašteni korisnik može zatražiti osobno u Regionalnom/poduzetničkom centru za gospodarstvo Banke ili pozivom na broj 0800 472 472 (iz inozemstva +385 1 4890 365).
- 13.4. Banka će Korisniku automatski onemogućiti korištenje usluge internetskog bankarstva putem pametne kartice ili USB uređaja ako prilikom prijave 5 (pet) puta unese netočne korisničke podatke. U tom slučaju pristup usluzi Korisnik ili Ovlašteni korisnik mora zatražiti osobno u Regionalnom/poduzetničkom centru za gospodarstvo Banke ili pozivom na broj 0800 472 472 (iz inozemstva +385 1 4890 365).
- 13.5. U slučaju da Korisnik ili Ovlašteni korisnik, ne obnovi pravodobno certifikat pohranjen na Uređaju dodijeljenom Ovlaštenom korisniku, Banka će tom Ovlaštenom korisniku privremeno do obnove postojećeg ili izdavanja novog certifikata onemogućiti pristup ugovorenoj Usluzi.
- 13.6. Banka nije dužna Korisnika odnosno Ovlaštenog korisnika obavijestiti o nemogućnosti korištenja pojedine Usluge u slučaju neispravnog unosa korisničkih podataka ili protoka roka važenja certifikata pohranjenih na Uređajima. Obavijest o nemogućnosti korištenja pojedine Usluge dostupna je kroz odgovarajuću Uslugu.
- 13.7. Banka je prema vlastitoj procjeni ovlaštena i bez prijave Korisnika, odnosno Ovlaštenog korisnika radi sigurnosti onemogućiti pristup pojedinim Uslugama blokadom Uređaja kojeg Korisnik ili Ovlašteni korisnik koristi kao Sredstvo za identifikaciju/autentifikaciju u slučaju sumnje na neovlašteno korištenje ili zlouporabu Uređaja ili u slučaju sumnje da se Usluga koristi za prijevaru ili zlouporabu. Ako Banka utvrdi ili posumnja na mogućnost kršenja odredbi propisa o sprječavanju pranja novca i financiranja terorizma, međunarodnim mjerama ograničavanja, odnosno sankcija koje primjenjuju Sjedinjene Američke Države i Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske ili u druge svrhe koje su protivne prisilnim propisima, te ako Korisnik ili Ovlašteni korisnik na zahtjev Banke ne dostavi tražene podatke i dokumentaciju potrebnu za nastavak i praćenje zasnovanoga poslovnog odnosa u skladu s odredbama propisa o sprječavanju pranja novca i financiranja terorizma, međunarodnim mjerama ograničavanja, odnosno sankcije koje primjenjuju Sjedinjene Američke Države, Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske i/ili drugih prisilnih propisa.
- 13.8. Sve troškove nastale neovlaštenim korištenjem Uređaja do zaprimanja pisane prijave nestanka snosi Korisnik.
- 13.9. Korisnik snosi sav rizik za moguće neovlašteno korištenje Usluge ukoliko se ne pridržava propisanih mjera sigurnosti.
- 13.10. Na osnovi pisane prijave nestanka Sredstva za identifikaciju, Banka izdaje Korisniku i novo Sredstvo za identifikaciju/autentifikaciju s novim PIN-om te naplaćuje Korisniku naknadu za njegovo izdavanje sukladno Odluci o naknadama.
- 13.11. Korisnik ima pravo jednostrano otkazati korištenje Usluge predajom pisanog zahtjeva osobno u poslovnoj mreži Banke pri čemu se dan i vrijeme odobrenja takvog zahtjeva za zatvaranjem od strane Banke ujedno smatra i trenutkom otkaza Usluge. Otkazivanjem Usluge Korisnik je obavezan vratiti i dodijeljene mu Uređaje koje koristi

kao Sredstva za identifikaciju/autentifikaciju u Regionalnom/poduzetničkom centru za gospodarstvo Banke, osobno ili preporučenom pošiljkom na adresu Banke, osim ako je ujedno Korisnik i druge usluge za koju koristi iste Uređaje kao Sredstva za identifikaciju/autentifikaciju.

- 13.12. Sve transakcije zadane unaprijed putem Usluge, koje do datuma otkaza nisu opozvane, biti će izvršene u slučaju da je račun aktivan.
- 13.13. Banka će Korisniku onemogućiti korištenje Usluge u slučaju da Korisnik zatvori sve Račune u Banci te u slučaju prestanka postojanja Korisnika, odnosno u slučaju smrti ako se radi o Korisniku - fizičkoj osobi koja djeluje u okviru svoje gospodarske djelatnosti ili slobodnog zanimanja. Korisnik ovlašćuje Banku da bez ikakve daljnje suglasnosti i obavijesti može trošak nastao korištenjem Usluge naplatiti bez intervencije suda sa svih njegovih računa koji se vode u Banci.
- 13.14. Banka može pisanim putem jednostrano otkazati Usluge bez ostavljanja otkaznog roka i s trenutnim učinkom. Usluge se u navedenom slučaju smatraju otkazane istekom otkaznog roka od 15 (petnaest) dana, računajući od dana slanja obavijesti o otkazu Usluge Korisniku preporučenom poštom na adresu sjedišta Korisnika odnosno drugu adresu za korespondenciju koju je Korisnik prijavio Banci, neovisno o tome da li je i kada je Korisnik preuzeo otkazno pismo.
- 13.15. Banka ima pravo jednostrano otkazati Usluge bez ostavljanja otkaznog roka i s trenutnim učinkom na način opisan u prethodnoj točki:
 - Ako je Korisnik ili Ovlašteni korisnik prilikom sklapanja Usluge dao Banci neistinite ili pogrešne podatke,
 - Ako Korisnik ne ispunjava uvjete za korištenje ugovorene Usluge,
 - Ako se korisnik ili Ovlašteni korisnik ne pridržava Ugovora, Općih uvjeta poslovanja, Korisničke upute, pojedinačnih uputa za korištenje Uređaja koje koristi kao Sredstva za identifikaciju/autentifikaciju ili ostalih akata koji se primjenjuju zajedno s ovim Općim uvjetima poslovanja,
 - Ako Korisnik ili Ovlašteni korisnik postupa protivno prisilnim propisima koji se primjenjuju na pravni odnos između Banke i Korisnika, uključujući propise koji se odnose na sprječavanje pranja novca i financiranje terorizma, obavljanje platnog prometa i elektroničko poslovanje
 - Ako Banka utvrdi ili posumnja na mogućnost prijave ili zlouporabe,
 - Ako Banka utvrdi ili posumnja na mogućnost kršenja odredbi propisa o sprječavanju pranja novca i financiranja terorizma, međunarodnim mjerama ograničavanja odnosno sankcija koje primjenjuju Sjedinjene Američke Države, Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske i/ili drugih prisilnih propisa,
 - Ako Banka utvrdi da je Klijent fizička ili pravna osoba za koju su propisane sankcijske mjere ograničavanja poslovanja ili koja krši propisane sankcijske mjere
 - Ako je protiv Klijenta poduzeta istražna radnja ili postupak radi primjene međunarodnih sankcija od strane nadležnih Tijela sukladno odredbama Zakona o međunarodnim mjerama ograničavanja
 - Ako Banka utvrdi ili posumnja da u poslovnom odnosu s Klijentom postoje indikatori da Klijent svjesno zaobilazi međunarodne sankcijske mjere ograničavanja, sankcije koje primjenjuju Sjedinjene Američke Države ili Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske.
 - Ako Korisnik ili Ovlašteni korisnik na zahtjev Banke ne dostavi tražene podatke i dokumentaciju potrebnu za korištenje Usluge te nastavak i praćenje zasnovanoga ugovornog odnosa u skladu s odredbama navedenih propisa o sprječavanju pranja novca i financiranja terorizma, međunarodnim mjerama ograničavanja, sankcija koje

primjenjuju Sjedinjene Američke Države i Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske i/ili drugih prisilnih propisa.

- Ukoliko Ovlašteni korisnik ni nakon 90 (devedeset) dana od ugovaranja usluge nije preuzeo Uređaj za autorizaciju,
- ukoliko Ovlašteni korisnik ni nakon ponovljenog poziva od strane Banke nije pristupio zamjeni Uređaja za autorizaciju, a niti jedan Ovlašteni korisnik ne posjeduje Uređaj koji zadovoljava tehničke preduvjete nužne za Sredstva za identifikaciju/autentifikaciju.

13.16. S danom prestanka važenja Usluge, Banka onemogućava uporabu ugovorene usluge i obračunava sve nepodmirene obveze Korisnika sukladno Odluci o naknadama i drugim troškovima Banke za usluge u poslovanju, a Korisnik je dužan vratiti dodijeljene mu Uređaje koje je koristio kao Sredstvo za identifikaciju/autentifikaciju, osim ako je korisnik i neke druge usluge za koju koristi iste Uređaje za identifikaciju/autentifikaciju.

14. PRAVA I OBVEZE KORISNIKA

- 14.1. Korisnik/Ovlašteni korisnik je obvezan čuvati tajnost svih podataka vezanih uz korištenje Usluga te voditi brigu da Uređaj koji se koristi kao Sredstvo za identifikaciju/autentifikaciju ne dospije u ruke trećoj, neovlaštenoj osobi i prihvaća potpunu odgovornost za sve obveze nastale njihovim korištenjem. Ukoliko Korisnik posumnja ili utvrdi da je s PIN-om upoznata druga osoba, dužan ga je promijeniti.
- 14.2. Korisnik/Ovlašteni korisnik je dužan odmah i neizostavno obavijestiti Banku o gubitku neovlaštenoj upotrebi ili mogućnosti neovlaštene uporabe tajnih podataka i Uređaja na broj 0800 472 472 od 0-24 sata, 7 (sedam) dana u tjednu (iz inozemstva +385 1 4890 365) te pisanu prijavu osobno predati najbližem Regionalnom/poduzetničkom centru za gospodarstvo Banke.
- 14.3. U slučaju da je Korisnik u svojem Uređaju koji koristi kao Sredstvo za identifikaciju/autentifikaciju aktivirao korištenje biometrijske autentifikacije, Korisnik mora osigurati da su u svakom trenutku u Uređaju koji koristi kao Sredstvo za identifikaciju/autentifikaciju pohranjeni isključivo Korisnikovi biometrijski podaci jer će se svaka prijava putem bilo koje metode biometrijske autentifikacije smatrati provedenom od strane Korisnika kao i svi eventualno provedeni nalozi nakon takve prijave te Korisnik prihvaća potpunu odgovornost za sve tako nastale obveze.
- 14.4. Korisnik se obvezuje da će koristiti Usluge u skladu s Uputom za uslugu koju ima aktiviranu. Pri popunjavanju naloga, Korisnik mora voditi računa o raspoloživom iznosu sredstava na računu u Banci, uključujući dnevni limit i dozvoljeno prekoračenje. Korisnik je odgovoran za točnost svih podataka na platnim nalogima te snosi rizik unosa netočnih podataka.
- 14.5. U slučaju provođenja neautorizirane transakcije od strane Korisnika, ako Korisnik smatra da je žrtva kaznenog djela, Korisnik je dužan isto odmah prijaviti Banci i Ministarstvu unutarnjih poslova/Državnom odvjetništvu Republike Hrvatske.
- 14.6. Korisnik prihvaća da Usluge, ovisno o njihovoj vrsti uključuju prijenos podataka putem telekomunikacijskih veza (internet, e-mail, telefon, GSM uređaj) te su stoga povezani s rizicima koji su uobičajeni za korištenje navedenih načina komunikacije. Banka jamči korisniku da je komunikacija putem internetskog i mobilnog bankarstva kriptirana.
- 14.7. Korisnik, odnosno Ovlašteni korisnik obvezuju se:
- sve transakcije zadata u skladu s Općim uvjetima poslovanja Hrvatske poštanske banke, dioničko društvo za transakcijske račune i obavljanje platnih usluga za poslovne subjekte te zakonskim i podzakonskim aktima,

- prijaviti promjenu svih osobnih ili drugih podataka neophodnih za korištenje Usluge ili koji mogu utjecati na korištenje Usluge podnošenjem potpisanog Zahtjeva za promjenu podataka,
- samostalno brinuti o zatvaranju ili promjeni ovlasti u korištenju Usluge za sve Ovlaštene korisnike.

15. PRAVA I OBVEZE BANKE

- 15.1. Banka za korištenje Usluga primjenjuje tehnološko rješenje koje omogućava sigurnu vezu između Korisnika i računala Banke, a koja predstavlja standard sigurne komunikacije u komercijalnoj primjeni.
- 15.2. Banka omogućuje korisniku raspolaganje sredstvima na svim računima do visine raspoloživih sredstava na Računu.
- 15.3. Banka ne snosi odgovornost u slučaju kada je nalog odbijen u sustavu platnog prometa ili kada ga nije moguće izvršiti točno i na vrijeme, uslijed pogreške Korisnika.
- 15.4. Banka ne snosi odgovornost za neizvršenu transakciju uslijed neispravno ili netočno unesenih podataka od strane Korisnika.
- 15.5. Banka ne preuzima odgovornost za nedostupnost Usluge koje je nastupila kao posljedica tehničkih problema na računalnoj opremi ili mobilnim (višenamjenskom) uređaju, ispada ili smetnji u telekomunikacijskim vezama, nestanka struje ili kao posljedica više sile.
- 15.6. Banka može, uz prethodnu najavu, privremeno onemogućiti korištenje ugovorenih direktnih kanala u slučaju promjena opsega usluga koje su dostupne putem određenog direktnog kanala, promjena i nadogradnji u informacijskom sustavu Banke, uključujući sustav njezine informacijske sigurnosti. Obavijest o privremenoj nemogućnosti korištenja direktnog kanala zbog navedenih razloga Banka dostavlja Korisniku putem istog direktnog kanala, te objavljuje na internetskim stranicama Banke.
- 15.7. Banka ne preuzima odgovornost za štetu nastalu uslijed ne dostave podataka o promjenama osobnih ili drugih podataka neophodnih za sigurno funkcioniranje pojedine Usluge.
- 15.8. Banka ne odgovara za štetu uzrokovanu neopravdanim zahvatima Korisnika ili trećih osoba zbog kojih je došlo do nefunkcioniranja Usluga.
- 15.9. Banka ne odgovara za gubitak ili uništenje podataka na opremi koju Korisnik koristi za pristup Uslugama.
- 15.10. Banka ne odgovara za štetu nastalu prije primitaka Korisnikove prijave gubitka, krađe, neovlaštenog korištenja, zlouporabe ili sumnje na zlouporabu Uređaja, mobilnog (višenamjenskog) uređaja na kojem je instaliran mToken ili mobilno bankarstvo.
- 15.11. Banka ne odgovara za štetu koja Korisniku ili Ovlaštenom korisniku nastane zbog:
 - nepridržavanja Ugovora, Općih uvjeta poslovanja, Korisničke upute, pojedinačnih uputa za korištenje Uređaja koji se koriste kao Sredstva za identifikaciju/autentifikaciju ili ostalih akata koji se primjenjuju zajedno sa ovim Općim uvjetima poslovanja od strane Korisnika ili Ovlaštenog korisnika,
 - nepridržavanja posljednjih sigurnosnih uputa koje je Banka objavila na svojim internetskim stranicama ili koje je dostavila Korisniku ili Ovlaštenom korisniku ugovorenom Uslugom od strane Korisnika ili Ovlaštenog korisnika,
 - prijevare ili drugog protupravnog postupanja od strane trećih osoba na štetu Korisnika ili Ovlaštenog korisnika,

- prestanka važenja certifikata pohranjenog na Uređaju, dodijeljenog Korisniku odnosno Ovlaštenom korisniku,
- ako je izvršenje, neizvršenje i/ili neuredno izvršenje platne transakcije posljedica iznimnih i nepredvidivih okolnosti na koje Banka nije mogla utjecati i čije se posljedice ne bi mogle izbjeći unatoč postupanju s potrebnom pozornošću,
- ako je neizvršenje ili neuredno izvršenje Platne transakcije u odnosu na Korisnika usluga Banke koji je primatelj plaćanja, posljedica postupanja Pružatelja platnih usluga Platitelja,
- odavanja PIN-a, neke druge sigurnosne vjerodajnice ili bilo kojeg drugog povjerljivog podatka trećoj osobi kao i u slučaju prijave ili provođenja naloga putem jedne od metoda biometrijske autentifikacije ako Korisnik u svojem Uređaju koji koristi kao Sredstvo za identifikaciju/autentifikaciju kojim pristupa internetskom ili mobilnom bankarstvu ima pohranjen biometrijski podatak koji se ne odnosi na Korisnika nego na drugu osobu,
- ako je neizvršenje ili neuredno izvršenje posljedica postupanja primatelja plaćanja kod platnih transakcija iniciranih od strane primatelja plaćanja ili preko primatelja plaćanja,
- postupanja ili propusta pružatelja usluge iniciranja plaćanja (PISP-a) i/ili pružatelja usluge informiranja o računu (AISP-a),
- privremene nedostupnosti on-line usluga izravnog bankarstva i/ili djelomične ili potpune nemogućnosti korištenja internetske i/ili mobilne aplikacije za vrijeme planiranih aktivnosti održavanja sustava Banke,
- posljedica tehničkih problema na računalnoj opremi ili mobilnim (višenamjenskom) uređaju, ispada ili smetnji u telekomunikacijskim vezama, nestanka struje ili više sile,
- Banka se također oslobađa odgovornosti za produljenje roka izvršenja ili neizvršenje naloga kojemu je uzrok obveza Banke da primjenjuje i provodi mjere sukladno propisima i međunarodno prihvaćenim obvezama na području sprječavanja pranja novca i financiranja terorizma, međunarodnih mjera ograničavanja, odnosno sankcija koje primjenjuju Sjedinjene Američke Države, Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske i/ili drugih prisilnih propisa, kao i propisima koji Banci nalažu obveze u pogledu provjere informacija koje moraju biti priložene prijenosu novčanih sredstava,
- u drugim slučajevima definiranim ovim Općim uvjetima poslovanja.

15.12. Banka ne odgovara za transakcije koje su učinjene preuzimanjem kontrole nad računalom ili mobilnim (višenamjenskim) uređajem Korisnika ili Ovlaštenog korisnika ili bilo kojem obliku zloupotrebe koja je uzrokovana instaliranim zloćudnim kodom na računalu ili mobilnom (višenamjenskom) uređaju Korisnika ili Ovlaštenog korisnika.

16. ZAŠTITA OSOBNIH PODATAKA I POVJERLJIVIH INFORMACIJA

- 16.1. Načela i pravila obrade osobnih podataka regulirana su Politikom zaštite osobnih podataka Hrvatske poštanske banke, dioničko društvo, javno dostupnoj na internetskoj stranici Banke <https://www.hpb.hr/zastita-osobnih-podataka>.
- 16.2. Banka u svrhu sprječavanja zloupotreba i iz sigurnosnih razloga prilikom korištenja izravnih kanala bankarstva (internetsko i mobilno bankarstvo) prikuplja i obrađuje podatke o IP adresi Uređaja koji se koristi kao Sredstvo za identifikaciju/autentifikaciju s kojega se pristupa izravnom kanalu te podatke o Uređaju (kao što su model Uređaja,

internetski preglednik, operativni sustav, dostupni jedinstveni identifikatori Uređaja i podaci o mobilnoj mreži s koje se pristupa izravnom kanalu).

17. NAKNADE

- 17.1. Za korištenje Usluga, izdavanje Uređaja koji se koriste kao Sredstva za identifikaciju/autentifikaciju, otkaz ili blokadu korištenja Usluge Banka naplaćuje naknade sukladno važećoj Odluci o naknadama.
- 17.2. Za ponovno izdavanje mToken-a, ponovno generiranje PIN-a za pametnu karticu, USB uređaj i token, Banka ne naplaćuje naknadu sukladno Odluci o naknadama.
- 17.3. Korisnik ovlašćuje Banku da bez ikakve daljnje suglasnosti i obavijesti može teretiti njegove Račune za sve troškove nastale korištenjem Usluga uključujući naknade i druge troškove koji mogu nastati uslijed npr. tečajnih razlika i sl.
- 17.4. Naknade su objavljene na internetskoj stranici Banke www.hpb.hr. Banka će Korisniku dostaviti fakturu ili učiniti raspoloživim putem Usluge za protekli period na mjesečnoj osnovi. Korisnik je suglasan da Banka tereti njegove Račune za sve naknade nastale korištenjem Usluga.
- 17.5. U slučaju otkaza Usluge od strane Banke kao i u slučaju otkaza od strane Korisnika, neovisno o uručenju Uređaja koji se koriste kao Sredstva za identifikaciju/autentifikaciju Korisniku/Banci, Korisnik nema pravo na povrat naknada.
- 17.6. Naknade i troškovi koje Banka obračunava Korisniku za korištenje Usluga su promjenjive, a Banka će Korisnika obavijestiti o njihovim promjenama najmanje 15 (petnaest) dana prije stupanja promjena na snagu, objavom na internetskim stranicama Banke www.hpb.hr ili na drugi način koji je ugovoren s Korisnikom. Smatra se da je Korisnik suglasan s promjenama ako do dana početka primjene promijenjene visine naknade ili troškova ne obavijesti Banku pisanim putem da ih ne prihvaća. Zaprimanjem pisane obavijesti Korisnika o neprihvatanju promijenjenih naknada i troškova smatra se da je korisnik otkazao sve Ugovore.

18. NAČIN I SREDSTVA KOMUNIKACIJE

- 18.1. Korisnik je odgovoran za sve kontakt informacije koje je predao Banci, a koje su neophodne za ispravno i sigurno funkcioniranje Usluge i dužan ih je ažurirati i obavijestiti Banku o svakoj njihovoj promjeni.
- 18.2. Banka je dužna Korisniku omogućiti spremanje i/ili tiskanje podataka o provedenim Uslugama tako da bi mu bili dostupni za kasniju uporabu u primjerenom razdoblju s obzirom na namjenu podataka. Banka je dužna Korisniku omogućiti neizmijenjeno reproduciranje spremljenih podataka.
- 18.3. Banka šalje Korisniku sve informacije koje Korisnik može preuzeti u elektroničkom obliku isključivo na zahtjev Korisnika.

19. RJEŠAVANJE PRIGOVORA

- 19.1. Korisnik može podnijeti Banci pisani prigovor ukoliko smatra da se Banka ne pridržava odredbi Ugovora, ovih Općih uvjeta poslovanja te zakona kojim je uređeno pružanje platnih usluga.

- 19.2. Korisnik je na prethodno naveden način dužan obavijestiti Banku o neautoriziranoj, neizvršenoj ili neuredno izvršenoj platnoj transakciji odmah nakon saznanja, a najkasnije u roku od 8 (osam) dana od dana terećenja njegovog računa.
- 19.3. Banka u poslovnim prostorima u kojima obavlja poslovanje s fizičkim i pravnim osobama i na internetskoj stranici Banke osigurava obavijesti o mogućnosti i načinu podnošenja prigovora te postupku rješavanja prigovora. Načela i pravila upravljanja prigovorima koje Korisnici/podnositelji prigovora podnose Banci uređena su Politikom upravljanja prigovorima koja je javno objavljena i dostupna na internetskim stranicama Banke www.hpb.hr.
- 19.4. Korisnik može podnijeti Banci prigovor na jedan od navedenih načina:
- osobno u poslovnoj mreži Banke (Regionalnom centru za stanovništvo) ili Regionalnom/poduzetničkom centru za gospodarstvo,
 - e-mailom: kvalitetausluge@hpb.hr i hpb@hpb.hr,
 - putem internetske stranice: www.hpb.hr, popunjavanjem forme za podnošenje prigovora,
 - poštom: Hrvatska poštanska banka, dioničko društvo, Ured za upravljanje kvalitetom usluge, Jurišićeva 4, 10 000 Zagreb
 - telefaksom: 01/4707 987.
- 19.5. Prigovore koji se odnose na usluge koje pružaju usluge iniciranja plaćanja (PISP) i usluge informiranja o računu (AISP), 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 vezanim za autorizaciju i izvršenje platnih transakcija iniciranih putem pružatelja usluge iniciranja plaćanja (PISP-a), isti se upućuju Banci na isti način kao i kad je riječ o prigovorima vezanim za platne transakcije inicirane korištenjem kanala izravnog bankarstva Banke.
- 19.6. Prigovori koji se odnose na obradu osobnih podataka podnose se službeniku za zaštitu osobnih podataka na e-mail: dpo@hpb.hr i rješavaju se na način uređen Politikom zaštite osobnih podataka Banke objavljenom na internetskoj stranici Banke www.hpb.hr.
- 19.7. Prigovor Banci treba sadržavati slijedeće podatke:
- naziv, adresu i OIB Korisnika,
 - detaljan opis događaja ili okolnosti koje su izazvale nezadovoljstvo, a koje su predmet prigovora te dokaz osnovanosti prigovora.
- 19.8. Banka će odgovoriti Korisniku najkasnije u zakonom propisanom roku od 10 (deset) dana od dana zaprimanja prigovora. Iznimno, u slučajevima kada Banka ne može dati odgovor u roku od 10 (deset) dana od dana zaprimanja, Banka će unutar naprijed navedenog roka dostaviti privremeni odgovor u kojem će obavijestiti Korisnika /podnositelja prigovora o razlozima odgode i kašnjenja odgovora te roku do kojeg će primiti konačan odgovor koji ne može biti duži od 35 (trideset pet) dana od dana zaprimanja prigovora.
- 19.9. Ukoliko Korisnik odnosno Ovlašteni korisnik i/ili Korisnik kao podnositelj prigovora smatra da Banka postupa protivno odredbama Zakona o platnom prometu koje se odnose na obveze informiranja ili na prava i obveze u vezi s pružanjem i korištenjem platnih usluga, Korisnik odnosno Ovlaštena osoba i/ili Korisnik koji je podnio prigovor može uputiti pritužbu protiv Banke Hrvatskoj narodnoj banci.
- 19.10. U svrhu rješavanja prigovora Korisnik/Ovlašteni korisnik je dužan priložiti dokumentaciju koja se tiče transakcije na koju se prigovor odnosi.

20. ZAVRŠNE ODREDBE

- 20.1. Ovi Opći uvjeti poslovanja su objavljeni na internetskoj stranici Banke www.hpb.hr.
- 20.2. Izmjene ovih Općih uvjeta poslovanja Banka će učiniti dostupnima na internetskoj stranici Banke www.hpb.hr najmanje 15 (petnaest) dana prije predloženog datuma početka primjene izmjena. Ako Korisnik nije suglasan s izmjenama, može bez otkaznog roka i bez naknade otkazati korištenje Usluge. Uslugu mora otkazati pisanim putem, najkasnije do predloženog datuma početka primjene izmjena ovih Općih uvjeta poslovanja.
- 20.3. Ovi Opći uvjeti poslovanja sastavljeni su na hrvatskom jeziku i komunikacija za vrijeme njegovog trajanja odvija se na hrvatskom jeziku.
- 20.4. Smatrat će se da je Korisnik prihvatio navedene izmjene ako do predloženog datuma početka primjene izmjena ovih Općih uvjeta poslovanja ne obavijesti Banku da ih ne prihvaća.
- 20.5. Na Ugovor i međusobna prava i obveze Korisnika i Banke primjenjuje se pravo Republike Hrvatske, a za sve sporove koje proizlaze iz Ugovora ili su u vezi s njim ugovara se nadležnost hrvatskih sudova te mjesna nadležnost suda u Zagrebu.
- 20.6. Danom stupanja na snagu ovih Općih uvjeta poslovanja prestaju važiti Opći uvjeti Hrvatske poštanske banke, dioničko društvo za korištenje usluga izravnog bankarstva za poslovne subjekte, od dana 15. prosinca 2020.godine.
- 20.7. Ovi Opći uvjeti poslovanja stupaju na snagu s danom donošenja, a primjenjuju se od 24. ožujka 2021. godine