**Informacije v skladu s 5., 7. in 8. členom zakona FernFinG**

**1. Opis družbe**

- Ime in sedež:
  PayLife Service Center
  BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft (v nadaljevanju: banka),
  Wiedner Gürtel 11, 1100 Wien

- Glavna dejavnost:
  Finančne posle v smislu 1. člena avstrijskega Zakona o bančništvu – Bankwesengesetz (BWG), predvsem opravljanje brezgotovinskega poslovanja

- Matična številka/krajevno pristojno sodišče za vodenje vpisa v register družb (Firmenbuchgericht)
  registrska številka FN 205340x , Handelsgericht Wien (gospodarsko sodišče na Dunaju)

- Pristojni nadzorni organ:
  avstrijski organ za finančni trg – Finanzmarktaufsicht (FMA), Otto-Wagner-Platz 5, 1090 Wien

**2. Opis finančne storitve**

Bistvene lastnosti finančnih storitev:
Banka za varen postopek plačevanja po internetu ponuja varnostni mehanizem 3D Secure, v katerega se lahko uporabnik registrira z vpisom izbora podatkov. Izvedba plačilnega naloga poteka na podlagi v sistemu vpisanih ali generiranih podatkov, ki omogočajo identifikacijo uporabnika.

S potrditvijo identifikatorja (v varnem postopku je to vnos gesla in dodatna avtorizacija z geslom mobileTAN ali biometričnim identifikatorjem idr.) se nalog nepreklicno izvede. Postopek transakcije plačilnega naloga poteka med pogodbenim podjetjem (trgovcem) in njegovim ponudnikom plačilnih storitev.

**3. Stroški uporabe finančne storitve**

(1) Z uporabo varnostnega mehanizma 3D Secure, ki ga ponuja družba banka nimate stroškov.
(2) Banka vas bremeni za strošek, ki ga ta poravnava pogodbenim podjetjem za vaš nakup blaga in storitev, ki je bil opravljen z uporabo postopka 3D Secure. Strošek se knjiži z direktno bremenitvijo na vašem računu, v dogovorjenem znesku, ki je zapisan v pogodbi med banka in stranko, npr. v pogodbi o osebnem računu.
(3) Stranka sama nosi strošek za uporabo mobilnega operaterja (npr. za pametni telefon).

**4. Obvestilo glede pravice odstopa od pogodbe v skladu z 8. členom avstrijskega Zakona o finančnih poslih na daljavo (FernFinG)**

Skladno z 8. členom avstrijskega Zakona o finančnih poslih na daljavo (FernFinG) imate pravico, da v 14 dneh od sklenjenega dogovora o uporabi varnostnega mehanizma 3D Secure odstopite od pogodbe. Rok za odstop od pogodbe prične teči skladno s 3. točko Posebnih pogojev za brezgotovinsko elektronsko poslovanje z uporabo varnostnega mehanizma 3D Secure z dnem registracije na spletni strani (t.j. datum sklenitve pogodbe).

V kolikor boste po 8. členu FernFinG-a uveljavljali pravico do odstopa od pogodbe, ste dolžni, da PayLife Service Center, Wiedner Gürtel 11, 1100 Wien svojo izjavo o odstopu posredujete izrecno pisno. Če pravice do odstopa od pogodbe ne uveljavite v roku 14 dni od dneva sklenitve pogodbe, velja sklenitev kartične pogodbe za nedoločen čas, vendar ne dlje od sklenjene kartične pogodbe.

V skladu s petim odstavkom 8. člena FernFinG-a se v času odstopnega roka izvajanje pogodbe lahko prične šele z vašim izrecnim strinjanjem. Za storitve, ki so bile opravljene pred iztekom roka za odstop od kartične pogodbe (8. člen FernFinG-a) je družba upravičena do nadomestil in stroškov za opravljene storitve.

**5. Prenehanje**

Dostop do varnostnega mehanizma 3D Secure lahko kadarkoli blokirate ali pa geslo za 3D Secure sami spremenite. Družba banka je upravičena, da varnostni mehanizem 3D Secure sama blokira, če obstajajo objektivni varnostni razlogi, ali sum na nepooblaščeno oz. goljufivo uporabo.
Prav tako lahko banka upoštevaje dvomesečnega roka kartično pogodbo, na katero je vezana uporaba varnostnega mehanizma 3D Secure prekine in kadarkoli iz opravičenih razlogov razdre.

**6. Izbira prava in pristojno sodišče**

Za dogovor o uporabi varnostnega mehanizma 3D Secure kot tudi za predpogodbena razmerja se uporablja avstrijsko pravo. Avstrijsko sodišče je pristojno tudi, če bi v primeru tožbe zoper banka in tožbe banka zoper vas po sklenitvi pogodbe svoje prebivališče selili v tujino, in so avstrijske sodne odločbe tam izvršljive.

**7. Informacije v skladu s 5. in 8. členom avstrijskega zakona FernFinG-a, kot tudi pogodbeni pogoji te pogodbe so zapisane v nemškem jeziku. V času trajanja pogodbe bo potekala komunikacija med banka in vami v nemškem jeziku.**

**8. Informacije o pritožbah v skladu s 4. točko prvega odstavka 5. člena avstrijskega zakona FernFinG**

Za izvensodno reševanje sporov v zvezi z nekaterimi pritožbami potrošnikov v finančnem sektorju je bil ustanovljen skupni odbor za mediacijo avstrijske bančne dejavnosti (Gemeinsame Schlichtungsstelle der Österreichischen Kreditwirtschaft), Wiedner Hauptstraße 63, 1045 Dunaj.
Pritožbe s kratkim opisom zadeve lahko skupaj s prilogami naslovite v pisni ali elektronski obliki na e-poštni naslov odbora za mediacijo (e-poštni naslov: office@bankenschlichtung.at).

različica september 2019, stanje marec 2020

# Posebni pogoji poslovanja za uporabo varnostnega mehanizma 3D Secure Postopek za predplačniške kartice z možnostjo polnitve

PayLife

Posebni pogoji poslovanja za uporabo varnostnega mehanizma 3D Secure za predplačniške kartice PayLife z možnostjo polnitve so zapisani v moški slovnični obliki, uporabljeni pa kot nevtralni za ženski in moški spol.

**1. Splošno**

S Posebnimi pogoji poslovanja za uporabo varnostnega mehanizma 3D Secure za predplačniške kartice PayLife (v nadaljevanju: Posebni pogoji 3DS) je urejen potek plačilnega prometa s predplačniškimi karticami PayLife z možnostjo polnitve v varnem sistemu 3D Secure. Posebni pogoji 3DS veljajo, ko je veljavnost dogovorjena. So del Splošnih pogojev poslovanja za uporabo predplačniških kartic PayLife (v nadaljevanju: Splošni pogoji), ki so osnova za sklenitev kreditne pogodbe o izdaji predplačniške kartice z možnostjo polnitve (v nadaljevanju: kartica) med družbo BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft (v nadaljevanju: banka) in imetnikom kartice.

**2. Definicija**

2.1. 3D Secure
Varnostni mehanizem 3D Secure se uporablja za dodatno avtentikacijo stranke pri potrditvi spletnih plačil.

2.2. "Geslo 3D Secure": Mastercard Identity Check (tehnologija za preverjanje istovetnosti)

2.3. Geslo 3D Secure je geslo, ki si ga je imetnik kartice ob registraciji v varnostni mehanizem 3D Secure določil sam (kombinacija znakov). »Mastercard Identity Check«, tehnologija, ki preprečuje zlorabo vašega računa, vas pozove k potrditvi svoje identitete pri spletnem nakupovanju.

2.4. Oddaljeno transakcijsko geslo mobileTAN (v nadaljevanju: mobileTAN)
mobileTAN je enkratno dodeljeno geslo, ki ga imetnik kartice prejme po SMS-u na mobilno številko, ki jo je navedel kot veljavno. Poleg varnostnega mehanizma 3D Secure je geslo mobileTAN dodatna identifikacija v postopkih spletnega plačevanja. Vnos gesla mobileTAN je potreben tudi pri registraciji v varnostni mehanizem 3D Secure.

2.5. Mobilna aplikacija PayLife secCheck
Bančna mobilna aplikacija PayLife secCheck (na voljo za operacijska sistema iOS in Android) omogoča biometrično avtentikacijo (npr. prstni odtis, prepoznava obraza) ali geslo za mobilno aplikacijo (App PIN). V postopku registracije v mobilno aplikacijo PayLife secCheck imetnik kartice za potrjevanje svoje identitete pri spletnem nakupovanju izbere biometrični identifikator in geslo (App PIN). V primeru, da mobilna končna naprava nima funkcije za preverjanje biometričnih varnostnih rešitev (npr. senzor za prstni odtis), imetnik kartice izbere geslo (App PIN).
Imetnik kartice ga lahko na spletni strani za registracijo kadarkoli spremeni.

2.6. Enkratno geslo
Enkratno geslo je naključno izbrano geslo, namenjeno verifikaciji imetnika kartice med postopkom registracije v varnostni mehanizem 3D Secure. Imetnik kartice nadomesti enkratno geslo z geslom 3D Secure, ki ga je določil sam in je znano le njemu oz. pri uporabi mobilne aplikacije PayLife secCheck z izbranim biometričnim identifikatorjem ter geslom za mobilno aplikacijo (App PIN).

2.7. Šifra za avtentikacijo
Šifra za avtentikacijo v smislu Delegirane uredbe Komisije (EU) 2018/389 je ustvarjena šifra za močno avtentikacijo stranke, s katero se dinamično povezuje dejavnost transakcije na daljavo (npr. avtorizacija naloga ali potrditev soglasja imetnika kartice). Oddaljeno transakcijsko geslo mobileTAN je takšna šifra za avtentikacijo.

2.8. Močna avtentikacija stranke
Skladno z Delegirano uredbo Komisije (EU) 2018/389 močna avtentikacija stranke temelji na dveh ali več elementih, ki spadajo v kategorije znanja (npr. geslo), lastništva (npr. pametni telefon) in inherence (npr. prstni odtis, prepoznava obraza), katerih rezultat je ustvarjanje šifre za avtentikacijo.

**3. Registracija v varnostni mehanizem 3D Secure**

3.1. Imetnik kartice se mora za uporabo varnostnega mehanizma 3D Secure predhodno registrirati. Registracijo lahko opravi na spletni strani www.paylife.at/3dsecure, na kateri je potek registracije tudi predstavljen. Za svojo identifikacijo imetnik kartice potrebuje veljavno enkratno geslo in geslo mobileTAN. Geslo mobileTAN prejme po SMS-u na mobilno številko, ki jo je za prejemanje mobileTAN-a navedel kot veljavno.

3.2. Imetnik kartice v postopku registracije sam določi osebne identifikacijske elemente:
- Geslo 3D Secure (Mastercard Identity Check) ali
- s pomočjo mobilne aplikacije PayLife secCheck App biometrični identifikator (npr. prstni odtis) ter geslo za mobilno aplikacijo

Imetnik kartice lahko kadarkoli spremeni svoje osebne identifikatorje. V primeru, da je pozabil geslo, lahko na spletni strani za registracijo določi novo geslo za varnostni mehanizem 3D Secure oz. za mobilno aplikacijo. Za registracijo v varnostni mehanizem pa mora imetnik kartice navesti svoj e- poštni naslov.
Za tehnične nastavitve za brezhibno prejemanje SMS-a in morebitne pripadajoče stroške je odgovoren imetnik kartice.

**4. Plačilni promet z varnostnim mehanizmom 3D Secure**

Elektronske plačilne transakcije lahko imetnik kartice opravi bodisi z geslom 3D Secure, ki si ga je določil sam in z mobileTAN-om ali z uporabo mobilne aplikacije PayLife secCheck z biometričnim identifikatorjem ali z geslom za mobilno aplikacijo.

**5. Odgovornost uporabnika in priporočeni varnostni ukrepi pri uporabi varnostnega mehanizma 3D Secure**

5.1. Upoštevanje predpisov in pravne posledice
Vsak imetnik kartice je dolžan spoštovati določila iz točke 5.4, v kateri je opisana odgovornost uporabnika. Uporabnik se tudi zavezuje spoštovati priporočene varnostne ukrepe, določene v točki 5.5. Banka imetnikom kartic kot potrošnikom priporoča spoštovati priporočene varnostne ukrepe, četudi ti niso izrecno zahtevani. Posledica kršitev teh zahtev je lahko po 6. točki odškodninska odgovornost imetnika kartice ali izguba oz. zmanjšanje odškodninskih zahtevkov do banke.

5.2. Tajnost podatkov in blokiranje dostopa

5.2.1 Imetnik kartice je dolžan, da geslo 3D Secure in geslo za mobilno aplikacijo zaščiti na način, da je nepooblaščenim tretjim osebam dostop onemogočen; dolžnost se ne nanaša na e-poštni naslov. Za zagotavljanje storitev za imetnika kartice je posredovanje osebnih identifikacijskih elementov ponudnikom storitev odreditve plačil in ponudnikom storitev zagotavljanja informacij o računih, kadar je to ustrezno, dovoljeno.

5.2.2. V izogib zlorabam je imetnik kartice dolžan poskrbeti za varno hrambo in uporabo gesel za 3D Secure in mobilno aplikacijo. Posebej mora paziti, da do gesel ni mogoče dostopati na nepooblaščen in enostaven način. To pomeni tudi, da gesel ne sme shraniti v mobilnih končnih napravah, na katerih ima inštalirano mobilno aplikacijo PayLife secCheck oz. teh ne sme zapisati, npr. v mobilni beležnici.

5.2.3. V primeru izgube gesla za 3D Secure in/ali mobilno aplikacijo, kot tudi, ko imetnik kartice zazna zlonamerno ali drugo nepooblaščeno uporabo postopka 3D Secure, nemudoma zahteva blokiranje dostopa do varnostnega mehanizma 3D Secure.

5.2.4. V primeru izgube ali kraje mobilne končne naprave, na kateri je inštalirana aplikacija PayLife secCheck, imetnik kartice nemudoma poskrbi za blokiranje dostopa do varnostnega mehanizma 3D Secure.

5.3. Onemogočanje nedovoljenega upravljanja z mobilno končno napravo in odgovornost ob namestitvi

5.3.1. Dolžnost imetnika kartice je, da nepooblaščenim osebam onemogoči upravljanje z mobilno končno napravo, na kateri je nameščena aplikacija PayLife secCheck, oz. dostop do shranjenih podatkov, v času, ko je ne uporablja.

5.3.2. Imetnik kartice lahko prenese aplikacijo PayLife secCheck izključno s spletnih portalov Apple App ali Google Play.

5.4. Preverjanje podatkov pri plačilnih transakcijah

5.4.1. Potrditev plačila z oddaljenim transakcijskim geslom (mobileTAN)

Imetnik kartice pred uporabo mobileTAN-a preveri pravilnost prikazanih podatkov. Geslo se lahko v postopkih spletnega plačevanja vnese le, če so navedeni podatki plačila točni in se skladajo z oddanim nalogom.

5.4.2. Potrditev plačilne transakcije s PayLife secCheck
Imetnik kartice preveri točnost posredovanih podatkov v aplikaciji PayLife secCheck. Plačilno transakcijo potrdi le, če se navedeni podatki skladajo z oddanim nalogom.

5.5. Priporočeni varnostni ukrepi pri uporabi elektronskega plačilnega postopka 3D Secure

5.5.1. Priporočljivo je, da imetnik kartice redno uporablja gesla za 3D Secure in mobilno aplikacijo (App PIN), ter poskrbi za spremembo gesel vsaj vsake dva meseca.

5.5.2 Priporočljivo je, da imetnik kartice nemudoma sproži blokiranje postopka 3D Secure, ko obstaja možnost, da so nepooblaščene tretje osebe pridobili dostop do gesel za 3D Secure in/ali mobilno aplikacijo, ali v drugih okoliščinah, ko bi lahko prišlo do takšne zlorabe.

5.5.3. Priporočljivo je, da imetnik kartice svojo končno mobilno napravo, na kateri prejema mobileTAN in/ali ima inštalirano aplikacijo PayLife secCheck, zaščiti glede spletnih nevarnosti tako, da ima nameščeno najnovejšo antivirusno zaščito in da redno posodablja operacijski sistem svoje mobilne končne naprave.

## 6. Jamstvo imetnika kartice

6.1. Imetnik kartice jamči za celotno škodo nastalo z nepooblaščenim spletnim nakupom, ki jo je povzročil banki z naklepnim ali hudo malomarnim ravnanjem in s tem kršil dolžnosti iz 5. točke. V primerih, ko za goljufivo ali naklepno ravnanje ter posledično nespoštovanje odgovornosti iz 5. točke ni odgovoren imetnik kartice, je pri morebitni delitvi škode med imetnikom kartice in banko treba upoštevati predvsem vrsto osebnih identifikacijskih elementov, kot tudi posebne okoliščine, v katerih je prišlo do zlorabe kartice.

6.2. Ne glede na določbe iz točke 6.1 imetnik kartice za lahko malomarno ravnanje in s tem kršitev dolžnosti iz 5. točke, za izgubo ali krajo osebnih identifikacijskih elementov, ki jih pred opravljanjem plačila ni bilo moč opaziti, ne jamči. Imetnik kartice za lahko malomarno ravnanje in posledično kršitev dolžnosti iz 5. točke tudi ne jamči, če je krivda za izgubo osebnih identifikacijskih elementov na strani banke.

6.3. Ne glede na določbe iz točke 6.1 imetnik kartice ne jamči, če banka v primeru, ko je prišlo do zlorabe ali druge nepooblaščene uporabe kartice ob spletnem nakupu ne zahteva nobene močne avtentikacije stranke (t.j., da je bil spletni nakup opravljen brez izvedenega varnostnega postopka 3D Secure). Imetnik kartice, ki je omogočil nepooblaščeno uporabo kartice na goljufiv način, jamči, ne glede na to ali je banka zahtevala močno avtentikacijo stranke ali ne.

6.4. Imetnik kartice ne jamči, če je škoda, ki izvira iz nepooblaščenega spletnega nakupa nastala po oddanem zahtevku za blokiranje iz točke 7, razen v primerih, ko je imetnik kartice ravnal na goljufiv način.

## 7. Blokiranje dostopa do varnostnega mehanizma 3D Secure

7.1. Samodejno blokiranje
Iz varnostnih razlogov se po zaporednih petih napačnih vnosih osebnega avtentikacijskega elementa blokira dostop do varnostnega mehanizma 3D Secure. V času trajanja blokade imetnik kartice ne more izvesti plačilnih transakcij s postopkom 3D Secure.

7.2. Blokiranje sproži imetnik kartice
Blokiranje varnostnega mehanizma 3D Secure lahko imetnik kartice sproži sam s petimi zaporednimi napačnimi vnosi osebnega avtentikacijskega elementa ali to kadarkoli zahteva na telefonski številki +43 (0)5 99 06 62 20.

7.3. Blokiranje sproži banka

7.3.1. Banka je pooblaščena, da za imetnika kartice izvede blokado varnostnega mehanizma 3D Secure, če obstajajo objektivni razlogi v zvezi z varnostjo ali pa sum na nepooblaščeno ali goljufivo uporabo.

7.3.2. Banka imetnika kartice z blokiranjem varnostnega mehanizma 3D Secure in njegovimi razlogi seznani pred, najkasneje pa takoj po blokadi, če z obvestilom o blokadi ali o razlogih ni v nasprotju s sodno ali upravno odredbo oz. z avstrijskim ali pravnim redom Skupnosti ali so v nasprotju z varnostnimi razlogi.

7.4. Seznanitev in preklic blokade

7.4.1. Preden postane blokada dokončna, imetnik kartice o njej prejme opozorilo.

7.4.2. Banka blokado v skladu s točko 7.3 prekliče, takoj ko zanjo ne obstajajo več razlogi. Banka imetnika kartice o preklicu blokade takoj obvesti.

7.4.3 Imetnik kartice lahko preklic blokade zahteva kadarkoli na telefonski številki +43 (0)5 99 06 62 20.

## 8. Sprememba Posebnih pogojev poslovanja za uporabo varnostnega mehanizma 3D Secure za predplačniške kartice z možnostjo polnitve

8.1. Banka ponudi imetniku kartice predvidene spremembe Posebnih pogojev 3DS vsaj dva meseca pred začetkom uveljavitve sprememb, stare določbe in predlagane nove spremembe pa prikaže v preglednici, ki je priloga k novi spremenjeni ponudbi, ki jo prejme imetnik kartice. Če imetnik kartice do začetka uveljavitve banki pisno ali po elektronski pošti ne sporoči svojega nestrinjanja glede spremenjene ponudbe, se smatra, da se strinja s spremembami.
Banka imetnika kartice v novi spremenjeni ponudbi opozori na obliko tihega strinjanja, ki nastopi, ko imetnik kartice banki ne izrazi nestrinjanja glede sprememb na pisni ali drug dogovorjeni elektronski način. Prav tako banka imetnika kartice opozori, da ima ta kot potrošnik pravico, da lahko dogovor o uporabi varnostnega mehanizma 3D Secure, kot tudi kreditno pogodbo pred začetkom uveljavitve sprememb takoj prekine. Banka bo prav tako na svojem spletnem mestu objavila primerjalno preglednico določb, kot tudi novo posodobljeno verzijo Posebnih pogojev. Imetniku kartice bo na njegovo zahtevo tudi posredovala novo verzijo Posebnih pogojev, in ga o tej možnosti seznanila v ponudbi sprememb.

8.2. Imetnik kartice je lahko o ponujeni spremembi obveščen v dogovorjeni obliki. Med dogovorjene oblike obveščanja o ponudbi sprememb vključno s primerjalno preglednico se šteje tudi e-poštni naslov, ki ga je imetnik kartice posredoval banki.

8.3. Sprememba pogojev je vezana na objektivno razloge. O objektivni utemeljenosti govorimo,

(i) ko je sprememba potrebna zaradi spremembe ključnih zakonskih določil ali navodil avstrijskega Urada za nadzor finančnega trga, Evropskega bančnega organa, Evropske centralne banke ali avstrijske narodne banke,

(ii) ko je sprememba vezana na spremembe v pravni podlagi za potek plačilnih poslov,

(iii) ko je sprememba smiselna zaradi sprememb v varnosti bančnega poslovanja ali v poteku poslovanja z imetnikom kartice glede uporabe varnostnega mehanizma 3D Secure,

(iv) ko je sprememba potrebna zaradi tehničnih posodobitev ali prilagoditev programov za uporabo končnih naprav,

(v) ko je sprememba potrebna zaradi zakonske spremembe za dodelitev naročil in za oddajo izjav o uporabi varnostnega mehanizma 3D Secure,

(vi) ko je sprememba potrebna zaradi sprememb v zakonskih določilih za bančno poslovanje imetnika kartice z uporabo varnostnega mehanizma 3D Secure.

Morebitna sprememba Posebnih pogojev ne predstavlja uvedbe ali spreminjanja dogovorjenih stroškov.

## 9. Sprememba e-poštnega naslova in mobilne številke imetnika kartice

Imetnik kartice je dolžan, da banki vsako spremembo svojega e-poštnega naslova in svoje mobilne številke sporoči pisno ali po elektronski pošti. Določbe v 16. členu Splošnih pogojev poslovanje ostanejo nespremenjene.

## 10. Varnostna opozorila

10.1. V času blokade varnostnega mehanizma 3D Secure, kartice ni možno uporabljati za plačilo spletnih nakupov pri tistih trgovcih, ki uporabljajo tak postopek.

10.2. Za preprečitev tveganj, povezana z osebnimi identifikacijskimi elementi (predvsem geslo za varnostni mehanizem 3D Secure), banka svetuje redno spreminjanje (npr. vsak mesec).

10.3. V primeru, da bi imetnik kartice posumil, da so nepooblaščene tretje osebe pridobile dostop do osebnih identifikacijskih elementov (predvsem do gesla za 3D Secure), banka svetuje zamenjavo osebnih identifikacijskih elementov.
10.4. Priporočljivo je, da se dostop do podatkov na mobilni končni napravi zaščiti. V primeru izgube ali kraje banka svetuje, da ponudnik mobilnih storitev blokira SIM kartico.
10.5. Upoštevati je treba, da predstavlja uporaba gesel na skupnih računalnikih in mobilnih končnih postajah (npr. v internetnih kavarnah, v hotelu, na delovnem mestu) varnostno tveganje, saj jih lahko izsledijo nepooblaščene tretje osebe.
10.6. Banka na spletni strani www.paylife.at ponuja v meniju pod točko „Service“ dodatne informacije o varnih sistemih in daje varnostne nasvete.

**11. Pogodbena doba, odpoved in prekinitev**

11.1. Dogovor o uporabi varnostnega mehanizma 3D Secure je sklenjen za nedoločen čas.
11.2. Imetnik kartice je upravičen, da lahko dogovor kadarkoli brez navedbe razloga in brez odpovednega roka odpove. Po prejemu obvestila o odpovedi bo banka blokirala dostop do postopka 3D Secure.
11.3. Banka je upravičena, da lahko dogovor kadarkoli upoštevaje dvomesečnega roka brez razloga odpove.
11.4 Tako imetnik kartice kot tudi banka imata pravico, da lahko dogovor kadarkoli iz pomembnih razlogov s takojšnjim učinkom prekineta.
11.5 Prekinitev dogovora ne vpliva na kreditno pogodbo, razen ko se imetnik kartice in banka ne dogovorita hkrati tudi za njeno prekinitev.
11.6 Dogovor avtomatsko preneha z iztekom kreditne pogodbe.

različica september 2019, stanje marec 2020