Posebni pogoji poslovanja za uporabo varnega sistema 3D Secure	Posebni pogoji poslovanja za uporabo varnostnega mehanizma 3D Secure za predplačniške kartice z možnostjo polnitve PayLife
Preambula Posebni pogoji poslovanja za uporabo varnega sistema 3D Secure (v nadaljevanju: posebni pogoji) dopolnjujejo Splošne pogoje poslovanja (splošni pogoji) za predplačniške kartice PayLife z možnostjo polnitve (v nadaljevanju: kartica) in so sestavni del sklenjene kartične pogodbe med družbo easybank AG (v nadaljevanju: Bank) in imetnikom kartice. Pravno podlago predstavljajo avstrijski Zakon o plačilnih storitvah (Zahlungsdienstegesetz ZaDiG) in avstrijski Zakon o finančnih storitvah na daljavo (Fernfinanzdienstleistungs-Gesetz FernFinG) v povezavi z ZaDiG-om, s katerimi je bil imetnik kartice seznanjen pred sklenitvijo pogodbe. Predpogodbene informacije so dostopne na spletni strani www.paylife.at/agb. Informacije tudi v vsakokratni različici dopolnjujejo veljavne posebne pogoje o storitvah SMS obveščanja, ki jih ponuja Bank. S posebnimi pogoji sta urejena prijava in potek plačilnega prometa v varnih sistemih. Postopek registracije v varne sisteme se opravi bodisi preko spletne strani www.paylife.at/3dsecure bodisi v elektronskem plačilnem postopku na internetu.	**Preambula** ~~Posebni pogoji poslovanja za uporabo varnega sistema 3D Secure~~ ~~(v nadaljevanju: posebni pogoji) dopolnjujejo Splošne pogoje poslovanja~~ ~~(splošni pogoji) za predplačniške kartice PayLife z možnostjo polnitve~~ ~~(v nadaljevanju: kartica) in so sestavni del sklenjene kartične pogodbe~~ ~~med družbo easybank AG (v nadaljevanju: Bank) in imetnikom kartice.~~ ~~Pravno podlago predstavljajo avstrijski Zakon o plačilnih storitvah~~ ~~(Zahlungsdienstegesetz ZaDiG) in avstrijski Zakon o finančnih storitvah na~~ ~~daljavo (Fernfinanzdienstleistungs-Gesetz FernFinG) v povezavi z ZaDiG-om,~~ ~~s katerimi je bil imetnik kartice seznanjen pred sklenitvijo pogodbe.~~ ~~Predpogodbene informacije so dostopne na spletni strani www.paylife.at/agb.~~ ~~Informacije tudi v vsakokratni različici dopolnjujejo veljavne posebne pogoje o~~ ~~storitvah SMS obveščanja, ki jih ponuja Bank.~~ ~~S posebnimi pogoji sta urejena prijava in potek plačilnega prometa v varnih~~ ~~sistemih. Postopek registracije v varne sisteme se opravi bodisi preko spletne~~ ~~strani www.paylife.at/3dsecure bodisi v elektronskem plačilnem postopku na~~ ~~internetu.~~ S Posebnimi pogoji poslovanja za uporabo varnostnega mehanizma 3D Secure za predplačniške kartice z možnostjo polnitve PayLife (v nadaljevanju: Posebni pogoji) je urejen potek plačilnega prometa s predplačniškimi karticami z možnostjo polnitve PayLife v varnem sistemu 3D Secure. Posebni pogoji veljajo, ko je veljavnost dogovorjena. So del Splošnih pogojev poslovanja za uporabo predplačniških kartic z možnostjo polnitve PayLife (v nadaljevanju: Splošni pogoji), ki so osnova za sklenitev kartične pogodbe o izdaji predplačniške kartice z možnostjo polnitve PayLife (v nadaljevanju: kartica) med družbo easybank AG (v nadaljevanju: banka) in imetnikom kartice.
1.1. Varnostni mehanizem Mastercard SecureCode	1.1. Varnostni mehanizem Mastercard ~~SecureCode~~ Identity Check
1.2. Oddaljeno transakcijsko geslo (v nadaljevanju: mobileTAN) Oddaljeno transakcijsko geslo mobileTAN, vezano na mobilno končno napravo (npr. mobilni telefon, tablični računalnik), je enkratno dodeljeno geslo za namen opravljanja oddaljenih transakcij in služi kot dodatna identifikacija pri kartičnem poslovanju z varnostnim mehanizmom Mastercard SecureCode. Vnos gesla mobileTAN je potreben tudi pri registraciji v varnostni mehanizem 3D Secure in pri nekaterih spremembah podatkov v 3D Secure upravljanje računa. Na spletni strani www.paylife.at so vam v meniju »Service« na voljo dodatne informacije o spletnih storitvah družbe Bank.	1.2. Oddaljeno transakcijsko geslo mobileTAN (v nadaljevanju: mobileTAN) ~~Oddaljeno transakcijsko geslo mobileTAN, vezano na mobilno končno~~ ~~napravo (npr. mobilni telefon, tablični računalnik), je enkratno dodeljeno~~ ~~geslo za namen opravljanja oddaljenih transakcij in služi kot dodatna~~ ~~identifikacija pri kartičnem poslovanju z varnostnim mehanizmom~~ ~~Mastercard SecureCode. Vnos gesla mobileTAN je potreben tudi~~ ~~pri registraciji v varnostni mehanizem 3D Secure in pri nekaterih~~ ~~spremembah podatkov v 3D Secure upravljanje računa. Na spletni strani~~ ~~www.paylife.at so vam v meniju »Service« na voljo dodatne informacije o~~ ~~1.3. spletnih storitvah družbe Bank.~~

	mobileTAN je enkratno dodeljeno transakcijsko geslo, ki služi kot dodatna identifikacija pri kartičnih plačilih z geslom za preverjanje istovetnosti (Mastercard Identity Check). Geslo mobileTAN je potrebno vnesti tudi pri registraciji v varnostni mehanizem 3D Secure in pri določenih spremembah podatkov v 3D Secure upravljanje računa. Imetnik kartice geslo mobileTAN prejme po SMS-u na mobilno številko, ki jo je za prejemanje mobileTAN-a navedel banki kot veljavno.
	1.4. 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.
	1.5. Močna avtentikacija stranke Delegirana uredba Komisije (EU) 2018/389 ureja postopek močne avtentikacije stranke. Ta 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.
1.4. Varni sistemi	1.6. ~~Varni sistemi~~ 3D Secure
1.4.1. Varnostni mehanizem 3D Secure Varnostni mehanizem 3D Secure se uporablja v postopkih spletnega plačevanja z namenom, da imetnika kartice prepozna kot nedvoumnega zakonitega imetnika kartice. 1.4.2. Varen aplikacijski protokol »https« za prenos hiperteksta Varen aplikacijski protokol služi kriptiranju podatkov imetnika kartice in zanj specifične varnostne nastavitve, da jih ne bi izsledile in zlorabile tretje osebe.	~~1.4.1. Varnostni mehanizem 3D Secure~~ ~~Varnostni mehanizem 3D Secure se uporablja v postopkih spletnega plačevanja z namenom, da imetnika kartice prepozna kot nedvoumnega zakonitega imetnika kartice.~~ ~~1.4.2. Varen aplikacijski protokol »https« za prenos hiperteksta~~ ~~Varen aplikacijski protokol služi kriptiranju podatkov imetnika kartice in zanj specifične varnostne nastavitve, da jih ne bi izsledile in zlorabile tretje osebe.~~ Varnostni mehanizem 3D Secure je varen postopek za opravljanje spletnega plačevanja, ki izpolnjuje zahteve močne avtentikacije stranke.
2.1. Registracija Imetnik kartice se mora za uporabo varnostnega mehanizma 3D Secure prehodno registrirati. Registracijo je možno opraviti na spletni strani www.paylife.at/3dsecure, možno jo je opraviti tudi med postopkom spletnega plačila pri trgovcu (pogodbena firma), ki omogoča uporabo varnostnega mehanizma 3D Secure.	2.1. Registracija Imetnik kartice se mora za uporabo varnostnega mehanizma 3D Secure predhodno registrirati. Registracijo ~~je možno opraviti na spletni strani~~ lahko opravi na spletni strani www.paylife.at/3dsecure.
Imetnik kartice prejme geslo mobileTAN po SMS-u, na mobilno številko, ki jo je navedel kot veljavno. Družba Bank si pridržuje pravico, da ponudi dodatne načine posredovanja gesla mobileTAN, katere so predstavljene na spletni strani www.paylife.at/3dsecure.	~~Imetnik kartice prejme geslo mobileTAN po SMS-u, na mobilno številko, ki jo je navedel kot veljavno. Družba Bank si pridržuje pravico, da ponudi dodatne načine posredovanja gesla mobileTAN, katere so predstavljene na spletni strani www.paylife.at/3dsecure.~~ Imetnik kartice prejme mobiTAN po SMS-u na mobilno številko, ki jo je za prejemanje navedel kot veljavno, ali na drug, v postopku registracije, dogovorjeni način.
2.2. V postopku registracije v varnostni mehanizem 3D Secure bodo	~~2.2. V postopku registracije v varnostni mehanizem 3D Secure bodo~~

imetniku kartice na voljo pričujoči posebni pogoji. Za nadaljnji postopek registracije se od imetnika kartice zahteva, da se strinja s posebnimi pogoji na označenem mestu, s čimer se vzpostavi dogovor o uporabi varnega sistema (v nadaljevanju: dogovor).	~~imetniku kartice na voljo pričujoči posebni pogoji. Za nadaljnji postopek registracije se od imetnika kartice zahteva, da se strinja s posebnimi pogoji na označenem mestu, s čimer se vzpostavi dogovor o uporabi varnega sistema (v nadaljevanju: dogovor).~~
2.3. Imetnik kartice v postopku registracije sam določi naslednje identifikacijske podatke: uporabniško ime • geslo (Mastercard SecureCode) • osebno sporočilo (se pojavi za namen kontrole ob vsakokratnem preverjanju gesla) Imetnik kartice lahko identifikacijske podatke kadarkoli sam spremeni. Če je izbrano geslo pozabil, se lahko v skladu s točko 2.1. ponovno registrira in si v postopku določi novo geslo. Za uporabo storitve varnostnega mehanizma 3D Secure je potrebno navesti mobilno številko in e-poštni naslov. Morebitne stroške, ki bi nastale zaradi prejemanja SMS-ov nosi imetnik kartice.	2.2. Imetnik kartice v postopku registracije sam določi naslednje elemente: • uporabniško ime • geslo (Mastercard SecureCode) • osebno sporočilo (se pojavi za namen kontrole ob vsakokratnem preverjanju gesla) ~~Imetnik kartice lahko identifikacijske podatke kadarkoli sam spremeni. Če je izbrano geslo pozabil, se lahko v skladu s točko 2.1. ponovno registrira in si v postopku določi novo geslo. Za uporabo storitve varnostnega mehanizma 3D Secure je potrebno navesti mobilno številko in e-poštni naslov. Morebitne stroške, ki bi nastale zaradi prejemanja SMS-ov nosi imetnik kartice.~~ Imetnik kartice lahko kadarkoli spremeni uporabniško ime, geslo in osebni pozdrav. V primeru, da je geslo, ki si ga je določil sam, pozabil, lahko skladno s točko 2.1. v postopku ponovne registracije in obnovitve gesla določi novo geslo.
3. Plačevanje z varnimi sistemi 3.1. Imetnik kartice naj pri uporabi kartice na internetu (e-commerce) za izvedbo plačilnih zahtevkov uporablja varne sisteme. Uporablja naj varnostni mehanizem 3D Secure (Mastercard SecureCode) in varen aplikacijski protokol »https« (varen protokol za prenos hiperteksta), če trgovec (pogodbena firma) ponuja tovrstne tehnične možnosti. 3.2. Imetnik kartice lahko plačilne transakcije opravi v varnih sistemih z geslom, ki si ga je določil sam in z geslom mobileTAN. Pred uporabo mobileTAN-a naj preveri pravilnost podatkov, ki so mu bili posredovani preko SMS-a. Geslo mobileTAN lahko za potrditev naročila uporabi le, če so podatki prejeti po SMS-u skladni z njegovim zahtevkom. V kolikor imetnik kartice opazi odstopanja podatkov v SMS-u od poslanega zahtevka, mora o tem nemudoma obvestiti družbo Bank na tel. številko +43 (0)5 99 06-6220 in plačilni postopek prekiniti. V primeru, da imetnik kartice plačilni postopek vseeno izvede, je s tem lahko sokriv za morebitno škodo. 3.3. V kolikor je trgovec vključen v postopek plačevanja z varnostnim mehanizmom 3D Secure, je imetnik kartice dolžan transakcijo opraviti z uporabo tega mehanizma. 3.4. Transakcija, predvsem zahtevek, je izvedena ob uporabi varnega sistema v skladu s 7. členom Splošnih pogojev poslovanja, ki so del pogodbe o predplačniški kartici. V kolikor pa je uporabljen varnostni mehanizem 3D Secure, imetnik kartice uporabi geslo, ki ga je določil sam in geslo mobileTAN. S potrditvijo vnosa lastnega gesla in generiranega gesla mobileTAN je zahtevek nepreklicno izveden.	~~**3. Plačevanje z varnimi sistemi** 3.1. Imetnik kartice naj pri uporabi kartice na internetu (e-commerce) za izvedbo plačilnih zahtevkov uporablja varne sisteme. Uporablja naj varnostni mehanizem 3D Secure (Mastercard SecureCode) in varen aplikacijski protokol »https« (varen protokol za prenos hiperteksta), če trgovec (pogodbena firma) ponuja tovrstne tehnične možnosti. 3.2. Imetnik kartice lahko plačilne transakcije opravi v varnih sistemih z geslom, ki si ga je določil sam in z geslom mobileTAN. Pred uporabo mobileTAN-a naj preveri pravilnost podatkov, ki so mu bili posredovani preko SMS-a. Geslo mobileTAN lahko za potrditev naročila uporabi le, če so podatki prejeti po SMS-u skladni z njegovim zahtevkom. V kolikor imetnik kartice opazi odstopanja podatkov v SMS-u od poslanega zahtevka, mora o tem nemudoma obvestiti družbo Bank na tel. številko +43 (0)5 99 06-6220 in plačilni postopek prekiniti. V primeru, da imetnik kartice plačilni postopek vseeno izvede, je s tem lahko sokriv za morebitno škodo.~~ **3. Plačilni promet z varnostnim mehanizmom 3D Secure** 3.1. Elektronske plačilne transakcije lahko imetnik kartice opravi z geslom 3D Secure, ki si ga je določil sam (Mastercard Identity Check) in z mobileTAN-om. Imetnik kartice pred uporabo mobileTAN-a preveri pravilnost prikazanih podatkov o avtorizaciji naloga. 3.2. Skladno s točko 7 Splošnih pogojev poslovanja lahko imetnik kartice z uporabo varnostnega mehanizma 3D Secure izvede zahtevek. Z vnosom gesla in mobileTAN-a v 3D Secure postopek je zahtevek imetnika kartice nepreklicno izveden.

	3.3. V kolikor je trgovec vključen v postopek plačevanja z varnostnim mehanizmom 3D Secure, je imetnik kartice dolžan transakcijo opraviti z uporabo tega mehanizma. 3.4. Transakcija, predvsem zahtevek, je izvedena ob uporabi varnega sistema v skladu s 7. členom Splošnih pogojev poslovanja, ki so del pogodbe o predplačniški kartici. V kolikor pa je uporabljen varnostni mehanizem 3D Secure, imetnik kartice uporabi geslo, ki ga je določil sam in geslo mobileTAN. S potrditvijo vnosa lastnega gesla in generiranega gesla mobileTAN je zahtevek nepreklicno izveden.
4. Tajnost podatkov Uporabnik kartice je dolžan, da identifikacijske podatke, navedene pod točko 2.3 in mobileTAN zaščiti na način, da je nepooblaščenim tretjim osebam dostop onemogočen. V primeru, da pride do kršitve te dolžnosti, imetnik kartice odgovarja za nastalo škodo, pri čemer je odgovornost pri lahki malomarnosti omejena na 50 EUR.	**4. Tajnost podatkov** Uporabnik kartice je dolžan, da identifikacijske podatke, navedene pod točko 2.3 in mobileTAN zaščiti na način, da je nepooblaščenim tretjim osebam dostop onemogočen. V primeru, da pride do kršitve te dolžnosti, imetnik kartice odgovarja za nastalo škodo, pri čemer je odgovornost pri lahki malomarnosti omejena na 50 EUR. **4. Dolžnost odgovornega ravnanja imetnika kartice** 4.1. Uporabnik kartice je dolžan, da svoje osebne identifikacijske elemente (geslo, mobileTan, enkratno geslo, osebno dostopna koda) zaščiti na način, da je dostop nepooblaščenim tretjim osebam ali na drug način onemogočen. 4.2. V izogib zlorabam in nepooblaščenim spletnim nakupom je imetnik kartice dolžan poskrbeti za varno hrambo in uporabo osebnih identifikacijskih elementov. Posebej mora paziti, da ob uporabi osebnih identifikacijskih elementov do njih ni mogoče dostopati na nepooblaščen in enostaven način. Gesel ne sme zapisati oz. shraniti (npr. v mobilno beležnico) ne v naprave, s katerimi izvaja spletne nakupe niti v mobilne končne naprave, v katere prejema identifikacijske elemente. 4.3. V primeru izgube ali kraje osebnih identifikacijskih elementov, kot tudi ko imetnik kartice zazna zlonamerno ali drugo nepooblaščeno uporabo kartice za spletne nakupe, mora imetnik kartice nemudoma zahtevati blokiranje dostopa do varnostnega mehanizma 3D Secure. 4.4. Imetnik kartice pred uporabo mobileTAN-a preveri pravilnost prikazanih podatkov. Geslo mobileTan se v postopku spletnega plačevanja vnese le, če se posredovani podatki po SMS-ju skladajo z oddanim nalogom.
	5. Jamstvo imetnika kartice 5.1. 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 4. točke. V primerih, ko za goljufivo ali naklepno ravnanje ter posledično nespoštovanje odgovornosti iz 4. 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.

	5.2. Imetnik kartice za izgubo ali krajo osebnih identifikacijskih elementov, ki jih pred opravljanjem plačila ni bilo moč opaziti, za lahko malomarno ravnanje in s tem kršitev dolžnosti iz 4. točke ne jamči. Imetnik kartice za lahko malomarno ravnanje in posledično kršitev dolžnosti iz 4. točke tudi ne jamči, če je krivda za izgubo osebnih identifikacijskih elementov na strani banke. 5.3. Ne glede na določbe iz točke 5.1 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. 5.4. Imetnik kartice ne jamči, če je škoda, ki izvira iz nepooblaščenega spletnega nakupa nastala po oddanem zahtevku za blokiranje iz točke 6, razen v primerih, ko je imetnik kartice ravnal na goljufiv način.
5. Blokiranje dostopa	~~5.~~ **6. Blokiranje dostopa**
5.1. Družba Bank iz varnostnih razlogov po šestkratnem napačnem vnosu gesla blokira dostop do varnostnega mehanizma 3D Secure. V času trajanje blokade, imetnik kartice le-te ne more uporabljati za opravljanje plačilnih transakcij z varnostnim mehanizmom 3D Secure. V tem primeru imetnik kartice zaprosi pri družbi Bank za preklic blokade pisno (po e-pošti) ali telefonsko. To naredi na e-poštni naslov: paylife24@paylife.at ali na telefon +43 (0)5 99 06-6220. 5.2. V primeru, ko uporabnik kartice ve ali sumi, da so tretje osebe pridobile informacije o dostopnih podatkih (predvsem o geslu), Bank priporoča spremembo dostopnih podatkov. V kolikor imetnik kartice iz kakršnih koli razlogov za to nima možnosti, ima pravico zahtevati, da mu Bank nemudoma blokira dostop. Bank je dolžan zahtevek opraviti takoj po prejemu zahtevka.	6.1. Družba Bank iz varnostnih razlogov po šestkratnem napačnem vnosu gesla blokira dostop do varnostnega mehanizma 3D Secure. ~~V času trajanje blokade, imetnik kartice le-te ne more uporabljati za opravljanje plačilnih transakcij z varnostnim mehanizmom 3D Secure. V tem primeru imetnik kartice zaprosi pri družbi Bank za preklic blokade pisno (po e-pošti) ali telefonsko. To naredi na e-poštni naslov: paylife24@paylife.at ali na telefon +43 (0)5 99 06-6220.~~ 6.2. ~~V primeru, ko uporabnik kartice ve ali sumi, da so tretje osebe pridobile informacije o dostopnih podatkih (predvsem o geslu), Bank priporoča spremembo dostopnih podatkov. V kolikor imetnik kartice iz kakršnih koli razlogov za to nima možnosti, ima pravico zahtevati, da mu Bank nemudoma blokira dostop. Bank je dolžan zahtevek opraviti takoj po prejemu zahtevka.~~ Imetnik kartice lahko blokado za dostop do varnostnega mehanizma 3D Secure zahteva kadarkoli na telefonski številki +43 (0)5 99 06 62 20. 6.3. Banka je pooblaščena, da izvede blokado varnostnega mehanizma 3D Secure, če obstajajo objektivni razlogi v zvezi z varnostjo ali pa obstaja sum na nepooblaščeno ali goljufivo uporabo. 6.4. Banka imetnika kartice o blokiranju dostopa do varnostnega mehanizma 3D Secure in o razlogih zanj seznani pred, najkasneje pa takoj po blokadi, če z obvestilom o blokadi ali o razlogih ni v nasprotju s sodnimi oz. upravnimi določili ali bi lahko informacija o blokadi povečala varnostno tveganje ali je bila blokada izvedena na željo imetnika kartice.

	6.5. V času blokade, kartice ni možno uporabljati za transakcije z varnostnim mehanizmom 3D Secure. 6.6. Imetnik kartice lahko banko o zahtevi za preklic blokade obvesti pisno (po elektronski pošti) ali po telefonu. To lahko stori na e-poštni naslov paylife24@paylife.at oz. na telefonsko številko +43 (0)5 99 06 62 20. 6.7. Banka blokado odpravi takoj, ko zanjo ne obstajajo več razlogi ali ko imetnik kartice zahteva odpravo blokade.
Splošni pogoji poslovanja in varnostne nastavitve 6.1. Spremembe posebnih pogojev 6.1.1. Spremembe posebnih pogojev se imetniku kartice sporočijo na e-poštni oz. hišni naslov, ki ga je družbi Bank posredoval sam, pri čemer se upoštevajo zadnji posredovani podatki. Imetnik kartice opravi komunikacijo v papirnati obliki oz. po predhodnem dogovoru na drug trajen nosilec podatkov (npr. e-pošta). Pri navedenem se ustrezno uporabljajo določila točke 15 splošnih pogojev. 6.2. Sprememba naslova, e-poštnega naslova in mobilne številke imetnika kartice Imetnik kartice je dolžan družbo Bank pisno obvestiti o vsaki spremembi svojega naslova, e-poštnega naslova in mobilne številke. Določilo v točki 16 splošnih pogojev se pri tem ne upošteva. 6.3. Varnostne nastavitve 6.3.1. V kolikor je dostop do varnih sistemov blokiran, kartice ni možno uporabljati na internetu pri elektronskem plačilu trgovcem, če ti v postopku uporabljajo le varnostni mehanizem 3D Secure. 6.3.2. V izogib situacijam, ki so povezane z varnostnim sistemom Mastercard SecureCode, družba Bank svetuje, da geslo redno (npr. vsak mesec) spremenite. 6.3.3. Priporočeno je, da zavarujete dostop do svojih mobilnih končnih naprav. V primeru izgube ali kraje mobilne končne naprave, družba Bank svetuje, da pri svojemu mobilnem operaterju zahtevate blokado SIM kartice. 6.3.4. Pazite, da z uporabo gesel na skupnih računalnikih in mobilnih končnih napravah (npr. v internetni kavarni, v hotelu, na delovnem mestu), tretjim osebam ne omogočate dostopa na nepooblaščen in enostaven način. 6.3.5. Računalnik in mobilne končne naprave naj bodo opremljene z najnovejšo protivirusno zaščito, s posodobljeno programsko opremo kot tudi s požarnim zidom. Na ta način tretjim osebam znatno zmanjšamo možnost odkrivanja in zlorabe podatkov. 6.3.6. Na spletni strani družbe Bank www.paylife.at so vam v meniju „Service“ na voljo informacije o varnih sistemih in varnostnih nastavitvah.	~~**Splošni pogoji poslovanja in varnostne nastavitve**~~ ~~6.1. Spremembe posebnih pogojev~~ ~~6.1.1. Spremembe posebnih pogojev se imetniku kartice sporočijo na~~ ~~e-poštni oz. hišni naslov, ki ga je družbi Bank posredoval sam, pri~~ ~~čemer se upoštevajo zadnji posredovani podatki. Imetnik kartice~~ ~~opravi komunikacijo v papirnati obliki oz. po predhodnem dogovoru~~ ~~na drug trajen nosilec podatkov (npr. e-pošta). Pri navedenem se~~ ~~ustrezno uporabljajo določila točke 15 splošnih pogojev.~~ ~~6.2. Sprememba naslova, e-poštnega naslova in mobilne številke imetnika~~ ~~kartice~~ ~~Imetnik kartice je dolžan družbo Bank pisno obvestiti o vsaki spremembi~~ ~~svojega naslova, e-poštnega naslova in mobilne številke. Določilo v~~ ~~točki 16 splošnih pogojev se pri tem ne upošteva.~~ ~~6.3. Varnostne nastavitve~~ ~~6.3.1. V kolikor je dostop do varnih sistemov blokiran, kartice ni možno~~ ~~uporabljati na internetu pri elektronskem plačilu trgovcem, če ti v~~ ~~postopku uporabljajo le varnostni mehanizem 3D Secure.~~ ~~6.3.2. V izogib situacijam, ki so povezane z varnostnim sistemom~~ ~~Mastercard SecureCode, družba Bank svetuje, da geslo redno (npr.~~ ~~vsak mesec) spremenite.~~ ~~6.3.3. Priporočeno je, da zavarujete dostop do svojih mobilnih končnih~~ ~~naprav. V primeru izgube ali kraje mobilne končne naprave, družba~~ ~~Bank svetuje, da pri svojemu mobilnem operaterju zahtevate blokado~~ ~~SIM kartice.~~ ~~6.3.4. Pazite, da z uporabo gesel na skupnih računalnikih in mobilnih~~ ~~končnih napravah (npr. v internetni kavarni, v hotelu, na delovnem~~ ~~mestu), tretjim osebam ne omogočate dostopa na nepooblaščen in~~ ~~enostaven način.~~ ~~6.3.5. Računalnik in mobilne končne naprave naj bodo opremljene z~~ ~~najnovejšo protivirusno zaščito, s posodobljeno programsko opremo~~ ~~kot tudi s požarnim zidom. Na ta način tretjim osebam znatno~~ ~~zmanjšamo možnost odkrivanja in zlorabe podatkov.~~ ~~6.3.6. Na spletni strani družbe Bank www.paylife.at so vam v meniju~~ ~~„Service“ na voljo informacije o varnih sistemih in varnostnih nastavitvah.~~
	7. Spremembe Posebnih pogojev poslovanja 7.1. Banka imetniku kartice ponudi spremembe Posebnih pogojev poslovanja 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 na drug dogovorjeni način, npr. po elektronski pošti, ne sporoči svojega nestrinjanja glede spremenjene ponudbe, se smatra, da se strinja s spremembami. Banka imetnika kartice v 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 kartično pogodbo pred začetkom uveljavitve sprememb brezplačno takoj prekine. Banka bo na svojem spletnem mestu prav tako objavila primerjalno preglednico določb, kot tudi posodobljeno verzijo novih pogojev. Imetniku kartice bo na njegovo zahtevo tudi posredovala novo verzijo pogojev, in ga o tej možnosti seznanila v ponudbi sprememb. 7.2. Imetnik kartice je lahko o ponujeni spremembi obveščen v vsaki z njim 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. 7.3. Sprememba navedenih 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 predstavlja sprememba povečanje varnosti bančnega poslovanja ali postopka poslovanja z imetnikom kartice glede uporabe varnostnega mehanizma 3D Secure, (iv) ko je sprememba potrebna zaradi tehničnih posodobitev ali prilagoditev novih programov za uporabo končnih naprav, (v) ko je sprememba potrebna zaradi spremembe zakonskih določil za dodelitev naročil z uporabo varnostnega mehanizma 3D Secure. Sprememba Posebnih pogojev poslovanja ne predstavlja uvedbe ali spreminjanja dogovorjenih stroškov.
	8. Sprememba naslova, e-poštnega naslova in mobilne številke imetnika kartice Imetnik kartice je dolžan, da banki vsako spremembo svojega naslova, e-poštnega naslova in svoje mobilne številke sporoči pisno ali po elektronski pošti. Določbe v 16. členu Splošnih pogojev poslovanje ostajajo nedotaknjene.
	9. Varnostna opozorila 9.1. V času blokade do varnostnega mehanizma 3D Secure, kartice ni

	možno uporabljati za spletne nakupe pri trgovcih, ki ponujajo omenjeni varen sistem. 9.2. V izogib tveganjem, povezana s poznavanjem gesla, banka priporoča, da se ga redno (npr. vsak mesec) spremenija.
	10. Pogodbena doba in prekinitev 10.1. Dogovor o uporabi varnostnega mehanizma 3D Secure za predplačniške kartice z možnostjo polnitve je sklenjen za nedoločen čas. 10.2. 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. 10.3. Banka je upravičena, da lahko dogovor kadarkoli upoštevaje dvomesečnega roka brez razloga odpove. 10.4. Tako imetnik kartice kot tudi banka imata pravico, da lahko dogovor kadarkoli iz pomembnih razlogov s takojšnjim učinkom prekineta. 10.5. Prenehanje dogovora ne vpliva na kartično pogodbo, razen ko se imetnik kartice oz. banka ne dogovorita hkrati tudi za njeno prenehanje. 10.6. Dogovor avtomatsko preneha z iztekom kreditne pogodbe.
Različica julij 2016, stanje maj 2018	~~Različica julij 2016, stanje maj 2018~~ Različica september 2019