

## **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](http://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](http://www.paylife.at/3dsecure) bodisi v elektronskem plačilnem postopku na internetu.

## **1. Definicija**

- 1.1. Varnostni mehanizem Mastercard SecureCode  
Geslo, ki si ga imetnik kartice izbere sam med postopkom registracije za uporabo varnostnega mehanizma 3D Secure.
- 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](http://www.paylife.at) so vam v meniju »Service« na voljo dodatne informacije o spletnih storitvah družbe Bank.
- 1.3. Enkratno geslo  
Enkratno geslo je naključno izbrano geslo, namenjeno verifikaciji imetnika kartice med postopkom registracije v varnostni mehanizem 3D Secure. Med postopkom registracije imetnik kartice nadomesti enkratno geslo z geslom, ki ga določi sam in je znano le njemu (Mastercard SecureCode).
- 1.4. Varni sistemi
  - 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.

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

- 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](http://www.paylife.at/3dsecure), možno jo je opraviti tudi med postopkom spletnega plačila pri trgovcu (pogodbena firma), ki omogoča uporabo varnostnega mehanizma 3D Secure.  
  
Potek registracije je predstavljen na spletni strani [www.paylife.at/3dsecure](http://www.paylife.at/3dsecure). Za identifikacijo imetnika kartice pri registraciji v varnostni mehanizem 3D Secure, potrebuje ta veljavno enkratno geslo kot tudi geslo mobileTAN.  
  
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](http://www.paylife.at/3dsecure).  
  
Imetnik kartice prejme enkratno geslo v obliki, kot jo je določil v postopku registracije (npr. preko e-pošte ali SMS-a).
- 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).

- 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 prejetja SMS-ov nosi imetnik kartice.

## **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 zahtevke, 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.

## **5. Blokiranje dostopa**

- 5.1. Družba Bank iz varnostnih razlogov po šestkratnem napačnem vnosu gesla blokira dostop do varnostnega mehanizma 3D Secure. V času trajanja 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](mailto: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. 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 svojem 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](http://www.paylife.at) so vam v meniju „Service“ na voljo informacije o varnih sistemih in varnostnih nastavitvah.

**7. Veljavnost in prenehanje dogovora**

Dogovor je sklenjen za nedoločen čas, vendar preneha s prekinitvijo pogodbenega kartičnega razmerja ali s prekinitvijo ali s prenehanjem delovanja varnostnega sistema 3D Secure, o čemer bo družba Bank imetnika kartice nemudoma obvestila.

Različica julij 2016, stanje maj 2018