Elektronikus Banki Szolgáltatások Általános Szerződési Feltételei

Hatályos: 2021. október 25. napjától

PREAMBULUM

Jelen Elektronikus Banki Szolgáltatások Általános Szerződési Feltételei azon elektronikus banki szolgáltatásokra vonatkoznak, amelyeket az ügyfelek a Citibank Europe plc magyarországi fióktelepe által vezetett számláik eléréshez használhatnak.

1. Fogalmak

A jelen Elektronikus Banki Szolgáltatások Általános Szerződési Feltételeiben (továbbiakban: Szerződési Feltételek) - hacsak a Szerződési Feltételek kifejezetten másképpen nem rendelkeznek - az alábbi fogalmak a következő jelentést hordozzák:

Bank:	a Citibank Europe plc képviseletében eljáró Citibank Europe plc Magyarországi Fióktelepe;
Ügyfél:	olyan jogi személy, vagy más szervezet, amely a Bankkal az Eszköz igénybevételére szerződést kötött és a jelen Szerződési Feltételeket magára nézve kötelezőnek ismerte el;
EB HelpDesk:	a Bank által az Ügyfelek számára a Szolgáltatásokhoz kapcsolódó szoftverhasználattal és esetleges szoftverhibák elhárításában segítséget nyújtó telefonos szolgáltatás, mely a +36 1 374 5518-as telefonszámon érhető el, munkanapokon 8.00-17.00 óra között, munkanapnak minősülő szombatokon 8.00-14.00 óra között;
Felhasználó:	A mindenkor érvényben lévő, ehhez szükséges nyomtatványon meghatalmazott olyan nagykorú, cselekvőképes természetes személy, aki a jelen Szerződési Feltételek 1. számú mellékletének 3. pontjában, illetve a 2. számú mellékletének 3. pontjában meghatározott tranzakciókat az Ügyfél nevében és képviseletében végrehajtja, vagy a jelen Szerződési Feltételek 3. számú mellékletének 2. pontjában meghatározott szolgáltatást igénybe veszi;
Szolgáltatások:	az Eszköz segítségével elérhető elektronikus banki szolgáltatások;
Számla:	az Ügyfél Banknál nyitott valamennyi fizetési számlája;
Citi:	a Bank és kapcsolt vállalkozásai;
CitiService:	a Bank Nagyvállalati Ügyfeleinek egyedi, magas szintű banki szolgáltatást nyújtó ügyfélszolgálata. A CitiService munkanapokon 8.00-17.00 óra között, munkanapnak minősülő szombatokon 8.00-14.00 óra között áll Ügyfelei rendelkezésére a +36 1 374 5000-es telefonszámon.

CCB Customer Service: a Bank Vállalati Ügyfeleinek egyedi, magas szintű banki szolgáltatást nyújtó ügyfélszolgálata, mely a +36 1 288 8880-as telefonszámon érhető el. A CCB Customer Service hétfőtől csütörtökig 8.00-17.00 óra között, pénteken 8.00-16.00 óra között, munkanapnak minősülő szombatokon 8.00-14.00 óra között áll Ügyfeleink rendelkezésére.

Távolról hozzáférést biztosító fizetési eszköz (Token/Eszköz): számítástechnikai eszközök, szoftverek és eljárások (kivéve bankkártyák) együttese, amely lehetővé teszi az Ügyfél számára a Szolgáltatások igénybevételét.

Hitelesítési módszerek

Az eljárások részét képezik bizonyos biztonsági hitelesítési módszerek ("Hitelesítési módszerek"), amelyeket az Ügyfél és/vagy az Ügyfél által felhatalmazott bármely felhasználó jogosultságának egyedileg történő azonosításához és ellenőrzéséhez használnak tipikusan egy vagy többféle mechanizmus kombinációján keresztül, mint például a felhasználói azonosító jelszóval párosítva, digitális tanúsítványok, biometrikus azonosítók, biztonsági kártyák (hardveres vagy szoftveres alkalmazással) és/vagy a hitelesítési módszerekkel társított eszközök (együttesen „hitelesítési eszközök"). A Hitelesítési módszerek és a hozzájuk kapcsolódó Hitelesítő eszközök lehetővé teszik a Bank számára, hogy ellenőrizze a beérkezett megbízások eredetét.

Az alábbi Hitelesítési módszerek segítségével érhetők el a Bank szolgáltatásai vagy csatornái:

Token: Hívó- és válaszkód vagy (i) egy mobil applikáció-alapú szoftver (pl. MobilePASS) vagy (ii) egy fizikai eszköz (pl. SafeWord kártya), melynek segítségével minden alkalommal egy dinamikus, belépésenként változó jelszót generálnak egy PIN kóddal (pl. 4 számjegyű PIN) történő azonosítás után. A CitiDirect BE-be történő belépés alkalmával a rendszer generál egy hívó kódot, melyre az eszközzel generált válasz kód beírásával biztosított a rendszerhez való hozzáférés.

Token: egyszeri jelszó: vagy (i) egy mobil applikáció-alapú szoftver (pl. MobilePASS) vagy (ii) egy fizikai eszköz (pl. SafeWord kártya), melynek segítségével egy dinamikus, belépésenként változó jelszót generálnak egy PIN kóddal (pl. 4 számjegyű PIN) történő azonosítás után. A rendszerhozzáférés a jelszó bevitelével biztosított.

SMS egyszeri jelszó: A felhasználók részére a dinamikus jelszó SMS útján érkezik. A felhasználó ezt a dinamikus jelszót és a biztonsági jelszavát beírva tud belépni a rendszerbe.

Hang-alapú egyszeri jelszó: A felhasználók részére generált dinamikus jelszót egy automata telefonhíváson keresztül kapja meg. A felhasználó ezt a dinamikus jelszót és a biztonsági jelszavát beírva tud belépni a rendszerbe.

Digitális tanúsítványok: A hitelesítésre egy jóváhagyott tanúsító hatóság által kiadott digitális tanúsítvány szolgál. A digitális tanúsítványok kulcstároló mechanizmust és a megfelelő PIN-kódot használnak, és az IdenTrust, a SWIFT (3SKey) vagy más megállapodott szolgáltatók bocsáthatják ki.

A digitális tanúsítványokat hitelesítés céljából egyedi felhasználóknak ("Személyes tanúsítványok") vagy vállalati jogi személyeknek ("Vállalati pecétek") állítják ki. Ahol a kapcsolati pontok támogatják a Vállalati pecséteket használó

	kommunikációt, az Ügyfél felelős azért, hogy a helyi törvényeknek megfelelően azonosítson minden természetes személyt, akik az Ügyfél nevében az Ügyfél számlája felett rendelkeznek. A Bank által bármely nyilvános internetkapcsolaton keresztül fogadott kommunikációval szemben (ideértve, de nem korlátozva a HTTPS-t, biztonságos FTP-t vagy FTPS-t) vagy egyéb módon nem biztonságos internetkapcsolat esetén elvárt, hogy a Bank és az Ügyfél előzetesen jóváhagyott digitális tanúsítványokat cseréljenek annak biztosítása érdekében, hogy mind a csatlakozási csatorna, mind a továbbított üzenetek teljesen titkosítva és védve legyenek.
Biztonságos jelszó	A felhasználó biztonságos jelszava segítségével fér hozzá a rendszerhez. A biztonságos jelszó tipikusan korlátozza a felhasználó rendszerjogosultságait, pl. csak bizonyos információk láthatók a felhasználó számára.
Biometrikus azonosítás	Digitális azonosítási eljárás, mely a felhasználó egyedi fizikai jellegeit felhasználva (mint pl. ujjlenyomat vagy arcfelismerés) a felhasználó mobil eszközébe beépített biometrikus technológia és kriptográfiai technikák segítségével biztosít belépést a CitiDirect BE-be a felhasználó részére. Ezen hitelesítési mód esetén a fizikai tulajdonságokra vonatkozó adatok nem kerülnek továbbításra a Bank felé.
PIN IVR-hoz (Interactive Voice Response)	Amikor az ügyfelek telefonon vagy e-mailen keresztül kommunikálnak a Bankkal, elvárt, hogy PIN kóddal vagy egyéb azonosítási eljárással bizonyítsák felhasználói jogosultságukat.
MTLS	Mandatory Transport Layer Security (MTLS) biztonságos, privát e-mail kapcsolatot létesít a Bank és az Ügyfél között. Az interneten keresztük ezen a csatornán továbbított e-mailek a kapcsolat által létrehozott titkosított TLS alagúton kerülnek továbbításra.
Biztonságos PDF	A titkosított e-mailek egy kiejlölt postafiókba PDF dokumentumként kerünek, melyeket egy privát, biztonságos jelszó megadásával lehet megnyitni. Az üzenet maga és a csatolmány is titkosításra kerül. Az egyéni jelszót az első biztonságos üzenet megnyitása alkalmával is meg lehet adni.
IP cím engedélyezési lista CitiConnect használatakor	Certain Internet communications received by the Bank, for example, via a Virtual Private Network (VPN), may also rely on the parties exchanging information using pre-agreed Internet Protocol (IP) addresses. The Bank will only accept communications originating from the Customer's designated IP address, and vice versa; and the Bank will only transmit Communications to the Customer's designated IP address, and vice versa.
SWIFT	Communications sent between the Bank and the Customer via the SWIFT network, including, but not limited to, account information, payment orders, and instructions to amend or cancel such orders, will be authenticated using procedures defined in SWIFT's Contractual Documentation (as amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in other terms and conditions that may be established by SWIFT. The Bank is not obliged to do anything

other than what is contained in the SWIFT procedures to establish the sender and authenticity of these Communications.

A Bank nem vállal felelősséget SWIFT rendszer hibáiért és késedelmeiért. Az Ügyfél felelős azért, hogy a Bank felé a SWIFT által megkövetelt formátumban és típusban továbbítsa az üzeneteket. A SWIFT rendszeren keresztül küldött vagy fogadott kommunikációkra a hatályos SWIFT szabályok és rendeletek vonatkoznak, ideértve a tagsággal kapcsolatos szabályokat is. Az Ügyfél felelõs a SWIFT üzenetküldési szabványok megismeréséért és az annak való megfelelésért.

A hitelesítési módszerekkel kapcsolatban további információkat talál a CitiDirect BE bejelentkezési felületén a súgó oldalon:

(https://portal.citidirect.com/portalservices/forms/loginHelp.pser)

2. Távolról hozzáférést biztosító fizetési eszköz

A Távolról hozzáférést biztosító fizetési eszközök, valamint az azokkal elérhető Szolgáltatások leírását és technikai követelményeit jelen Szerződési Feltételek mellékletei tartalmazzák.

Attól függően, hogy az Ügyfél milyen Távolról hozzáférést biztosító fizetési eszközt használ, a Bank megkövetelheti a SafeWord kártya vagy MobilPASS eszköz használatát a Felhasználóktól. A SafeWord kártya és MobilPASS használatának feltételeit a jelen Szerződési Feltételek 1. számú melléklete tartalmazza.

3. Az Ügyfél és a Felhasználó feladatai az Eszközhöz való jogosulatlan hozzáférés elleni védelemmel kapcsolatban

Az Ügyfél és a Felhasználó köteles minden szükséges intézkedést megtenni annak érdekében, hogy illetéktelenek ne férhessenek hozzá az Eszköz használatához szükséges azon szoftverekhez, IT eszközökhöz (különös tekintettel, de nem kizárólag a SafeWord kártyára vagy a MobilePASS alkalmazást működtető eszközre), azonosító kódokhoz, informatikai rendszerekhez, amelyek az Ügyfél vagy a Felhasználó üzemeltet, illetve birtokában tart. Az Ügyfél köteles rendszeresen ellenőrizni, hogy az Eszköz védelmét szolgáló intézkedései megfelelőek-e vagy fejlesztést igényelnek.

4. Az Ügyfél és a Felhasználó bejelentési kötelezettsége

Az Ügyfél és a Felhasználó köteles a Bank Digital Client Support osztályának haladéktalanul bejelenteni, amennyiben azt észlelik vagy gyanítják, hogy illetéktelen személyek férhetnek/férhettek hozzá az Eszközhöz, vagy az ahhoz kapcsolódó szoftverekhez, IT eszközökhöz (különös tekintettel a SafeWord kártyára vagy a MobilePASS alkalmazást működtető eszközre), azonosító kódokhoz, informatikai rendszerekhez. Az esetet munkatársainknak telefonon keresztül hétfőtől - péntekig 8:30 – 17:00 óra között, banki munkanapnak minősülő szombati napokon pedig 8:30 – 14:00 között a +36 1 374 5518-as telefonszámon-, vagy egyéb esetben emailben a DCS.Hungary@citi.com címen jelezhetik.
A telefonon bejelentést tevő személy köteles megadni személyes azonosító adatait, az Ügyfél és a Felhasználó adatait és a bejelentést megalapozó esemény helyét, idejét és leírását. Ha a bejelentő nem ismeri az esemény helyét, illetve idejét, akkor a feltételezett helyet és időpontot kell bejelentenie. A bejelentést az Eszköz letiltására irányuló utasításnak kell tekinteni. A Bank haladéktalanul tájékoztatja az Ügyfelet, amennyiben az Ügyfél részéről közreműködés szükséges a Safeword kártya vagy a MobilePASS válasz kód letiltásának érdekében. Írásban tett bejelentés esetén a tárgy mezőben feltétlenül tüntessék fel Safeword kártya és/vagy MobilePass letiltására irányuló szándékukat.

5. Felelősség

5.1. Az Ügyfél viseli az Ügyfél vagy a Felhasználó oldalán bekövetkező visszaélések, illetve a jelen Szerződési Feltételek 3. vagy 4. pontjában meghatározott kötelezettségek Ügyfél vagy Felhasználó által szándékos vagy súlyos gondatlansággal történt megszegése miatt bekövetkezett kárát.

5.2. A fenti 4. pont szerinti bejelentést követően a jogosulatlan hozzáférésből eredően az Ügyfélnél felmerült károkat a Bank köteles viselni.

5.3. Ügyfél elfogadja, hogy a Felhasználók által kezdeményezett fizetési műveletek az Ügyfél által jóváhagyott fizetési műveletnek minősülnek.

5.4 Ha jogszabály másként nem rendelkezik, akkor az Ügyfél felelős minden olyan következményért, illetve viseli a felmerülő kockázatokat, abban az esetben, ha a MobilePASS alkalmazásra vonatkozó azonosító kódok illetéktelen személyek számára elérhetővé válnak. A Felhasználó köteles megváltoztatni a MobilePASS jelszavát, ha gyanítja, hogy illetéktelen személyek tudomást szereztek róla.

6. Letiltás

A Bank fenntartja magának a jogot, hogy letiltsa a Safeword kártya vagy a MobilePASS válasz-kód engedélyezését, annak jogosulatlan vagy csalárd módon történő használatának gyanúja esetén vagy az Eszköz biztonsága érdekében.

7. Használati jog

7.1. A jelen Szerződési Feltételek hatálya alatt az Ügyfél számára átadott, birtokába került bármely dokumentáció, szoftver, hardver a Bank kizárólagos tulajdonát képezi, azokon az Ügyfél a nem kizárólagos felhasználói jogon kívül semmilyen jogot nem szerez.

7.2. Az Eszközzel kapcsolatos bármely dokumentáció, információ, hardver, szoftver, egyéb eszköz a Bank üzleti titkát képezi, és annak harmadik személyek számára bármely módon történő kiszolgáltatása kizárólag a Bank előzetes írásbeli hozzájárulásával lehetséges, mely hozzájárulásban a Bank megjelöli a kiszolgáltatható információ pontos körét is.

8. Megszűnés

8.1. Bármelyik fél jogosult a másik Félhez intézett írásbeli rendes felmondással, 60 napos felmondási idővel, indokolás nélkül megszüntetni egyes Eszközök, illetve az összes Eszköz használatára vonatkozó szerződést. Az Ügyfél hozzáférése a felmondással érintett Eszközökhöz a felmondási idő utolsó napján megszűnik.

8.2 Bármely fél jogosult írásbeli azonnali hatályú felmondással megszüntetni egyes Eszközök, illetve az összes Eszköz használatára vonatkozó szerződést, ha a másik fél súlyos szerződésszegést követ el. A Bank különösen az alábbi esetekben jogosult az azonnali hatályú felmondásra:

a) az Ügyfél vagy a Felhasználó a Szerződési Feltételekből eredő bármely kötelezettségét nem teljesíti;

b) az Ügyfél pénzügyi- vagy bármely más, a Bank megítélése szerint a Szerződési Feltételek szempontjából jelentős körülményei hátrányosan változnak meg;

c) az Ügyfél a Szerződési Feltételekkel kapcsolatban valótlan adatot szolgáltatott;

d) az Eszköz letiltás utáni, vagy érvényességi időn, területen túli használata;

e) az Eszköz használatára vonatkozó szabályok megsértése.

8.3. A Bank súlyos szerződésszegés esetén az Eszköz használatát felfüggesztheti.

8.4. A felmondás hatályba lépését követően az Eszköz használatával kapcsolatban a Bank által hozzáférhetővé tett szoftverek, IT eszközök, kódok és rendszerek használata tilos.

9. Átruházás, részleges érvénytelenség

9.1. Az Ügyfél a Bank előzetes hozzájárulása nélkül a Szerződési Feltételekből eredő jogait harmadik felekre nem engedményezheti, kötelezettségeit nem ruházhatja át (a továbbiakban együttesen: “Átruházás”). A Bank jogosult jogait és kötelezettségeit harmadik személyre átruházni az Ügyfél engedélye nélkül. Az Átruházás alapján az engedményes és a kötelezettséget átvállaló személy az Átruházás keretei között megszerzi a Bank jogait és kötelezettségeit, és a Bank az Átruházás keretei között mentesül minden itt megjelölt kötelezettsége alól.

9.2. Ha a jelen Szerződési Feltételek bármely előírása érvénytelen vagy nem érvényesíthető, az nem érinti a jelen Szerződési Feltételek egyéb rendelkezéseinek érvényességét és érvényesíthetőségét.

10. Díjak és jutalékok

A Szolgáltatásra vonatkozó díjak jegyzékét a Bank aktuális Vállalati és/vagy Nagyvállalati Kondíciós Listájának első fejezete tartalmazza.

11. Általános Üzleti Feltételek

A jelen Szerződési Feltételekben nem rendezett kérdésekben a Bank mindenkor hatályos Vállalati Szolgáltatások Általános Üzleti Feltételei az irányadóak.

1. számú melléklet
CitiDirect for Cash

1. CitiDirect for Cash

A CitiDirect for Cash (CitiDirect) egy web-alapú, interneten elérhető elektronikus banki rendszer. A következő pontban meghatározott technikai feltételeken kívül a CitiDirect eléréséhez SafeWord kártya vagy MobilePASS aktiváló kód is szükséges. A Bank az adott Ügyfél összes Felhasználójának rendelkezésére bocsát egy SafeWord kártyát vagy MobilePASS aktiváló kódot.

A CitiDirect használatának részletes leírása a CitiDirect Online Help-ben található, amely a CitiDirect szoftverbe beépített, a szoftver használatát támogató, keresési funkcióval ellátott, online számítógépes súgó.

2. Technikai feltételek

A CitiDirect szolgáltatások igénybevételéhez szükséges minimális technikai feltételek a https://www.citidirect.com internetes oldalon találhatók.

Abban az esetben, ha a fenti technikai feltételek megváltoznak, a Bank a körülmények megváltozása előtt 30 nappal értesíti az Ügyfelet. Az Ügyfél köteles haladéktalanul megteremteni a CitiDirect igénybevételének megváltozott technikai feltételeit. Ha az Ügyfél e kötelezettségének nem tesz maradéktalanul eleget, úgy a Bank nem felel az ebből eredő károkért.

3. CitiDirecten keresztül elérhető Szolgáltatások

A CitiDirect használatával az Ügyfél

(a) a Számlára vonatkozó számlainformációt, egyenleget és a Számlán végzett valamennyi tranzakcióra vonatkozó információt kérdezhet le;

(b) letöltheti a Számláról indított és arra érkező tranzakciók listáját;

(c) a Számláról átutalást, fizetési megbízást kezdeményezhet külföldre, illetve belföldre, forintban és devizában;

(d) csoportos átutalási megbízásokat, azonnali beszedési-, csoportos beszedési megbízásokat adhat;

(e) betétet köthet le;

(f) a Bank számára megbízásnak nem minősülő tájékoztatást, leveleket küldhet a Banknak;

(g) postai utalványon történő kifizetést kezdeményezhet;

(h) GIRO átutaláshoz kapcsolódó EBÜK elektronikus vám-üzenet küldést kezdeményezhet;

(i) a fenti (a) és (b) pontokban meghatározott információkat titkosított adatállomány formájában, e-mailben is megkaphatja.

A fenti i) pontban meghatározott szolgáltatáshoz az Ügyfél levelezési (e-mail) programja a CitiDirect által támogatott titkosító profilok valamelyikét kell, hogy tartalmazza. A CitiDirect által támogatott titkosító profilok listáját a https://www.citidirect.com internetes oldal tartalmazza. A különböző titkosító profilokra vonatkozóan a Bank semmilyen felelősséget nem vállal, így különösen a Bank nem felel a titkosító profilok mindenkori hibamentes

működéséért. A szerzői jogokkal és a titkosító profilok használatáért az Ügyfél által fizetendő díjakkal kapcsolatos kötelezettségekért közvetlenül az Ügyfél felel.

4. PIN Kód

A Bank a CitiDirect szolgáltatások igénybevételéhez az Ügyfél választása szerint SafeWord kártyát és hozzátartozó PIN kódot és/vagy MobilePASS aktiváló kódot bocsát az Ügyfél Felhasználóinak rendelkezésére, melyek által generált dinamikus jelszó/válasz kód szükséges a 3. pontban felsorolt minden szolgáltatás igénybevételéhez. Az Ügyfél, valamint a Felhasználó a PIN és MobilePASS aktiváló kódot köteles titokban tartani.

A Bank a szolgáltatások, vagy bizonyos funkciók eléréséhez, az Ügyfél érdekében, jogosult a PIN kód és MobilePASS aktiváló kód segítségével generált jelszón kívül további belépés biztonsági feltételeket is alkalmazni.

5. SafeWord kártya és MobilePASS

A SafeWord kártya a Bank tulajdona, át nem ruházható, harmadik személy birtokába nem adható, óvadékként vagy zálogként nem köthető le, letétként nem helyezhető el, harmadik személynek nem adható át.

Ügyfél jogosult a SafeWord kártya inaktív státuszban történő kézbesítését kérni. Az inaktív státuszban kézbesített SafeWord kártya aktiválásának feltétele, hogy Ügyfél cégszerűen aláírt és a Banknak eredetiben eljutatott nyilatkozatban, a sorozatszám feltüntetésével igazolja a kézbesített SafeWord kártya és a hozzá tartozó PIN kód átvételét. Ha az Ügyfél nem inaktív státuszban kéri a SafeWord kártya kézbesítését, akkor a SafeWord kártyának az Ügyfél által megjelölt helyen található bármely személy által történő átvétele után a SafeWord kártya aktív státuszban történő átadásával kapcsolatos minden kockázat az Ügyfelet terheli. Az Ügyfél közvetlenül felelős azért, hogy a Felhasználók megismerjék a SafeWord kártya és a MobilePASS aktiváló kód használatának és őrzésének (biztonságban tartásának) szabályait, valamint az ezekkel kapcsolatos felelősségi szabályokat.

Az Ügyfél a Felhasználóval egyetemlegesen felel azokért a károkért, amik a Bankot annak következtében érik, hogy a Felhasználó megszegi a jelen Szerződési Feltételek rendelkezéseit.

Az Ügyfél közvetlenül felelős a MobilPass alkalmazást működtető eszköz biztonságáért és működtetésért.

A Bank jogosult a SafeWord kártya használata során keletkezett információk rögzítésére és jogvita esetén azok bizonyítékként való felhasználására. A MobilePass alkalmazás feltételeire, használatára vonatkozó részletes tájékoztatást a Bank a https://portal.citidirect.com oldalon teszi közzé.

6. A CitiDirect használata

A Bank az Ügyfél kérésére a CitiDirect igénybevételéhez a hozzáférést a megfelelően kitöltött és cégszerűen aláírt, a mindenkor érvényben lévő, ehhez szükséges nyomtatvány Bankhoz történő beküldésével biztosítja. A CitiDirect igénybevételének feltétele, hogy a Bank a Felhasználókat a mindenkor hatályos, a pénzmosás megelőzéséről és megakadályozásáról szóló jogszabályokkal összhangban beazonosítsa, és ezzel kapcsolatban mind az Ügyfél, mind a Felhasználó valamennyi adatot és/vagy nyilatkozatot megadjon.

Az Ügyfél köteles valamennyi, a Felhasználónak a pénzmosás megelőzéséről és megakadályozásáról szóló jogszabályokkal összhangban történő beazonosításához szükséges adatot és/vagy nyilatkozatot megadni.

A Bank kizárólag technikai és biztonsági okból jogosult bármikor – az ügyfél egyidejű értesítése és a jelen Szerződés hatályban tartása mellett – megváltoztatni, felfüggeszteni vagy megszüntetni a CitiDirect szolgáltatást vagy az Ügyfél, vagy a Felhasználó azon jogát, hogy a CitiDirect szolgáltatást igénybe vegye. Ennek megtörténtéről a Bank az Ügyfelet elektronikus

levélben, vagy a CitiDirect rendszerbe történő következő belépés folyamán írásban értesíti. A Bank nem felel a fenti változtatás, felfüggesztés vagy megszüntetés miatt az Ügyfél által elszenvedett semmilyen kárért vagy veszteségért.

2. számú melléklet
File-alapú Fizetési Szolgáltatások

1. A File-alapú fizetési Szolgáltatások leírása

A file-alapú fizetési Szolgáltatások olyan Eszközök, amelyek használatával az Ügyfél a Citi által támogatott formátumú titkosított fizetési információkat tartalmazó számítógépes állományt (file-t) küld saját pénzügyi rendszeréből a Bank számítógépes kiszolgálójára a Citi által támogatott valamely kapcsolódási módszer (pl. FTP, HTTPS, CitiConnect, CitiDirect) használatával. A Citi automatikusan dolgozza fel a fizetési instrukciókat.

A file-alapú fizetési Szolgáltatásoknál használt titkosítási és azonosítási eljárások a nyílt kulcsú titkosító infrastruktúrán alapulnak (Public Key Infrastructure-PKI).

A Bank kizárja a felelősségét a Bank rendszere általi befogadást megelőzően a file-ok feltöréséből, átalakításból vagy egyéb módosításából származó károkért.

A Bank a file-alapú Fizetési Szolgáltatásokon keresztül érkező tranzakciókat a benyújtási határidők figyelembe vételével dolgozza fel.

Nem tartoznak jelen Szerződési Feltételek hatálya alá a Banktól eltérő Citi tagvállalattal kötött File-alapú fizetési szolgáltatásra vonatkozó szerződések. A Bank kizárja a felelősséget ezen szerződések teljesítésével, díjazásával, feltételeivel, ide értve a megbízások benyújtási határidejével és annak teljesítésével kapcsolatos bármely kéréssel, panasszal, valamint igénnyel szemben.

2. Technikai követelmények

A file-alapú fizetési Szolgáltatások technikai (hardver és szoftver) követelményei a Bank által az Ügyfélnek ajánlott konkrét megoldás jellemzőitől függenek. A file-alapú fizetési Szolgáltatások Ügyfél oldali technikai specifikációiról és követelményeiről az Ügyfél és a Bank közösen állapodnak meg az implementációs és tesztelési időszak alatt. Az implementációs és tesztelési időszak alatt a Bank az Ügyfél rendelkezésére bocsátja a File-alapú Fizetési Szolgáltatások használatához szükséges információkat.

3. A file-alapú fizetési Szolgáltatások listája

A File-alapú Fizetési Szolgáltatások használatával az Ügyfél

(a) a Számláról átutalást, fizetési megbízást kezdeményezhet külföldre, illetve belföldre, forintban, devizában;

(b) csoportos átutalási és postautalvány megbízásokat, azonnali beszedési, csoportos beszedési megbízásokat adhat belföldre, forintban.

4. A file-alapú fizetési Szolgáltatások használata

A szolgáltatás igénybevételének feltétele a megfelelően kitöltött és cégszerűen aláírt, a mindenkor érvényben lévő, ehhez szükséges nyomtatvány Bankhoz történő benyújtása, illetve feltétele, hogy a Bank a Felhasználókat a mindenkor hatályos, a pénzmosás megelőzéséről és megakadályozásáról szóló jogszabályokkal összhangban beazonosítsa, és ezzel kapcsolatban mind az Ügyfél, mind a Felhasználó valamennyi adatot és/vagy nyilatkozatot megadjon.

Az Ügyfél köteles valamennyi, a Felhasználónak a pénzmosás megelőzéséről és megakadályozásáról szóló jogszabályokkal összhangban történő beazonosításához szükséges adatot és/vagy nyilatkozatot megadni.

A Bank kizárólag technikai és biztonsági okból jogosult bármikor az ügyfél egyidejű értesítése és a jelen Szerződés hatályban tartása mellett megváltoztatni, felfüggeszteni vagy megszüntetni a CitiDirect szolgáltatást vagy az Ügyfél, vagy a Felhasználó azon jogát, hogy a CitiDirect szolgáltatást igénybe vegye. A Bank nem felel a fenti változtatás, felfüggesztés vagy megszüntetés miatt az Ügyfél által elszenvedett semmilyen kárért vagy veszteségért.