TERMENI ŞI CONDIŢII PRIVIND UTILIZAREA E-XIM BANKING

I. DEFINIȚII ȘI CONSIDERENTE GENERALE

În înțelesul prezentului document, termenii de mai jos vor avea următoarele semnificații:

1. **Banca** - Exim Banca Românească - S.A., cu sediul social în Municipiul București, Sector 1, strada Barbu Delavrancea nr. 6A, corpurile de cladire A1, A2, B1, B2a, B2b, C (etaj 1 și mansardă), cod poștal 011355, înregistrată în Registrul Instituțiilor de Credit sub nr. RB-PJR-40-015/18.02.1999 și în Registrul Comerțului sub nr. J1992008799402, având codul unic de înregistrare RO 361560, identificatorul unic la nivel european (EUID) ROONRC.J199200879940 și capitalul social subscris și vărsat de 2.022.528.336 RON, website www.eximbank.ro, e-mail office@eximbank.ro.

   Banca este prestator de servicii de plată (PSP) în sensul prevederilor *Directivei (UE) nr. 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 2002/65/CE, 2009/110/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010, și de abrogare a Directivei 2007/64/CEt*.

2. **Client -** orice persoană juridică, entitate fără personalitate juridică sau persoană fizică autorizată, care utilizează sau beneficiază de unul sau mai multe servicii și/sau produse bancare oferite de Bancă.

3. **Serviciul e-xim Banking (e-xim Banking) -** instrument de plată cu acces la distanță de tip Internet Banking și/sau Mobile Banking, ce permite Clientului accesul la fondurile aflate în conturile acestuia deschise la Bancă, prin intermediul Utilizatorilor săi desemnați, pe baza Elementelor de securitate furnizate acestora,

Prin intermediul e-xim Banking se pot efectua diverse tipuri de plăti prin transfer credit, precum și alte tipuri de tranzacții precum: schimburi valutare, constituire/desființare depozite, vizualizare solduri și tranzacții pe conturi, extrase de cont, alte informații financiare etc .
Banca va putea introduce noi funcționalități ale e - x i m Banking care vor putea fi puse la dispoziția Clientului, începând cu data comunicată de Bancă pentru activarea lor.

4. **Identificator Utilizator (alias/username)** - denumirea atribuită de Bancă fiecărui Utilizator în scopul accesării serviciului e-xim Banking, care poate fi ulterior schimbată, de către utilizator, direct în aplicație.

5. **Set de credențiale (elemente de securitate)-** cuprinde datele de logare ale fiecărui Utilizator, necesare accesării aplicației e-xim Banking,

6. **TPP** - prestator de servicii de plată, altul decât Banca, autorizat să presteze Servicii de informare cu privire la conturi (AIS) sau Servicii de inițiere a plății (PIS).

7. **Serviciu de informare cu privire la conturi (AIS)** - serviciul online, furnizat Clientului de un TPP, care constă în oferirea de informații consolidate în legătură cu unul sau mai multe Conturi de plăți accesibile online, deținut(e) de Client. TPP care prestează Clientului AIS va fi denumit AISP în continuare în cadrul prezentului document.

8. **Serviciu de inițiere a plății** (**PIS**) - serviciul online, furnizat Clientului de un TPP, care constă în inițierea de ordine de plată, la cererea Clientului, cu privire la unul sau mai multe Conturi de plăți accesibile online, deținut(e) de Client. TPP care prestează Clientului PIS va fi denumit PISP în continuare în cadrul prezentului document.

9. **Cont de plăți accesibil online** - cont de plăți care poate fi accesat de Client prin intermediul unei interfețe online (de ex. e-xim Banking). Pentru evitarea oricărui dubiu, Clientul înțelege faptul că, dintre conturile accesibile prin Serviciul Internet Banking, doar conturile curente deținute de Client la Bancă sunt considerate Conturi de plăți accesibile online, cu privire la care AISP și PISP pot presta în favoarea Clientului AIS și PIS.

10. **Aplicația TPP (PISP/AISP)** reprezintă interfața pusă la dispoziție Utilizatorului în vederea acordării/retragerii consimțământului și inițierii plăților.

11. **Formulare** – documente puse la dispoziția Clientului/Utilizatorului, de către Bancă, în vederea activării/actualizării/anulării drepturilor ce i se cuvin, semnate de către Reprezentații Legali ai părților și care conțin datele de identificare și drepturile care îi sunt alocate Clientului ce solicită e-xim Banking

12. **Utilizator** - persoană fizică, cu sau fără drept de semnătură, împuternicită de Client să acceseze e-xim Banking și să efectueze în numele și pe contul Clientului, în condițiile și limitele mandatului acordat de Client, toate operațiunile specifice Serviciului, inclusiv să primească, să utilizeze DIGIPASS-ul, să primească elementele de securitate, să reseteze, să blocheze și/sau să deblocheze elementele de securitate care i-au fost puse la dispoziție de către Bancă. Toate instrucțiunile date și toate operațiunile efectuate de Utilizatori prin intermediul Serviciului e-xim Banking sunt considerate a fi ale Clientului însuși, acesta neputând opune Băncii lipsa acordului său până la momentul notificării menționate în *Cap. III, clauza 9, lit. f)* de mai jos.

13. **Utilizator comun** - utilizator care folosește un singur set de credențiale și date de contact comune, pentru accesarea aplicației e-xim Banking, pe mai multi clienti (persoane fizice si juridice).

Clientul ia la cunostinta si accepta in mod expres ca, în cazul în care o persoană fizică este desemnată Utilizator al Serviciului e-xim Banking pentru mai multe companii, clienți ai Băncii, în legătură cu conturile acestora, Banca poate aloca Utilizatorului, la solicitarea acestuia, un singur Identificator Utilizator căruia ii vor fi alocate corespunzător drepturile stabilite conform fiecărui contract privind furnizarea Serviciului e-xim Banking, cu aceleași date de contact (un singur numar de telefon mobil și o singura adresa de e-mail), care vor fi folosite de Bancă pentru trimiterea Elementelor de Securitate, valabile pentru accesul Utilizatorului în aplicație, în temeiul tuturor contractelor în care este desemnat Utilizator.

În cazul Utilizatorului care detine și calitatea de utilizator client persoană fizică al e-xim Banking, Clientul (prin reprezentantul legal sau conventional) acceptă, în mod expres, ca Utilizatorul autorizat să poată accesa Serviciul e-xim Banking prin utilizarea acelorași date de contact (un singur număr de telefon mobil și o singură adresă de e-mail) și folosirea unui singur set de credențiale, aferente clientului persoană fizică, la solicitarea acestuia.

În cazul în care Utilizatorul își schimbă ulterior numărul de telefon mobil și/sau adresa de e-mail, folosite în relația cu Banca, aceste date se vor actualiza la nivelul tuturor clientilor (persoane juridice/fizice) la care Utilizatorul are acces comun în e-xim Banking.

Pentru Utilizatorul, care are statutul de utilizator client persoană fizică și/sau juridică și dorește date de contact și set de credențiale diferite, va solicita Băncii Utilizatori diferiți.

Mandatul este acordat de către Client fiecărui Utilizator cu respectarea deplină a actelor constitutive ale Clientului și/sau a prevederilor legale în vigoare, iar Utilizatorii acționează în numele Clientului și pentru acesta, în limitele și în condițiile mandatului primit.

Tipuri de Utilizatori:

Utilizator cu drept de semnătură (*aprobator*) - persoană fizică împuternicită de Client să vizualizeze informații privind contul(rile) Clientului accesibil(e) prin e-xim Banking, să efectueze și să autorizeze/avizeze efectuarea de operațiuni în/din acest(e) cont(uri);

Utilizator fără drept de semnătură (*operator*) - persoana fizică împuternicită de Client numai să vizualizeze informații privind contul(rile) Clientului accesibil(e) prin e-xim Banking și să completeze câmpurile din formularele electronice disponibile în cadrul Serviciului prin care poate fi dispusă efectuarea de operațiuni în/din contul(rile) Clientului accesibil(e) prin e-xim Banking, urmând ca acestea să fie autorizate/avizeze de un Utilizator cu drept de semnătură (aprobator).

14. **Utilizator exclusiv modul Carduri** – utilizatorul care nu deține produse bancare și utilizează exclusiv un card business. Accesul utilizatorului la modulul de Carduri este acordat automat si este limitat la vizualizare tranzactii card / blocare temporara, deblocare card, adaugare card in portofel digital, autentificare / autorizare tranzactii de tip e-commerce (online).

15. **Help Desk** - serviciul de support, pus la dispoziția Clienților de către Bancă (telefonic, prin e-mail sau prin chat-ul aplicației, în fiecare Zi bancară, în intervalul orar 08:30:00-17:00) pentru a le permite să primească informații cu privire la utilizarea aplicației. Prin serviciul Help Desk, Clientul, prin Utilizatori, poate notifica Banca, **telefonic, chat** sau **prin e-mail**, în fiecare zi bancară în intervalul orar 08:30:00-17:00 , iar în afara orelor de program, telefonic, prin intermediul Call Center Carduri, doar cu privire la pierderea, furtul, deteriorarea, distrugerea, deturnarea elementelor de securitate (inclusiv a DIGIPASS-ului) sau orice utilizare neautorizată a acestora sau a e-xim Banking, conform prevederilor *Cap. II, clauza 6 și Cap. III, clauza 9, litera f)* de mai jos.

16. **Call Center Carduri-** serviciul oferit de Bancă pentru blocarea accesului unui utilizator la aplicația e-xim Banking, la cererea telefonică a acestuia, în cazul pierderii/furtului elementelor de securitate, de luni până vineri, în intervalul orar 17:00-8:30 și în zilele nelucrătoare sau de sărbătoare legală.

17. **Date de contact**- numărul de telefon mobil și adresa de e-mail declarate de utilizator, în relația cu Banca, inclusiv pentru activarea aplicației Mobile Banking. Pentru a se asigura securitatea datelor, este recomandat ca acestea să fie unice (diferite) la nivelul utilizatorilor unei companii. Datele de contact sunt folosite pentru instalarea aplicației mobile, pe baza elementelor de identificare pe care clientul le furnizează în Formulare si care sunt validate la instalarea aplicației (CNP, pentru persoane rezidente sau echivalent, seria și numărul pașaportului/numărul (și seria, dacă există), pentru persoane nerezidente; număr de telefon mobil și adresa de e-mail).

În cadrul convorbirilor telefonice, Banca va identifica Utilizatorul prin: (a) denumirea Clientului, (b) numele, prenumele Utilizator, (c) alias-ul- Utilizatorul cu care se loghează în aplicație (d) număr de telefon (apelul trebuie să fie de pe numărul înregistrat în relație cu Banca, comunicat de către Utilizator, prin intermediul Formularelor), e) CUI-ul companiei, iar pentru siguranța identificării, Banca poate solicita Utilizatorului și alte date (ex: CNP/echivalent și/sau adresa de e-mail,), iar in caz de incertitudine, Banca poate solicita Utilizatorului si alte informatii financiare. În cazul în care toate datele de identificare comunicate Băncii în cadrul convorbirii telefonice corespund cu datele existente în sistemul Băncii (puse anterior la dispoziția Băncii de către Client și/sau fiecare dintre Utilizatori), identificarea Utilizatorului se consideră a fi realizată.

Banca va arhiva corespondența electronică și va înregistra și arhiva convorbirile telefonice, pentru o perioadă de 18 luni, de la data înregistrării. Prin semnarea Termenilor și Condițiilor e-xim Banking, Banca și Clientul convin asupra utilizării convorbirilor telefonice astfel înregistrate și arhivate și a corespondenței electronice arhivate ca mijloc de probă în cazul oricărui litigiu și/sau a oricărei neînțelegeri dintre Client (inclusiv Utilizator) și Bancă cu privire la accesarea și utilizarea

Serviciului e-xim Banking, precum și pentru a demonstra Clientului și/sau autorității de supraveghere din domeniul serviciilor de plată, primirea notificărilor prevăzute *in Cap. II, clauza 6 și în Cap. III, clauza 9, litera f)* de mai jos.

Accesarea Help Desk sau Call Center Carduri se face utilizând datele de contact ale Băncii, care se regăsesc pe site-ul www.eximbank.ro în secțiunea "Documente utile" sau direct în aplicația e-xim Banking.

18. **Manual de utilizare** - set de instrucțiuni de utilizare a e-xim Banking care pot fi consultate de către Client și/sau Utilizatori prin accesarea secțiunii "Documente utile" de pe site-ul www.eximbank.ro sau direct în aplicația e-xim Banking. Manualul de utilizare face parte integrantă din prezentul document intitulat "Termeni și condiții privind utilizarea serviciului e-xim Banking" (denumit în continuare "Termeni și Condiții e-xim Banking").

19. **Autentificare** - procedura care permite Prestatorului de Servicii de Plată (PSP) să verifice identitatea unui Utilizator al serviciilor de plată sau valabilitatea utilizării unui anumit instrument de plată și care include utilizarea elementelor de securitate ale Utilizatorului Serviciilor de Plată.

20. **Autorizare** procedura care permite exprimarea consimțământului Utilizatorului pentru executarea operațiunilor prin e-xim Banking (ex. operațiuni de plată, schimb valutar, constituire și lichidare depozit etc.) instructate prin e-xim Banking direct sau prin intermediul unui PISP.

21. **Parola e-xim Banking** -serie de caractere alphanumerice stabilită de Utilizator, necesară pentru acces în e-xim Banking și care se schimbă de fiecare Utilizator la prima conectare și este folosită împreună cu Identificatorul Utilizator, permițând accesul la serviciul e-xim Banking.

Autentificare strictă a Clienților (***Strong Customer Authentication -SCA)*** - permite accesul Utilizatorilor la Serviciul e-xim Banking utilizând niveluri suplimentare de Securitate. Este bazată pe utilizarea a două sau mai multe elemente incluse în categoria cunoștințelor deținute (ceva ce doar Clientul cunoaște), a posesiei (ceva ce doar Clientul posedă) și a inerenței (ceva ce reprezintă Clientul), care sunt independente, iar compromiterea unui element nu conduce la compromiterea fiabilității celorlalte elemente, și care sunt concepute în așa fel încât să protejeze confidențialitatea datelor de autentificare.

22. **DIGIPASS -** dispozitiv de securitate fizic, de tip hard token, fiind utilizat la accesarea serviciului de Internet Banking.

23. **PIN DIGIPASS** – cod de securitate, stabilit de către Utilizator, care permite utilizarea DIGIPASS-ului și care se blochează după 5 introduceri greșite ale acestuia.

24. **Cod generat de DIGIPASS –** cod furnizat de către DIGIPASS, în baza solicitării Utilizatorului:
(i) la autentificarea în e-xim Banking,
(ii) la acordarea/retragerea consimțământului unui TPP pentru a accesa Conturile de plăți accesibile online deținute de Client la Bancă și/sau pentru a iniția plăți din Conturile de plăți accesibile online deținute de Client la Bancă și (iii) la autorizarea operațiunilor prin e-xim Banking.

24. **Cod primit prin SMS-** - cod unic generat de aplicație și transmis Utilizatorului prin SMS, pe numărul de telefon mobil comunicat de Client Băncii. Metoda de autentificare/autorizare, prin cod SMS, presupune existența unui telefon mobil al cărui număr a fost comunicat Băncii și care a fost configurat la nivel de utilizator în aplicația de administrare e-xim Banking. Cartela SIM, pe al cărei număr de telefon se primește SMS–ul cu codul unic utilizat pentru autentificare, trebuie păstrată în siguranță.

25. **Cod HASH** - cod generat pe baza unui algoritm specific ce are la bază detalii alte tranzacțiilor, respectiv suma tranzacției/tranzacțiilor și informații ale IBAN-ului(rilor) beneficiarului(lor) operațiunii.

26. **Cod acces-** serie de caractere numerice stabilita de Utilizator, utilizat pentru:
(i) accesarea Serviciului e-xim Banking sau pentru autorizare tranzacții;
(ii) la acordarea/retragerea consimțământului unui TPP, pentru a accesa Conturile de plăți accesibile online deținute de Client la Bancă și/sau pentru a iniția plăți din Conturile de plăți accesibile online deținute de Client la Bancă și
(iii) la autorizarea operațiunilor prin e-xim Banking.

27. **Mobile Token -** aplicație integrată a aplicației mobile, de tip Mobile Banking, ce are ca rol principal aprobarea/autorizarea anumitor operațiuni în condiții de securitate ridicată, având la bază setarea unui Cod de acces.

28. **Amprentă digitală / Recunoaștere facială (Face ID)**: date biometrice ale Utilizatorului, cum au fost înregistrate în dispozitivul (telefon mobil) Utilizatorului, și care sunt folosite de acesta, pentru accesarea Serviciului e-xim Banking. Clientul poate opta pentru utilizarea Amprentei digitale sau a Face ID, în funcție de opțiunea acestuia. Această opțiune poate fi dezactivată oricând de către Utilizator, din meniul ,,Setări" al aplicației mobile. Totodată, această opțiune se dezactivează automat atunci când dispozitivul utilizat nu mai este înregistrat pentru utilizări viitoare.

Stocarea datelor biometrice - datele sunt stocate doar la nivel local în dispozitivul mobil și validate de dispozitivul mobil. Aplicația Mobile Banking nu stochează informații de natură biometrică.

29. **Zi bancară** - orice zi calendaristică, cu excepţia zilelor de sâmbătă şi duminică şi a sărbătorilor legale din România.

30. **CGA** - Condițiile Generale de Afaceri ale Exim Banca Românească S.A. semnate de Client la data deschiderii relației de afaceri cu Banca, precum și oricare și toate modificările aduse acestora din timp în timp și care se regăsesc pe siteul băncii www.eximbank.ro.

II. ACCESAREA ȘI UTILIZAREA SERVICIULUI

1. Pentru a beneficia de e-xim Banking, Clientul solicită Băncii activarea acestui serviciu prin completarea formularelor specifice (Formulare).

2. Banca își rezervă dreptul de a refuza furnizarea serviciului e-xim Banking sau de a restricționa accesul clienților la acest serviciu, total sau pentru o parte dintre tipurile de operațiuni disponibile în meniu, de a impune anumite limite de tranzacționare, conform politicii sale în materia cunoașterii clientelei, prevenirii spălării banilor și finanțării terorismului.
Banca impune clienților săi limite zilnice de tranzacționare, cât și limite aferente plăților instant.
Limitele plăților instant se regăsesc pe site-ul Băncii, în rubrica Documente utile: https://www.eximbank.ro/documente-diverse/.
Utilizatorul poate modifica oricând limita plăților instant prin apelarea Serviciului de Suport. Aceste limite se pot modifica, în sensul diminuării acestora, față de limita standard sau se poate solicita chiar și limita 0, astfel încât plățile să se direcționeze către transferurile standard.
Clientul ia la cunostință si acceptă în mod expres ca, în cazul în care o persoană fizică, desemnată Utilizator cu drept de aprobare, în cadrul Serviciului e-xim Banking, să poată solicita modificarea limitei plăților instant.la nivel de Client.

3. Termenii și Condițiile e-xim Banking (inclusiv documentele menționate ca făcând parte integrantă din acestea), împreună cu Formularele formează documentația contractuală specifică / aplicabilă Serviciului e-xim Banking care se completează cu prevederile CGA și cu prevederile legale în vigoare. In caz de discrepanțe între CGA și documentația contractuală specifică, prevederile acesteia din urmă vor prevala față de prevederile CGA. In caz de discrepanțe între prevederile legale în vigoare și documentația contractuală specifică (inclusiv CGA), prevederile legale vor prevala. Prezentul document

4.

5. reglementează, printre altele, drepturile și obligațiile Clientului în cazul în care TPP prestează Clientului AIS și PIS în legătură cu unul sau mai multe Conturi de plăți accesibile online deținut(e) de Client la Bancă.

6. După aprobarea de către Bancă a Formularelor, aceasta furnizează Clientului un exemplar al Termenilor și Condițiilor exim Banking, iar fiecărui Utilizator:

a) elementele de securitate, respectiv, Identificatorul Utilizator. Parola e-xim Banking se va seta obligatoriu de Utilizator la prima conectare la Serviciul de Internet Banking, prin resetare de parolă, în baza Identificatorului Utilizator primit de la Bancă și a CNP/echivalent--ului, respectiv a actului de identitate înregistrat, în cazul persoanelor nerezidente. Acestea vor fi transmise/retransmise (la solicitarea Utilizatorului) printr-o metodă securizată (în plic confidențial sigilat, care se înmânează personal Utilizatorului sau prin intermediul poștei electronice/ adresei de e-mail declarată de client Băncii, utilizând un document protejat cu parolă).

b) DIGIPASS-ul în stare blocată (dacă se optează pentru autentificare prin cod unic generat de DIGIPASS).

7. Utilizarea e-xim Banking:

a) **Pentru accesarea versiunii web e-xim Banking** este necesar un calculator/ telefon mobil/ tabletă conectat/ă la internet și un browser de internet.

b) **Pentru accesarea versiunii mobile e-xim Banking** este necesară instalarea aplicației specifice din magazinele dedicate pentru sistemele de operare, pe un dispozitiv mobil (smartphone, tabletă), cu acces la internet

6. Elementele de securitate necesare Utilizatorului pentru accesarea e-xim Banking (inclusiv pentru autorizarea tranzacțiilor), utilizând versiunea web sunt următoarele:

a) Identificator Utilizator;
b) Parolă e-xim Banking;
c) CNP/echivalent (se solicită doar pentru prima setare a parolei sau pentru resetarea parolei, direct din aplicație);
d) PIN DIGIPASS (dacă se optează pentru autentificare prin cod unic generat de DIGIPASS);
e) Cod generat de DIGIPASS/ cod unic primit prin SMS pe numărul de telefon mobil comunicat de Client Băncii sau Mobile Token, accesibil doar după instalarea aplicației mobile.

Pentru autorizarea operațiunilor, cu ajutorul Digipass-ului, se folosește funcția E-SIGN care asigură o legătură dinamică între suma operațiunii și beneficiarul acesteia, prin introducerea în DIGIPASS a unui cod, denumit Cod HASH, definit mai sus. Digipass-ul este predat în stare blocată de către Bancă, iar deblocarea acestuia (in vederea setării unui PIN) se poate face doar de către Utilizator, prin intermediul serviciului HelpDesk.
Digipass-ul este predat în stare blocată de către Bancă, iar deblocarea acestuia se poate face direct de către Utilizator, prin intermediul serviciului HelpDesk

7. Elementele de securitate necesare Utilizatorului pentru accesarea e-xim Banking (inclusiv pentru autorizarea tranzacțiilor), utilizând aplicația mobilă sunt următoarele:

a) Identificator Utilizator;
b) CNP/echivalent (necesar pentru instalare/reistalare);
c) e-mail primit la adresa de e-mail comunicată de Client Băncii (validare link primit, pentru instalare/reinstalare);
d) cod unic primit prin SMS pe numărul de telefon mobil comunicat de Client Băncii (necesar pentru instalare/reinstalare);
e) PIN (setare Cod Access, folosit pentru accesare aplicație/autorizare prin Mobile Token integrat);
f) f) Biometrie (opțional).

Instrucțiunile de utilizare a e-xim Banking pot fi consultate de către Client și/sau Utilizatori în **Manualul de utilizare.**

8. Clientul și Utilizatorii sunt obligați să păstreze confidențialitatea elementelor de securitate menționate la pct. 5 de mai sus,

precum și a oricăror altor elemente de securitate furnizate de către Bancă. Orice divulgare voluntară sau involuntară (pierdere, sustragere etc.) va fi considerată a fi făcută pe riscul şi răspunderea Clientului. Clientul şi/sau Utilizatorii vor anunța imediat Banca prin serviciul Help Desk sau Call Center Carduri despre orice divulgare şi utilizare frauduloasă a elementelor de securitate, iar aceasta va bloca serviciul E-xim Banking până la atribuirea unor noi elemente de securitate pentru Utilizator, după preluarea notificării, prevederile *Cap. III, clauza 9, litera f)* aplicându-se în mod corespunzător.

Dacă Utilizatorul folosește greșit: de 3 ori consecutiv Parola e-xim Banking, 5 încercări eronate ale PIN-ului Digipass sau de 5 ori codul de validare furnizat de Digipass-ul fizic sau 5 încercări eronate ale codului primit prin SMS, va fi blocat automat de sistemul Băncii.

Dacă Utilizatorul folosește de 3 ori consecutiv PIN-ul/biometria greșit/ă, la accesarea aplicației mobile sau la autorizarea operațiunilor, aplicația se blochează și necesită reinstalare.

Pentru cazul în care Utilizatorul își blochează parola (prin introducerea a 3 încercări eronate), în aplicația de tip web, acesta are posibilitatea de a-și reseta parola, direct în aplicație, utilizând Identificatorul utilizator, CNP-ul (pentru persoane rezidente) sau echivalent (pentru persoane nerezidente) și codul de validare generat de Digipass, codul primit prin SMS sau utilizând Mobile Token-ul. În situația în care nu se reușește deblocarea direct din aplicație, Utilizatorul poate contacta serviciul HelpDesk.

Pentru cazul în care Utilizatorul își blochează PIN-ul/ biometria (prin introducerea a 3 încercări eronate), acesta are posibilitatea de a-și reinstala aplicația mobilă, conform pașilor regăsiți în Manualul de utilizare. Utilizatorul poate contacta serviciul HelpDesk pentru suport.

Activarea Digipass-ului și deblocarea posibilitatii de utilizare a metodei de autentificare/ autorizare (prin Digipass-ul fizic sau prin SMS) se poate face doar telefonic cu suportul serviciul HelpDesk, după identificarea corespunzătoare a Utilizatorului.În cazul în care solicit area vine din partea Utilizatorului, pe alt canal, decât cel telefonic, serviciul HelpDesk va indica Utilizatorului necesitatea apelului telefonic, în vederea soluționării solicitării.
Pentru situații excepționale, când identificarea telefonică eșuează, telefonic, deblocarea se poate face printr-o solicitare scrisă din partea companiei (semnată de reprezentanții legali), transmisă prin intermediul Băncii.

9. Banca nu oferă suport pentru sistemele hardware sau software ale Clientului şi nu răspunde de securitatea sistemului informatic al Clientului. Banca nu va fi responsabilă în cazul în care Utilizatorii nu pot avea acces la e-xim Banking din cauza deficienţelor de conectare care ţin de echipamentele Utilizatorilor sau din culpa altor persoane fizice sau juridice, altele decât Banca.

10. Banca nu este răspunzătoare pentru pierderi sau alte daune pe care Clientul le-ar putea avea din cauza întreruperii furnizării e-xim Banking din motive de natură tehnică. Banca va remedia defecțiunile apărute în funcționarea e-xim Banking în termen de 3 zile lucrătoare de la sesizarea de către Client. În aceste situații, Clientul va putea efectua operațiuni prin celelalte mijloace puse la dispoziția sa de către Bancă.

11. Rețeaua publică Internet este în afara controlului Băncii, care nu poate fi răspunzătoare în cazul în care rețeaua publică de Internet este compromisă, caz asimilat cu forța majoră.

12. Banca are drept exclusiv de proprietate asupra programelor software şi a întregii documentații (inclusiv asupra Manualului de utilizare), care privesc e-xim Banking şi care sunt puse la dispoziția Clientului si Utilizatorilor numai pe perioada de valabilitate a documentației contractuale specifice Serviciului e-xim Banking.

13.

14. Clientul nu va atribui altor persoane, fără acordul prealabil al Băncii, drepturile ce decurg din calitatea sa de beneficiar al serviciului e-xim Banking.

III. OPERAȚIUNI PRIN e-xim Banking

1. Clientul, prin Utilizatori, poate efectua prin serviciul e-xim Banking toate tipurile de operațiuni disponibile (astfel cum sunt acestea indicate în *Cap. I, clauza 9* de mai sus), în condițiile și limitele prevăzute în Formulare. Banca poate defini anumite limite zilnice/ standard de tranzacționare.

2. Clientul autorizează în mod expres și irevocabil Banca să execute instrucțiunile trimise prin intermediul e-xim Banking de către Utilizatorii mandatați și în limitele mandatului acordat acestora.

3. Banca execută instrucțiunile Utilizatorilor pentru care s-au folosit elementele de securitate menționate în *Cap. II, clauza 5* de mai sus, instrucțiunile fiind considerate astfel autentice și corecte.

4. Condiții specifice privind AIS și PIS prestate Clientului de către un TPP cu privire la unul sau mai multe Conturi de plăți accesibile online deținut(e) de Client la Bancă:

4.1. Clientul poate obține de la Bancă prin intermediul unui AISP informații consolidate referitoare la unul sau mai multe Conturi de plăți accesibile online deținut(e) de Client la Bancă. Pentru a obține în acest mod informațiile despre conturile sale, Clientul, printr-un Utilizator cu/fără drept de semnătura, își va exprima consimțământul prin intermediul aplicației AISP, folosind aceleași elemente de securitate pe care le utilizează și la Autentificarea strictă în aplicația e-xim Banking, astfel cum acestea sunt detaliate în Cap. I, clauza 16 litera a) de mai sus. Valabilitatea consimțământului este limitată la maxim 90 zile de la acordare, după care va fi necesară acordarea unui nou consimțământ conform celor descrise la prezentul punct.

Clientul poate revoca consimțământul acordat unui AISP prin accesarea aplicației AISP și folosirea elementelor de securitate utilizate la Autentificarea Strictă. Clientul, prin semnarea prezentului document, declară că înțelege și acceptă faptul că:
(i) după revocarea consimțământului acordat unui AISP, Banca va refuza orice cerere primită din partea respectivului AISP și (ii) pentru noi accesări ale informațiilor de către respectivul AISP, va fi nevoie de un nou consimțământ.
Clientul este răspunzător pentru orice dată și/sau informație divulgată(e) AISP, Banca nefăcând nicio divulgare de date (inclusiv de date cu caracter personal) și/sau informații, prin transmitere, diseminare sau prin altă formă de punere la dispoziție, către AISP până la momentul acordării accesului la Contul(rile) de plăți accesibil(e) online deținut(e) de Client la Bancă, conform procedurii descrise la prezentul punct 4.1. sau după retragerea consimțământului acordat AISP.

4.2. Clientul are dreptul să inițieze un ordin de plată dintr-un Cont de plăți accesibil online prin intermediul unui PISP. Pentru ca Banca să execute un ordin de plată inițiat de un PISP dintr-un Cont de plăți accesibil online deținut de Client la Bancă Clientul, printr-un Utilizator cu drept de semnătura, trebuie să autorizeze instrucțiunea, prin aplicația PISP, folosind elementele de securitate, astfel: (i) inițial, elementele de securitate pe care le utilizează și la Autentificarea strictă în aplicația e-xim Banking, astfel cum sunt acestea detaliate în Cap. I, clauza 16 litera a) de mai sus și (ii) ulterior, elementele de securitate pe care le utilizează pentru Autorizare, astfel cum sunt acestea detaliate în Cap. I, clauza 16 litera b) de mai sus. Consimțământul (autorizarea) se acordă la fiecare plată/fișier de plăți inițiate(e) de PISP. După acordarea consimțământului (autorizării), Clientul nu va putea revoca ordinul de plată inițiat prin intermediul PISP, cu excepția plăților recurente sau a celor introduse cu data de procesare viitoare.

4.3. Clientul este răspunzător pentru orice dată și/sau informație divulgată(e) PISP, Banca nefăcând nicio divulgare de date (inclusiv de date cu caracter personal) și/sau informații, prin transmitere, diseminare sau prin altă formă de punere la dispoziție, către PISP până la momentul autorizării realizate conform procedurii descrise la prezentul

4.4. punct 4.2., sau după retragerea consimțământului (autorizării).

5. Banca nu are nicio responsabilitate pentru neexecutarea instrucțiunilor date de Utilizatori, ca urmare a disponibilului insuficient din contul(rile) Clientului, a blocării contului(rilor) prin adrese de înființare de popriri, prin ordonanțe dispuse de organele judiciare ori de către alte instituții abilitate în acest sens prin lege, ca urmare a nerespectării oricăror angajamente asumate de Client față de Bancă sau dacă, în aprecierea Băncii, instrucțiunile i-ar putea cauza acesteia un prejudiciu.
Operațiunile instructate prin intermediul e-xim Banking vor fi executate de Bancă numai în măsura în care Utilizatorii au urmat toate etapele necesare realizării operațiunilor și au respectat dispozițiile legale în vigoare.

6. Momentul primirii unei instrucțiuni transmisă prin e-xim Banking este reprezentat de data şi ora la care instrucțiunea are afișată în e-xim Banking starea „În curs de procesare" în dreptul operațiunii instructate în cadrul e-xim Banking de către Client prin Utilizatori. Operațiunile sunt procesate, conform Orarului de procesare plăți regăsit pe site-ul Băncii, în rubrica Documente utile sau direct în aplicația e-xim Banking.

7. O instrucțiune transmisă de către Client prin intermediul e-xim Banking este considerată ca fiind autorizată de către acesta şi executată de către Bancă numai dacă aceasta ajunge în starea „Procesat cu succes". Dacă executarea unei

instrucțiuni este programată pentru o anumită zi, Clientul o poate revoca cel târziu până la sfârșitul zilei lucrătoare care precede ziua convenită. În cazul în care una sau mai multe instrucțiuni transmise Băncii de către Client nu sunt reflectate în extrasele de cont, Clientul va contacta imediat Banca pentru clarificarea situației.

8. În cazul în care disponibilul din contul Clientului nu acoperă integral operațiunea instructată de către Client prin Utilizatori sau Banca observă o eroare în datele completate de Utilizatori, executarea operațiunii va fi refuzată de Bancă. Refuzul va fi notificat Clientului în e-xim Banking prin afișarea stării „Respins/anulat" în dreptul operațiunii.

9. Clientul şi fiecare Utilizator au obligația:

a) să utilizeze e-xim Banking cu respectarea Termenilor și Condițiilor e-xim Banking, a prevederilor CGA și a legislației în vigoare;
b) să instructeze operațiuni numai cu respectarea prevederilor legale în vigoare şi cu indicarea tuturor informațiilor necesare efectuării acestora;
c) să utilizeze ordine de plată în conformitate cu termenii care reglementează emiterea şi utilizarea acestora; o instrucțiune de plată trebuie să conțină elementele obligatorii de identificare a beneficiarului (ex.: numărul de cont IBAN al beneficiarului);
d) la solicitarea Băncii, să prezinte în termen de maximum 10 zile bancare de la instructarea operațiunii, documentele justificative prevăzute de lege, în original (e.g. factura pro-formă, factura, declarația vamală, alte documente); e) să respecte indicațiile și/sau etapele din Manualul de utilizare;
f) să notifice/contacteze Banca prin serviciul Help Desk sau Call Center Carduri, fără întârziere nejustificată, de îndată ce ia cunoștință de pierderea, furtul, deteriorarea, distrugerea, deturnarea elementelor de securitate (inclusiv a DIGIPASS-ului sau telefonului mobil) sau de orice utilizare neautorizată a acestora sau a e-xim Banking.
Notificarea nu va presupune niciun cost pentru Client și va fi preluată de Bancă imediat, în timpul programului său de lucru (astfel cum apare acesta menționat pe site-ul Băncii www.eximbank.ro - Imediat după preluarea notificării telefonice, realizate conform celor menționate anterior, Banca va bloca accesul la e-xim Banking până la furnizarea unui nou set de elemente de securitate și/sau a unui nou DIGIPASS. Ulterior preluării notificării, utilizarea e-xim Banking

nu va mai fi posibilă și nicio instrucțiune de plată primită ulterior notificării telefonice nu va fi procesată de către Bancă.

Până la momentul notificării telefonice, Clientul este răspunzător pentru toate operațiunile efectuate, urmând să suporte pierderile aferente acestor operațiuni. Clientul este deplin răspunzător dacă, prin neglijența sa sau în mod fraudulos sau prin încălcarea prevederilor legale, elementele de securitate (inclusiv DIGIPASS-ul,cartelă SIM, pe al cărei număr de telefon se primește SMS sau dispozitivul mobil, pe care este instalată aplicația Mobil Banking) sunt pierdute, furate, deteriorate, distruse, folosite fără drept sau toate acestea sau e-xim Banking sunt/este utilizat(e) în mod neautorizat;

g) să ia toate măsurile rezonabile pentru a păstra în siguranță elementele de securitate personalizate (inclusiv DIGIPASS, telefon/dispozitiv mobil/cartela SIM);
h) să despăgubească integral Banca pentru orice pierderi, amenzi, penalități sau cheltuieli de orice natură suportate în urma efectuării unor operațiuni instructate de Client prin Utilizatori cu încălcarea prevederilor legale în vigoare sau ca o consecință a nerespectării instrucțiunilor Băncii; pentru toate și oricare din aceste sume reprezentând pierderi, amenzi, penalități sau cheltuieli de orice natură suportate de Bancă, Banca va percepe dobânda legală pentru fiecare zi de întârziere în plată de către Client a acestor obligații;
i) să informeze în scris Banca, imediat și explicit, despre orice modificare cu privire la situația sa juridică inclusiv, dar fără a se limita la schimbare denumire, schimbare sediu, schimbare drept de reprezentare etc., alăturând respectivei informări documentele justificative ale modificărilor.

10. Clientul este răspunzător pentru felul în care terţe persoane utilizează e-xim Banking, în situația în care acestora leau fost dezvăluite, în orice mod, de către Client și/sau Utilizatori elementele de securitate, suportând toate pierderile izvorâte, Banca fiind exonerată de răspundere pentru oricare pierdere sau prejudiciu suferit de Client ca urmare a nerespectării Termenilor și Condițiilor e-xim Banking.

11. În cazul în care Clientul decide modificarea datelor din Formular (e.g. schimbarea persoanelor care au calitatea de Utilizatori, modificarea competențelor acordate etc.), va actualiza informațiile din Formular.

IV. RESPONSABILITĂȚILE PĂRȚILOR

1. Banca își rezervă dreptul ca, din motive justificate obiectiv, legate de securitatea e-xim Banking sau de suspiciuni de utilizare neautorizată sau frauduloasă a acestuia, să blocheze serviciul e-xim Banking. Banca procedează la deblocare, imediat ce motivele de blocare încetează să mai existe.

2. Banca are obligația de a se asigura că elementele de securitate personalizate nu sunt accesibile altor părți în afară de Client și Utilizatorii care au dreptul să utilizeze e-xim Banking, fără a aduce atingere obligațiilor acestora prevăzute în Termenii și Condițiile e-xim Banking și în legislație.

3. Banca are obligația de a se asigura că în orice moment sunt disponibile mijloace corespunzătoare care să permită Clientului și Utilizatorilor să facă notificarea prevăzută în *Cap. II, clauza 6 și în Cap. III, clauza 9, litera f)* de mai sus sau să ceară deblocarea e-xim Banking.

4. Banca va pune la dispoziția Clientului, la cerere, timp de 18 luni de la notificarea menționată mai sus, mijloacele de a dovedi că a făcut o astfel de notificare.

5. Banca are dreptul să refuze executarea oricărei operațiuni instructate, ulterior notificării prevăzute în *Cap. II, clauza 6 și în Cap. III, clauza 9, litera f)* de mai sus.

6. Banca are dreptul de a suspenda pe termen nedeterminat efectuarea de către Client, prin intermediul e-xim Banking, a unui tip de operațiuni (e.g. operațiuni de plăți), în situaţia în care Clientul nu își respectă obligațiile prevăzute în *Cap. III, clauza 9, litera i)* și/sau *în Cap. III, clauza 11* de mai sus.

7. Banca va permite unui TPP accesul la unul sau mai multe Conturi de plăți accesibile online deținut(e) de Client la Bancă și/sau va executa instrucțiuni de plată inițiate prin intermediul aplicației acestuia doar dacă sunt îndeplinite condițiile legale de acces, precum și cele menționate în acest document.

8. Banca poate refuza accesul unui AISP sau al unui PISP la un cont curent accesibil online în cazul în care există motive justificate în mod obiectiv și susținute de dovezi corespunzătoare legate de accesarea neautorizată sau frauduloasă a contului curent accesibil online de către AISP sau PISP, inclusiv de inițierea neautorizată sau frauduloasă a unei instrucțiuni de plată de către PISP. În acest caz, Banca va comunica Clientului faptul că accesul AISP sau al PISP a fost refuzat și motivele acestui refuz, cu excepția cazului în care comunicarea este împiedicată de motive de siguranță justificate sau dacă prevederile legale aplicabile interzic o astfel de conduită.

9. Banca este exonerată de răspundere în cazul în care Clientul e-xim Banking a retras mandatul unui Utilizator, dar nu a adus la cunoștința Băncii, în scris, retragerea mandatului, iar Utilizatorul revocat a autorizat instrucțiuni de plată în numele și pe seama Clientului.

10. În situația în care Clientul se consideră prejudiciat în urma neefectuării/efectuării necorespunzătoare de către Bancă a unei operațiuni instructate prin e-xim Banking, acesta o poate contesta în scris în termen de maximum 10 zile lucrătoare de la data înscrierii operațiunii în contul său. Banca va răspunde în scris Clientului în termen de maximum 10 zile de la data primirii contestației. În situația în care Clientul nu este satisfăcut de răspunsul Băncii şi se consideră în continuare prejudiciat, se poate adresa instanței competente.

11. Operațiunile instructate prin e-xim Banking vor fi executate de Bancă numai în măsura în care Utilizatorul a urmat toate etapele necesare realizării acestora şi a respectat instrucțiunile scrise, atât cele din formularele electronice din exim Banking, cât şi cele din mesajele automate apărute în timpul efectuării operațiunilor.

12. Clientul suportă pierderile legate de orice operațiuni neautorizate care rezultă din încălcarea de către Client a obligației de a lua toate măsurile rezonabile pentru a păstra în siguranță elementele de securitate personalizate, operațiuni finalizate până la momentul notificării realizate conform prevederilor din *Cap. II, clauza 6 și/sau Cap. III, clauza 9, litera f)* de mai sus.

13. Evaluarea răspunderii Clientului se face ținând cont, înspecial, de natura elementelor de securitate afectate şi de situațiile în care acestea au fost pierdute, furate sau folosite fără drept.

14. Clientul nu suportă nicio consecință financiară care rezultă din procesarea unei instrucțiuni după notificarea realizată conform prevederilor din *Cap. II, clauza 6 și/sau Cap. III, clauza 9, litera f)* de mai sus, exceptând cazul în care acesta a acționat în mod fraudulos.

15. Clientul are obligația să informeze Utilizatorii despre prevederile Termenilor și Condițiilor e-xim Banking, acestea fiindu-le opozabile în egală măsură. Clientul este responsabil pentru utilizarea produselor/serviciilor de către Utilizatori, toate operațiunile fiindu-i opozabile Clientului, care suportă eventualele prejudicii produse. Clientul se obligă să notifice Băncii orice anulări/modificări a oricărora dintre drepturile acordate Utilizatorilor, acestea fiind opozabile

16. Băncii numai după completarea formularului specific pus la dispoziție de Bancă.

17. Clientul are obligația ca la orice modificare a specimenului de semnături, care ar avea drept consecință retragerea/ modificarea drepturilor de autorizare ale unui utilizator, să depună și documentul necesar anulării, respectiv actualizării drepturilor în aplicația e-xim Banking.

18. Clientul înțelege și acceptă că, în conformitate cu prevederile legale aplicabile, în situațiile în care interfața între aplicația TPP și aplicațiile Băncii nu funcționează la nivelul standardelor sau este indisponibilă, Banca va permite TPP, ca parte a unui mecanism de urgență, să utilizeze interfața aplicației de internet banking pusă la dispoziția Clientului pentru autentificare și comunicare cu Banca. TPP este obligat să ia toate măsurile necesare pentru a nu accesa, stoca sau prelucra datele Clientului decât în scopul furnizării serviciului solicitat de Client. În situația aplicării măsurilor de urgență prevăzute de prezentul articol, pentru prestarea AIS și PIS, TPP este exclusiv și pe deplin responsabil în ceea ce privește utilizarea interfeței Serviciului e-xim Banking, înregistrarea datelor accesate prin Serviciului E-xim Banking și informarea Băncii despre această utilizare.

V. CONDIȚII FINANCIARE

1. e-xim Banking este comisionat conform prevederilor Comisioanelor Exim Banca Românească S.A. / Ofertelor personalizate în vigoare la data perceperii comisionului(lor).

2. Operațiunile instructate de Client prin e-xim Banking sunt comisionate de Bancă conform Comisioanelor Exim Banca Românească S.A./ Ofertelor personalizate în vigoare la data executării operațiunii, Clientul autorizând Banca să debiteze contul său cu valoarea acestora.

3. Comisioanele percepute pentru fiecare DIGIPASS solicitat pentru Utilizatorii e-xim Banking, desemnați în Formular, se regăsesc în Comisioane Exim Banca Românească S.A. în vigoare la data predării acestora către Client.

4. Banca este îndreptățită să rețină comisionul aferent digipass-ului (constituit cu garantie) în următoarele cazuri:

a) Clientul nu restituie Băncii DIGIPASS-ul în termen de 15 zile de la data înștiințării Băncii cu privire la renunțarea la serviciul e-xim Banking, conform prevederilor *Cap. VII, clauza 4, litera a)* de mai jos;

b) Clientul nu restituie Băncii DIGIPASS-ul în termen de 15 zile de la data la care Banca blochează accesul și/sau utilizarea e-xim Banking sau Banca încetează furnizarea acestui serviciu în conformitate cu oricare dintre situațiile prevăzute în *Cap.VII, clauza 3 și clauza 4* de mai jos;

c) Clientul solicită Băncii înlocuirea DIGIPASS-ului ca urmare a pierderii, furtului, distrugerii sau deteriorării acestuia. În aceste cazuri, înlocuirea dispozitivului de autentificare și reconectarea la serviciul de e-xim Banking se face doar după achitarea comisionului aferent.

VI. DURATA UTILIZĂRII e-xim Banking. FORȚA MAJORĂ

1. Clientul poate utiliza e-xim Banking pe o durată nedeterminată, începând cu data primirii Termenilor și Condițiilor e-xim Banking, a credențialelor, a DIGIPASS-ului și a Manualului de utilizare, conform prevederilor *Cap. II, clauza 3* de mai sus.

Forța majoră, așa cum este definită de lege, incluzând și compromiterea rețelei Internet, suspendă de drept, pe perioada existenței evenimentului de forță majoră, utilizarea de către Client a e-xim Banking. Partea care invocă forța majoră va aduce la cunoștință celeilalte Părți acest lucru, în scris, în termen de 3 zile calendaristice de la data producerii evenimentului. În situația în care evenimentul de forță majoră durează mai mult de 30 de zile, oricare dintre Părți poate denunța Termenii și Condițiile e-xim Banking.

VII. ALTE CLAUZE

1. Clientul se obligă să nu furnizeze către nicio terță persoană informații de securitate legate de serviciul e-xim Banking, sistemul de acces la acest serviciu, DIGIPASS, telefonul/dispozitiv mobil/cartelă SIM și elementele de securitate.

2. Clientul declară că a fost informat cu privire la drepturile și obligațiile care îi revin din utilizarea serviciului e-xim Banking și că a primit, la cererea sa, Comisioanele Exim Banca Românească S.A. și un exemplar al Manualului de utilizare.

3. Banca are dreptul (dar nu și obligația) de a bloca accesul și/sau utilizarea e-xim Banking, fără informarea prealabilă a Clientului, cu excepția cazului în care însuși Clientul a solicitat acest lucru în mod expres, în scris, în următoarele situații:

a) Clientul nu a păstrat și nu a asigurat confidențialitatea tuturor elementelor de securitate, precum și a altor elemente de securitate ce i-au fost furnizate de către Bancă și nu a notificat Banca, conform prevederilor Termenilor și Condițiilor exim
Banking, cu privire la orice divulgare și utilizare frauduloasă a elementelor de securitate;

b) Operațiunile instructate de către Client nu pot fi aduse la îndeplinire de către Bancă ca urmare a faptului că acestea presupun riscuri de securitate a operațiunii sau interdicții și restrângeri prevăzute de legislație, cum ar fi prevenirea spălării banilor și combaterea terorismului;

c) Clientul încalcă orice altă obligație ce îi revine potrivit Termenilor și Condițiilor e-xim Banking;

d) Când s-au instituit măsuri asiguratorii pe contul(rile) Clientului de către autoritățile competente, când s-au înființat popriri de către executorul judecătoresc, bugetar și/sau în alte cazuri similare care fac obligatorie pentru Bancă blocarea contului(rilor). Deblocarea accesului la cont(uri) se va realiza numai după încetarea cauzei care a condus la blocarea contului(rilor).

e) Când utilizatorii, cu drept de semnătură, sunt inactivi în aplicația e-xim Banking mai mult de 6 luni.

4. Banca încetează furnizarea serviciului e-xim Banking, Termenii și Condițiile e-xim Banking încetându-și valabilitatea, în următoarele situații:

a) prin denunțare unilaterală a Termenilor și Condițiilor e-xim Banking, la inițiativa oricăreia dintre părți, cu un preaviz de cel puțin 15 zile calendaristice; e-xim Banking va înceta a mai fi furnizat la expirarea termenului de 15 zile calendaristice, calculat de la data primirii notificării scrise privind denunțarea unilaterală a Termenilor și Condițiilor e-xim
Banking;

b) de plin drept și fără obligația vreunei notificări, în cazul în care Clientul închide toate conturile curente deschise la Bancă;

c) de plin drept și fără obligația vreunei notificări, în cazul în care Clientul acumulează restanțe la comisioanele aferente serviciului e-xim Banking, mai mult de 6 luni;

d) cauzele care atrag blocarea accesului și/sau a utilizării serviciului e-xim Banking durează mai mult de 30 de zile calendaristice; în acest caz, Banca își rezervă dreptul unilateral de a considera încetat furnizarea serviciului e-xim Banking, notificând ulterior Clientul cu privire la încetarea furnizării serviciului e-xim Banking;

e) de plin drept și imediat, fără obligația vreunei notificări, atunci când Banca va considera că este expusă riscurilor legale, reputaționale sau operaționale, ca urmare a tranzacțiilor derulate de Client sau când Clientul nu-și execută obligațiile stabilite prin Termenii și Condițiile e-xim Banking;

f) dacă una dintre părți își încetează activitatea, indiferent de motiv, este supusă procedurii insolvenței (dacă Clientului i s-a retras dreptul de a-și administra conturile), falimentului sau dacă, cu privire la una dintre părți, a fost instituită de către instanța competentă procedura de lichidare.

5. Obligațiile Clientului și ale Utilizatorului, precum și drepturile Băncii născute în baza Termenilor și Condițiilor e- xim Banking vor rămâne în vigoare până la restituirea DIGIPASS-ului(rilor) (dacă este cazul) și plata integrală de către Client a tuturor sumelor datorate Băncii în baza Termenilor și Condițiilor e-xim Banking.

6. Banca își rezervă dreptul de a introduce condiții suplimentare ce ar modifica utilizarea de către Client a serviciului e-xim Banking în situația schimbărilor legislative, actualizări de funcționalități și sau de securitate, sau a normelor interne ale Băncii. Modificările menționate anterior vor fi aduse la cunoștință Clientului de către Bancă prin afișare pe pagina internet www.eximbank.ro și/sau prin una dintre modalitățile agreate de comun acord cu Clientul. Clientul este de acord că această modalitate reprezintă o notificare și o înștiințare suficientă cu privire la modificările efectuate de Bancă. Clientul înțelege să verifice periodic pagina de internet a Băncii pentru a se informa cu privire la varianta în vigoare a Termenilor și Condițiilor e-xim Banking, a Comisioanelor și a Orarului de procesare plati.

7. Clientul înțelege că obligațiile pe care și le asumă și declarațiile pe care le formulează, în conformitate cu prevederile și în baza Termenilor și Condițiilor e-xim Banking, incumbă și aparțin în egală măsură și Utilizatorilor și, în consecință, se obligă să comunice acestora termenii și condițiile de utilizare a e-xim Banking. Totodată, Clientul înțelege că este singur răspunzător față de Bancă pentru orice neconformare a Utilizatorilor, în condițiile Termenilor și Condițiilor e-xim Banking.

Prezentul document s-a semnat **astăzi**, …… , în două exemplare originale, câte unul pentru fiecare parte, și intră în vigoare la data semnării sale de către ambele părți.

Denumire Client:

_____

Nume și prenume Reprezentant Legal:

_____

Semnătură:

Bancă:

Nume și prenume Manger Relații Clienți:

_____

Semnătură:

Nume și prenume Director Unitate:

_____

Semnătură:

Exim Banca Românească

România crește cu noi!

Anexa 1 la Termeni şi condiţii privind utilizarea e-xim Banking

Funcționalități e-xim Banking

Funcționalitățile principale ale e-xim Banking:

- obținerea informațiilor cu privire la contul(rile) Clientului accesibil(e) prin e-xim Banking și a operațiunilor efectuate;
- generarea de extrase de cont;
- efectuarea de schimburi valutare;
- constituirea și lichidarea de depozite;
- schimbare/resetare PIN/Parolă;
- operațiuni de plată în/din acest(e) cont(uri):

  ☑ în lei

Efectuarea operațiunilor de plată, efectuarea de schimburi valutare, constituirea de depozite se derulează cu respectarea limitelor zilnice standard impuse de Bancă și pe tranzacție în cazul plăților instant, a orarului de procesare și/sau a celor menționate în formularele specifice de setare acces la e-xim Banking.

DATA:

Nume și Prenume Reprezentant Legal :

Semnătură Reprezentant Legal:

_____

Verificat de Bancă:
Nume și Prenume:

Manager Relații Clienți:

Semnătură:

_____

Director Unitate Teritorială:

Semnătură:

_____

Anexa 2 la Termeni şi condiţii privind utilizarea e-xim Banking
INFORMARE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL IN CONTEXTUL INSTRUMENTULUI DE PLATA ELECTRONICA CU ACCES LA DISTANTA TIP MOBILE BANKING DESTINAT CLIENTILOR PERSOANE JURIDICE
versiunea 1.0. aplicabila din 08.08.2024

Incepand cu data mentionata mai sus, **Exim Banca Românească S.A.** a pus in circulatie un **instrument de plată electronică cu acces la distanță tip mobile-banking**, destinat **clienților** sai **persoane juridice** ("Clienti"), care poate fi utilizat numai după descărcarea din Google Play (Google)/App Store (Apple) a **aplicației mobile** a Exim Banca Românească S.A., denumita „**e-ximBanking**" („aplicația mobila"), pe dispozitive electronice de tipul telefon inteligent (smartphone), tableta etc. deținute/folosite de către persoanele fizice desemnate de către Clienti sa utilizeze, in numele Clientilor, respectivul instrument de plată.

In acest context, **Exim Banca Românească S.A.** („***Banca***", "***Operatorul de date cu caracter personal***" sau „***Operatorul***"), având următoarele date de identificare: înregistrată în Registrul Instituțiilor de Credit sub nr. RB-PJR-40-015/18.02.1999 si in Registrul Comerțului sub nr. J1992008799402, având codul de identificare fiscala RO 361560, identificatorul unic la nivel european (EUID) ROONRC.J1992008799402 si capitalul social subscris si vărsat de 2.022.528.336 RON și următoarele date de contact: sediul social în Municipiul București, Strada Barbu Delavrancea nr. 6A, Sector 1, telefonul +4021.405.30.96 si e-mail-ul "office@eximbank.ro", prelucrează date cu caracter personal. Prezentul document („Informare specifica") vine in completarea "Informarii privind prelucrarea datelor cu caracter personal" ("Informare generala") pusa de Banca la dispozitia Clientilor, prin reprezentanti (si postata pe site-ul Bancii in sectiunea "Protectia datelor" (la adresa *https://www.eximbank.ro/wp-content/uploads/2023/05/Informare-prelucrare-date-cu-caracter-personal-non-consumatori.pdf)* si are ca obiectiv informarea persoanelor fizice menționate mai jos în legătură cu aceasta prelucrare.

Inainte de a realiza informarea specifica, precizam faptul ca, potrivit Legii nr. 129/2019 pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului, precum şi pentru modificarea şi completarea unor acte normative, cu modificarile si completarile ulterioare si Regulamentului BNR nr. 2/2019 privind prevenirea şi combaterea spălării banilor şi finanţării terorismului, cu modificarile si completarile ulterioare, Banca are obligatia, in scopul prevenirii si combaterii spalarii banilor si finantarii terorismului, de a aplica masuri de cunoastere a clientelei pentru a identifica Clientul si persoana care il reprezinta. Cat priveste persoana care reprezinta Clientul, comunicam faptul ca Banca aplica masurile de cunoastere a clientelei doar in ceea ce priveste utilizatorul aprobator, prelucrand datele cu caracter personal impuse de legislatia anterior mentionata si redate in Informarea generala.

DESTINATARII INFORMARII SPECIFICE

Informarea specifica este adresata **persoanelor fizice** („***Persoana vizata***" sau „***Dvs.***") **desemnate de cate Clientii Bancii sa utilizeze, in numele Clientilor si in calitate de utilizatori, instrumentul de plată electronică al Băncii cu acces la distanță tip mobile-banking** (utilizatori cu drept de semnatura ["aprobatori"] si utilizatori fara drept de semnatura ["operatori"]). Regasiti Informarea specifica in aplicatia mobila de unde o puteti accesa oricand pe durata cat detineti calitatea de utilizatori.

SCOPURILE PRELUCRARII

Prin formularele puse de Banca la dispozitia Clientilor sai, Banca colecteaza de la acestia date cu caracter personal care va privesc cum ar fi nume, prenume, CNP in cazul in care sunteti rezident sau un echivalent al CNP-ului in cazul in care sunteti nerezident (i.e. seria si, daca exista, numarul pasaportului/unui document de identitate cu fotografia Dvs., emis de o autoritate oficiala), ce tip de utilizator sunteti (aprobator sau operator), restricțiile referitoare la modul (i.e. ecran) si/sau conturi, limitele pe tranzacție, tipul semnaturii si regulile de autorizare, setate de Client, precum si numarul de telefon (cel obligatoriu - mobil si, dupa caz, cel optional - fix sau mobil) si adresa de e-mail. Pe baza codului de client al

Clientului si a numelui si, dupa caz, a prenumelui Dvs., Banca genereaza un alias (username) cu care Dvs. sa va identificati in aplicatia mobila.

Toate aceste date cu caracter personal sunt prelucrate de Banca in scopul *setarii Dvs. ca utilizator in sistemul informatic*. Dupa setare, Banca va comunica prin e-mail, in conditii depline de securitate, alias-ul si restul informatiilor necesare pentru instalarea/reinstalarea aplicatiei mobile.

In procesul de instalare/reinstalare a aplicatiei mobile, Banca *va identifica* astfel: (a) initial, pe baza alias-ului si a CNP-ului/a echivalentului CNP-ului Dvs., pe care le completati in campurile afisate in aplicatie (daca acestea corespund cu datele detinute de Banca, se realizeaza prima etapa a identificarii) si (b) ulterior, pe baza codurilor de validare comunicate de Banca prin SMS (sub forma de cod OTP) si prin e-mail (sub forma de link) si completate, respectiv accesate de Dvs. (daca acestea corespund cu cele generate de Banca, numarul de telefon mobil si adresa de e-mail sunt validate, iar procesul de identificare este finalizat).

Dupa instalare/reinstalare, Banca colecteaza, prin aplicatia mobila, codul setat de Dvs. in aplicatie pe baza caruia puteti sa accesati aplicatia si sa autorizati operatiunile permise de aplicatie (e.g. instrucțiuni de plata, schimburi valutare, depozite etc.). Pe baza acestui cod de acces/PIN, pe care nu trebuie sa-l divulgati Clientului, colegilor Dvs. sau altor terti, Banca *va identifica* cand accesati aplicatia mobila si cand autorizati operatiuni in cadrul aplicatiei. Identificarea este realizata cand codul completat de Dvs. in aplicatia mobila corespunde cu cel detinut de Banca.

Pentru *a asigura realizarea de catre Dvs., in cadrul aplicatiei mobile, a operatiunilor permise de aplicatie, conform regulilor stabilite de Client*, Banca prelucreaza urmatoarele date care va privesc: tipul semnaturii, regulile de autorizare si limitele pe tranzactie setate de Client (in cazul utilizatorului aprobator), restrictiile referitoare la modul (i.e. ecran) si/sau conturi, setate de Client, precum si tipul utilizatorului (aprobator sau operator), setat de Client.

In eventualitatea in care Banca constata probleme legate de funcționarea aplicației mobile sau Dvs. sesizați dificultăți in accesarea si/sau in utilizarea aplicației mobile, Banca prelucreaza date privind dispozitivul Dvs. pe care aveti instalata aplicatia mobila (ID-ul dispozitivului (identificator unic al dispozitivului), producatorul, modelul, sistemul de operare, versiunea sistemului de operare, data activarii aplicatiei mobile pe dispozitiv, versiunea aplicatiei mobile instalata pe dispozitiv si host IP-ul) independent sau, dupa caz (i.e. in functie de problema sesizata de Dvs./identificata de Banca), impreuna cu datele privind tipul semnaturii, regulile de autorizare si limitele pe tranzactie, restrictiile referitoare la modul (i.e. ecran) si/sau conturi, precum si tipul utilizatorului (aprobator sau operator), mentionate mai sus, si/sau cu datele Dvs. de identificare si/sau cu datele Dvs. de contact, pentru a *va acorda suportul necesar in vederea utilizarii aplicatiei mobile si a instrumentului de plată electronică cu acces la distanță tip mobile-banking* conform contractului incheiat intre Banca si Client. Banca prelucreaza, in acelasi scop, mentionat anterior, in functie de problema sesizata de Dvs./identificata de Banca, si date privind ultimele doua dispozitive pe care Dvs. ati avut instalata aplicatia mobila (ID-ul dispozitivului (identificator unic al dispozitivului), producatorul, modelul, sistemul de operare, versiunea sistemului de operare, data activarii aplicatiei mobile pe dispozitiv, versiunea aplicatiei mobile instalata pe dispozitiv si data dezactivarii aplicatiei mobile).

Cand Dvs. ne comunicati pierderea, furtul sau coruperea dispozitivului pe care aveti instalata aplicatia mobila (de aplicatii malitioase care au preluat controlul asupra dispozitivului), Banca colecteaza datele privind statusul dispozitivului Dvs. (“dispozitiv pierdut”, “dispozitiv furat” sau “dispozitiv corupt”) in vederea *blocarii accesului Dvs. la aplicatia mobila*.

Banca prelucreaza numarul Dvs. de telefon (atat cel obligatoriu, cat si cel optional) si adresa Dvs. de e-mail in scop de *comunicare* in legatura cu instrumentul de plată electronică cu acces la distanță tip mobile-banking si cu aplicatia mobila.

Prin structura interna responsabila de elaborarea/modificarea instrumentului de plată electronică cu acces la distanță tip mobile-banking, Banca va realiza *analize* pe baza datelor privind utilizarea aplicatiei mobile de catre Client prin utilizatorii sai (e.g. frecventa si vechimea accesarilor, actiunile intreprinse in aplicatie ca tip, frecventa si vechime) *pentru*

identificarea eventualelor probleme si/sau aspecte de imbunatatit in legatura cu acest instrument de plata electronica si cu aplicatia mobila in vederea mentinerii clientelei actuale si atragerii de clienti noi.

Avand in vedere cele de mai sus, ***scopurile prelucrarii*** realizate de Banca sunt:
(i) setarea Dvs. ca utilizator in sistemele Bancii astfel încât Clientul sa poată utiliza instrumentul de plată electronică al Băncii cu acces la distanță tip mobile-banking conform contractului încheiat cu Banca;
(ii) identificarea Dvs. pe baza alias-ului si a CNP-ului/echivalentului la instalarea/reinstalarea aplicației mobile, inclusiv validarea adresei de e-mail si a numărului de telefon mobil pe baza codurilor de validare, ca etapa in procesul de identificare a utilizatorilor;
(iii) identificarea Dvs. cu ocazia autentificării in aplicația mobila si a autorizării operațiunilor in cadrul aplicației;
(iv) asigurarea realizării de către Dvs., in cadrul aplicatiei mobile, a operatiunilor permise de aplicatie, conform regulilor setate prin contractul dintre Banca si Client privind instrumentul de plată electronică cu acces la distanță tip mobile-banking;
(v) acordarea suportului necesar in vederea utilizarii de catre Dvs. a aplicatiei mobile si a instrumentului de plată electronică cu acces la distanță tip mobile-banking conform contractului incheiat intre Banca si Client;
(vi) blocarea accesului Dvs. la aplicatia mobila in cazul in care comunicati Bancii pierderea sau furtul dispozitivului (pe care este instalata aplicația mobila) sau existenta unor aplicatii care au preluat controlul dispozitivului;
(vii) comunicarea cu Dvs. in legatura cu instrumentul de plată electronică al Bancii cu acces la distanță tip mobile-banking si cu aplicatia mobila, inclusiv pentru transmiterea codurilor de validare;
(viii) analize pentru identificarea eventualelor probleme si/sau aspecte de imbunatatit in legatura cu instrumentul de plată electronică cu acces la distanță tip mobile-banking si cu aplicatia mobila;
(ix) proba.

Sopurile prelucrării, mentionate mai sus, sunt determinate, explicite și nu contravin legii (sunt legitime).

TEMEIURILE LEGALE

Temeiul legal al prelucrării îl constituie ***interesul legitim al Bancii*** de a furniza Clientilor sai servicii bancare (inclusiv, dar fara a se limita la servicii de plata) conform obligatiilor asumate prin documentatia contractuala privind instrumentul de plată electronică cu acces la distanță tip mobile-banking evitând astfel sancțiunile contractuale si legale decurgând din prestarea necorespunzătoare/neprestarea serviciilor (i.e. cu încălcarea obligatiilor asumate fata de Clienti sau, după caz, a obligatiilor decurgand din legislație), inclusiv de a-si menține clientela actuala si de a atrage clienți noi.

DATELE CU CARACTER PERSONAL PRELUCRATE SI DESTINATARII

Datele cu caracter personal prelucrate de Banca conform celor precizate in Informarea specifica sunt: **(i)** datele Dvs. de identificare: nume, prenume, CNP/echivalent CNP, alias, cod PIN/de acces; **(ii)** datele Dvs. de contact: numar de telefon si adresa de e-mail; **(iii)** date legate de calitatea Dvs. de utilizator al aplicatiei mobile: tipul utilizatorului (aprobator/operator), restricțiile referitoare la modul (i.e. ecran) si/sau conturi, limitele pe tranzacție, tipul semnaturii si regulile de autorizare; **(iv)** date privind dispozitivul Dvs. pe care aveti instalata aplicatia mobila: ID-ul dispozitivului (identificator unic al dispozitivului), producatorul, modelul, sistemul de operare, versiunea sistemului de operare, data activarii aplicatiei mobile pe dispozitiv si versiunea aplicatiei mobile instalata pe dispozitiv); **(v)** date privind dispozitivele pe care Dvs. ati avut instalata aplicatia mobila (ultimele doua astfel de dispozitive): ID-ul dispozitivului (identificator unic al dispozitivului), producatorul, modelul, sistemul de operare, versiunea sistemului de operare, data activarii aplicatiei mobile pe dispozitiv, versiunea aplicatiei mobile instalata pe dispozitiv si data dezactivarii aplicatiei mobile; **(vi)** date privind statusul dispozitivului Dvs. pe care aveti instalata aplicatia mobila: "dispozitiv pierdut", "dispozitiv furat" sau "dispozitiv corupt"; **(vii)** host IP-urile dispozitivelor pe care Dvs. aveti si ati avut instalata aplicatia mobila si **(viii)** date privind utilizarea aplicatiei mobile de catre Client prin utilizatorii sai (e.g. frecventa si vechimea accesarilor, actiunile intreprinse in aplicatie ca tip, frecventa si vechime).

Prin prezenta informare, **Banca** va comunica faptul ca **nu colecteaza si nu prelucreaza datele Dvs. biometrice** (amprenta digitala sau structura fetei) si nu aplica tehnici biometrice (tehnici de verificare a amprentei digitale - touch ID sau tehnici de recunoastere faciala - face ID) **in vederea identificarii Dvs. sau in alt scop**. Datele biometrice (amprenta digitala sau structura fetei) sunt stocate in dispozitivul pe care Dvs. aveti instalata aplicatia mobila si care

incorporeaza tehnologiile touch ID si/sau face ID. Colectarea si prelucrarea acestor date (inclusiv stocarea) se realizeaza cu acordul Dvs., conform regulilor setate de catre furnizorii sistemului de operare existent pe dispozitivul Dvs. pe care aveti instalata aplicatia mobila. Face ID-ul/touch ID-ul reprezinta metode de autentificare care asigura acelasi grad de securitate precum codul PIN/de acces. De asemenea, **Banca** va comunica faptul ca **nu colecteaza si nu prelucreaza datele Dvs. de localizare** (locatie aproximativa sau locatie exacta), in vederea afisarii, in cadrul aplicatiei mobile, a sucursalelor si a ATM-urilor Bancii, **in momentul in care accesati functia "Sucursale si ATM" in aplicatia mobila**. Ori de cate ori accesati aceasta functie, Dvs. sunteti directionat catre furnizorul sistemului de operare existent pe dispozitivul pe care Dvs. aveti instalata aplicatia mobila, care, dupa colectarea datelor de localizare, va comunica sucursalele si ATM-urile Bancii din locatia Dvs. aproximativa sau exacta, in functie de datele puse de Dvs. la dispozitia acestuia. Colectarea si prelucrarea datelor de localizare de catre furnizorul anterior mentionat se realizeaza cu acordul Dvs., conform regulilor setate de catre furnizor.

Intern, datele sunt divulgate/vor fi divulgate către un număr limitat de structuri interne si angajați din cadrul acestor structuri interne. Extern, datele sunt divulgate/vor fi divulgate auditorilor externi, Bancii Nationale a Romaniei (BNR), altor autoritati de supraveghere si/sau control, competente sa primeasca aceste date, instantelor de judecata, Dvs. (datele proprii), Clientului Bancii. La cererea intemeiata a autoritatilor si a institutiilor de tipul Parchetului European (EPPO), Ministerului Afacerilor Interne, tribunalelor, parchetelor, DIICOT, DNA, Banca are obligatia legala de a comunica host IP-ul dispozitivelor Dvs. pe care aveti, respectiv ati avut instalata aplicatia mobila.

DURATA DE STOCARE

Datele cu caracter personal mentionate mai sus sunt prelucrate in scopurile enumerate in Informarea specifica pe durata cat Dvs. aveti calitatea de utilizator. Banca va pastra, pe o durata de 30 de zile, fisierul prin care v-a transmis alias-ul pentru a face dovada indeplinirii obligatiilor asumate prin contractul privind instrumentul de plată electronică cu acces la distanță tip mobile-banking, incheiat intre Banca si Client.

Astfel cum este precizat si in Informarea generala, datele cu caracter personal enumerate in Informarea specifica, prelucrate de Banca si in scop de prevenire şi combatere a spălării banilor şi finanţării terorismului si/sau in scopul executarii instructiunilor de plata vor fi stocate de Banca pe durata prevazuta in legislatie: 5 ani de la incetarea relatiei de afaceri cu Clientul, termen care poate fi prelungit cu maxim 5 ani, la cererea autoritatilor competente (conform legislatiei privind prevenirea şi combaterea spălării banilor şi finanţării terorismului), respectiv 5 ani de la terminarea operatiunii de plata (conform legislatiei privind serviciile de plata).

DREPTURILE DVS.

Potrivit GDPR (Regulamentul nr. 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE), Dvs. aveți o serie de drepturi, cel mai important fiind **dreptul la opoziție** pe care dorim sa vi-l aducem la cunoștință in mod explicit conform prevederilor art. 21 alin. 4 din GDPR, dat fiind faptul ca temeiul legal al prelucrării descrise in Informarea specifica îl constituie si interesul legitim al Operatorului:

Astfel, in orice moment, Dvs. aveți dreptul de a va opune, din motive legate de situația particulară în care va aflați, prelucrării în temeiul interesului legitim a datelor cu caracter personal care va privesc, inclusiv creării de profiluri. Odată exercitat acest drept, Banca nu mai prelucrează datele cu caracter personal, cu excepția cazului în care Banca „demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță".

De asemenea, Dvs. beneficiați si de următoarele drepturi, conform GDPR:

(1) dreptul de acces la datele cu caracter personal care va privesc

Dvs. aveți dreptul de a obține din partea Bancii o confirmare că se prelucrează sau nu date cu caracter personal care va privesc si, in caz afirmativ, de a obține informații, spre exemplu, despre datele cu caracter personal prelucrate, scopul prelucrării, destinatarii datelor etc.;

(2) dreptul la rectificarea datelor

Dvs. aveți dreptul de a obține din partea Bancii, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care va privesc, precum si completarea datelor cu caracter personal care sunt incomplete;

(3) dreptul la ștergerea datelor ("dreptul de a fi uitat")

Dvs. aveți dreptul de a obține din partea Bancii ștergerea datelor cu caracter personal care va privesc, fără întârzieri nejustificate, iar Banca are obligația sa șteargă datele cu caracter personal fără întârzieri nejustificate în situațiile expres prevăzute de lege (e.g. datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate etc.);

(4) dreptul la restricționarea prelucrării

Dvs. aveți dreptul de a obține din partea Bancii restricționarea prelucrării in cazurile expres prevăzute de lege (e.g. Persoana vizată contestă exactitatea datelor sau prelucrarea este ilegală, iar Persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor etc.);

(5) dreptul la portabilitatea datelor

Dvs. aveți dreptul de a primi datele cu caracter personal care va privesc și pe care le-ați furnizat Bancii într-un format structurat, utilizat în mod curent și care poate fi citit automat și de a transmite aceste date altui operator, fără obstacole din partea Bancii daca: prelucrarea se bazează pe consimțământ sau pe un contract & prelucrarea este efectuată prin mijloace automate;

(6) dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automata, inclusiv crearea de profiluri

Dvs. aveți dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care va privesc sau va afectează în mod similar într-o măsură semnificativă si

(7) dreptul de a va adresa cu o plângere Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), ale cărei date de contact se regăsesc la adresa: www.dataprotection.ro.

Pentru orice informație, solicitare, inclusiv reclamație in legătură cu prelucrarea de către Banca a datelor cu caracter personal, Dvs. puteți contacta responsabilul cu protecția datelor ("DPO") la adresa de e-mail: dpo@eximbank.ro sau va puteți adresa direct Bancii, utilizand datele de contact mentionate in preambul.