Politica privind prelucrarea datelor cu caracter personal

UniCredit Bank S.A., societate administrată în sistem dualist, cu sediul în Romania, București, Bulevardul Expoziției nr. 1F, sector 1, înarticulată la Registrul Comerțului sub nr. J1991007706408, în Registrul Bancar sub nr. RB-PJR-40-011/18.02.1999, cod unic de înregistrare 361536, atribut fiscal RO, Identificator Unic la Nivel European (EUID): ROONRC.J1991007706408, capital social subscris și vărsat 589.955.162,70 Lei
și
UniCredit Consumer Financing IFN S.A. societate administrată în sistem dualist, înregistrată la Registrul Comerțului sub nr. J2008013865401/14.08.2008, EUID ROONRC.J2008013865401, atribut fiscal RO CUI 24332910, atribut fiscal RO, înscrisă în Registrul General al Băncii Naționale a României sub numărul RG-PJR-41-110247/24.10.2008, Registrul Special sub numărul RS-PJR-41-110065/09.02.2010 și Registrul instituțiilor de plată sub numărul IP-RO-0009/02.03.2015, cu sediul în București, sector 1, Bulevardul Expoziției, nr. 1F, etaj 6, capital social subscris și vărsat: 173.269.200 Lei

denumite în comun în continuare "Operatorul" și individual UniCredit Bank S.A. sau UniCredit Consumer Financing

în calitate de Operator de date cu caracter personal, prelucrează datele cu caracter personal cu buna-credință și în realizarea scopurilor specificate în prezenta Politica privind prelucrarea datelor cu caracter personal, în conformitate cu prevederile Regulamentului (UE) nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE („Regulamentul"), denumit în continuare "GDPR".

Aceste date personale sunt furnizate Operatorului fie de către Persoana Vizata, fie, în cazul în care Persoana Vizata este împuternicit/utilizator suplimentar/reprezentant legal, de către titularul produsului/serviciului bancar, fie sunt preluate de Operator, atunci când este cazul, din alte surse disponibile externe (cum ar fi, dar fără a se limita la: procesatorii de plăți sau tranzacții, organizații de carduri, terți prestatori de servicii de plată (terți PSP), de la cealaltă parte implicată în tranzacția de plata, precum și din schimbul de mesaje dintre participanți prin infrastructura centrală RoPay, terțe părți (conform accepțiunii date acestei noțiuni la articolul 18 (1) din Legea nr. 129/2019), Direcția Generala pentru Evidența Persoanelor, Agenția Națională de Administrare Fiscala (ANAF), Oficiul Național al Registrului Comerțului, portalul instanțelor de judecată din România, Biroul de Credit SA, alte companii din cadrul Grupului UniCredit, baze de date publice sau private (inclusiv entități specializate în agregarea de date), biroul de carte funciara, mass media, angajatorul persoanei vizate, autorități) la data încheierii contractului cu Operatorul și/sau a unei polițe de asigurare și/sau la data formulării unei cereri prin care se solicită prestarea unor servicii de către Operator și/sau pe parcursul derulării relației contractuale/ de afaceri și/sau de către un terț PSP contractat de persoana vizata.

Prezentul document se dorește a fi o sursa importanta de informare oferita Persoanei vizate cu privire la modalitatea în care Operatorul efectuează operațiunile de prelucrare a Datelor personale, suplimentar informărilor separate pe care Operatorul le furnizează Persoanelor vizate conform art. 12 – 13 sau, după caz, art. 14 din Regulament.

CE ÎNSEAMNĂ PRELUCRAREA DATELOR PERSONALE?

Prelucrarea înseamnă orice operațiune sau set de operațiuni efectuate asupra Datelor personale sau asupra seturilor de Date personale, cu sau fără utilizarea de mijloace automatizate, cum ar fi: colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea. Operatorul aplica cu privire la prelucrarea Datelor Personale măsuri tehnice și organizatorice adecvate pentru a proteja aceste date împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, precum și împotriva oricărei alte forme de prelucrare

ilegală. Datele Personale sunt prelucrate în mod individual, în considerarea temeiurilor legale aplicabile. În situația în care operațiunea de prelucrare a Datelor personale se întemeiază pe acordul Persoanei vizate, acesta este obținut de către Operator prin documente separate în condițiile GDPR.

TEMEIURI LEGALE – CARE ESTE BAZA LEGALA A PRELUCRĂRII?

Banca prelucrează Datele personale în considerarea următoarelor temeiuri legale din Regulament:

a) în baza consimțământului Persoanei vizate – art. 6 alin. (1) lit. a);

b) pentru încheierea și executarea unui contract la care Persoana vizată este parte sau pentru a face demersuri la cererea Persoanei vizate înainte de încheierea unui contract – art. 6 alin. (1) lit. b);

c) prelucrarea este necesara în vederea îndeplinirii unei obligații legale care îi revine Operatorului – art. 6 alin. (1) lit. c);

d) prelucrarea este necesară pentru a proteja interesele vitale ale Persoanei vizate sau ale altei persoane fizice – art. 6 alin. (1) lit. d);

e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit Operatorul – art. 6 alin. (1) lit. e);

f) prelucrarea este necesară în scopul intereselor legitime urmărite de Operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale Persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când Persoana vizată este un minor – art. 6 alin. (1) lit. f).

CARE SUNT PRINCIPIILE DE PRELUCRARE A DATELOR PERSONALE?

În prelucrarea Datelor personale, Operatorul și persoanele împuternicite de acesta, respectă întocmai principiile de prelucrare a datelor prevăzute de art. 5 din Regulament, astfel:

a) legalitate, echitate și transparență – Datele personale sunt prelucrate în mod legal, corect și transparent, Persoana vizată fiind informată cu privire la existența unei operațiuni de prelucrare și la scopurile acesteia legitime, stabilite pe criterii de echitate față de drepturile și interesele fundamentale ale Persoanei vizate;

b) limitarea scopului operațiunii de prelucrare – Datele personale se colectează de către Operator în scopuri determinate, explicite și legitime și nu se prelucrează ulterior pentru scopuri adiționale care nu sunt compatibile cu aceste scopuri;

c) proporționalitatea și reducerea la minim – Datele personale se prelucrează de o maniera adecvată, relevantă și limitată la necesitatea de a realiza scopurile legitime și precis determinate pentru care sunt prelucrate;

d) exactitatea și actualizarea – Datele personale prelucrate sunt exacte și, în cazul în care este necesar, acestea sunt actualizate; în acest sens, Banca ia toate măsurile necesare pentru a se asigura că Datele personale care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere;

e) limitarea stocării – Datele personale sunt păstrate într-o forma care permite identificarea Persoanelor vizate pentru o perioada care nu depășește perioada necesară pentru scopurile pentru care sunt prelucrate Datele personale;

f) integritatea și confidențialitatea – Datele personale sunt prelucrate în condiții de securitate adecvate, astfel încât să se asigure protecția acestora împotriva prelucrării neautorizate sau ilegale, respectiv împotriva pierderii, distrugerii sau deteriorării accidentale a Datelor personale.

CE INTRA ÎN SFERA DATELOR PERSONALE?

În cadrul activităților desfășurate, raportat la scopul prelucrării, Operatorul prelucrează Datele personale ale Persoanei vizate cum ar fi, dar fără a se limita la acestea:

a) date de identificare (ex. prenumele, numele, numele anterior, pseudonimul, adresa de domiciliu și de reședință, data și locul nașterii, codul numeric personal, seria și numărul actului de identitate/ pașaportului), alte date care apar în actul de identitate, alte date din actele de stare civilă, cetățenia etc.;

b) date de contact (ex. adresa, numărul de telefon fix/mobil, faxul, adresa de poșta electronică etc.);

c) date privind studiile, profesia, ocupația, locul de muncă, numărul dosarului de pensie;

d) date privind situația economică și financiară, date privind bunurile și proprietățile deținute, garanții reale/personale, date privind angajamentele financiare și sursele de venit;

e) sursa fondurilor, date privind beneficiarul real, expunerea publică, dacă este cazul, și funcția publică deținută, date privind sancțiuni, dacă este cazul;

f) date financiare/bancare, inclusiv privind produsele achiziționate și tranzacțiile realizate, numele de utilizator pentru Online Banking și Mobile Banking;

g) vocea, semnătura, imaginea

h) date biometrice, în cadrul procesului de identificare la distanță realizată prin mijloace video, fără interacțiunea directă cu un reprezentant al Operatorului

i) alte categorii similare de date cu caracter personal din evidențele Operatorului, referitoare la relația contractuală cu Operatorul derivate, în principal, din documentația contractuală semnată și din informațiile colectate de Operator, din executarea legii.

În unele cazuri, este posibil să fie solicitate date privind situația litigiilor în care Persoana vizată este implicată, precum și alte date în funcție de situația Persoanei vizate, acestea fiind necesare Operatorului pentru evaluarea eligibilității Persoanei vizate în calitate de client si/sau garant în relația cu Operatorul, în scopul acordării finanțării solicitate (ex: stabilirea bonității și gradului de îndatorare etc.), precum și pentru stabilirea riscului de credit asociat.

CARE SUNT SCOPURILE PRELUCRĂRII DATELOR PERSONALE?

Scopul Principal al prelucrării Datelor Personale este prestarea serviciilor financiare de către Operator clienților săi. Acest scop presupune realizarea, în cadrul raportului concret cu fiecare client, a tuturor activităților legate de încheierea, modificarea și executarea contractului aferent produsului/ serviciului financiar solicitat de către client. În cadrul acestor activități sunt incluse și verificările necesare pentru evaluarea eligibilității Persoanei vizate pentru acordarea produsului/ serviciului solicitat ori a oricărui alt produs sau serviciu avantajos.

Operatorul prelucrează Date Personale și în următoarele Scopuri strâns corelate celui principal:

a) realizarea analizei de cunoaștere a clientelei, a analizelor de risc, respectiv de raportare a tranzacțiilor suspecte, conform legislației privind cunoașterea clientelei în scopul prevenirii spălării banilor și finanțării terorismului;

b) realizarea raportărilor către instituțiile statului, conform legislației speciale, respectiv pentru îndeplinirea activităților aferente controalelor autorităților (ex. ANAF, ANPC, BNR, ANSPDCP etc.);

c) executarea silită a sumelor datorate, colectarea debitelor/ recuperarea creanțelor datorate Operatorului, conform contractelor încheiate și a interesului legitim al Operatorului de a recupera creanțele aferente relației contractuale existente cu clientul/ Persoana vizată;

d) administrarea popririlor și sechestrelor, conform Codurilor de Procedură Civilă și Penală;

e) realizarea raportărilor în cadrul Grupului UniCredit și consolidarea contabilă la nivelul Grupului UniCredit, inclusiv realizarea unui proces eficient de management al riscurilor la nivel de Grup și de gestionare și monitorizare a clienților Grupului, prin activități care includ, fără a se limita la calcularea indicatorilor folosiți în evaluarea bonității, a riscului de credit, stabilirea gradului de îndatorare, monitorizarea adecvata a tuturor obligațiilor asumate față de Grup etc.;

f) realizarea raportărilor FATCA în cazul în care Persoana vizată este cetățean sau rezident al SUA, precum și al raportărilor CRS (Common Reporting Standard) pentru combaterea evaziunii fiscale;

g) pentru monitorizarea, securitatea și paza persoanelor, spațiilor, bunurilor, prin camerele video amplasate în sediile Operatorului, conform Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor;

h) pentru înregistrarea comunicărilor prin fax, canale digitale (ex. Online Banking, Mobile Banking, email) și a apelurilor și convorbirilor telefonice realizate prin intermediul Contact Center-ului Operatorului, în scopul eficientizării și îmbunătățirii serviciilor acordate, precum și al încheierii și executării în condiții optime a contractelor, respectiv al realizării tranzacțiilor telefonice și online;

i) realizarea analizelor ce pot conduce la profilarea în scopul marketingului direct (ex. evaluarea produselor bancare deținute, istoricului tranzacțiilor bancare efectuate, calcularea unor indicatori în evaluarea solvabilității/ riscului de creditare etc.) și marketingul direct, prin utilizarea mijloacelor de comunicare, inclusiv a sistemelor automate de apelare care nu necesită intervenția unui operator uman, respectiv email, SMS, fax, cum ar fi pentru primirea de newsletter/alte comunicări comerciale, pentru promovarea produselor/serviciilor Grupului UniCredit (de finanțare/creditare/alte tipuri), în cazul în care ați exprimat un astfel de acord de marketing;

j) pentru verificarea satisfacției clientului și a calității serviciilor și produselor achiziționate, în temeiul interesului legitim al îmbunătățirii permanente a serviciilor/ produselor Operatorului;

k) în scopuri statistice;

l) în scopul prevenirii, investigării și limitării consecințelor fraudelor rezultate din orice arie care privește activitatea curentă a Operatorului;

m) îndeplinirea cerințelor legale din aria plăților/serviciilor de plăți

n) furnizarea de către UniCredit Bank a unui serviciu de plăți instant sigur și eficient, inclusiv prezentarea ordinului de plată precompletat, în cadrul serviciului RoPay;

o) respectarea de către Unicredit Bank a obligațiilor asumate în cadrul Schemelor Naționale de Plăți în legătură cu returul sumelor în caz de erori operaționale/probleme tehnice datorate prestatorului de servicii de plată al persoanei ca a efectuat plăți în conturile dvs. sau returul /blocarea sumelor pe motiv de fraudă.

DE CE PRELUCRĂM DATELE PERSONALE PRIN UTILIZAREA MIJLOACELOR DE SUPRAVEGHERE VIDEO ȘI PRIN ÎNREGISTRARE TELEFONICĂ?

Pentru protejarea securității Persoanelor vizate (ex. clienți, vizitatori, angajați) și pentru asigurarea pazei și protecției bunurilor Operatorului și ale angajaților acestuia, sediile Operatorului sunt supravegheate video, iar imaginile obținute prin mijloace de supraveghere video sunt înregistrate. Pentru aceste scopuri, Persoanele vizate anterior menționate, precum și bunurile utilizate de acestea când sosesc, accesează sau vizitează sediile Operatorului si/sau spațiile exterioare adiacente, sunt filmate cu mijloace de supraveghere video instalate în locuri vizibile și utilizate în conformitate cu reglementările legale în vigoare. Supravegherea video are loc doar

în spațiile destinate publicului, inclusiv pe căile de acces situate în interiorul sau exteriorul imobilului unde sunt situate sediile Operatorului, locul amplasării mijloacelor de supraveghere video fiind semnalat prin intermediul unei pictograme care conține o imagine reprezentativă și are vizibilitate suficientă, poziționată în apropierea locului de amplasare. Imaginile înregistrate prin utilizarea mijloacelor de supraveghere video vor fi transmise de către Operatorului către organele de poliție și alte autorități cu atribuții privind apărarea drepturilor și libertăților fundamentale ale persoanei, a proprietății private și publice, prevenirea, descoperirea și sancționarea infracțiunilor, respectarea ordinii și liniștii publice, în condițiile legii. Imaginile astfel obținute nu vor fi transmise în străinătate.

Operatorul poate înregistra apelurile telefonice către/de la Operator, purtate de Operator cu Persoanele vizate, indiferent de persoana care a inițiat apelul, și poate păstra aceste înregistrări, în baza consimțământului obținut în acest sens de la Persoanele vizate în cauză și cu respectarea prevederilor legale aplicabile. Înregistrările astfel obținute vor fi utilizate de Operator în scopul eficientizării activităților și produselor achiziționate, respectiv al încheierii și executării în condiții optime a contractelor cu clienții, al analizării anumitor situații apărute în derularea sau în legătură cu acestea. De asemenea, aceste înregistrări telefonice vor putea fi utilizate și în instanță, ca probe, în cazul unor litigii rezultate din sau în legătură cu contractele respective, vor putea fi transmise, în condițiile legii, autorităților cu atribuții privind apărarea persoanelor, proprietății private și publice, prevenirea, descoperirea și sancționarea infracțiunilor.

DE CE ESTE NEVOIE CA OPERATORUL SĂ PRELUCREZE DATE PERSONALE?

Datele Personale sunt prelucrate în scopurile legitime menționate mai sus, inclusiv pentru îndeplinirea obligațiilor ce decurg din relația contractuală încheiată, atât de către Operator, cât și de către Persoana vizată. Astfel, se vor avea în vedere următoarele aspecte:

a) Date personale necesare pentru realizarea Scopului Principal – în situația în care Persoana vizată nu este de acord cu/ refuză prelucrarea Datelor sale personale, Operatorul va fi în imposibilitatea de a iniția sau continua cu Persoana vizată raporturi juridice contractuale, întrucât este în imposibilitatea de a respecta cerințele reglementărilor speciale din domeniul financiar privind cunoașterea clientelei, prevenirea și sancționarea spălării banilor, precum și pentru instituirea unor măsuri de prevenire și combatere a finanțării terorismului, inclusiv de a analiza cererea privind prestarea serviciilor solicitate și de a încheia/ derula/ executa relația contractuală;

b) Date personale necesare pentru realizarea Scopurilor Corelate – în situația în care Persoana vizată își va exprima dreptul de obiecțiune pentru operațiunile de prelucrare în scopuri ce țin de supervizarea activității Operatorului și consolidarea contabilă la nivel de Grup, Operatorul va fi în imposibilitatea de a încheia sau continua un raport juridic cu Persoana vizata, deoarece nu va putea realiza un proces eficient de management al riscurilor la nivelul Grupului și a unui proces cuprinzător de gestionare și monitorizare a riscurilor aferente finanțării clienților Grupului. În cazul operațiunilor de prelucrare a datelor în scop de statistică, obiecțiunea Persoanei vizate va fi luată în considerare, în funcție de particularitățile situației, în conformitate cu art. 21 din Regulament;

c) Date personale necesare pentru realizarea Scopului Corelat constând în marketing direct – în situația în care Persoana vizată nu își dă acordul pentru marketing direct sau își exprimă dreptul de obiecțiune la operațiunea de prelucrare în acest scop, Operatorul nu va putea transmite către Persoana vizată informări comerciale prin sms, e-mail, poștă, despre propriile produse sau despre cele ale partenerilor săi/membrilor Grupului;

d) Date personale necesare pentru realizarea Scopului Corelat constând în monitorizarea și supravegherea persoanelor și bunurilor prin amplasarea camerelor video în sediile Operatorului – în situația în care Persoana vizată își exprimă dreptul de obiecțiune, acesta va fi analizat în funcție de particularitățile situației, în conformitate cu art. 21 din Regulament, întrucât Operatorul are obligația de a asigura paza bunurilor și persoanelor conform Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor,

precum și de a transmite autorităților publice competente informațiile necesare acestora pentru menținerea ordinii publice și combaterea/ sancționarea infracționalității.

CĂTRE CINE TRANSMITE BANCA DATE PERSONALE?

Operatori/ Persoane Împuternicite și Destinatarii Datelor personale

Datele personale pot fi transmise către următoarele categorii de destinatari:

a) Persoana vizată, reprezentanții persoanei vizate

b) entități din Grupul UniCredit

c) parteneri contractuali ai Operatorului din toate ariile necesare derulării optime a activității curente a Băncii (ex.: asiguratori, agenții de recuperare creanțe, avocați, notari, executori judecătorești, evaluatori, auditori, consultanți, societăți din aria IT/plăți, furnizori ai serviciilor de investigare și documentare fraude, servicii poștale și de curierat

d) organizații internaționale (ex. de carduri – Visa, Mastercard etc.)

e) prestatori de servicii tehnice de procesare facilitare a plăților (ex. Romcard, Transfond, Society for Worldwide Interbank Financial Telecommunications etc.)

f) autorități publice din România (ex. Banca Națională a României, ANAF, Oficiul Național de Prevenire şi Combatere a Spălării Banilor, etc.) şi din străinătate (ex. Comisia Europeană, autorități fiscale etc.

g) alte instituții de drept public și privat (ex: Direcția Generală pentru Evidenta Persoanelor, Registrul Național de Publicitate Mobiliară, Fondul Național de Garantare a Creditelor pentru IMM-uri)

h) angajatorul Persoanei vizate

i) alte bănci (inclusiv bănci corespondente) sau alta entitate financiară/ prestator de servicii de plată, Organizații de Carduri, inclusiv terț PSP (precum prestatori de servicii de inițiere a plății, prestatori de servicii de informare cu privire la conturi, și prestatori de servicii de plată care emit instrumente de plata bazate pe card) pentru a executa anumite servicii de plată, retrageri de numerar sau retururi în situații de erori operaționale/probleme tehnice sau fraudă

j) orice alte categorii de parteneri contractuali necesari desfășurării activității curente a Operatorului.

Datele personale pot fi transferate către entități din Uniunea Europeana/EEA. În situația transmiterii Datelor personale către un terț sau organizație internațională din afara UE, sunt aplicabile informațiile din secțiunea Transfer International.

Datele personale transmise terților vor fi adecvate, pertinente și neexcesive prin raportare la scopul în care au fost colectate și care permite transmiterea către un anumit terț.

Transferul International

Datele personale vor fi transferate către SWIFT (Society for Worldwide Interbank Financial Telecommunications), având calitatea de operator, în cazul în care realizarea de operațiuni de transfer credit - plăti solicitate de către dvs. include procesarea prin sistemul SWIFT. În acest sens, există posibilitatea ca datele transferate către SWIFT, în calitate de operator, să fie accesibile Departamentului Trezoreriei SUA. În situația în care sunteți cetățean al Statelor Unite ale Americii (SUA) sau rezident pe teritoriul SUA, vă informăm că, potrivit FATCA, vă sunt aplicabile direct dispozițiile legale privind regimul fiscal al statului SUA, datele fiind transmise de Operatorului către autoritățile fiscale din România, care, ulterior, le pot trimite către autoritățile fiscale din SUA. În toate situațiile în care va fi necesar transferul internațional de date, acest lucru se va realiza

doar dacă în țara destinatară este asigurat un nivel adecvat de protecție a datelor personale recunoscut prin decizie a Comisiei Europene, cum ar fi țările membre ale Uniunii Economice Europene (EEA). În absența unei astfel de decizii a Comisiei Europene, Operatorul va putea transfera date cu caracter personal către o țară terță numai dacă persoana care va prelucra datele a oferit garanții corespunzătoare, prevăzute de lege în vederea protejării datelor personale, cum ar fi, fără a se limita la utilizarea regulilor corporatiste obligatorii, a clauzelor standard de protecție a datelor adoptate de Comisia Europeană, a clauzelor standard de protecție a datelor adoptate de o autoritate de supraveghere, a clauzelor contractuale autorizate de o autoritate de supraveghere, aderarea la un cod de conduită aprobat de autoritatea de supraveghere. Operatorul poate fi contactat pentru obținerea de informații suplimentare cu privire la garanțiile oferite pentru protejarea datelor personale în cazul fiecărui transfer de date în străinătate, printr-o solicitare scrisă în acest sens.

CÂT TIMP PRELUCREAZĂ BANCA DATELE PERSONALE?

Datele personale sunt prelucrate pe următoarele perioade de timp:

a) pe durata de valabilitate a contractelor încheiate cu Operatorul, la care se adaugă 10 ani de la încetarea relației contractuale raportat la prevederile Legii nr. 82/1991, Legea nr.129/2019 și bazat pe interesul legitim al Operatorului de a lua masurile adecvate și necesare de conservare a documentației contractuale în vederea apărării corespunzătoare a drepturilor sale în raport de orice persoana fizica sau juridica, cum ar fi instanțe de judecată, auditori, autorități de supraveghere, în linie cu legislația aplicabilă, potrivit art. 6, alin.1, lit. c) și f) din RGPD; fac excepție situațiile când, printr-o prevedere legală aplicabilă, este necesară păstrarea pe o perioadă mai mare ori atunci când Operatorul justifică un interes legitim, caz în care durata prelucrării se poate prelungi până la realizarea acelui interes legitim;

b) pe o durată de 5 ani, la care se poate adăuga o perioadă de max. 5 ani, la solicitarea autorității competente, în cazul în care nu s-a încheiat o relație contractuală în vederea prestării/ furnizării unor servicii/ produse, conform legii (Legea nr. 129/2019 și Regulamentul BNR nr. 2/2019);

c) daca prelucrarea este efectuată în scop de marketing direct (i) dacă opțiunile Persoanei vizate sunt "NU", la încetarea ultimei relații contractuale cu entitățile din Grupul UniCredit (în ipoteza când sunt relații contractuale cu mai multe entități), participante la acordul de marketing direct (conform anexei la Nota de Informare), Persoana vizată nu va mai primi comunicări comerciale, iar datele aferente se vor mai păstra 3 ani; (ii) dacă opțiunea Persoanei vizate este "DA", la încetarea ultimei relații contractuale cu entitățile din Grupul UniCredit (în ipoteza când sunt relații contractuale cu mai multe entități), participante la acordul de marketing direct, Persoana vizată va mai primi comunicări comerciale 1 an, după care opțiunea Persoanei vizate va fi "NU" în sistemele Operatorului, iar datele aferente se vor mai păstra 3 ani;

d) prelucrarea Datelor personale prin înregistrarea imaginilor captate de camerele video, respectiv a apelurilor telefonice realizate pe linia de suport clienți sunt păstrate pe o perioadă de 30 de zile de la data înregistrării acestora, cu excepția cazului în care există temeiuri legale justificative pentru a fi păstrate pe o perioadă mai îndelungată;

e) privitor la raportările FATCA și CRS, potrivit legislației fiscale aplicabile (ex.: Legea nr. 207/2015, revizuită prin OUG nr. 102/2022): Datele personale aferente se păstrează 10 ani de la expirarea termenului de raportare către autoritățile fiscale, care curge de la data de 15 mai inclusiv a anului calendaristic curent pentru informațiile aferente anului calendaristic precedent);

f) în cazul în care Persoana Vizată alege să parcurgă un proces de identificare la distanță, prin mijloace video, însă acest proces nu va fi finalizat, datele privind motivele întreruperii procesului de identificare (inclusiv imaginile video) vor fi stocate pentru o perioada de 3 ani, conform normelor emise de către Autoritatea privind Digitalizarea României, aprobate prin Decizia nr. 564/2021.

CE DREPTURI ARE PERSOANA VIZATĂ ȘI CUM LE EXERCITĂ?

Persoana vizată are următoarele drepturi cu privire exclusiv la datele acesteia:

a) dreptul de acces la date conform art. 15 din Regulament;

b) dreptul de rectificare a datelor, conform art. 16 din Regulament;

c) dreptul de ștergere a datelor, conform art. 17 din Regulament;

d) dreptul la restricționarea datelor, conform art. 18 din Regulament;

e) dreptul la portabilitatea datelor, conform art. 20 din Regulament;

f) dreptul de a obiecta, conform art. 21 din Regulament;

g) dreptul de a nu fi supus unei decizii individuale automatizate, inclusiv profilare, conform art. 22 din Regulament;

h) dreptul de a va adresa Autorității Naționale pentru Supravegherea Prelucrării Datelor cu Caracter Personal și justiției;

i) dreptul de a retrage oricând consimțământul de marketing direct și de realizare a profilului dumneavoastră în scop de marketing, confirm art. 7 alin. (3) din Regulament.

Pentru exercitarea acestor drepturi, Persoana vizată poate adresa o cerere scrisă, datată și semnată olograf, transmisă, în funcție de entitatea care a emis cardul, către:

- UniCredit Bank SA, la adresa: Bulevardul Expoziției, nr.1 F, sector 1, București, cod poștal 01210, sau pe email la infocenter@unicredit.ro, respectiv apelând la numărul +40 21 200 2020 (apel cu tarif normal în rețeaua fixă Telekom România) sau *2020 (apel tarif normal în rețelele mobile Telekom România, Orange, RCS&RDS, Vodafone)

  sau

- UniCredit Consumer Financing IFN SA, la adresa: Bd. Expoziției nr. 1F, et. 6, sector 1 București, cod poștal 01210 sau la numărul de fax : +40 21 200 97 01 sau la adresa de e-mail: ucfin.contactclienti@unicredit.ro.

Informațiile privind Datele personale si, după caz, măsurile luate, vor fi transmise Persoanei vizate la adresa menționată în solicitare sau la cea aflată în evidența Operatorului, în termenul de 1 lună prevăzut de Regulament. Acest termen poate fi prelungit cu două luni atunci când este necesar, ținându-se seama de complexitatea solicitării.

Operatorul își rezervă dreptul de a stabili o taxă în cazul cererilor repetate conform GDPR.

Informații complete privind prelucrarea datelor se găsesc în notele de informare specifice, prezente în orice moment în varianta actualizată pe site-ul Operatorului, în sectiunile dedicate Protecției Datelor Personale:

Pentru UniCredit Bank SA:

https://www.unicredit.ro/ro/persoane-fizice/Diverse/protectia-datelor.html, respectiv https://www.unicredit.ro/ro/imm/Diverse/protectia-datelor.html

Pentru UniCredit Consumer Financing IFN SA:

https://www.ucfin.ro/protectia-datelor

Policy on the processing of personal data

UniCredit Bank S.A., a company managed in a dualist system, headquartered in Romania, Bucharest, Street Expozitiei nr. 1F, sector 1, registered with the Trade Register under no. J1991007706408, in the Banking Register under no. RB-PJR-40-011/18.02.1999, unique registration code 361536, tax attribute RO, Unique Identifier at European Level (EUID): ROONRC. J1991007706408, subscribed and paid-up share capital 589,955,162.70 Lei
and
UniCredit Consumer Financing IFN S.A., a company managed in a dualist system, registered with the Trade Register under no. J2008013865401/14.08.2008, EUID ROONRC. J2008013865401, tax attribute RO CUI 24332910, tax attribute RO, registered in the General Register of the National Bank of Romania under the number RG-PJR-41-110247/24.10.2008, the Special Register under the number RS-PJR-41-110065/09.02.2010 and the Register of Payment Institutions under the number IP-RO-0009/02.03.2015, headquartered in Bucharest, sector 1, Bulevardul Expozitiei, no. 1F, 6th floor, subscribed and paid-up share capital: 173,269,200 Lei

hereinafter jointly referred to as the "Operator" and individually UniCredit Bank S.A. or UniCredit Consumer Financing

As a Personal Data Controller, it processes personal data in good faith and for the purposes specified in this Personal Data Processing Policy, in accordance with the provisions of Regulation (EU) no. 679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (the "Regulation"), hereinafter referred to as the "GDPR".

Such personal data is provided to the Controller either by the Data Subject or, where the Data Subject is an additional processor/user/legal representative, by the owner of the banking product/service, or is retrieved by the Controller, where applicable, from other available external sources (such as, but not limited to: payment or transaction processors, card organizations, third-party payment service providers (third-party PSPs), from the other party involved in the payment transaction, as well as from the exchange of messages between participants through the central RoPay infrastructure, third parties (according to the meaning given to this notion in Article 18 (1) of Law no. 129/2019), the General Directorate for Persons Records, the National Agency for Fiscal Administration (ANAF), The National Trade Register Office, the portal of the courts of law in Romania, the Credit Bureau SA, other companies within the UniCredit Group, public or private databases (including entities specialized in data aggregation), the land registry office, mass media, the employer of the data subject, authorities) on the date of conclusion of the contract with the Operator and/or of an insurance policy and/or on the date of formulation of a request requesting the provision of services by the Controller and/or during the course of the contractual/business relationship and/or by a third-party PSP contracted by the data subject.

This document is intended to be an important source of information provided to the Data Subject regarding the manner in which the Controller carries out the operations of processing Personal Data, in addition to the separate information that the Controller provides to the Data Subjects according to art. 12 – 13 or, as the case may be, art. 14 of the Regulation.

WHAT DOES PROCESSING OF PERSONAL DATA MEAN?

Processing means any operation or set of operations performed on Personal Data or on sets of Personal Data, with or without the use of automated means, such as: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise

making available, alignment or combination, restriction, erasure or destruction. The Controller applies regarding the processing of Personal Data appropriate technical and organizational measures to protect such data against accidental or unlawful destruction, loss, alteration, disclosure or unauthorized access, as well as against any other form of unlawful processing. Personal Data is processed individually, taking into account the applicable legal bases. In the event that the processing of Personal Data is based on the consent of the Data Subject, it is obtained by the Controller through separate documents under the GDPR conditions.

LEGAL BASES – WHAT IS THE LEGAL BASIS FOR THE PROCESSING?

The Bank processes Personal Data in consideration of the following legal bases in the Regulation:

a) based on the consent of the Data Subject – art. 6 para. (1) letter a);

b) for the conclusion and performance of a contract to which the Data Subject is a party or to take steps at the request of the Data Subject before concluding a contract – art. 6 para. (1) letter b);

c) the processing is necessary in order to fulfill a legal obligation incumbent on the Controller – art. 6 para. (1) letter c);

d) the processing is necessary to protect the vital interests of the Data Subject or of another natural person – art. 6 para. (1) letter d);

e) the processing is necessary for the performance of a task that serves a public interest or that results from the exercise of the public authority with which the Controller is invested – art. 6 para. (1) letter e);

f) the processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, unless the interests or fundamental rights and freedoms of the Data Subject, which require the protection of personal data, in particular when the Data Subject is a minor – Art. 6 para. (1) letter f).

WHAT ARE THE PRINCIPLES OF PERSONAL DATA PROCESSING?

In the processing of Personal Data, the Controller and the persons empowered by it, fully comply with the principles of data processing provided by art. 5 of the Regulation, as follows:

a) legality, fairness and transparency – Personal data are processed in a lawful, fair and transparent manner, the Data Subject being informed about the existence of a processing operation and its legitimate purposes, established on criteria of fairness to the fundamental rights and interests of the Data Subject;

b) limitation of the purpose of the processing operation – Personal Data is collected by the Controller for determined, explicit and legitimate purposes and is not subsequently processed for additional purposes that are not compatible with these purposes;

c) proportionality and minimization – Personal data are processed in an appropriate, relevant manner and limited to the need to achieve the legitimate and precisely determined purposes for which they are processed;

d) accuracy and up-to-date – The personal data processed are accurate and, where necessary, updated; in this regard, the Bank takes all necessary measures to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is processed, is deleted or rectified without delay;

e) storage limitation – Personal Data is kept in a form that allows the identification of Data Subjects for a period not exceeding the period necessary for the purposes for which the Personal Data is processed;

f) integrity and confidentiality – Personal Data is processed under appropriate security conditions so as to ensure its protection against unauthorized or unlawful processing, respectively against accidental loss, destruction or damage to Personal Data.

WHAT FALLS WITHIN THE SCOPE OF PERSONAL DATA?

As part of the activities carried out, in relation to the purpose of the processing, the Controller processes the Personal Data of the Data Subject, such as, but not limited to:

a) identification data (e.g. first name, last name, previous name, pseudonym, home and residence address, date and place of birth, personal identification number, series and number of the identity document/passport), other data that appear in the identity document, other data from the civil status documents, citizenship, etc.;

b) contact details (e.g. address, landline/mobile phone number, fax, e-mail address, etc.);

c) data regarding studies, profession, occupation, place of work, pension file number;

d) data on the economic and financial situation, data on the assets and properties held, real/personal guarantees, data on financial commitments and sources of income;

e) the source of the funds, data on the beneficial owner, public exposure, if applicable, and the public office held, data on sanctions, if applicable;

f) financial/banking data, including on the products purchased and the transactions made, username for Online Banking and Mobile Banking;

g) voice, signature, image

h) biometric data, as part of the remote identification process carried out by video means, without direct interaction with a representative of the Operator

i) other similar categories of personal data from the Operator's records, relating to the contractual relationship with the Operator, derived, mainly, from the signed contractual documentation and from the information collected by the Operator, from the execution of the law.

In some cases, data on the situation of disputes in which the Data Subject is involved may be requested, as well as other data depending on the situation of the Data Subject, which are necessary for the Controller to assess the eligibility of the Data Subject as a customer and/or guarantor in relation to the Controller, for the purpose of granting the requested financing (e.g. establishing creditworthiness and degree of indebtedness, etc.), as well as for establishing the associated credit risk.

WHAT ARE THE PURPOSES OF THE PROCESSING OF PERSONAL DATA?

The Main Purpose of the processing of Personal Data is the provision of financial services by the Controller to its customers. This purpose involves carrying out, within the concrete relationship with each client, all the activities related to the conclusion, modification and execution of the contract related to the financial product/service requested by the client. These activities also include the necessary checks to assess the eligibility of the Data Subject for the provision of the requested product/service or any other advantageous product or service.

The Controller also processes Personal Data for the following Purposes closely related to the main one:

a) carrying out the know-your-customer analysis, risk analysis, respectively reporting of suspicious transactions, according to the legislation on know-your-customer for the purpose of preventing money laundering and terrorist financing;

b) reporting to state institutions, according to special legislation, respectively for carrying out activities related to the authorities' controls (e.g. ANAF, ANPC, BNR, ANSPDCP, etc.);

c) forced execution of the amounts due, collection of debts/recovery of debts owed to the Operator, according to the concluded contracts and the legitimate interest of the Operator to recover the debts related to the existing contractual relationship with the Client/Data Subject;

d) the administration of garnishments and seizures, according to the Codes of Civil and Criminal Procedure;

e) reporting within the UniCredit Group and accounting consolidation at the level of the UniCredit Group, including the implementation of an efficient risk management process at Group level and the management and monitoring of the Group's customers, through activities that include, but are not limited to, the calculation of the indicators used in the assessment of creditworthiness, credit risk, indebtedness, adequate monitoring of all obligations assumed towards the Group, etc.;

f) carrying out FATCA reports if the Data Subject is a citizen or resident of the USA, as well as CRS (Common Reporting Standard) reports to combat tax evasion;

g) for the monitoring, security and security of persons, spaces, goods, through the video cameras located in the Operator's premises, according to Law no. 333/2003 on the protection of objectives, goods, values and protection of persons;

h) for recording communications by fax, digital channels (e.g. Online Banking, Mobile Banking, email) and calls and telephone conversations made through the Operator's Contact Center, in order to streamline and improve the services provided, as well as to conclude and execute contracts in optimal conditions, respectively to carry out telephone and online transactions;

i) carrying out analyses that can lead to profiling for the purpose of direct marketing (e.g. evaluation of banking products, history of banking transactions performed, calculation of indicators in assessing solvency/credit risk, etc.) and direct marketing, by using means of communication, including automatic calling systems that do not require the intervention of a human operator, namely email, SMS, fax, etc. such as for receiving newsletters/other commercial communications, for promoting UniCredit Group's products/services (financing/lending/other types), if you have expressed such a marketing agreement;

j) for verifying customer satisfaction and the quality of the services and products purchased, based on the legitimate interest of the permanent improvement of the Operator's services/products;

k) for statistical purposes;

l) for the purpose of preventing, investigating and limiting the consequences of fraud resulting from any area concerning the Operator's current activity;

m) fulfillment of legal requirements in the area of payments/payment services

n) the provision by UniCredit Bank of a secure and efficient instant payment service, including the presentation of the pre-filled payment order, within the RoPay service;

o) the compliance by Unicredit Bank with the obligations assumed within the National Payment Schemes in relation to the return of the amounts in case of operational errors/technical problems due to the payment service provider of the person who made payments to your accounts. or the return/blocking of amounts due to fraud.

WHY DO WE PROCESS PERSONAL DATA THROUGH THE USE OF VIDEO SURVEILLANCE MEANS AND TELEPHONE RECORDING?

In order to protect the security of the Data Subjects (e.g. customers, visitors, employees) and to ensure the security and protection of the assets of the Operator and its employees, the Operator's premises are video-surveilled, and the images obtained by means of video surveillance are recorded. For these purposes, the

aforementioned Data Subjects, as well as the goods used by them when they arrive, access or visit the Operator's premises and/or adjacent outdoor spaces, are filmed with video surveillance means installed in visible places and used in accordance with the legal regulations in force. Video surveillance takes place only in spaces intended for the public, including on access roads located inside or outside the building where the Operator's premises are located, the location of the video surveillance means being signaled by means of an icon containing a representative image and having sufficient visibility, positioned near the location. The images recorded through the use of video surveillance means will be transmitted by the Operator to the police and other authorities with attributions regarding the defense of the fundamental rights and freedoms of the person, private and public property, prevention, discovery and punishment of crimes, respect for public order and peace, under the conditions of the law. The images thus obtained will not be transmitted abroad.

The Operator may record telephone calls to/from the Operator, carried out by the Operator with the Data Subjects, regardless of the person who initiated the call, and may keep these recordings, based on the consent obtained in this regard from the Data Subjects concerned and in compliance with the applicable legal provisions. The records thus obtained will be used by the Operator for the purpose of streamlining the activities and products purchased, respectively for the conclusion and execution in optimal conditions of contracts with customers, for analyzing certain situations arising in the course of or in connection with them. Also, these telephone recordings may also be used in court, as evidence, in the event of disputes arising from or in connection with the respective contracts, they may be transmitted, under the law, to the authorities with powers regarding the defense of persons, private and public property, prevention, discovery and sanctioning of crimes.

WHY DOES THE CONTROLLER NEED TO PROCESS PERSONAL DATA?

The Personal Data is processed for the legitimate purposes mentioned above, including for the fulfillment of the obligations arising from the contractual relationship concluded, both by the Controller and by the Data Subject. Thus, the following aspects will be taken into account:

a) Personal Data necessary for the achievement of the Main Purpose – in the event that the Data Subject does not agree with/refuse the processing of his/her Personal Data, the Operator will be unable to initiate or continue contractual legal relations with the Data Subject, as it is unable to comply with the requirements of the special regulations in the financial field regarding know-your-customer, preventing and sanctioning money laundering, as well as for the establishment of measures to prevent and combat the financing of terrorism, including analyzing the request for the provision of the requested services and concluding/dismantling/executing the contractual relationship;

b) Personal data necessary for the achievement of the Related Purposes – in the event that the Data Subject expresses the right to object to the processing operations for purposes related to the supervision of the Controller's activity and accounting consolidation at Group level, the Controller will be unable to conclude or continue a legal relationship with the Data Subject, as it will not be able to carry out an effective risk management process at Group level and a process comprehensive management and monitoring of risks related to the financing of the Group's clients. In the case of data processing operations for statistical purposes, the objection of the Data Subject will be taken into account, depending on the particularities of the situation, in accordance with Art. 21 of the Regulation;

c) Personal data necessary for the achievement of the Related Purpose consisting of direct marketing – in the event that the Data Subject does not give his/her consent to direct marketing or expresses his/her right to object to the processing operation for this purpose, the Controller will not be able to send the Data Subject commercial information by SMS, e-mail, mail, about its own products or those of its partners/members of the Group;

d) Personal data necessary for the achievement of the Correlated Purpose consisting of monitoring and surveillance of persons and goods by placing video cameras in the Controller's premises – in the event that the Data Subject expresses his/her right to object, it will be analyzed according to the particularities of the situation, in accordance with Art. 21 of the Regulation, since the Operator has the obligation to ensure the security of goods and persons according to Law no. 333/2003 on the protection of objectives, goods, values and protection of persons, as well as to transmit to the competent public authorities the information necessary for them to maintain public order and combat/sanction crime.

TO WHOM DOES THE BANK TRANSMIT PERSONAL DATA?

Controllers/Processors and Recipients of Personal Data

Personal data may be transmitted to the following categories of recipients:

a) Data subject, representatives of the data subject

b) entities of the UniCredit Group

c) contractual partners of the Operator in all areas necessary for the optimal performance of the Bank's current activity (e.g.: insurers, debt collection agencies, lawyers, notaries, bailiffs, appraisers, auditors, consultants, IT/payment companies, providers of fraud investigation and documentation services, postal and courier services

d) international organizations (e.g. cards – Visa, Mastercard, etc.)

e) providers of technical services for payment processing and facilitation (e.g. Romcard, Transfond, Society for Worldwide Interbank Financial Telecommunication, etc.)

f) public authorities in Romania (e.g. the National Bank of Romania, ANAF, the National Office for the Prevention and Combating of Money Laundering, etc.) and abroad (e.g. the European Commission, tax authorities, etc.

g) other public and private law institutions (e.g. the General Directorate for Persons Records, the National Register of Movable Publicity, the National Credit Guarantee Fund for SMEs)

h) the employer of the Data Subject

i) other banks (including correspondent banks) or other financial entity/payment service provider, Card Organizations, including third party PSPs (such as payment initiation service providers, account information providers, and payment service providers issuing card-based payment instruments) to perform certain payment services, cash withdrawals or returns in situations of operational errors/technical problems or fraud

j) any other categories of contractual partners necessary for the performance of the Operator's current activity.

Personal data may be transferred to entities in the European Union/EEA. In the event of the transmission of Personal Data to a third party or international organization outside the EU, the information in the International Transfer section is applicable.

The personal data transmitted to third parties will be adequate, pertinent and not excessive in relation to the purpose for which they were collected and which allows the transmission to a specific third party.

International Transfer

The personal data will be transferred to SWIFT (Society for Worldwide Interbank Financial Telecommunication), having the capacity of controller, in case the performance of credit transfer operations - payments requested by you. includes SWIFT processing. In this regard, there is a possibility that the data transferred to SWIFT, as controller, may be accessible to the US Treasury Department. If you are a citizen of the United States of America

(USA) or resident in the United States, we inform you that, according to FATCA, the legal provisions regarding the tax regime of the US state are directly applicable to you, the data being transmitted by the Operator to the tax authorities in Romania, which can subsequently send them to the tax authorities in the USA. In all situations where international data transfer will be necessary, this will only be achieved if an adequate level of protection of personal data recognized by decision of the European Commission is ensured in the recipient country, such as the member countries of the European Economic Union (EEA). In the absence of such a decision by the European Commission, the Controller will only be able to transfer personal data to a third country if the person who will process the data has provided appropriate safeguards, provided by law in order to protect personal data, such as, without limitation the use of mandatory corporate rules, the standard data protection clauses adopted by the European Commission, standard data protection clauses adopted by a supervisory authority, contractual clauses authorized by a supervisory authority, adherence to a code of conduct approved by the supervisory authority. The Controller may be contacted for further information on the safeguards offered for the protection of personal data in the case of each data transfer abroad, by means of a written request to this effect.

HOW LONG DOES THE BANK PROCESS PERSONAL DATA?

Personal data is processed for the following periods of time:

a) during the validity period of the contracts concluded with the Operator, to which is added 10 years from the termination of the contractual relationship in relation to the provisions of Law no. 82/1991, Law no. 129/2019 and based on the legitimate interest of the Operator to take the appropriate and necessary measures to preserve the contractual documentation in order to properly defend its rights in relation to any natural or legal person, such as courts, auditors, supervisory authorities, in line with the applicable legislation, according to art. 6, paragraph 1, letters c) and f) of the GDPR; exceptions are situations when, by an applicable legal provision, it is necessary to keep it for a longer period or when the Operator justifies a legitimate interest, in which case the duration of the processing may be extended until that legitimate interest is achieved;

b) for a period of 5 years, to which a period of max. 5 years may be added, at the request of the competent authority, if a contractual relationship has not been concluded for the provision of services/products, according to the law (Law no. 129/2019 and NBR Regulation no. 2/2019);

c) if the processing is carried out for direct marketing purposes (i) if the Data Subject's options are "NO", at the end of the last contractual relationship with the entities of the UniCredit Group (in the event that they are contractual relations with several entities), participating in the direct marketing agreement (according to the annex to the Information Note), the Data Subject will no longer receive commercial communications, and the related data will be kept for another 3 years; (ii) if the Data Subject's option is "YES", at the end of the last contractual relationship with the entities of the UniCredit Group (in the event that there are contractual relations with several entities), participating in the direct marketing agreement, the Data Subject will receive commercial communications for another 1 year, after which the Data Subject's option will be "NO" in the Operator's systems, and the related data will be kept for another 3 years;

d) the processing of Personal Data by recording the images captured by the video cameras, respectively the telephone calls made on the customer support line are kept for a period of 30 days from the date of their registration, unless there are legal justifications for them to be kept for a longer period;

e) regarding FATCA and CRS reporting, according to the applicable tax legislation (e.g.: Law no. 207/2015, revised by GEO no. 102/2022): The related personal data are kept for 10 years from the expiry of the reporting deadline to the tax authorities, which runs from May 15 inclusive of the current calendar year for the information related to the previous calendar year);

f) if the Data Subject chooses to go through a remote identification process, by video means, but this process will not be completed, the data on the reasons for the interruption of the identification process (including video images) will be stored for a period of 3 years, according to the rules issued by the Authority for the Digitization of Romania, approved by Decision no. 564/2021.

WHAT DOES THE DATA SUBJECT HAVE AND HOW DOES HE EXERCISE THEM?

The data subject has the following rights with regard exclusively to his or her data:
a) the right of access to data according to art. 15 of the Regulation;
b) the right to rectification of data, according to art. 16 of the Regulation;
c) the right to erase data, according to art. 17 of the Regulation;
d) the right to data restriction, according to Article 18 of the Regulation;
e) the right to data portability, according to art. 20 of the Regulation;
f) the right to object, according to Article 21 of the Regulation;
g) the right not to be subject to an automated individual decision, including profiling, according to art. 22 of the Regulation;
h) the right to address the National Authority for the Supervision of Personal Data Processing and the judiciary;
i) the right to withdraw your consent to direct marketing and profiling for marketing purposes at any time, I confirm art. 7 para. (3) of the Regulation.
In order to exercise these rights, the Data Subject may send a written, dated and handwritten request, sent, depending on the entity that issued the card, to:

1. UniCredit Bank SA, at the address: Bulevardul Expozitiei, nr.1 F, sector 1, Bucharest, postal code 01210, or by email at infocenter@unicredit.ro, respectively by calling +40 21 200 2020 (normal rate call in the Telekom Romania fixed network) or *2020 (normal rate call in Telekom Romania, Orange, RCS&RDS, Vodafone mobile networks)
   or
2. UniCredit Consumer Financing IFN SA, at the address: Bd. Expozitiei nr. 1F, et. 6, sector 1 Bucharest, postal code 01210 or at the fax number: +40 21 200 97 01 or at the e-mail address: ucfin.contactclienti@unicredit.ro.

The information regarding the Personal Data and, as the case may be, the measures taken, will be sent to the Data Subject to the address mentioned in the request or to the one in the Controller's records, within the period of 1 month provided by the Regulation. This deadline may be extended by two months if necessary, taking into account the complexity of the request.

The operator reserves the right to set a fee in case of repeated requests according to GDPR.

Complete information on data processing can be found in the specific information notes, present at any time in the updated version on the Controller's website, in the sections dedicated to Personal Data Protection:

For UniCredit Bank SA:

https://www.unicredit.ro/ro/persoane-fizice/Diverse/protectia-datelor.html and
https://www.unicredit.ro/ro/imm/Diverse/protectia-datelor.html respectively

For UniCredit Consumer Financing IFN SA:

https://www.ucfin.ro/protectia-datelor