POLITICA CU PRIVIRE LA PROTECTIA DATELOR CU CARACTER PERSONAL

Mai 2022

Nivelul de clasificare	**INFORMAŢII RESTRICŢIONATE**
Denumirea bunului informaţional	***Politica cu privire la protectia datelor cu caracter persoanl***
Proprietar	*Departament Conformitate si AML*
Disclaimer	Acest document este destinat exclusiv uzului persoanei fizice sau juridice căreia îi este adresat sau la cererea legală a autorităţilor şi conţine informaţii restricţionate. Dacă nu sunteţi un destinatar al informaţiei sau autorizat în alt mod să utilizaţi acest document, sunteţi notificat prin prezenta că orice divulgare, copiere, distribuţie a informaţiei sau orice altă acţiune luată în baza conţinutului acestui document este strict interzisă şi poate fi ilegală. Dacă aţi accesat acest material dintr-o eroare, vă rugăm să informaţi imediat proprietarul informaţiei şi Ofiterul Bancar de Securitate a Informaţiei, să ştergeţi orice copie stocată local şi să distrugeţi orice copie fizică a documentului.

Domeniul funcţional al organizaţiei:	**Conformitate**
Reglementare:	**Politica cu privire la protectia datelor cu caracter personal**
Responsabil:	**Departamentul Conformitate si AML**

VERSIUNI					
Nr	**Data aprobarii de Consiliul de Administratie**	**Data aprobarii de Directorii Bancii**	**Data intrarii in vigoare**	**Continutul modificarii**	**Decizia Directorilor Bancii/ Consiliului de Administratie**
1	24.05.2018	-	25.05.2018	-	Decizia Consiliului de Administratie nr. 1/24.05.2018
2	21.11.2019	-	25.11.2019	-	Decizia Consiliului de Administratie nr. 8/21.11.2019
3	30.05.2022		31.05.2022	-	Decizia Consiliului de Administrație nr. 4/30.05.2022

CUPRINS

1. SCOPUL POLITICII

Această politică trebuie să fie cuprinzătoare, oferind îndrumare personalului Băncii la toate nivelurile, cu privire normele referitoare la protectia datelor cu caracter personal in conformitate cu legislatia nationala in domendiu precum si in conformitate cu Regulametul UE 2016/679 al Parlamentului European

Scopul Politicii ProCredit Bank cu privire la Protectia Datelor cu Caracter Personal este de a stabili principiile de bază pentru stocarea, utilizarea, gestionarea, transferul şi disponibilitatea datelor cu caracter personal, cu scopul de a asigura protectia drepturilor si libertatilor fundamentale ale persoanelor fizice si in special dreptul acestora la protectia datelor cu caracter personal.

Cadrul de administrare pentru protectia datelor cu caracter personal ar trebui să respecte următoarele principii:

- **Principiul legalității, echității și transparenței:** banca se va asigura ca prelucrează în mod legal, transparent și echitabil datele cu caracter personal, cum ar fi dar fara a se limita la, cele ale angajaților, potențialilor angajați, clienților, potențialilor clienți și ale oricăror persoane fizice cu care banca colaboreaza. Prelucrarea de date cu caracter personal prin mijloace frauduloase, neloiale sau ilegale este interzisă. Prelucrarea datelor cu caracter personal va fi considerată legală dacă este indeplinita cel putin una dintre urmatoarele conditii:
    a) Banca are consimțământul persoanei vizate în legătură cu prelucrarea,
    b) Prelucrarea este realizata în scopul executării unui Contract, la care persoana vizata este parte sau in scopul încheierii unui contract la inițiativa persoanei vizate,
    c) Prelucrarea este realizată în vederea respectării unei obligații legale a Bancii,

d) Prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altor persoane fizice,

e) Banca prelucrează datele în executarea unei sarcini ce servește unui interes public,

f) Prelucrarea este necesară pentru realizarea intereselor legitime Bancii.

- **Principiul limitării scopului:** Banca se va asigura că datele cu caracter personal sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri. Datele nu sunt păstrate intr-o forma care permite identificarea persoanelor vizate pe perioade mai lungi decât este necesar pentru indeplinirea scopurilor in care sunt prelucrate datele.
- **Principiul reducerii la minimum a datelor**: Banca va prelucra date cu caracter personal care sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate.
- **Principiul exactității datelor:** Banca trebuie să ia toate măsurile necesare si rezonabile pentru a se asigura că datele cu caracter personal sunt exacte, iar cele care sunt inexacte să fie șterse sau rectificate fără întârziere.

- **Principiul integrității și confidențialității:** Banca va lua măsuri tehnice si organizatorice corespunzătoare pentru a se asigura securitatea datelor cu caracter personal, inclusiv pentru a preveni pierderea, deteriorarea distrugerea sau indisponibilitatea datelor prelucrate.

- **Principiul responsabilității :** Banca va fi întrutotul responsabila de prelucrările de date cu caracter personal efectuate în cadrul activitatii, inclusiv în cazul transferurilor de date către terți, va asigura respectarea principiilor de prelucrare a datelor și va lua toate măsurile necesare pentru a putea dovedi respectarea acestora.

Această politică poate fi completată cu linii directoare, standarde tehnice, ghiduri şi proceduri care să ajute la implementarea sa şi să asigure că intenţiile acestei politici sunt îndeplinite în totalitate la toate nivelurile în cadrul întregii organizaţii.

Prin urmare, Politica cu privire la prelucrarea datelor cu caracter personal se adresează tuturor angajaţilor ProCredit Bank, precum şi terţilor care sunt legaţi prin contract de activităţile operaţionale ale Băncii. Prin prezenta, toţi angajaţii sunt responsabili de punerea în practică a acestei politici şi a ghidurilor care vin în completarea sa, în domeniul lor de activitate.

2. DEFINIŢII

Date cu caracter personal – orice informatii privind o persoana fizica identificata sau identificabila („persoana vizata”); o persoana identificabila este o persoana care poate fi identificata, direct sau indirect, in special prin referire la un element de identificare, cum ar fi un nume, un numar de identificare, date de localizare, un identificator online, sau unul sau mai multe elemente specifice, proprii identitatii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

Prelucrare - orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, 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;

Restricționarea prelucrării- marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

Pseudonimizare -prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

Sistem de evidență a datelor - orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;

Operator - ProCredit Bank SA singura sau împreună cu alte entitati (persoane fizice sau juridice, autoritatea publică, agenția sau alt organism), stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal;

Persoană împuternicită de operator- persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

Destinatar - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

Parte terță - o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

Consimțământ al persoanei vizate - orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

Incălcarea securității datelor cu caracter personal - o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

Autoritate de supraveghere- Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

3. SFERA DE ACȚIUNE

Această politică se aplică tuturor angajaţilor, persoanelor aflate in formare profesionala şi personalului angajat temporar din toate locaţiile şi sucursalele/agenţiile, precum şi tuturor persoanelor fizice sau juridice (parteneri de afaceri) care au legătură procesele legitime ale activităţii ProCredit Bank SA

Această politică se aplică de asemenea tuturor sistemelor informatice utilizate în scopurile legitime ale activităţii Băncii. Ea acoperă orice informatie care cuprinde date cu caracter personal, indiferent de tipul său, de suportul de stocare, de metoda de creare şi transmitere, cum ar fi documentele pe suport hârtie, informaţii electronice sau exprimări verbale şi conversaţii de afaceri sau în legătură cu activitatea de muncă.

Scopurile acestei politici sunt următoarele:

- Definirea cadrului de administrare a prelucrarii datelor cu caracter personal de către Bancă;
- Identificarea tuturor riscurilor de securitate pentru organizaţie şi pentru informaţiile acesteia;
- Ilustrarea efectelor incidentelor de securitate a datelor cu caracter personal;
- Îndeplinirea cerinţelor de securitate care decurg din prevederile legale şi contractuale.

Strategia pentru atingerea unui nivel adecvat de conformare a proceselor interne care implica prelucrarea de date cu caracter personal este de a defini şi actualiza prezenta politică în concordanţă cu legislatia aplicabila si cu evoluţia strategiei de afaceri, identificarea riscurilor asociate prelucrarii deficitare a datelor cu caracter personal si de a propune masuri adecvate in vederea conformarii la scopul prezentei politici.

4. OFITERUL PROTECTIA DATELOR (DPO)

4.1 Responsabilitatile Ofiterului responsabil cu Protectia Datelor

- informarea și consilierea Bancii, sau a persoanei împuternicite de Banca, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin referitoare la protecția datelor;

- monitorizarea respectării reglementarilor legale incidente referitoare la protecția datelor și a policitii Bancii sau ale persoanei împuternicite de catre Banca în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
- furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;
- cooperarea cu autoritatea de supraveghere;
- asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

- prezintă directorilor Băncii, în vederea aprobării, la începutul fiecărui an, Planul de Lucru al Ofiţerului Protecţia Datelor pentru anul în curs;
- prezintă anual către directorii Băncii propunerea de desfăşurare a procesului de anonimizare bulk
- pregăteşte şi coordonează împreună cu Departamentul Suport Aplicaţii Bancare procesul annual de anonimizare bulk a datelor cu caracter personal;

In îndeplinirea sarcinilor sale stipulate in fisa de post, responsabilul cu protecția datelor ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.

4.2 Raportari

Ofiterul cu protectia datelor raporteaza conducerii Bancii astfel:

- raportari ad-hoc in cazul in care constata deficiente in procesul de prelucarea datelor precum si in cazul constatarii unor incidente de securitate. In vederea evaluarii situatiei constatate, Ofiterul cu protectia datelor va solicita informatii relevante de la departamentele implicate in procesele de securitate a datelor (IT, departamentele implicate in activitatile

operationale, audit, risc) in vederea intocmirii unui raport de situatie. Acest raport va cuprinde in mod obligatoriu : prezentarea situatiei, eventualele riscuri generate, masurile ce au fost luate sau/ si vor fi luate in vederea remedierii deficientei precum si propunerea de rezolutie finala. Acest raport va fi inaintat Sefului Departamentului Conformitate si AML, precum si conducerii Bancii

- raportari trimestriale catre Comitelul de Risc Operational. Raportarile vor cuprinde situatia incidentelor de securitate a datelor personale aferente trimestrului anterior, rezolutia Ofiterului responsabil cu protectia datelor, precum si masurile agreate si nu in ultimul rand propuneri cu privire la imbunatatirea proceselor interne ale Bancii in vederea asigurarii unui nivel corespunzator de protectia a datelor cu caracter personal;
- raportari bi-anuale catre Comitelul de Conformitate. Raportarile vor cuprinde analiza situatiei clientilor ce urmeaza a fi anonimizati in procesul periodic si prezentarea generala a activitatii din domeniul protectiei datelor din ultimele 6 luni

5. INFORMAREA SI INTRUIREA ANGAJATILOR

La angajarea personalului, Banca va pune la dispozitia candidaţilor materiale informative cu privire la obligatiile ce le revin referitoare la respectarea reglementarilor in vigoare din aria protectiei datelor cu caracter personal. De asemenea, Banca va solicita o declaratie semnata de catre candidat prin care acesta să confirme ca a fost informat corect si complet cu privire la aspectele din prezenta politica.

Pentru evitarea incalcarii prezentei politici si a legislatiei aplicabile, la nivelul instituţiei se consideră necesar ca toţi angajaţii să aibă o pregătire corespunzătoare în domeniul prelucrarii datelor cu caracter personal.

Instruirea se poate face atât prin participarea la sesiuni de pregătire de tipul seminariilor, cât şi prin furnizarea/ distribuirea unor materiale didactice prin platforma de e-learning.

În conformitate cu prevederile prezentei politici, pentru categoriile de personal ale căror activități profesionale includ prelucrarea datelor cu caracter personal, trebuie să se asigure cel puțin o dată pe an sesiuni de pregătire de tipul ”față în față”.

De asemenea, toţi noii angajaţi beneficiază, în cadrul unui curs introductiv, de un modul în care le sunt aduse la cunoştinţă informaţiile de bază referitoare la reglementările în domeniul prelucrarii datelor cu caracter personal.

Responsabilităţile legate de instruirea personalului revin Ofiterului cu Protectia Datelor, care va realiza de asemenea şi evaluarea personalului în timpul instruirii.

Evaluarea personalului se va realiza prin susţinerea unor teste pentru verificarea cunoştinţelor angajaţilor în domeniul. Evaluarea prin testare se va face în mod obligatoriu pentru toţi angajaţii cu excepţia următoarelor categorii:

- directorii băncii;
- personal administrativ (secretariat, șoferi, femei de serviciu).

Testarea se va desfăşura anual, în trimestrul IV, prin intermediul platformei de e-learning, după parcurgerea materialului pregătit special în acest scop. În cazuri excepţionale, dacă la sfârşitul perioadei de testare vor exista angajaţi care nu au apucat să susţină testul se vor putea organiza sesiuni de testare suplimentare și la începutul anului următor.

6. EVIDENTELE ACTIVITATILOR DE PRELUCRARE

Banca păstrează o evidență a activităților de prelucrare desfășurate. Evidență cuprinde următoarele informații:

- numele și datele de contact ale Bancii și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;
- scopurile prelucrării;
- descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
- dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective

și, în cazul transferurilor menționate la articolul 49 alineatul (1) al doilea paragraf, din Regulamentul UE 2016/679 documentația care dovedește existența unor garanții adecvate;

- acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
- acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate ;

Banca și, după caz, persoana împuternicită de Banca păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind:

- numele și datele de contact ale persoanei sau persoanelor împuternicite de Banca și ale fiecărui operator în numele căruia acționează această persoană (aceste persoane), precum și ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;
- categoriile de activități de prelucrare desfășurate în numele Bancii;
- dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor prevăzute la articolul 49 alineatul (1) al doilea paragraf, Regulamentul UE 2016/679 documentația care dovedește existența unor garanții adecvate;
- acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate

Evidențele se formulează în scris, sau/ si format electronic. Banca va pune evidențele la dispoziția autorității de supraveghere, la cererea acesteia.

7. SECURITATEA DATELOR CU CARACTER PERSONAL

Banca va implementa măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător, incluzând printre altele, după caz:

- pseudonimizarea și criptarea datelor cu caracter personal;

- anonimizarea datelor atunci când acestea şi-au atins termenul de retenţie conform nomenclatorului Băncii şi a legislaţiei în vigoare prin desfăşurarea unui proces de anonimizare o data pe an;
- ştergerea datelor cu caracter personal în termen de maximum 6 luni în cazul persoanelor pentru care nu s-a finalizat procesul de contractare cu Bănca;
- capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
- capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

*Banca va aderat la **CODUL DE CONDUITĂ AL ASOCIATIEI ROMANE A BANCILOR PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL** la momentul definitivarii si implementarii acestuia la nivelul sistemului bancar romanesc.*

8. SOLICITARI ALE PERSOANEI VIZATE CU PRIVIRE LA ACCES, RECTIFICARE, STERGERE, RESTRICTIONARE A PRELUCRARII PRECUM SI LA PORTABILITATE

8.1 Accesul persoanei vizate la datele prelucrate de catre Banca

In conformitate cu prevederile legale, Banca va pune la dispozitia oricarei persoane interesate prin intermediul paginii de webside precum si prin alte canale de comunicatie utilizate, datele de contact ale Ofiterului cu protectia datelor.

Persoana vizata poate obtine de la Banca, prin intermediul Ofiterului cu pretectia datelor, o confirmare ca se prelucreaza sau nu date cu caracter personal, iar in caz afirmativ persoana vizata va avea acces la urmatoarele informatii:

- scopurile prelucrarii;
- categoriile de date cu caracter personal vizate;
- destinatarii carora le-au fost sau urmeaza sa le fie divulgate (in special destinatari din tari terte sau organizatii internationale);
- acolo unde este posibil, perioada pentru care se preconizeaza a fi stocate datele cu caracter personal sau criteriile utilizate pentru a stabili aceasta perioada;
- dreptul de a solicita Bancii rectificare/ stergerea ori restrictionarea datelor sau dreptul de a se opune prelucrarii;
- dreptul de a depune o plangere la autoritatea de supraveghere;
- in cazul in care informatiile nu au fost colectate de la persoana vizata, sursa acestora;
- existanta unui proces automatizat incluzand crearea de profiluri (daca este cazul);
- in cazul in care datele au fost transferate catre o tara terta sau organizatie internationala, persoana vizata poate solicita informatii cu privire la garantiile adecvate in conformitate cu legislatia aplicabila;

Persoana vizata poate solicita o copie a datelor cu caracter personal care fac obiectul prelucrarii. In cazul in care solicitarea este facuta pe un suport electronic, Banca va furniza aceste informatii tot pe suport electronic exceptand cazul in care persoana vizata solicita ca informatia sa-i fie comunicate pe un alt suport.

8.2 Rectificarea si stergerea

Persoana vizata are dreptul de a obtine de la Banca, fara intarziere nejustificata, rectificarea datelor cu caracter personal inexacte care o privesc. Tinand seama de scopul prelucrarii, persoana vizata are dreptul de a obtine completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declaratii suplimentare.

Persoana vizata are dreptul de a obtine din partea Bancii stergerea datelor cu caracter personal, fara intarzieri nejustificate, in cazul in care:

- datele cu caracter personal nu mai sunt necesare pentru indeplinirea scopurilor pentru care au fost colectate sau prelucrate;

- persoana vizata isi retrage consimtamantul, in cazul in care colectarea si procesarea a avut la baza consimtamantul persoanei vizate;
- persoana vizata se opune prelucrari si nu exista motive legitime care sa prevaleze sau persoana vizata se opune prelucrarii in scop de marketing direct
- datele au fost prelucrate ilegal;
- datele cu caracter personal trebuie sterse pentru respectarea unei obligatii legale care revine Bancii in temeiul dreptului Uninii Europene sau a dreptului intern;

Banca, prin intermediul Ofiterului cu protectia datelor, se poate opune in cazul in care prelucrarea este necesara:

- pentru exercitarea dreptului la libera exprimare si la informare;
- pentru respectarea unei obligatii legale sau pentru indeplinirea unei sarcini executate in interes public sau in cazul exercitarii unei autoritati oficiale cu care este investita Banca;
- din motive de interes public in domeniul sanatatii publice;
- pentru constatarea, exercitarea sau apararea unui drept in instanta.

8.3 Restrictionarea prelucrarii

Persoana vizata are dreptul de a obtine din partea Bancii restrictionarea prelucrarii in cazul in care:

- persoana vizata contesta exactitatea datelor;
- prelucrarea este ilegala iar persoana vizata se opune stergerii si solicita doar restrictionarea;
- Banca nu mai are nevoie de datele respective insa persoana vizata i le solicita pentru constatarea, exercitarea sau apararea unui drept in instanta;
- In cazul in care persoana vizata se opune dreptul Bancii de prelucrare iar Banca este in perioada de verificare a drepturilor sale legitime;

Persoana vizata care a obtinut restrictionarea prelucrarii este informata de catre Banca inainte de ridicarea restrictiei de prelucrare.

Banca va comunica fiecarui destinatar caruia iau fost divulgate datele cu caracter personal orice rectificare/ stergere a datelor cu caracter personal sau restrictionarea a prelucrarii cu exceptia cazului in care acest lucru se dovedeste imposibil sau presupune eforturi disproportionate. De

asemenea, Banca informeaza persoana vizata cu privire la destinatarii respectivi daca persoana vizata solicita expres acest lucru.

8.4 Portabilitatea datelor

Persoana vizata are dreptul de a primi datele cu caracter perosnal care o privesc si pe care le-a furnizat Bancii, intr-un format structurat, utilizat in mod curent si care poate fi citit automat si are dreptul de a transmite aceste date altui operator in cazul in care:

- Prelucrarea se bazeaza pe consimtamantul persoanei vizate sau pe un contract;
  si
- Prelucrarea este efectuata prin mijloace automate;

De asemenea, persoana vizata poate solicita Bancii sa trasmita in mod direct altui operator datele. Banca va da curs solicitarii daca acest lucru este fezabil din punct de vedere tehnic.

9. INFORMAREA /NOTIFICAREA IN CAZUL INCALCARII SECURITATII

9.1 Informarea persoanei vizate:

- incalcarea securitatii datelor cu caracter personal este susceptibila sa genereze un risc ridicat pentru drepturile si libertatile persoanelor fizice, iar Banca, prin intermediul Ofiterului responsabil cu protectia datelor, va informa fara intarziere persona vizata intr-un limbaj clar si simplu cu privire la caracterul incalcarii securitatii datelor cu caracter personal precum si masurile luate de catre institutie. Notificarea va fi transmisa in cel mult 72 de ore. In cazul depasirii termenului stabilit in prezentul paragraf, Banca va mentiona in notificare si o explicatie motivata cu privire la depasirea termenului.

- decizia cu privire la informarea persoanei vizate se va face in baza unei evaluarii intocmite de Ofiterul responsabil cu protectia datelor impreuna cu alte persoane responsabile (”Emergency Response Team”) care va curpinde:

- daca masurile de protectie tehnice si organizatorice sunt adecvate, in special daca au fost luate masuri care sa asigure ca datele cu caracter personal devin intangibile oricarei persoane care nu este autorizata (ex: criptarea);
- Banca a luat ulterior incidentului masuri prin care eventualele riscuri ridicate la adresa drepturilor si libertatilor persoanei vizate nu mai sunt susceptibile sa se materializeze;
- ar necesita un efort disproportionat

9.2 Informarea autoritatii de supraveghere

- in cazul in care are loc o incalcare a securitatii datelor, Banca notifica autoritatea de supraveghere competenta fara intarzieri nejustificate si daca este posibil in termen de 72 de ore de la data la care a luat la cunostinta. In cazul in care termenul nu poate fi respectat, Banca va adauga o explicatie motivata cu privire la imposibilitatea respectarii termenului mai sus mentionat.

- Notificarea trebuie sa cuprinda cel putin urmatoarele informatii:

- o descriere a caracterului incalcarii (acolo unde este posibil categorii si numarul aproximativ al persoanelor vizate, precum si categorii precum si numarul aproximativ al inregistrarilor
- comunica datele de contact ale responsabilului cu protectia datelor
- descrie consecintele posibile ale incalcarii
- descrie masurile luate sau propuse spre a fi luate pentru a remedia problema sau dupa caz de atenuare a efectelor negative.

9.3 Registrul de Evidenta a incidentelor de securitate DP

Banca va pastra, prin Ofierul responsabil cu protectia datelor, un Registru de Evidenta a Incidetelor de Securitate a DP in format electronic in care va evidentia toate cazurile de incalcare a securitatii datelor cu caracter personal impreuna cu toate documentele cazurilor respective.

10. TRANSFERUL DE DATE CU CARACTER PERSONAL

Avand in vedere ca in cursul normal de activitate Banca poate initia rapoarte juridice care pot genera un impact asupra datelor cu caracter personal, inainte de initierea unor astfel de rapoarte juridice, Ofiterul cu protectia datelor va verifica si aviza respectivul document din perspectiva respectarii reglementarilor nationale si europene cu privire la protectia datelor cu caracter personal si in special cu privire la reglementarile incidente cu privire la transfer.

11. REVIZUIREA PREZENTEI POLITICI

O revizuire cuprinzătoare a prezentei politici în toate segmentele sale trebuie realizată cel puţin anual de către Şeful Departamentului Conformitate si AML, pe baza feedback-ului primit de la Ofiţerul cu Protectia Datelor.

Prezenta politică este considerată o unitate auditabilă şi, prin urmare, implementarea sa trebuie să facă obiectul planurilor generale de audit intern şi extern.