POLITICA
privind Protectia Datelor Personale
v5

Cuprins

1. SCOPUL POLITICII DE PROTECTIE A DATELOR

Ca parte a responsabilității sale sociale, Grupul Salt Bank se angajează să respecte prevederile legislatiei în vigoare privind protecția datelor cu caracter personal („datele"). Ca urmare a acestui angajament, Salt Bank a adoptat prezenta Politică și asigură publicarea acesteia prin afișarea pe web-site-ul oficial www.salt.bank , pentru a putea fi consultată de orice parte interesată.
Prezenta politică de protecție a datelor se aplică la nivelul întregului Grup Salt Bank și se bazează pe principii de bază acceptate la nivel european privind protecția datelor.
Asigurarea protecției datelor reprezintă fundamentul relațiilor de afaceri de încredere și al reputației Grupului Salt Bank ca angajator atractiv.

Politica de protecție a datelor oferă una dintre condițiile-cadru necesare pentru asigurarea unui nivel adecvat de protecție a datelor cu caracter personal, conform prevederilor Regulamentului (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date (denumit in continuare GDPR), cu directă aplicabilitate în toate statele membre ale Uniunii Europene începând cu data de 25 mai 2018, precum și ale legislației naționale adoptate in domeniul protecției datelor.

2. DOMENIUL DE APLICARE SI MODIFICAREA POLITICII DE PROTECTIE A DATELOR

Această politică de protecție a datelor se aplică tuturor companiilor din Grupul Salt Bank, adică Salt Bank, tuturor companiilor sale dependente de grup, companiilor afiliate și angajaților acestora. 'Dependente', în acest caz, înseamnă societățile în care Grupul Salt Bank poate impune adoptarea directă sau indirectă a acestei Politici de Protecție a Datelor, pe baza majorității voturilor în adunarea generală a acționarilor, reprezentării conducerii majoritare sau prin acord.

Politica privind protecția datelor se extinde la toate prelucrările de date cu caracter personal.

Companiile individuale din Grupul Salt Bank pot adopta reglementări interne proprii care să asigure respectarea prezentei politici de protecție a datelor. Această politică de protecție a datelor poate fi modificată doar sub coordonarea directă a Ofițerului de Protecția Datelor din cadrul Salt Bank. Modificările vor fi raportate imediat companiilor din cadrul Grupului Salt Bank utilizând procesul de modificare a politicilor.

Cea mai recentă versiune a politicii de protecție a datelor poate fi accesată cu informațiile privind confidențialitatea datelor pe site-ul Salt Bank: www.salt.bank

3. APLICAREA LEGISLATIEI NATIONALE

Această politică de protecție a datelor cuprinde principiile de confidențialitate reglementate pe plan european, fără a înlocui legile naționale existente. În cazul în care, la nivel național,

sunt adoptate reglementări specifice de aplicare a Regulamentului General privind Protectia Datelor, Grupul Salt Bank va aplica legislația cea mai restrictivă.

Fiecare companie a Grupului Salt Bank este responsabilă de respectarea acestei politici de protecție a datelor și a obligațiilor legale impuse de reglementarile in vigoare.

4. PRINCIPII DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

a. Corectitudinea și legalitatea

Salt Bank protejează drepturile individuale ale persoanelor vizate cu ocazia prelucrării datelor cu caracter personal, datele cu caracter personal fiind prelucrate în mod legal și corect.

b. Restricții la un anumit scop

Datele cu caracter personal sunt prelucrate numai în scopul definit înainte de începerea colectării datelor. Modificările ulterioare ale scopului sunt posibile doar cu titlu excepțional, într-o măsură limitată și necesită o fundamentare.

c. Transparenta

Persoana vizată este informată cu privire la modul în care sunt prelucrate datele sale. În general, datele cu caracter personal sunt colectate direct de la persoana în cauză. Atunci când datele sunt colectate, persoana vizată trebuie să fie conștientă sau să fie informată despre:

» Identitatea Operatorului de Date,
» Datele de contact ale Responsabilului cu protecția datelor
» Scopurile și temeiurile legale aplicabile prelucrărilor de date,
»Terțe părți sau categorii de terțe părți cărora le-ar putea fi transmise datele
» Drepturile persoanelor vizate.

d. Reducerea prelucrării datelor și economia colectării datelor

Înainte de prelucrarea datelor cu caracter personal, trebuie determinat dacă și în ce măsură prelucrarea datelor cu caracter personal este necesară pentru atingerea scopului pentru care este efectuată. Atunci când scopul permite acest lucru și unde cheltuielile implicate sunt proporționale cu scopul urmărit, sunt utilizate date anonime sau statistice. Datele cu caracter personal nu sunt colectate în avans și stocate în scopuri potențiale viitoare, cu excepția cazului în care acest lucru este impus sau permis de legislația in vigoare.

e. Ștergerea

Datele personale care nu mai sunt necesare după expirarea perioadelor legate de procesele legale sau de afaceri sunt șterse. În cazul în care sunt identificate indicii cu privire la existenta unor interese care necesită protejarea sau legate de importanța istorică a acestor date în cazuri individuale, este posibil ca Banca să păstreze datele până când interesele care merită protejate au fost clarificate în mod legal, sau arhiva corporativă a evaluat datele pentru a determina dacă trebuie păstrate în scopuri istorice/ arhivistice. Atunci când ștergerea datelor poate avea impact asupra sistemelor

informatice ale bancii, datele vor fi anonimizate ireversibil, astfel încât să nu mai existe indicii care să poată conduce la identificarea persoanei vizate.

f. Precizia faptică; actualizarea datelor

Datele cu caracter personal trebuie să fie corecte, complete și, dacă este necesar, să fie actualizate. Banca ia măsuri adecvate pentru a se asigura că datele eronate sau incomplete sunt șterse, corectate, completate sau actualizate.

g. Confidențialitatea și securitatea datelor

Datele cu caracter personal sunt supuse obligațiilor legale de păstrare a secretului datelor. Acestea trebuie să fie tratate ca fiind confidențiale de fiecare angajat al Băncii și sunt asigurate măsuri organizatorice și tehnice adecvate pentru a preveni accesul neautorizat, prelucrarea sau distribuția ilegală, precum și pierderea accidentală, modificarea sau distrugerea.

5. FIABILITATEA PROCESARII DATELOR

Prelucrarea datelor cu caracter personal este permisă numai în temeiurile legale enumerate mai jos:

a. Date despre clienti și parteneri

a.1. Prelucrarea datelor pentru o relație contractuală

Datele personale ale contrapartidelor, clienți și parteneri pot fi procesate pentru a stabili, executa și rezilia un contract. Pot fi incluse, de asemenea, servicii de consultanță pentru partener în cadrul contractului, dacă acest lucru este legat de scopul contractual. Înainte de încheierea contractului - în timpul fazei de inițiere a contractului - datele personale pot fi prelucrate pentru a pregăti ofertele sau comenzile de cumpărare sau pentru a îndeplini alte cerințe din perspectiva care se referă la încheierea contractului. Contrapartidele pot fi contactate în timpul procesului de pregătire a contractului, utilizând informațiile pe care le-au furnizat. Orice restricții solicitate de contrapartide trebuie să fie respectate. Pentru cerințe de publicitate, care sunt suplimentare, trebuie respectate cerințele de la punctul 5.a.2.

a.2. Prelucrarea datelor în scopuri publicitare

Dacă persoana vizată contactează o companie din cadrul Grupului Salt Bank pentru a solicita informații (de exemplu, cererea de a primi materiale informative despre un produs), este permisă prelucrarea datelor pentru a răspunde acestei solicitări.

Activitățile de loializare sau de publicitate ale clienților fac obiectul unor cerințe legale suplimentare. Datele personale pot fi prelucrate în scopuri publicitare sau în cadrul cercetării de piață și de opinie, cu condiția ca acest lucru să fie compatibil cu scopul pentru care datele au fost colectate inițial. Persoana vizată trebuie informată cu privire la utilizarea datelor sale în scopuri publicitare. Dacă datele sunt colectate numai în scopuri publicitare, dezvăluirea de către persoana vizată este voluntară. Persoana vizată este informată că furnizarea de date în acest scop este voluntară. Atunci când comunică cu persoana vizată, este obținut consimțământul de a procesa datele în scopuri publicitare. Atunci când acordă consimțământul, persoana vizată ar trebui să

aibă posibilitatea de a alege între formele de contact disponibile, cum ar fi poșta obișnuită, e-mail și telefon (Consimțământul, a se vedea 5.a.3).
Dacă persoana vizată refuză utilizarea datelor sale în scopuri publicitare, datele acesteia nu mai poate fi utilizate în aceste scopuri și trebuie să fie blocate pentru utilizarea în aceste scopuri.

a.3. Consimțământul pentru prelucrarea datelor

Datele pot fi prelucrate după primirea acordului persoanei vizate. Înainte de a-și da consimțământul, persoana vizată trebuie informată în conformitate cu 4.c. din această politică de protecție a datelor. Consimțământul trebuie obținut în scris sau în format electronic în scopul documentării. În anumite circumstanțe, cum ar fi conversațiile telefonice, consimțământul poate fi dat verbal. Este obligatorie documentarea acordării consimțământului.

a.4. Prelucrarea datelor în conformitate cu autorizația legală

Prelucrarea datelor cu caracter personal este permisă și în cazul în care legislația aplicabilă solicită, impune sau permite acest lucru. Tipul și amploarea procesării datelor trebuie să fie necesare pentru activitatea legală de prelucrare a datelor și trebuie să respecte dispozițiile legale relevante.

a.5. Prelucrarea datelor în conformitate cu interesele legitime

Datele cu caracter personal pot fi procesate și în cazul în care prelucrarea este necesara pentru un interes legitim al Grupului Salt Bank. Interesele legitime sunt în general de natură juridică (de exemplu, colectarea creanțelor restante) sau comerciale (de exemplu, evitarea încălcărilor contractului). Datele cu caracter personal nu pot fi prelucrate în scopul unui interes legitim dacă, în cazuri individuale, există dovezi conform cărora interesele persoanei vizate merită protecție și că aceasta are prioritate. Înainte de prelucrarea datelor, este necesar să se determine dacă există interese care merită protejate.

a.6. Prelucrarea datelor foarte sensibile

Datele cu caracter personal foarte sensibile pot fi prelucrate numai dacă legea impune acest lucru sau persoana vizată a dat consimțământul expres. Aceste date pot fi, de asemenea, prelucrate dacă este obligatorie pentru afirmarea, exercitarea sau apărarea revendicărilor legale referitoare la persoana vizată. Dacă există planuri de prelucrare a datelor extrem de sensibile, Ofiterul de Protectia Datelor trebuie informat în prealabil.

a.7. Decizii individuale automatizate

Prelucrarea automatizată a datelor cu caracter personal care este utilizată pentru a evalua anumite aspecte nu poate constitui singura bază pentru deciziile care au consecințe juridice negative sau care ar putea afecta în mod semnificativ persoana vizată. Persoana vizată trebuie informată cu privire la faptele și rezultatele deciziilor

individuale automatizate și la posibilitatea de a răspunde. Pentru a evita deciziile eronate, un angajat trebuie să efectueze testarea și verificarea plauzibilității rezultatului.

a.8. Datele utilizatorilor și internetul

Dacă datele cu caracter personal sunt colectate, prelucrate și utilizate pe site-uri web sau în aplicații, persoanele vizate trebuie să fie informate despre aceasta într-o declarație de confidențialitate și, dacă este cazul, informații despre cookie-uri. Declarația de confidențialitate și orice informație privind modulele cookie trebuie să fie integrate astfel încât să fie ușor de identificat, direct accesibile și disponibile în mod consecvent pentru persoanele vizate.

Dacă sunt create profiluri de utilizare (urmărire) pentru a evalua utilizarea site-urilor web și a aplicațiilor, persoanele vizate trebuie să fie întotdeauna informate în mod corespunzător conform declarației de confidențialitate. Urmărirea personală poate fi efectuată numai dacă este permisă în conformitate cu legislația in vigoare sau după consimțământul persoanei vizate. Dacă urmărirea utilizează un pseudonim, persoana vizată ar trebui să aibă posibilitatea de a-si retrage consimțământul conform declarației de confidențialitate.

În cazul în care site-urile sau aplicațiile pot accesa date cu caracter personal într-o zonă limitată la utilizatorii înregistrați, identificarea și autentificarea persoanei vizate trebuie să ofere protecție suficientă în timpul accesului.

b. Datele angajatului

b.1. Prelucrarea datelor pentru relația de muncă

În relațiile de muncă, datele cu caracter personal pot fi prelucrate, dacă este necesar, pentru inițierea, executarea și încetarea contractului de muncă. La inițierea unui raport de muncă, datele personale ale solicitanților pot fi procesate. În cazul în care candidatul este respins, datele sale trebuie șterse în conformitate cu perioada de păstrare necesară, cu excepția cazului în care solicitantul a fost de acord să rămână la dosar pentru un viitor proces de selecție. De asemenea, este necesar consimțământul pentru utilizarea datelor pentru procesele de aplicare suplimentare sau înainte de partajarea aplicației cu alte companii din grup.

În raportul de muncă existent, prelucrarea datelor trebuie să se refere întotdeauna la scopul contractului de muncă dacă nu se aplică niciuna dintre următoarele circumstanțe pentru prelucrarea datelor autorizate.

Dacă în timpul procedurii de solicitare ar trebui să fie necesară colectarea de informații despre un solicitant de la o terță parte, trebuie respectate cerințele legilor naționale corespunzătoare. În caz de îndoială, trebuie obținut un acord de la persoana vizată.

Trebuie să existe o autorizație legală pentru prelucrarea datelor cu caracter personal care au legătură cu relația de muncă, dar care nu a făcut parte inițial din executarea contractului de muncă. Acestea pot include cerințe legale, reglementări colective cu reprezentanții angajaților, consimțământul angajatului sau interesul legitim al companiei.

b.2. Prelucrarea datelor în conformitate cu autorizația legală

Prelucrarea datelor personale ale angajaților este permisă și în cazul în care legislația națională solicită, impune sau autorizează acest lucru. Tipul și amploarea procesării datelor trebuie să fie necesare pentru activitatea legală de prelucrare a datelor și trebuie să respecte dispozițiile legale relevante. Dacă există o anumită flexibilitate juridică, trebuie luate în considerare interesele angajatului care merită protejate.

b.3. Acorduri colective privind prelucrarea datelor

În cazul în care o activitate de prelucrare a datelor depășește scopul îndeplinirii unui contract, aceasta poate fi permisă dacă este autorizată printr-o convenție colectivă. Acordurile colective sunt acorduri de salarizare sau acorduri încheiate între angajatori și reprezentanții angajaților, în limita permisă de legislația în materie de muncă.
Acordurile trebuie să acopere scopul specific al activității de prelucrare a datelor intenționate și trebuie întocmite în limitele parametrilor legislației naționale privind protecția datelor.

b.4. Consimțământul la prelucrarea datelor

Datele angajatului pot fi prelucrate după consimțământul persoanei în cauză. Declarațiile de consimțământ trebuie prezentate în mod voluntar. Acordul involuntar este nul. Declarația de aprobare trebuie obținută în scris sau în format electronic în scopul documentării. În anumite circumstanțe, consimțământul poate fi dat verbal, caz în care trebuie să fie documentat corespunzător. În cazul furnizării informate și voluntare de date de către partea relevantă, se poate presupune acordul dacă legislația națională nu necesită consimțământul expres. Înainte de a da consimțământul, persoana vizată trebuie informată în conformitate cu paragraful 4.c. din această politică de protecție a datelor.

b.5. Prelucrarea datelor în baza unui interes legitim

Datele personale pot fi procesate și în cazul în care este necesar să se impună un interes legitim al Grupului Salt Bank . Interesele legitime sunt în general de natură juridică (de exemplu, depunerea, aplicarea sau apărarea împotriva revendicărilor legale) sau financiare (de exemplu, evaluarea întreprinderilor).
Datele cu caracter personal nu pot fi prelucrate pe baza unui interes legitim dacă, în cazuri individuale, există dovezi că interesele angajatului merită protecție. Înainte de procesarea datelor, trebuie să se determine dacă există interese care merită protejate.
Măsurile de control care necesită prelucrarea datelor angajatului pot fi luate numai dacă există o obligație legală in acest sens sau dacă există un motiv legitim. Chiar dacă există un motiv legitim, trebuie examinată și proporționalitatea măsurii de control. Interesele justificate ale companiei (de exemplu, respectarea dispozițiilor legale și a reglementărilor interne ale societății) trebuie să fie cântărite în raport cu interesele angajatului care trebuie protejate si care pot fi afectate de măsura de control ce urmeaza a fi adoptată. Interesul legitim al companiei și orice interese ale angajatului care merită protejat trebuie să fie identificate și documentate înainte de luarea oricăror măsuri. În plus, trebuie luate în considerare orice cerințe suplimentare din legislația

națională (de exemplu, drepturile de co-decizie pentru reprezentanții angajaților și drepturile de informare ale persoanelor vizate).

b.6. Prelucrarea datelor personale sensibile

Datele personale sensibile pot fi procesate numai în anumite condiții. Datele personale sensibile sunt date despre originea rasială și etnică, convingerile politice, convingerile religioase sau filozofice, calitatea de membru al unei uniuni/formațiuni și sănătatea și viața sexuală a persoanei vizate. În conformitate cu legislația națională, alte categorii de date pot fi considerate sensibile sau conținutul categoriilor de date poate fi completat diferit. Mai mult, datele care se referă la o infracțiune pot fi procesate numai în conformitate cu cerințele speciale din legislația națională.
Prelucrarea trebuie permisă în mod expres sau prescrisă de legislația națională. În plus, prelucrarea poate fi permisă dacă este necesar ca autoritatea responsabilă să își îndeplinească drepturile și obligațiile în domeniul dreptului muncii. Angajatul poate, de asemenea, să consimtă în mod expres prelucrarea.
Dacă există planuri de prelucrare a datelor personale sensibile, Ofițerul de Protecția Datelor trebuie informat în prealabil.

b.7. Decizii automate

În cazul în care datele personale sunt prelucrate automat, ca parte a relației de muncă, și sunt evaluate datele personale specifice (de exemplu, în cadrul selecției personalului sau al evaluării profilurilor de competențe), această prelucrare automată nu poate constitui singura bază pentru deciziile care ar avea consecințe negative sau probleme semnificative pentru angajatul afectat. Pentru a evita deciziile eronate, procesul automatizat trebuie să asigure că o persoană evaluează rezultatul și că această evaluare este baza deciziei. Persoana vizată trebuie, de asemenea, să fie informată cu privire la faptele și rezultatele deciziilor individuale automatizate și la posibilitatea de a răspunde.

b.8. Telecomunicații și internet

Echipamentele telefonice, adresele de e-mail, intranetul și internetul împreună cu rețelele sociale interne sunt furnizate de companie în primul rând pentru misiuni legate de muncă. Ele sunt un instrument și o resursă a companiei. Acestea pot fi utilizate în cadrul reglementărilor legale aplicabile și al politicilor interne ale companiei. În cazul utilizării autorizate în scopuri personale, legile privind secretul telecomunicațiilor și legile naționale privind telecomunicațiile trebuie să fie respectate, dacă este cazul.
Pentru a asigura confidențialitatea, integritatea și disponibilitatea datelor, Banca poate implementa măsuri de protecție automate, inclusiv analiza traficului, în vederea detectării vectorilor sau modelelor de atac și prevenirii acestora, ca și în cazul răspunsului la incidentele de securitate informatică. Pentru asigurarea unui grad ridicat al securității informatice și în vederea soluționării incidentelor de securitate informatică, utilizarea echipamentelor telefonice, a adreselor de e-mail, a rețelelor intranet / internet și a rețelelor sociale interne poate fi înregistrată pentru o perioadă temporară. Evaluările acestor date și identificarea/profilarea unei anumite persoane poate fi făcută doar într-un caz concret și justificat de încălcări suspectate a legilor in vigoare sau politicilor

Grupului Salt Bank. Evaluările pot fi efectuate numai de către departamentele de investigare, asigurându-se, în același timp, respectarea principiului proporționalității. Legislația națională relevantă trebuie respectată în același mod ca și regulamentele interne ale Grupului.

Banca nu va prelucra date cu caracter personal în absența unuia dintre motivele de mai sus. Aceeași regulă se aplică, de asemenea, în cazul în care scopul colectării, prelucrării și utilizării datelor cu caracter personal trebuie să fie modificat față de scopul inițial.

6. TRANSMITEREA DATELOR CU CARACTER PERSONAL

Transmiterea datelor cu caracter personal către destinatarii din afara sau în interiorul Grupului Salt Bank face obiectul cerințelor de autorizare pentru prelucrarea datelor cu caracter personal în conformitate cu secțiunea 5. Beneficiarul datelor trebuie să fie obligat să utilizeze datele numai în scopurile definite.

În cazul în care datele sunt transmise unui destinatar din afara Grupului Salt Bank către o țară terță, această țară trebuie să accepte să mențină un nivel de protecție a datelor echivalent cu această politică de protecție a datelor. Acest lucru nu se aplică în cazul în care transmiterea se bazează pe o obligație legală. O obligație legală de acest tip se poate baza pe legile țării domiciliate a societății Grupului care transmite datele. În subsidiar, legile țării domiciliate a societății din grup pot recunoaște scopul transmiterii datelor în baza obligației legale a unei țări terțe.

În cazul în care datele sunt transmise de o terță parte unei companii a Grupului Salt Bank, trebuie să se asigure că datele pot fi utilizate în scopul dorit.

Dacă datele cu caracter personal sunt transferate de la o companie a Grupului cu sediul social în Uniunea Europeană / Spațiul Economic European către o societate a Grupului cu sediul social în afara Spațiului Economic European (țara terță), societatea care importă datele este obligată să coopereze cu orice anchetă făcută de autoritatea de supraveghere competentă din țara în care își are sediul social partea care exportă datele și de a se conforma observațiilor autorității de supraveghere cu privire la prelucrarea datelor transmise. Același lucru este valabil și pentru transmiterea datelor de către companiile din grupuri din alte țări. Dacă fac parte dintr-un sistem internațional de certificare pentru respectarea regulilor corporative obligatorii privind protecția datelor, acestea trebuie să asigure cooperarea cu birourile și agențiile de audit relevante. Participarea la astfel de sisteme de certificare trebuie să fie convenită cu responsabilul cu protecția datelor.

În cazul în care un subiect de date pretinde că această politică de protecție a datelor a fost încălcată de societatea din Grup care se află într-o țară terță care importa datele, compania Grupului cu sediul în Spațiul Economic European care exportă datele se angajează să sprijine partea în cauză, ale căror date au fost colectate în Spațiul Economic European, pentru a stabili faptele și pentru a-și afirma drepturile în conformitate cu această politică împotriva societății de grup care importă datele.

7. PRELUCRAREA DATELOR PRIVIND CONTRACTELE

Prelucrarea datelor în numele său înseamnă că un furnizor este angajat să proceseze date cu caracter personal, fără a-și asuma responsabilitatea pentru procesul de afaceri afiliat. În

aceste cazuri, un acord privind prelucrarea datelor în numele acestuia trebuie încheiat cu furnizori externi și printre companiile din cadrul Grupului Salt Bank. Clientul își păstrează întreaga responsabilitate pentru performanța corectă a procesării datelor. Furnizorul poate procesa date personale numai conform instrucțiunilor clientului. La emiterea ordinului, departamentul care plasează comanda trebuie să se asigure că sunt îndeplinite următoarele cerințe:

a. Furnizorul trebuie ales pe baza capacității sale de a acoperi măsurile tehnice și organizatorice de protecție necesare.

b. Ordinul trebuie trimis în scris. Instrucțiunile privind prelucrarea datelor și responsabilitățile clientului și furnizorului trebuie să fie documentate.

c. Trebuie luate în considerare standardele contractuale privind protecția datelor furnizate de responsabilul cu protecția datelor.

d. Înainte de începerea prelucrării datelor, clientul trebuie să aibă încredere că furnizorul își va respecta obligațiile. Un furnizor poate documenta conformitatea cu cerințele de securitate a datelor, în special prin prezentarea unei certificări adecvate.

În funcție de riscul de prelucrare a datelor, revizuirile trebuie repetate în mod regulat pe durata contractului.

e. În cazul procesării transfrontaliere a datelor din contracte, trebuie îndeplinite cerințele naționale relevante pentru divulgarea datelor cu caracter personal în străinătate. În special, datele cu caracter personal din Spațiul Economic European pot fi procesate într-o țară terță numai dacă furnizorul poate dovedi că are un standard de protecție a datelor echivalent cu această politică de protecție a datelor. Instrumentele adecvate pot fi:

i. Acordul privind clauzele contractuale standard ale UE pentru prelucrarea datelor din contracte în țările terțe cu furnizorul și cu orice subcontractanți.

ii. Participarea furnizorului la un sistem de certificare acreditat de UE pentru asigurarea unui nivel suficient de protecție a datelor.

iii. Recunoașterea regulilor corporative obligatorii ale furnizorului pentru a crea un nivel adecvat de protecție a datelor de către autoritățile de supraveghere responsabile pentru protecția datelor.

8. DREPTURILE PERSOANEI VIZATE

Fiecare persoană vizată are următoarele drepturi. Afirmația lor trebuie să fie tratată imediat de către unitatea responsabilă și nu poate constitui un dezavantaj pentru persoana vizată.

a. Persoana vizată poate solicita informații privind datele cu caracter personal care i-au fost stocate, modul în care au fost colectate datele și în ce scop. Dacă există alte drepturi de a vizualiza documentele angajatorului (de exemplu, dosarul personalului) pentru relația de muncă în conformitate cu legile relevante privind ocuparea forței de muncă, acestea nu vor fi afectate.

b. Dacă datele cu caracter personal sunt transmise terților, trebuie furnizate informații despre identitatea destinatarului sau categoriile de destinatari.

c. Dacă datele cu caracter personal sunt incorecte sau incomplete, persoana vizată poate solicita corectarea sau completarea acesteia.

d. Persoana vizată poate contesta prelucrarea datelor sale în scopuri de publicitate sau de cercetare a pieței / opiniei publice. Datele trebuie să fie blocate pentru aceste tipuri de utilizare.

e. Persoana vizată poate cere ca datele sale să fie șterse în cazul în care prelucrarea acestor date nu are un temei juridic sau dacă temeiul juridic nu mai este valabil. Același lucru este valabil dacă scopul care a stat la baza procesării datelor a expirat sau a încetat să mai fie aplicabil din alte motive.
Perioadele de păstrare existente și interesele conflictuale care merită protejate trebuie respectate.
f. Persoana vizată are, în general, dreptul de a se opune prelucrării datelor sale și aceasta trebuie luată în considerare dacă protecția intereselor sale are prioritate față de interesul operatorului de date în urma unei situații personale specifice. Acest lucru nu se aplică în cazul în care o dispoziție legală impune ca datele să fie procesate.

În plus, fiecare persoană vizată poate pretinde drepturile de la punctele 3.b, 4, 5, 6, 9, 10 și 14.c. ca beneficiar terț dacă o companie care a acceptat să respecte Politica de protecție a datelor nu respectă cerințele și încalcă drepturile părții.

9. CONFIDENTIALITATEA PROCESARII

Datele personale sunt supuse secretului datelor. Orice colectare, prelucrare sau utilizare neautorizată a acestor date de către angajați este interzisă. Orice procesare de date efectuată de un angajat, care nu a fost autorizată să fie desfășurată ca parte a îndatoririlor sale legitime, este considerate ca fiind neautorizată. Se aplică principiul 'necesitatea de a cunoaște'. Angajații pot avea acces la informații personale în funcție de adecvarea acestui acces la tipurile de date și de scopul determinat. Acest lucru se bazează pe defalcarea și separarea atentă a atributiilor angajaților băncii și presupune punerea în aplicare a rolurilor și responsabilităților pentru fiecare angajat.
Angajaților li se interzice să utilizeze date cu caracter personal în scopuri private sau comerciale, să le dezvăluie persoanelor neautorizate sau să le pună la dispoziție în orice alt mod. Superiorii ierarhici își informează angajații la începutul relației de muncă cu privire la obligația de a proteja secretul datelor.
În cazul utilizării neautorizate a datelor personale, angajații pot fi sancționați în conformitate cu legislatia aplicabilă și cu reglementările în vigoare în cadrul Grupului Salt Bank.
Obligația menținerii confidențialității datelor personale rămâne în vigoare și după încheierea perioadei de angajare, sancțiunile aplicabile în caz de încălcare a obligației de confidențialitate fiind cele prevăzute de cadrul legislativ în vigoare.

10. SECURITATEA PRELUCRARII

Datele personale sunt protejate împotriva accesului neautorizat și împotriva prelucrării sau divulgării ilegale, precum și pierderii accidentale, modificării sau distrugerii. Acest lucru se aplică indiferent dacă datele sunt prelucrate electronic, pe suport de hârtie sau prin alte mijloace. Înainte de introducerea noilor metode de prelucrare a datelor, în special a noilor sisteme informatice, sunt definite și implementate măsuri tehnice și organizatorice de protecție a datelor cu caracter personal. Aceste măsuri trebuie să se bazeze pe stadiul tehnicii, pe riscurile procesării și pe necesitatea de a proteja datele (determinate de procesul de clasificare a informațiilor).
În special, structura organizatorică responsabilă se poate consulta cu Direcția de Securitate a Informației (DSI) și cu responsabilul pentru protecția datelor. Măsurile tehnice și organizatorice pentru protecția datelor personale fac parte din managementul securității

informațiilor corporative și sunt adaptate în mod continuu la evoluțiile tehnice și schimbările organizaționale.

11. CONTROLUL PROTECTIEI DATELOR

Respectarea politicii de protecție a datelor și a legilor aplicabile privind protecția datelor este verificată în mod regulat prin intermediul auditurilor de protecție a datelor precum și al altor controale. Realizarea acestor controale este responsabilitatea responsabilului cu protecția datelor, a coordonatorilor de protecție a datelor și a altor unități ale grupului cu drepturi de audit sau a auditorilor externi angajați. Rezultatele controalelor privind protecția datelor sunt raportate responsabilului cu protecția datelor. Consiliul de Administratie al Salt Bank este informat despre rezultatele primare ca parte a sarcinilor de raportare ale responsabilului cu protectia datelor cu caracter personal. La cerere, rezultatele controalelor privind protecția datelor vor fi puse la dispoziția autorității responsabile de protecția datelor. Autoritatea responsabilă cu protecția datelor poate efectua propriile controale de conformitate cu reglementările din această politică, conform legislației naționale.

12. INCIDENTE DE PROTECTIE A DATELOR

Toți angajații sunt obligati să informeze imediat superiorul sau Ofițerul de Protecția Datelor cu privire la cazurile de încălcare a acestei politici de protecție a datelor sau alte reglementări privind protecția datelor cu caracter personal (incidente de protecție a datelor), indiferent dacă este vorba despre o încălcare a confidențialității, a integrității datelor sau a disponibilității acestora. Conducătorul structurii organizatorice este obligat să informeze imediat Ofițerul de Protecția Datelor cu privire la incidentele de protecție a datelor. În cazurile de:

- » Transmitere necorespunzătoare a datelor cu caracter personal către terțe părți,
- » Acces neadecvat la datele cu caracter personal sau
- » Pierdere, distrugere sau alterare a datelor cu caracter personal,

conducătorul structurii organizaționale în cauza întocmește, de urgență, rapoartele de sesizare, conform regulilor stabilite pentru Gestionarea Incidentelor de Securitate a Datelor cu Caracter Personal, astfel încât să poată fi luate măsurile urgente pentru limitarea afectării titularilor de date cu caracter personal și pentru respectarea obligațiilor de raportare și notificare a incidentelor către autoritatea de supraveghere.

13. RESPONSABILITATI SI SANCTIUNI

Conducerea fiecărei companii din Grupul Salt Bank precum și angajații și prepușii acestora sunt responsabili de prelucrarea datelor în zona lor de responsabilitate. Prin urmare, aceștia sunt obligați să se asigure că sunt îndeplinite cerințele legale pentru protecția datelor și cele conținute în politica de protecție a datelor (de exemplu, obligațiile naționale de raportare). Organele de conducere au responsabilitatea de a se asigura că există măsuri organizaționale, resurse umane și tehnice pentru ca orice prelucrare a datelor să fie efectuată în conformitate cu protecția datelor. Respectarea acestor cerințe reprezinta responsabilitatea conducatorilor de structuri organizatorice.
Ofițerul de Protecția Datelor al Salt Bank este informat de îndată despre controalele efectuate de autoritățile de supraveghere cu privire la protecția a datelor.

Organele de conducere ale companiilor din Grupul Salt Bank informeaza Ofițerul de Protecția Datelor al Salt Bank cu privire la numele Ofițerului de Protecția Datelor din cadrul companiei pe care o reprezintă fără a exclude posibilitatea ca mai multe societăți din grup să numească aceeași persoana în rolul de Ofițer de Protecția Datelor.
Ofițerii de Protecția Datelor sunt persoanele de contact mentionate pe siteurile companiilor din Grup, în secțiunea destinată protecției datelor. Aceștia pot efectua verificări și își familiarizează angajații cu conținutul politicilor de protecție a datelor. Departamentele responsabile de procesele și proiectele de afaceri informează în timp util Ofițerul de Protecția Datelor cu privire la noile prelucrări de date cu caracter personal. Pentru planurile de prelucrare a datelor care pot prezenta riscuri speciale pentru drepturile individuale ale persoanelor vizate, Ofițerul de Protecția Datelor este informat înainte de începerea procesării. Acest lucru se aplică în mod obligatoriu datelor cu caracter personal sensibile. Managerii se asigură că angajații lor sunt suficient de instruiți în protecția datelor. Prelucrarea necorespunzătoare a datelor cu caracter personal sau alte încălcări ale legilor privind protecția datelor pot conduce la cereri de despăgubire pentru prejudicii. Încălcările pentru care angajații individuali sunt responsabili pot conduce la sancțiuni prevăzute în dreptul muncii.

14. OFITERUL DE PROTECTIA DATELOR (DPO)

Ofițerul de Protecția Datelor, fiind independent din punct de vedere al ordinelor profesionale, își desfășoară activitatea pentru respectarea legislației în vigoare privind protecția datelor. El este responsabil pentru politica de protecție a datelor și supraveghează respectarea acesteia. Ofițerul de Protecția Datelor are linie de raportare directă către Consiliul de Administrație al companiei în cadrul căreia își desfășoară activitatea.
Companiile din Grupul Salt Bank care sunt obligate din punct de vedere juridic să numească un responsabil cu protecția datelor vor desemna un Ofițer de Protecția Datelor.
Ofițerii de Protecția Datelor din subsidiarele băncii informează fără întârziere Ofițerul de Protecția Datelor al Salt Bank cu privire la orice risc de protecție a datelor.
Orice persoană vizată poate aborda Ofițerul de Protecția Datelor, în orice moment să ridice preocupări, să pună întrebări, să solicite informații sau să depună plângeri legate de protecția datelor sau de problemele de securitate a datelor. Dacă se solicită, preocupările și plângerile vor fi tratate în mod confidențial.
În cazul în care coordonatorul de date în cauză nu poate rezolva o plângere sau remedia încălcarea politicii de protecție a datelor, Ofițerul de Protecția Datelor este consultat de îndată. Deciziile luate de Ofițerul de Protecția Datelor pentru remedierea încălcărilor privind protecția datelor trebuie să fie susținute de conducerea societății în cauză. Anchetele autorităților de supraveghere sunt întotdeauna raportate responsabilului cu protecția datelor.

Datele de contact ale responsabilului cu protecția datelor și ale personalului sunt următoarele:
Salt Bank S.A. , Ofițer de Protecție a Datelor (DPO),
E-mail: dpo@salt.bank

15. DEFINITII

» *Datele sunt anonime* dacă identitatea personală nu poate fi niciodată urmărită de nimeni sau dacă identitatea personală ar putea fi recreată doar cu un timp, cheltuieli și muncă nerezonabile.

» *Consimțământul* este acordul voluntar, obligatoriu din punct de vedere juridic pentru prelucrarea datelor în situația în care nu sunt aplicabile alte temeiuri legale .

» *Incidentele de protecție a datelor* sunt toate evenimentele în care există suspiciuni justificate că datele cu caracter personal sunt capturate, colectate, modificate, copiate, transmise sau utilizate ilegal.
Aceasta se referă la acțiunile unor terți sau angajați.

» *Persoana vizată* în cadrul acestei politici de protecție a datelor este orice persoană fizică a cărei date pot fi prelucrate. În unele țări, persoanele vizate pot fi și persoane juridice.

» *Spațiul Economic European (SEE)* este o regiune economică asociată cu UE și include Norvegia, Islanda și Liechtenstein.

» *Datele personale sensibile* sunt date despre originea rasială și etnică, opiniile politice, credințele religioase sau filosofice, calitatea de membru al unei formatiuni/uniuni sau sănătatea și viața sexuală a persoanei vizate.
În conformitate cu legislația nationala, si alte categorii de date pot fi considerate foarte sensibile sau conținutul categoriilor de date poate fi structurat diferit. Mai mult, datele care se referă la o infracțiune pot fi procesate adesea numai în conformitate cu cerințele speciale din legislația națională.

» *Datele personale* reprezintă toate informațiile despre anumite persoane fizice sau persoane care pot fi definite. O persoană poate fi definită, de exemplu, dacă relația personală poate fi determinată utilizând o combinație de informații cu cunoștințe suplimentare suplimentare.

» *Prelucrarea datelor personale* înseamnă orice proces, cu sau fără utilizarea sistemelor automate, pentru colectarea, stocarea, organizarea, păstrarea, modificarea, interogarea, utilizarea, transmiterea, transmiterea, difuzarea sau combinarea și compararea datelor. Aceasta include, de asemenea, eliminarea, ștergerea și blocarea datelor și a suporturilor de stocare a datelor.

» Prelucrarea datelor cu caracter personal este necesară în cazul în care scopul permis sau interesul justificat nu au putut fi obținute fără datele personale sau numai cu cheltuieli excepțional de mari.

» Operatorul de date este compania independentă din punct de vedere legal a Grupului Salt Bank, a cărei activitate de afaceri inițiază măsura relevantă de prelucrare.

» Un nivel suficient al protecției datelor în țările terțe este recunoscut de Comisia Europeană dacă nucleul personal al vieții private, așa cum este definit în unanimitate în țările membre ale UE, este asigurat în mod adecvat. Atunci când ia decizia, Comisia Europeană contabilizează toate circumstanțele care joacă un rol în transmiterea datelor sau o categorie de transmitere a datelor. Acestea includ opiniile în conformitate cu legislația națională și standardele profesionale relevante aplicabile și măsurile de securitate relevante.

»*Țările terțe* în cadrul politicii de protecție a datelor sunt toate națiunile din afara Uniunii Europene / SEE. Aceasta definitie nu include țările cu un nivel de protecție a datelor considerat suficient de către Comisia Europeană.

» *Părțile terțe* sunt oricine în afară de persoana vizată și de operatorul de date. Într-un caz de prelucrare a datelor in numele procesatorilor din UE, entitatile nu sunt terțe părți în temeiul legilor privind protecția datelor, deoarece sunt atribuite prin lege entității responsabile.

» *Transmiterea* reprezinta o divulgare a datelor protejate de către entitatea responsabilă către terțe părți.