

CAIET DE SARCINI

Aplicație de calcul a provizioanelor de risc de credit conform IFRS9

1. Informații generale

Obiectul prezentului caiet de sarcini îl reprezintă achiziționarea unei soluții software integrate (licențe, servicii de implementare, customizare, training și suport tehnic) pentru:

- Calculul ajustărilor pentru pierderi așteptate pe 12 luni (12-month ECL) și pe durata de viață a expunerii (Lifetime ECL) pentru toate expunerile relevante băncii (credite, tranzacții interbancare, titluri, garanții de portofoliu și individuale acordate).
- Generarea notelor contabile pentru provizioanele calculate și transferul acestora către sistemul core banking printr-o interfață specifică.
- Alocarea și managementul marcajelor specifice pentru credite, inclusiv:
 - Starea de nerambursare (default).
 - Creditele restructurate cu dificultăți financiare (forbearance), cu sub-categoriile aferente.
 - Alocarea automată a expunerilor pe stadii de depreciere (Stage 1, Stage 2, Stage 3) conform IFRS 9, pe baza unui set configurabil de criterii cantitative și calitative.
 - Identificarea evenimentelor de derecunoastere.
 - Identificarea contractelor non-SPPI
- Monitorizarea criteriilor de intrare și ieșire din diverse stări (default, forbearance, stadii IFRS 9).
- Implementarea unor fluxuri pentru migrarea expunerilor între diferitele stări de credit și marcaje.

Cerințele impuse prin acest caiet de sarcini, enumerate în secțiunile următoare, sunt detaliate și în anexa "Formular cerințe". Ofertanții vor transmite acest formular completat împreună cu documentele solicitate în secțiunea 7.

2. Cerințe funcționale specifice

Serviciile necesare includ:

- I. Modulul 1 – aplicație de calcul a ajustărilor pentru pierderi așteptate (provizioane de risc de credit) conform standardelor IFRS9:
 - a) Calculul provizioanelor în funcție de alocarea pe stadii de depreciere:
 - i. pentru expunerile clasificate în stadiul 1 – estimarea pierderilor așteptate generate de evenimente ce se pot produce în următoarele 12 luni;
 - ii. pentru expunerile clasificate în stadiul 2 – estimarea pierderilor așteptate reflectând posibilitatea apariției stării de nerambursare pe toata durata de viață a instrumentului financiar;

- iii. pentru expunerile clasificate în stadiul 3 și POCI- evaluare pe baza individuala prin actualizarea sumelor estimate a se recupera.
- b) Aplicația trebuie să preia în mod automat din sistemele băncii datele necesare calculului (e.g.: tabele de rambursare a creditelor, rata efectivă a dobânzii – EIR), și trebuie să ofere posibilitatea de a introduce sumele estimate de recuperare în cazul expunerilor clasificate în stadiul 3 și POCI.
- c) Aplicația trebuie să genereze, pe baza planului de conturi și monografiilor contabile furnizate de Bancă, note contabile pentru înregistrarea contabilă a ajustărilor pentru pierderi așteptate în formatul necesar preluării acestora în sistemul informatic principal.
- d) Aplicația trebuie să transfere către sistemele băncii marcajele stadiilor de depreciere, a evenimentelor de nerambursare, a creditelor restructurate sau derecunoscute din punct de vedere contabil.
- e) Soluția trebuie să permită actualizarea parametrilor de risc (probabilități de nerambursare (PD), ratele de pierdere în caz de nerambursare (LGD), coeficienții de conversie în echivalent credit (CCF));
- f) Aplicația să aibă capacitatea ca pe baza unor date încărcate să calculeze îndeplinirea criteriului de clasificare SPPI (*"solely payments of principal and interest"*) pentru diferite active financiare (credite acordate, titluri de stat, depozite plasate);
- g) Aplicația trebuie să efectueze calculul ajustării dintre dobânda contractuală a unui credit prin aplicarea dobânzii contractuale la expunerea brută și dobânda calculată prin aplicarea ratei efective a dobânzii la costul amortizat al creditului („unwinding of interest adjustment”) pentru creditele depreciate la data raportării și să genereze notele contabile aferente în formatul necesar pentru preluarea în sistemul informatic principal. Aplicația de asemenea trebuie să permită transmiterea ajustării calculate în aplicația de bază a băncii;
- h) Aplicația trebuie să efectueze calculul ajustării de valoare justă la recunoașterea inițială a unui credit POCI și să genereze notele contabile aferente în formatul necesar pentru preluarea în sistemul informatic principal al Băncii;
- i) Aplicația trebuie să efectueze calculul periodic al diferențelor între ajustarea inițială și soldul provizioanelor calculat la data ajustării pentru credite POCI și să genereze notele contabile aferente în formatul necesar pentru preluarea în sistemul informatic principal al Băncii;
- j) Aplicația trebuie să efectueze calculul ajustării de valoare justă pentru creditele măsurate la valoare justă prin Contul de profit și pierdere (FVPL) pentru credite care nu îndeplinesc criteriul SPPI și să genereze notele

contabile aferente în formatul necesar pentru preluarea în sistemul informatic principal al Băncii;

- k) Aplicația trebuie să identifice evenimentele de derecunoaștere datorate modificărilor semnificative cantitative (e.g. modificări ale scadențarului care determină o modificare mai mare de 10% a NPV-ului creditului modificat) sau calitative (e.g. modificare debitor, modificare produs, split credit sau merge credite etc.) apărute la nivelul unui credit și transmiterea acestora în aplicația informatică principală a băncii;
- l) Aplicația trebuie să permită calculul diferenței între NPV inițial și NPV credit modificat în cazul modificării nesemnificative (care nu conduce la derecunoaștere: e.g. modificări care modifică NPV cu mai puțin de 10% din NPV inițial) a unui credit și să genereze notele contabile aferente în formatul necesar pentru preluarea în sistemul informatic principal al Băncii;

II. Modulul 2 – modul de alocare marcaje / clasificare pentru:

- a) starea de nerambursare: marcarea clienților în stare de nerambursare ("*default event*") conform cerințelor Regulamentul (UE) nr. 575/2013 *privind cerințele prudențiale pentru instituțiile de credit*, (art.178) și a indicațiilor ghidului EBA/GL/2018/06 "*Guidelines on management of non-performing and forborne exposures*".
- b) creditele restructurate cu dificultate financiară ("*forbearance*");
- c) alocarea expunerilor pe stadii de depreciere în funcție de un set de criterii;
- d) soluția trebuie să asigure o monitorizare automată a criteriilor de intrare și ieșire din starea de nerambursare;
- e) soluția trebuie să asigure un flux automat de migrare a expunerilor în diferite stări ale creditelor restructurate (e.g.: "*performing forbearance*", "*non-performing forbearance*", "*probation period*").
- f) algoritm de identificarea contractelor non-SPPI

III. Reportare și analiză

- a) Rapoarte de management privind calitatea portofoliului, structura pe stadii, expuneri în default, expuneri în forbearance, etc.
- b) Rapoarte de audit și reconciliere.
- c) Capacitatea de a exporta datele în formate standard (Excel , CSV).
- d) Instrumente de analiză ad-hoc și de tip "drill-down".
- e) Posibilitatea de customizare a rapoartelor existente și de creare de rapoarte noi de către utilizatorii Băncii.

IV. Audit și trasabilitate

- a) Înregistrarea tuturor acțiunilor utilizatorilor și modificărilor de sistem.
- b) Istoric complet al modificărilor de parametri, reguli, clasificări.
- c) Posibilitatea de a reproduce calculele pentru o dată anterioară (funcționalitate "as-of").

- V. Oferta trebuie să cuprindă un plan de livrare pentru informațiile solicitate, specificând metodele și timpul estimat de furnizare, separat pentru fiecare modul. De asemenea, trebuie să demonstreze capacitatea de a oferi asistență tehnică pentru pe durata contractului.

3. Criterii tehnice

- a) Arhitectură și Tehnologie:
- Soluția va fi implementată on-premise sau într-un mediu cloud privat/public acceptat de Bancă.
 - Arhitectură scalabilă (cu posibilitatea de a adăuga resurse pe măsură ce volumul de date crește).
 - Tehnologii moderne, stabile și recunoscute pe piață.
 - Specificații privind sistemul de operare, baza de date suportată (preferabil compatibilitate cu infrastructura existentă a Băncii – ex: Windows Server, MS SQL Server).
- b) Integrare cu Sistemele Existente:
- Capacitatea de a se integra cu sistemul bancar central (Core Banking System) al Băncii și alte surse de date relevante (sistem de rating, data warehouse, sistem de management al garanțiilor etc.).
 - Suport pentru multiple formate de import/export de date (flat files, CSV, XML, API-uri, conexiuni directe la baze de date).
 - Procese ETL (Extract, Transform, Load) robuste, monitorizabile și configurabile pentru preluarea datelor necesare.
- c) Performanță și Scalabilitate
- Capacitatea de a procesa volume mari de date într-un timp rezonabil (SLA-uri pentru procesările cheie, cum ar fi calculul ECL lunar).
 - Scalabilitate arhitecturală verticală și orizontală.
- d) Securitate
- Controlul Accesului logic
 - Nu este permis accesul neautentificat în aplicație. Orice acces în aplicație (atât la nivelul utilizatorilor cât și la nivelul altor module de aplicație) va fi precedat de identificarea, autentificarea și autorizarea accesului.
 - Nu este permisă hard-codarea în aplicație a credențialelor de acces.
 - Nu este permisă utilizarea în script-uri a useri/parole în clar utilizate pentru conectarea cu alte medii / baze de date / module de aplicație
 - Nu este permisă stocarea în clar (fișiere, baze de date) a credențialelor de acces
 - Nu este permisă transmiterea în clar în rețea a credențialelor de acces ale utilizatorilor sau ale serviciilor.
 - Sesiunile de lucru ale utilizatorilor trebuie să expire și să se închidă automat după o perioadă de timp configurabilă.
 - Autentificare și autorizare
 - Pentru respectarea cerințelor interne cu privire la acces, complexitate parola, convenție nume utilizatori se va folosi autentificarea în aplicație folosind SSO.
 - Integritate securizată cu directorul de utilizatori ai Băncii (LDAPs)

- Posibilitate de implementare autentificare multifactor pentru anumite roluri (MFA)(ex: Pentru useri administrativi sau locali, daca este cazul), unde se va respecta:
 - impunere / verificare factor de complexitate a credentialelor conform politicii Băncii;
 - blocarea accesului după un număr de încercări eșuate de logare
- Păstrarea credentialelor pentru alte tipuri de autentificări trebuie să se facă în zone protejate și cu mecanisme de hashing rezistente la atacuri (algoritm one-way - Argon2, Bcrypt, cu salt generat automat, random și unic pentru fiecare ID)
- Nu este permisă afișarea sau printarea caracterelor (de exemplu *) în momentul în care parola este introdusă de la terminal; camuflarea parolei prin afișarea de caractere "**";
- Se va folosi în cazul autentificării serverelor, serviciilor și modulelor de aplicație prin schimb de certificate / chei publice.
- Accesul administrativ (administratori aplicație) se va face în urma autentificării cu MFA.
- Administrarea utilizatorilor / privilegiilor
 - Fiecare utilizator trebuie să aibă un identificador (User ID) unic și atribuit un profil unic.
 - Pentru administrarea utilizatorilor / privilegiilor se vor folosi profile de securitate (machete, template) asociate utilizatorilor (roluri model RBAC)
 - Înscrierea utilizatorilor/ crearea ID-urilor se va face prin asocierea/atașarea utilizatorului la un profil de utilizator (macheta, template)
 - Nu este permisă crearea de utilizatori care să nu aibă asociat un profil de securitate
 - Se vor utiliza profile de securitate diferite pentru administrarea / managementul utilizatorilor / profilelor și pentru introducerea / prelucrarea datelor.
 - Privilegiile acordate profilelor / utilizatorilor trebuie alocate respectând principiul "strict necesar pentru a-si desfășura activitatea"
 - Toate acțiunile de administrare a utilizatorilor trebuie să fie auditate și jurnalizate
- Comunicații
 - Toate fluxurile de date stabilite în afara (daca este cazul) și în interiorul băncii vor fi securizate prin criptarea comunicațiilor
 - Fluxurile de date vor fi securizate pe fiecare segment al traseului (TLS, VPN, IPSec);
 - Nu este permisă transmiterea în clar a informațiilor din aplicație prin infrastructura informatica.
 - Se vor implementa mecanisme de control / chei de verificare a integrității informațiilor transmise între modulele aplicației (CRC, Hashing) sau alte integrări cu soluții externe;
- Confidențialitate și integritate
 - Opțiunile de meniu nepermise unui utilizator / profil vor fi inhibitate / inaccesibile
 - Este obligatorie non persistența oricărei informații reziduale (fișiere temporare, buffered data areas etc) care ar putea conține informații folosite de către aplicație – credentiale de acces sau de interconectare între modulele aplicației
 - Accesul la informațiile confidențiale se va acorda numai în urma autentificării și autorizării utilizatorilor

- Orice modificare/vizualizare a datelor se va face numai prin intermediul aplicației, accesul direct în baza de date sau pe mediul de stocare este interzis cu excepția administratorilor TIC cu mecanisme de control suplimentare;
- Pentru datele confidențiale se va asigura criptarea la nivelul fișierelor / bazelor de date cu algoritmi de criptare acceptați și rezistenți la atacuri. Datele vor fi criptate atât în tranzit cât și "on rest".
- Non repudiarea: orice acțiune sensibilă în aplicație va avea atașate: ID-ul utilizatorului preluat din informațiile de login un identificator de înregistrare și time-stamp privind data/ora operației efectuate.
- Din punct de vedere al integrității datelor:
 - Versionare pentru rapoarte generate.
 - Validări și controale interne în aplicație
 - Checksum / hash (SHA-256) pentru verificarea fiabilității fișierelor generate/exportate.
- Jurnalizare, monitorizare, auditare
 - Jurnalizarea evenimentelor semnificative legate de controlul accesului:
 - Înregistrarea în jurnal a logarilor soldate cu succes (data, ora, user id, modulul la care s-a primit accesul)
 - Înregistrarea în jurnal a logarilor soldate cu insucces (data, ora, user id, modulul la care s-a refuzat accesul)
 - Înregistrarea în jurnal a încercărilor repetate eșuate, soldate cu blocarea id-ului
 - Înregistrarea în jurnal a reactivării id-urilor blocate
 - Jurnalizarea evenimentelor semnificative din punct de vedere al managementului utilizatorilor
 - Înregistrarea în jurnal a evenimentelor: creare /ștergere/modificare utilizatori
 - Înregistrarea în jurnal a evenimentelor: creare/modificare/ștergere profile (machete) utilizator
 - Înregistrarea în jurnal a evenimentelor: modificare corespondența utilizator-profil alocat
 - Înregistrarea în jurnal a activității utilizatorilor cu profile administrative
 - Înregistrarea în jurnal a modificărilor de profile de securitate
 - Înregistrarea în jurnal a trecerii unui utilizator de pe un profil pe alt profil
 - Jurnalizarea evenimentelor semnificative din punct de vedere al trasabilității unei acțiuni (id acțiune, utilizatorul responsabil, data /ora), upload, ștergere, creare, modificare fișiere.
 - Trebuie asigurată consistența informațiilor jurnalizate pe diverse subsisteme pentru păstrarea trasabilității de-a lungul proceselor
 - Jurnalizarea evenimentelor legate de confidențialitatea comunicațiilor (schimbul de certificate, transmisie criptată / necriptată, metoda și algoritmul de criptare, lungimea cheii, etc.).
 - Jurnalizarea evenimentelor soldate cu insucces (cheie coruptă, cheie lipsă, eroare la criptare / decriptare, etc)
 - Orice modificare la nivel de date este logată
 - Toate interfețele de integrare între modulele aplicației vor comunica doar securizat (criptat) și autentificarea este recomandată să fie mutuală și pe baza de certificate.
 - Toate cheile secrete (certificate, secrete, chei) vor fi păstrate în dispozitive dedicate tip vault
 - Interfața cu clientul web-based va respecta toate cerințele standard OWASP cu privire la aplicații web Aceste cerințe vizează în primul rând următoarele categorii:

- Input validation
 - Output encoding
 - Session management
 - Authentication
 - Acces control
 - Criptografie (certificate..etc)
 - Trataterea erorilor
 - Protectia datelor
 - Comunicatii
 - Configurarea sistemelor si bazelor de date
 - Cerințe Continuitate - aplicația va suporta arhitectura de înalta disponibilitate si backup-uri tip GFS (Grandfather-Father-Son)
 - Cerințe retenție date - aplicația va oferi posibilitatea ca informațiile sa fie păstrate pentru o perioadă de 5 ani având implementate mecanisme automate/semi-automate de arhivare a datelor – ștergerea din sistemele de producție si mutarea acestora in tabele/structuri de tip arhiva.
- e) Administrare și Mentenanță
- Instrumente de administrare și monitorizare a soluției.
 - Proceduri clare pentru backup și restaurare.
 - Ușurință în aplicarea patch-urilor și actualizărilor, cu posibilitatea revenirii la varianta anterioara in caz de esec.
 - Optiuni de gestiune semi-automate a comutarii functionarii intre mediul de principal de productie si mediul secundar/alternativ.
 - Optiuni de gestiune a mediilor de test semi-automate prin preluarea aplicatiei si a datelor aferente din mediul de productie sau prin import de date.

4. Cerințe privind implementarea soluției

- a) Ofertantul va prezenta un plan detaliat de implementare, incluzând faze, activități, resurse necesare și termene.
- b) Metodologie de implementare va fi prezentata detaliat.
- c) In scopul implementarii si al licentierii solutiei intra mediul de productie, mediul secundar/alternativ pentru situatiile de nefunctionare al mediului principal, precum si a unui mediu de test/dezvoltare.
- d) Ofertantul va asigura serviciile de analiză și design pentru adaptarea soluției la specificul Băncii.
- e) Ofertantul va asigura toate serviciile de configurare și customizare a soluției
- f) Ofertantul va asigura o testare riguroasă a soluției (testare unitară, de integrare, UAT - *User Acceptance Testing*) împreună cu echipa Băncii.
- g) Ofertantul va asigura testarea proceselor de comutare intre mediile de productie principal si secundar/alternativ, precum si catre mediile de test/dezvoltare, precum si documnetarea detaliata a procedurilor de transfer.
- h) Ofertantul va asigura suport de tipul „golden” pe parcursul perioadei de "go-live" și stabilizare post-implementare de minim 3 luni.
- i) Ofertantul va asigura un management de proiect dedicat.

5. Cerințe privind suportul tehnic și mentenanța post-implementare

- a) Descrierea pachetelor de suport tehnic și mentenanță disponibile (niveluri de servicii - SLA, program de suport, canale de comunicare).
- b) Suport pentru rezolvarea incidentelor și erorilor.

- c) Furnizarea de actualizări și noi versiuni ale software-ului;
- d) Furnizarea de adaptari și actualizări generate de modificări de reglementare aplicabile bancilor de dezvoltare/.
- e) Perioada minimă de suport și mentenanță asigurată de cel puțin 3 ani.

6. Cerințe privind training-ul utilizatorilor

- a) Ofertantul va furniza sesiuni de training complete pentru diferitele categorii de utilizatori ai Băncii (utilizatori finali, administratori de sistem, personal IT).
- b) Materiale de training în limba română și/sau engleză.
- c) Training-ul poate fi realizat la sediul Băncii sau online.

7. Criterii de calificare:

- a) Experiență în dezvoltarea de aplicații de calcul al provizioanelor conform IFRS 9, cu prezentarea a minimum 2 referințe de preferat de la bănci locale.
- b) Ofertantul va prezenta un document care să cuprindă cifra de afaceri pe ultimii 3 ani, iar valoarea acesteia nu trebuie să fie mai mică de 5 milioane lei.
- c) Certificatul constatator eliberat de Oficiul Național al Registrului Comerțului din care să rezulte adresa actuală, obiectul de activitate al societății, acționarii/asociații, administratorii societății, eliberat cu cel mult 3 luni în urmă;
- d) Certificatul eliberat de Oficiul Național al Registrului Comerțului "Furnizare Informații din Registrul Beneficiarilor Reali" din care să rezulte beneficiarii reali declarați ai societății, în conformitate cu Legea 129/2019, eliberat cu cel mult 3 luni în urmă.
- e) În cazul unei structuri de proprietate complexe se va prezenta Schema structurii actuale de proprietate care să includă toate entitățile din lanțul de proprietate (inclusiv jurisdicția de înregistrare, cota de participare în capitalul social) și membrii organelor de conducere ale acestora, semnată de persoana împuternicită a Ofertantului.
- f) Chestionarul asupra politicii de risc social și de mediu (modelul furnizat de Bancă), completat și semnat de reprezentantul legal al societății;
- g) Declarația privind conflictele de interese (terți) (modelul furnizat de Bancă), completată și semnată de reprezentantul legal al societății
- h) Certificat de atestare fiscală privind lipsa datoriilor restante cu privire la plata impozitelor, taxelor, sau a contribuțiilor la bugetul general consolidat (buget local, buget de stat etc.), valabil la data prezentării
- i) Cazierul Fiscal al ofertantului - operator economic, valabil la data prezentării;
- j) Cazierul Judiciar al ofertantului - operator economic, valabil la data prezentării;
- k) Cazierul Judiciar al membrilor organului de administrare/conducere sau de supraveghere, sau a celor care au putere de reprezentare, de decizie sau control în cadrul acestuia, așa cum rezultă din certificatul constatator emis de ONRC/actul constitutiv, valabile la data prezentării;
- l) Chestionar de securitate și protecția datelor - (model furnizat de Bancă) **se va solicita doar ofertantului clasat pe primul loc.**

8. Criterii de evaluare

Nr. crt.	Denumire factor de evaluare	Pondere
1	Costul aplicației și al serviciilor furnizate	60%
2	Experiență în domeniul dezvoltării de aplicații bancare	8%
3	Arhitectura aplicației, tehnologia implementată, integrare cu sistemele existente	8%
4	Gradul de acoperire al cerințelor funcționale	8%
5	Securitate (controlul accesului, administrarea utilizatorilor)	8%
6	Timpul de implantare estimat	8%
Nota ofertă	Suma ponderată a notelor	100%

9. Garanții

- i. Garanția de participare 5,000 lei fără TVA
- ii. Garanția de bună execuție se constituie de către contractant în scopul asigurării Băncii de îndeplinirea cantitativă, calitativă și în perioada convenită a contractului, care însă nu trebuie să depășească 10% din prețul contractului fără TVA.

Modalitatea de constituire a garanțiilor

Garanția de participare și garanția de bună execuție se pot constitui în oricare dintre următoarele variante:

- a) virament bancar;
- b) instrumente de garantare emise în condițiile legii astfel:
 - (i) scrisori de garanție emise de instituții de credit bancare din România sau din alt stat;
 - (ii) scrisori de garanție emise de instituții financiare nebancare din România sau din alt stat;
 - (iii) asigurări de garanții emise:
 - fie de societăți de asigurare care dețin autorizații de funcționare emise în România sau într-un alt stat membru al Uniunii Europene și/sau care sunt înscrise în registrele publicate pe site-ul Autorității de Supraveghere Financiară, după caz;
 - fie de societăți de asigurare din state terțe prin sucursale autorizate în România de către Autoritatea de Supraveghere Financiară.

10. Contestațiile

Orice persoană care se consideră vătămată într-un drept al său ori într-un interes legitim, printr-un act al Băncii sau prin nesoluționarea unei cereri, are dreptul de a contesta procedura de achiziție în termen de 3 zile lucrătoare de la comunicarea rezultatului.

Contestația va cuprinde următoarele informații:

- datele de identificare a contestatorului;
- obiectul contestației;
- motivele contestației;
- dovezile pe care se întemeiază;
- semnătura contestatorului sau a împuternicitului acestuia.

Contestațiile sau orice altă nemulțumire legată de procesul de achiziție se va face prin intermediul uneia dintre următoarele modalități:

- serviciilor poștale/curierat la adresa sediului Băncii;
- depunere personală la sediul Băncii;
- adresei electronice dedicate: reclamatii@bidromania.eu;
- formularului dedicat pe pagina de internet a Băncii (<https://www.bidromania.eu/contact> - secțiunea *Reclamații*).

Termenul de soluționare este de maximum 30 zile de la data depunerii și înregistrării contestațiilor, iar soluția comunicată este definitivă.

11. Perioada contractuală

Perioada ferma de 2 ani, cu prelungirea automata pe perioade de 1 an din partea Bancii.

12. Plăți

Termen de plata 30 de zile de la emiterea facturii.

13. Clauze contractuale obligatorii

Contractul va trebui să cuprindă clauze speciale privind obligația ofertantului de a respecta cadrul reglementar și legal aplicabil băncilor privind conformitatea cu Strategia Națională de Anticorupție, evitarea conflictelor de interese, respectarea regimului de Sancțiuni Financiare Internaționale, respectarea prevederilor privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date („GDPR”), precum și oricăror alte acte normative aplicabile pentru asigurarea protecției datelor cu caracter personal.

Contractul va cuprinde etapele și livrabilele conform planului de proiect propus în ofertă precum și penalitățile aplicabile în cazul nerespectării acestora de către furnizor. De asemenea, contractul va include în anexă caietul de sarcini, clarificările ulterioare, precum și oferta transmisă de către furnizor, acestea fiind documentele care clarifică scopul contractului.