17.12.2012

Nr. 118718/17.12.2012

Către,

CURTEA DE APEL BUCUREŞTI
SECŢIA A VIII-A DE CONTENCIOS ADMINISTRATIV ŞI FISCAL

Ministerul Justiției, în calitate de petent, în temeiul art. 281 alin.1 şi art. 283 alin. 1 din O.U.G. nr. 34/2006 privind atribuirea contractelor de achiziție publică, a contractelor de concesiune de lucrări publice şi a contractelor de concesiune de servicii, cu modificările şi completările ulterioare, formulează

PLÂNGERE

împotriva Deciziei nr. 4442/C2/5172/5182 din 04.12.2012, pronunțată de Consiliul Național de Soluționare a Contestațiilor, în soluționarea contestației înregistrate la C.N.S.C. sub nr. 35964 din 15.11.2012 depusă de S.C. OMNIASMART S.R.L. şi a contestației înregistrate la C.N.S.C. sub nr. 35874 din 14.11.2012 depusă de S.C. STAUROS CONSULTING S.R.L. împotriva documentației de atribuire elaborată de Ministerul Justiției în cadrul procedurii de „licitație deschisă" organizată pentru atribuirea contractului de achiziție publică de furnizare având ca obiect „Achiziționare platformă de e-learning cu specific IT pentru Ministerul Justiției şi sistemul judiciar" din prin care vă solicităm următoarele:

1. **Suspendarea executării deciziei atacate până la soluționarea prezentei plângeri, în temeiul art. 283[1] din O.U.G. nr. 34/2006.**
2. **Anularea Deciziei nr. 4442/C2/5172/5182 din 04.12.2012 a Consiliul Național de Soluționare a Contestațiilor.**

În considerarea prevederilor art.281 din OUG nr.34/2006, vă rugăm să dispuneți comunicarea plângerii instanței competente conform art. 283 din actul normativ citat anterior.

În fapt, prin contestația nr.235 din 13.11.2012 înregistrată la Ministerul Justiției sub nr.8422/30/14.11.2012 şi la CNSC sub nr. 35874 din 14.11.2012, contestatoarea S.C. STAUROS CONSULTING SRL a solicitat pronunțarea unei decizii prin care să se dispună obligarea autorității contractante la refacerea documentației de atribuire prin eliminarea cerințelor de natură a restricționa participarea la procedură şi anularea criteriilor de atribuire, învederând că cerința privind **experiența** specialiştilor dezvoltator software, coordonator dezvoltare conținut şi dezvoltator conținut educațional **într-un proiect de implementare a unui sistem informatic în**

domeniul educației este excesivă şi irelevantă aducând astfel atingere dispozițiilor art.8 alin.1 din HG nr.925/2006. De asemenea, contestatoarea, susține că raportat la obiectul contractului care este dezvoltarea unei platforme de e-learning cu specific IT **nu est relevant a se solicita un expert de securitate, respectiv un expert în testarea securității sistemelor informatice**. În privința criteriului de atribuire - oferta cea mai avantajoasă din punct de vedere economic - se arată că factorii de evaluare din grilă sunt subiectivi şi nerelevanți în raport cu obiectul contractului, solicitându-se în acest sens anularea acestor criterii de atribuire care descriu o aplicație deja existentă, fiind de natură a favoriza un producător care are deja aceste criterii implementate.

Analizând susținerile şi documentele depuse de părți CNSC a admis în parte contestația formulată de S.C. STAUROS CONSULTING SRL, respectiv criticile privind sintagma ,, în domeniul educației" şi ,,expert în testarea securității sistemelor informatice", dispunând obligarea autorității contractante de a modifica documentația de atribuire, reținând că impunerea cerințelor privind experiența într-un proiect de implementare a unui sistem informatic în domeniul educației/expert de securitate sunt restrictive, disproporționate deoarece nu corespund obiectului contractului care este de furnizare a unui produs şi de nu prestare a unor servicii în domeniul educațional. În acest sens, sunt invocate dispozițiile art.8 ali.1 lit. b) din HG nr.925/2006 conform cărora ,, Autoritatea contractantă nu are dreptul de a restricționa participarea la procedura de atribuire prin introducerea unor cerințe minime de calificare care sunt disproporționate în raport de natura sau complexitatea contractului." De asemenea, se arată că este încălcat şi principiul proporționalității care trebuie înțeles în sensul asigurării unei corelații între necesitățile autorității contractante, obiectul contractului de achiziție publică şi cerințele solicitate a fi îndeplinite. În final, se arată că scopul noii legislații privind achizițiile publice este de a asigura accesul la cât mai mulți operatori economici la procedurile de atribuire, de promovare a concurenței între aceştia şi de garantare a tratamentului egal şi nediscriminatoriu. Menționăm că CNSC a menținut acelaşi argumente şi în cazul cerinței privind ,,expertul în testarea securității sistemelor informatice", concluzionând că securizarea sistemului informatic ar putea face obiectul unei alte proceduri.

În legătură cu solicitarea privind anularea criteriului de atribuire, CNSC a dispus respingerea ca nefondată a criticii privind factorii de evaluare şi continuarea procedurii de atribuire cu respectarea celor descrise anterior.

În considerarea argumentelor pe care le vom expune în continuare, vă rugăm să dispuneți:

- **suspendarea efectelor deciziei nr. 4442/C2/5172/5182 din 04.12.2012 a CNSC până la soluționarea pe fond a plângerii;**
- **anularea Deciziei nr. 4442/C2/5172/5182 din 04.12.2012i a CNSC în privința admiterii cererilor de eliminare a cerințelor privind experiența ,,în domeniul educației şi ,,expert în testarea securității sistemelor informatice" ca fiind nelegală şi netemeinică şi continuarea procedurii de achiziție publică**

I. În primul rând, raportat la prevederile art.283[1] alin.1 şi 2 din OUG nr.34/2006 conform cărora ,,**În cazuri temeinic justificate şi pentru prevenirea unei pagube iminente, preşedintele instanței**

poate dispune, la cererea părții interesate, prin încheiere dată cu citarea părților, suspendarea executării contractului.

(2) Instanța soluționează cererea de suspendare luând în considerare consecințele probabile ale acesteia asupra tuturor categoriilor de interese ce ar putea fi lezate, inclusiv asupra interesului public. Instanța va putea să nu dispună măsura prevăzută la alin. (1) în cazul în care consecințele negative ale acesteia ar putea fi mai mari decât beneficiile ei. Hotărârea de a nu dispune suspendarea executării contractului nu trebuie să prejudicieze niciun alt drept al persoanei care a înaintat cererea prevăzută la alin. (1).'' solicităm suspendarea executării Deciziei CNSC atacate până la soluționarea pe fond a plângerii motivat de faptul că implementarea proiectului **trebuie finalizată în 12 luni de la data semnării contractului dar nu mai târziu de 01.12.2013**, conform contractului de finanțare nr.517/323 semnat între Ministerul Justiției în calitate de beneficiar şi Ministerul Comunicațiilor şi Societății Informaționale în calitate de Organism Intermediar, or prin modificarea documentației de atribuire conform Deciziei CNSC se prorogă toate termenele aferente procedurii de achiziție publică respectiv termenul pentru solicitare clarificări, termen pentru răspuns la clarificări, etc. având ca efect amânarea datei prognozate pentru atribuirea şi executarea contractului de achiziție publică. Menționăm că fondurile pentru realizarea acestui proiect sunt asigurate printr-o finanțare nerambursabilă pentru implementarea proiectului SMIS 22996 ,,Platformă de e-Learning cu specific IT pentru Ministerul Justiției şi sistemul judiciar din România (format din ICCJ, CSM, SNG) în cadrul programului Operațional Sectorial Creşterea Competitivității Economice care se poate pierde în cazul prelungirii procedurii de atribuire cu riscul neatingerii scopului proiectul, lezându-se astfel interesul public ce constă în asigurarea condițiilor unei bune funcționări a sistemului judiciar şi a justiției ca serviciu public. Mai mult decât atât, prin suspendarea procedurii de achiziție publică de către CNSC, toate etapele fixate pentru derularea achiziției publice au fost decalate, existând deja o întârziere în graficul estimativ de atribuire a contractului în discuție. În consecință, vă rugăm să observați că în cauza de față sunt întrunite condițiile legale pentru a opera suspendarea Deciziei CNSC. Astfel, prin prorogarea procedurii de atribuire se produce un prejudiciu viitor şi previzibil autorității contractante care va fi în imposibilitate de a se încadra până la finele anului 2013 cu atribuirea şi executarea contractului implicând inclusiv efectuarea plăților din fondurile nerambursabile.

De asemenea, proiectul **„Achiziționare platformă de e-learning cu specific IT pentru Ministerul Justiției şi sistemul judiciar''** a fost aprobat în cadrul strategiei de informatizare a sistemului judiciar.

Potrivit dispozițiilor art. 120 alin. 4 din Legea nr. 304/2004 privind organizarea judiciară cu modificările şi completările ulterioare, strategia de informatizare a sistemului judiciar se aprobă prin hotărâre a Guvernului, la propunerea Ministerului Justiției. În acelaşi text de lege este prevăzut faptul că în vederea creării unui sistem informatic unitar şi funcțional, instituțiile sistemului judiciar au obligația de a duce la îndeplinire măsurile prevăzute în strategia de informatizare. În temeiul acestor dispoziții prin H.G. nr. 543/2005 a fost aprobata Strategia de informatizare a sistemului judiciar pe perioada 2005-2009.

II. Cu privire la obligația de a elimina cerința ca **experiența experților 4 – dezvoltator software, 5 – Coordinator Dezvoltare Conținut si 6 – dezvoltator conținut educațional să fie într-un proiect de implementare sistem informatic din domeniul educației**, impusă prin decizia CNSC, vă solicităm să constatați că aceasta este lipsită de fundament, şi pe cale de consecință să o înlăturați în baza următoarelor argumente:

Conform art.178 alin.2 din OUG nr.34/2006 **„Autoritatea contractantă nu are dreptul de a solicita îndeplinirea unor cerințe minime referitoare la situația economică și financiară și/sau la capacitatea tehnică și profesională, care ar conduce la restricționarea participării la procedura de atribuire."**

Potrivit art.179 alin.1 și 2 din OUG nr.34/2006 **„ Criteriile de calificare și selecție stabilite de către autoritatea contractantă trebuie să aibă o legătură evidentă cu obiectul contractului ce urmează să fie atribuit.**

(2) Autoritatea contractantă are obligația de a respecta principiul proporționalității atunci când stabilește criteriile de calificare și selecție, precum și nivelul cerințelor minime pe care ofertanții/candidații trebuie să le îndeplinească."

Prin introducerea cerințelor minime de calificare pentru cei 3 experți al căror scop a fost descris mai sus, vă învederăm că nu se încalcă dispozițiile legale citate anterior, câtă vreme sunt într-o legătură indisolubilă cu specificul contractului de achiziție publică ce urmează a fi atribuit, corespund necesității autorității contractante, neputând fi impuse de către ofertanți, în funcție de posibilitățile acestora și este respectat inclusiv principiul proporționalității reflectat prin solicitarea unor cerințe minime raportat la complexitatea contractului în discuție care garantează atingerea scopului acestuia. Prin Decizia nr.6954 din 24.06.2009 CNSC a reținut că „atunci când autoritatea contractantă găsește de cuviință să introducă anumite cerințe de calificare pentru ofertanți ea este ținută să se limiteze cu aceste opreliști în calea participării la achiziția publică doar la cele absolut necesare și strict la pragurile care îngrădesc cel mai puțin operatorii economici." La această practică a achiesat și jurisprudența Curții de Apel Brașov care prin decizia nr.593 R/25.09.2009 a reținut că „autoritatea este competentă să introducă cerințe de calificare cu anumite praguri, însă trebuie să fie preocupată ca exigențele astfel impuse să fie suficient de rezonabile încât să nu antreneze, în considerarea prevenirii unor eventuale abuzuri, la o restrângere excesivă a exercițiului drepturilor operatorilor economici de a concura la câștigarea contractului".

După cum se poate observa, normele privind achizițiile publice nu limitează dreptul autorității contractante de a stabili cerințe minime obligatorii conforme strict cu necesitățile sale ci numai pe cele care ar nu ar corespunde scopului contractului și nu ar avea o justificare rezonabilă. Or, în prezenta speță, cerințele minime contestate și eliminate prin decizia CSNS sunt de deplin justificate prin Nota de justificare întocmită de autoritatea contractantă, fiind imperios necesare pentru îndeplinirea contractului având ca obiect tocmai platforma e-learning. Precizăm că realizarea sarcinilor de către dezvoltatorul e-learning presupune cunoștințe teoretice și practice de științele educației, servicii clienți și personal, comunicare și media, limbă și comunicare, psihologie, calculatoare și software, precum și deprinderi utilizate în învățare, deprinderi de rezolvare de probleme și deprinderi de gestionare a resurselor. Sistemul e-learning are drept scop furnizarea unor soluții de învățământ prin mijloace electronice, ceea ce semnifică faptul că experții IT trebuie să cunoască și să fi creat programe informatice în care au aplicat noțiuni/concepte din sfera domeniul educațional (arie curriculară, proces de instruire, instrumente de predare a testelor metode de curs, etc.), astfel încât să garanteze atingerea obiectivelor de instruire a personalului Ministerului Justiției și al instanțelor judecătorești, cetățeni, de simplificare a accesului la resursele educaționale prin cursuri la distanță, fără profesor, prin instruire în ritmul propriu al fiecărei persoane, de realizare a laboratoarelor de la distanță. De asemenea, portalul educațional care ar urma să se realizeze (site) trebuie să asigure și posibilitatea înscrierii on-line la diverse evenimente de instruire, cursuri, seminarii, conferințe, diverse forme de învățământ, furnizarea de suporturi de curs/tutoriale, activități de testare on-line a cunoștințelor, forumuri de discuții, activități pentru a căror realizare presupune

imperios necesar ca experții ce vor fi implicați în proiect să aibă experiență în crearea de site-uri educaționale, un exemplu în acest sens fiind site-ul: ,,http://portal.edu.ro". Menționăm că soluțiile de tip portal nu se aplică exclusiv în domeniul de activitate al Ministerului Educației, Cercetării, Tineretului şi Sportului ci pot avea diferite destinații de la publicului larg, portaluri specifice unui domeniu (de ex. educație specială), portaluri guvernamentale până la portaluri regionale.

În plus, vă solicităm să observați că achiesarea de către CNSC la susținerile contestatorului privind experiența pentru **dezvoltatorii software**, pentru coordonatorul de dezvoltare conținut şi pentru dezvoltatorii de conținut educațional într-un proiect de implementare sistem informatic din domeniul educației ca fiind excesivă şi neavând relevanță cu activitatea pe care aceşti experți urmează să o desfăşoare în cadrul proiectului nu are temei întrucât cei 3 experți solicitați pentru aceasta poziție vor avea sarcina de a dezvolta funcționalitatea pentru un sistem destinat susținerii procesului educațional, care include şi o componenta de portal educațional. Dezvoltarea funcționalităților implică transpunerea cerințelor autorității contractante în funcționalități ale unui sistem software care poate fi realizată în mai multe moduri, unele mai adecvate, altele mai puțin adecvate scopului sistemului, şi anume acela de susținere a procesului educațional. **Astfel, consideram că experiența anterioară în astfel de implementări, a dezvoltatorilor software, poate rezulta într-o implementare cu un grad mai mare de aplicabilitate la scopul pentru care sistemul este achiziționat şi care să răspundă mai bine utilizatorilor preconizați, în particular cursanți şi instructori. În practică, implementările efective ale cerințelor software, pot face distincția netă între un sistem care să eficientizeze activitatea şi unul care să îngreuneze activitatea utilizatorilor.**

De asemenea, calificarea de către contestator a cerinței privind experiența în calitate de Coordonator dezvoltare conținut/Coordonator Ştiințific în cel puțin un proiect de implementare sistem informatic în domeniul educației ce a inclus dezvoltarea de conținut digital de instruire pentru adulți ca fiind excesivă şi neavând relevanță cu activitatea pe care acest expert urmează să o desfăşoare în cadrul proiectului nu poate fi primită, fiind total nejustificată câtă vreme este esențială experiența anterioară a expertului într-un astfel de proiect, deoarece în acest mod conținutul educațional ce urmează a fi dezvoltat va profita pe deplin utilizatorilor şi se va integra perfect cu sistemul educațional ofertat, în contrast cu situații în care sistemul informatic educațional, respectiv dezvoltarea de conținut digital s-au realizat separat, în proiecte diferite. Prin faptul ca experții ce participă la implementarea sistemului informatic şi cei care sunt responsabili cu dezvoltarea conținutului de instruire fac parte din aceeaşi echipă, in cadrul aceluiaşi proiect, consideram ca se dobândeşte o experiență specifică, valoroasă, care permite tuturor experților realizarea mai eficientă a activităților de coordonare, dezvoltare si implementare. Aceleaşi argumente pledează şi în favoarea cerinței privind experiența pentru dezvoltatorii de conținut educațional intr-un proiect de implementare sistem informatic din domeniul educației.

Referitor la disproporționalitatea cu obiectul contractului dorim să atragem atenția că obiectivul contractului vizează exact un sistem informatic destinat educației şi dezvoltarea de conținut digital interactiv de instruire pentru adulți.

III. Cu privire la **obligația de a elimina cerința pentru expertul 10. ,,Expert în testarea securității sistemelor informatice"** vă solicităm să constatați că aceasta este lipsită de fundament şi pe cale de consecință să o înlăturați în baza următoarelor argumente:

Sistemul informatic solicitat va fi accesibil prin Internet şi va avea şi componente dezvoltate în cadrul proiectului, ceea ce poate conduce la implementarea unor funcționalități cu un nivel de

securizare mai mare sau mai mic, ce poate fi afectat de aşa-numitele „bug-uri software de securitate". În aceste condiţii, considerăm imperios necesară testarea securităţii sistemului înainte de a începe exploatarea acestuia. Motivarea CNSC conform căreia este lipsită de relevanta utilizarea unui expert de testare a securităţii sistemului informatic din partea furnizorului, este absolut nesusţinută. În plus, decizia CNSC cu privire la acest aspect este practic nemotivată făcându-se doar trimitere la considerentele reţinute privind experienţa în domeniul educaţional a experţilor.

CNSC mai reţine că, întrucât obiectul contractului este de furnizare a unei platforme e-learning nu de securizare a unui sistem informatic, securizarea sistemului informatic ar putea face obiectul unei alte proceduri, fără nici o lămurire în acest sens. În sens contrar celor reţinute de CNSC prin decizia sa, arătăm că în caietul de sarcini au fost incluse cerinţe specifice de securitate în cadrul unui capitol distinct, care reiau prevederile din proiectul tehnic anexă la Cererea de finanţare care a fost depusă de către MJ la MCSI în vederea evaluării şi obţinerii finanţării proiectului. Astfel de cerinţe au tocmai scopul de a asigura servicii de securitate avansată în scopul prevenirii şi protecţiei diverselor tipuri de ameninţări care există în mediul virtual, cerinţe care nu au fost contestate.

Mai mult decât atât, prin Cererea de finanţare, anexă la contractul de finanţare încheiat între MCSI şi MJ, secţiunea 2.3.3. Activităţi preconizate a se realiza, se precizează că se vor desfăşura inclusiv activităţi de auditare informatică şi a securităţii reţelei. În cadrul aceluiaşi document la descrierea arhitecturii sistemului se precizează că trebuie asigurată protecţia sistemului e-learning prin utilizare de mecanisme de tip proxy şi sistem de detectare a intruziunilor, cu filtrare dinamică a pachetelor şi mod transparent de lucru.

Pentru a asigura implementarea acestor cerinţe de securitate, este evident necesar ca printre experţii propuşi de ofertanţi să se numere în mod obligatoriu şi un **expert în testarea securităţii sistemelor informatice.**

Văzând considerentele expuse mai sus, vă solicităm să admiteţi plângerea astfel cum a fost formulată şi, pe cale de consecinţă, să dispuneţi anularea ca nelegală şi netemeinică a Deciziei Consiliul Naţional de Soluţionare a Contestaţiilor nr.4442/C2/5172/5182 din 04.12.2012 şi continuarea procedurii de atribuire, cu suspendarea executării acesteia până la soluţionarea plângerii.

În cazul în care nu ne vom putea prezenta în instanţă la termenul când se va soluţiona cauza, vă rugăm ca, în temeiul articolului 242 alin.2 din Codul de procedură civilă să procedaţi la soluţionarea cauzei şi în lipsa noastră.

Anexăm în copie: extras din cerere de finanţare, proiectul tehnic şi contractul de finanţare.

pentru Mona-Maria PIVNICERU,
ministrul justiţiei, semnează,

Ovidiu PUŢURA

Secretar de Stat

Ministerul Comunicațiilor și Societății Informaționale - Organismul Intermediar pentru Promovarea Societății Informaționale

Cod SMIS – CSNR 22996

CONTRACT DE FINANȚARE

Nr. 171 323 / 19.04.2012

Între:

Ministerul Comunicațiilor și Societății Informaționale, în calitate de Organism Intermediar (denumit în continuare OI), în numele și pentru Ministerul Economiei, Comerțului și Mediului de Afaceri în calitate de Autoritate de Management (denumită în continuare AM) pentru Programul Operațional Sectorial „Creșterea Competitivității Economice"(denumit în continuare POS CCE), cu sediul în B-dul Libertății nr. 14, sector 5, cod 050706, București – Romania Tel./fax 021.311.41.55, poșta electronică fonduri@mcsi.ro., cod de înregistrare fiscală 4220947 reprezentat legal de Valerian VREME, în funcția de ministru, pe de o parte,

Și

Ministerul Justiției cu sediul în str. Apolodor, nr. 17, sector 5, București, cod poștal 050741, telefon 0372041146, fax 0372041148, poștă electronică dtia@just.ro, cod de înregistrare fiscală 4265841, reprezentat de dna Alina Mihaela BICA, în funcția de secretar de stat, în calitate de **Beneficiar** pe de altă parte,

în calitate de **Beneficiar** pe de altă parte,

au convenit încheierea prezentului ***Contract*** pentru acordarea ***finanțării nerambursabile*** în baza Cererii de finanțare nr. SMIS 22996 în următoarele condiții:

ARTICOLUL 1 – OBIECTUL CONTRACTULUI

(1) Obiectul acestui Contract îl reprezintă acordarea finanțării nerambursabile de către Autoritatea de Management, pentru implementarea proiectului nr. SMIS 22996 intitulat: *„Platformă de e-Learning cu specific IT pentru Ministerul Justiției și sistemul judiciar din România"*, denumit în continuare Proiect.

(2) Beneficiarului i se va acorda finanțarea nerambursabilă în termenii și condițiile stabilite în prezentul Contract, care este constituit din Contractul de finanțare și anexele acestuia, pe care Beneficiarul declară că le cunoaște și le acceptă.

(3) Cererea de finanțare depusă de Beneficiar, rezultată în urma verificărilor, modificărilor și completărilor efectuate pe parcursul procedurii de evaluare și selecție, devine anexă la prezentul Contract, făcând parte integrantă din acesta.

(4) Beneficiarul acceptă finanțarea nerambursabilă și se angajează să implementeze Proiectul pe propria răspundere, în conformitate cu prevederile cuprinse în prezentul Contract și în legislația națională și comunitară.

PROIECT TEHNIC

Cuprins

1. OBIECTIVELE PROIECTULUI 4
2. CERINTE PRIVIND SOLUTIA TEHNICA 8
2.1. Cerinte generale 8
2.2. Prevederi de securitate 11
3. DESCRIEREA TEHNICA A PROIECTULUI 15
3.1. Cerintele functionale ale sistemului 15
3.2. Arhitectura funcțională a sistemului 23
3.2.1. Portalul educational 26
3.2.2. Componenta de administrare a procesului de invatamant 28
3.2.3. Componenta de management al continutului de invatare 28
3.2.4. Componenta creare a continutului digital de invatare 29
3.2.5. Continut digital 29
3.2.6. Componenta de integrare 29
3.2.7. Infrastructura software necesara functionarii solutiei 30
a. Platforma de colaborare si portal 30
b. Baze de date 33
c. Platforma de integrare 34
3.2.8. Infrastructura hardware si de comunicatii necesara functionarii solutiei 34
3.2.8.1 Arhitectura tehnica a mediului de productie 34
3.2.8.2 Arhitectura tehnica a mediului de dezvoltare si testare 76
3.3 Managementul utilizatorilor si accesul la sistem 91
Generalitati 91
Managementul utilizatorilor si accesul la sistem 92
3.4 Securitatea sistemului 97

2.2. Prevederi de securitate

- Sistemul e-learning va avea implementate servicii de securitate avansata de:
  - Autentificare: verificarea si validarea credentialelor utilizatorilor. Trebuie sa permita inclusiv autentificare cu certificate digitale.
  - Autorizare: restrictionarea accesului utilizatorului numai la resursele la care acesta are permisiuni conform rolului acestuia. Solutia trebuie sa permita aplicarea regulilor intr-un mod centralizat, dintr-un singur loc pentru toate resursele organizatiei.
  - Single Sign-On: implementarea de mecanisme de tip Single Sign-On (SSO).

  Administrarea identitatii: managementul politicilor de securitate intr-un mod automatizat si centralizat.

  Securitatea și autenticitatea comunicării.

- Se va asigura prevenirea si protectia impotriva amenintarilor de tipul:
  - Compromiterea metodelor de autentificare si obtinerea accesului la aplicatii si date. Sistemul propus pentru realizare va utiliza metode de autentificare puternice ca de exemplu certificate digitale sau protocol Kerberos.
  - Distrugerea deliberata a datelor sau manipularea lor atat in tranzit (fizic sau electronic) sau atunci cand sunt stocate. Sistemul propus pentru realizare va utiliza criptarea datelor senzitive folosind facilitati de tipul SSL/TLS care asigura securizarea datelor in tranzit sau TDE care asigura protectia datelor stocate prin criptarea bazelor de date fara a afecta aplicatiile existente.
  - Repudierea serverelor. Sistemul propus pentru realizare va urmari logurile despre eventuale actiuni neautorizate in sistem.
  - Negarea serviciului (DoS): Sistemul propus pentru realizare va utiliza filtrarea pachetelor prin solutia de un firewall.

- Modelul de securitate va fi unul complet integrat bazat pe politici si reguli pentru informatii si date cat si pentru utilizatori.

    - Asigurarea securitatii fizice se va realiza prin implementarea unei politici de acces perimetral, cu zone de acces si mod de acces controlat in locatii si la consolele echipamentelor componente ale sistemului e-learning.

      Asigurarea securitatii logice se va realiza prin implementarea echipamentelor hardware firewall. Sistemul de e-learning propus contine un nivel firewall hardware construit in tehnologie toleranta la defect hardware. Acest nivel este dispus in punctul de acces dinspre reteaua externa (Internet) si asigura protectia traficului dispre exterior catre zona DMZ (nivelul de prezentare) catre portalul Web si componenta de comunicatii. Pentru protectie suplimentara portalul Web este publicat la nivelul fermei firewall si proxy, cererile dinspre exterior fiind deservite de aceasta si nu direct de catre serverele fermei Web. Ferma firewall si proxy va prelua cererile dinspre exterior, va aplica mecanismele si politicile de protectie pentru acces neautorizat sau de tip "denial of service" si va transmite cererea mai departe portalului Web. Traficul dinspre zona DMZ catre zona de aplicatii se realizeaza prin intermediul clusterul firewall conform politicilor de protectie configurate in sistem. Echipamentele firewall precum si ferma de servere firewall si proxy componente ale sistemului e-learning vor inspecta conexiunile si traficul dinspre reteaua externa si vor bloca accesul neautorizat catre serviciile portalului educational. Pentru protectia impotriva programelor de tip virus, spyware si spam sistemul de e-learning contine la nivelul componentei de securitate aplicatii antivirus atat pentru portalul educational cat si pentru sistemele de operare ale serverelor componente sistemului e-learning. Aplicatiile antivirus vor asigura protectia atat pentru procesele de upload si respectiv download continut digital ale portalul educational, cat si in sesiunile de colaborare si navigare Internet. Componenta de securitate contine si politicile de securitate, de autentificare si autorizare si acces la informatii cu consola de administrare centrala inclusiv pentru componentele antivirus mai sus enuntate. O masura in plus sistemul e-learning contine si componenta de backup si restaurare date.

Accesul utilizatorilor in sistemul e-learning se realizeaza la nivelul portalului educational Web. Sistemul informatic propus pentru realizare va utiliza pentru procesele de autentificare si autorizare un serviciu director compatibil LDAP (Lightweight Directory Access Protocol). In plus pentru scaderea costurilor operationale sistemul informatic propus pentru realizare va contine si mecanism de administrare a contului de tip "self service" pentru utilizatorii sistemului. Serviciul director compatibil LDAP asigura baza de date cu structuri de tip arbore cu obiecte si atribute conturi utilizatori. Toate serverele de aplicatie din sistem vor fi integrate si vor folosi protocol LDAP pentru comunicare inclusiv cu serverele de baze de date in cadrul proceselor de autentificare si autorizare. Accesul la baza de date a serviciului director va fi restrictionata pe nivele de acces cu drepturile aferente.

Sistemul e-learning propus pentru realizare va fi dezvoltat pe principiul autentificarii per sesiune (Single Sign On). Acest lucru conduce la generarea unui identificator unic pentru o operatie de autentificare reusita, identificator ce va fi asociat sesiunii respective. Toate resursele si serviciile sistemului e-learning accesate ulterior de catre utilizator vor contine acest identificator, serverele de aplicatii utilizand aceasta informatie pentru identificarea unica a utilizatorului. La finalizarea procesului de autentificare permisiunile vor fi asociate cererii de acces si va fi permis accesul la date. Terminarea unei sesiuni va putea fi facuta in sistemul e-learning propus pentru realizare atat la cererea utilizatorului cat si la expirarea timpului de sesiune.

Sistemul e-learning propus pentru realizare va avea definite roluri pe baza carora se vor atribui privilegii conturilor utilizator. Un cont utilizator va putea fi asociat mai multor roluri, permisiunile contului fiind rezultatul dat de acestea. Informatiile la care utilizatorii nu au acces vor fi invizibile pentru acestia. Sistemul e-learning va contine administrare centralizata a conturilor utilizator si a drepturilor de acces la aplicatiile componente. De asemenea sistemul e-learning va contine si functia de monitorizare a actiunilor utilizatorilor in aplicatii prin mecanisme de fisiere log si audit, functie ce va folosi identitatea unica a utilizatorului (SSO).

Componenta de securitate contine si securitatea bazei de date pentru protectie la acces neautorizat sau fau intentionat. Sistemul e-learning propus spre realizare va utiliza mecanismele de protectie proprii bazei de date, mecanisme ce vor asigura:

- autentificarea utilizatorilor;
- accesul controlat;
- criptarea datelor din baza de date;

- verificarea integritatii datelor din baza de date;
- audit.

Pentru procesul de autentificare a utilizatorilor in baza de date se va utiliza identitatea unica a utilizatorului (SSO) precum si politicile de securitate definite in infrastructura Ministerului Justitiei. Dupa finalizarea cu succes a procesului de autentificare utilizatorii vor accesa datele din baza de date functie de rolurile detinute la nivelul bazei de date. Accesul la functionalitatile aplicatiilor sistemului e-learning este dat de rolurile gestionate la nivelul aplicatiilor. Pentru un nivel ridicat de securitate baza de date va permite criptarea si decriptarea datelor din baza de date, accesul fiind permis numai utilizatorilor autorizati si numai functie de rolurile detinute de acestia. Pentru asigurarea unui nivel ridicat de securitate accesul administratorilor sistemului e-learning la datele criptate din baza de date va fi restrictionat. In plus sistemul e-learning propus pentru realizare va contine la nivelul bazei de date mecanisme de pastrare a consistentei datelor pentru incidente logice sau fizice. In cazul aparitiei unui eveniment nedorit ce necesita repornirea bazei de date, modulul de gestiune a bazei de date va verifica integritatea datelor recuperate inclusiv a celor aferente conturilor utilizator iar apoi va trece in mod de lucru de productie.

Ministerul Comunicațiilor și Societății Informaționale
Organismul Intermediar pentru Promovarea Societății Informaționale

FORMULARUL CERERII DE FINANȚARE

★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★

INSTRUMENTELE STRUCTURALE ALE UE

FORMULAR PENTRU PROGRAMUL OPERAȚIONAL SECTORIAL CREȘTEREA COMPETITIVITĂȚII ECONOMICE

Axa Prioritară III "Tehnologia Informației și Comunicațiilor pentru sectoarele privat și public"

Domeniul Major de Intervenție 2 „Dezvoltarea și creșterea eficienței serviciilor publice electronice"

Operațiunea 3 „Susținerea implementării de aplicații de E-Educație"

CUPRINSUL CERERII DE FINANȚARE

În cazul parteneriatelor, cererea de finanțare va fi completată și transmisă de liderul de proiect, însă va conține informații referitoare la toți partenerii.

.....

1. Informații privind solicitantul

2. Descrierea proiectului

3. Concordanța cu politicile UE și legislația națională

4. *Finanțarea Proiectului*

5. Lista de anexe

Ministerul Comunicațiilor și Societății Informaționale
Organismul Intermediar pentru Promovarea Societății Informaționale

TITLUL PROIECTULUI

„PLATFORMĂ DE E-LEARNING CU SPECIFIC IT PENTRU MINISTERUL JUSTIȚIEI ȘI SISTEMUL JUDICIAR DIN ROMÂNIA"

INFORMAȚII PRIVIND TIPUL ASISTENȚEI FINANCIARE NERAMBURSABILE SOLICITATE

Tipul asistenței comunitare nerambursabile:

Fondul European de Devoltare Regională.

Bugetul de stat

I. INFORMAȚII PRIVIND SOLICITANTUL

I.1. SOLICITANT

Numele instituției conform actului de înființare: Ministerul Justiției

Cod de înregistrare fiscală 4265841

Nr. de la Registrul Asociațiilor și Fundațiilor (dacă este cazul).....

Adresa poștală: Str. Apolodor, nr. 17, Sector 5, București

Telefon / Fax: 037 204 1027 037 204 1030

Adresa e-mail alina.bicaz@just.ro

I.2. TIPUL SOLICITANTULUI:

- ☐ Autoritate a administrației publice locale (API) și unități administrativ teritoriale
- ☐ Structuri asociative ale autorităților administrației publice locale
- ☐ Instituție publică ce funcționează la nivel local
- ☐ Autoritate a administrației publice centrale
- ☐ Instituție publică ce funcționează la nivel central
- ☐ Instituții de învățământ superior de drept public acreditate
- ☐ Parteneriate între autorități publice locale sau și instituții publice ce funcționează [illegible]

f) Microsoft Outlook – 50 pagini

g) Microsoft Power Point 2010 – 70-100 pagini

h) Microsoft Excel 2010 – 150 pagini

i) Securitatea IT – 50-70 pagini

Perioada de derulare: Lunile 4 – 24 de implementare a proiectului

4. Activitati de informare si promovare

Acest proiect va reprezenta o oportunitate pentru beneficiar de a se promova si de a determina cresterea increderii institutiilor implicate (beneficiare) in serviciile oferite. Astfel, in toate activitatile de comunicare și promovare relevante pe care beneficiarul le va organiza in timpul proiectului va fi mentionată și noua platformă de e-learning ce urmeaza a fi lansată.

Perioada de derulare: Pe toată perioada derulării proiectului (Lunile 1 – 24)

5 Activitati de auditare informatică și a securității rețelei și auditarea financiară a proiectului

In cadrul proiectului se vor realiza 2 auditari distincte:

- Auditul informatic și de securitate al proiectului
- Auditul financiar al proiectului

Astfel, in urma efectuarii acestor activitati echipa de management al proiectului va lua la cunostinta despre respectarea sau nerespectarea legislatiei in vigoare si a procedurilor interne ale beneficiarului pe durata implementarii proiectului. Auditarile se vor realiza la jumatatea perioadei de implementare a proiectului (Luna 12) si la finalul implementarii proiectului, astfel incat orice abatere de la legislatia in vigoare sau de la normele interne sa poata fi corectata, *in conditiile legii.*

Perioada de derulare: Lunile 12 – 24 de implementare a proiectului

Arhitectura propusa este bazata pe tehnologie moderna de tip Internet si este organizata pe principal 3 nivele:

- Nivel client;
- Nivel aplicatie;
- Nivel baza de date.

Arhitectura sistemului e-learning propus pentru realizare contine si componenta de administrare a configuratiilor, componenta de securitate si componenta de backup si restaurare date.

Nivelul client

Nivelul client este reprezentat de doua subniveluri dupa cum urmeaza:

- **Nivelul utilizatori**: reprezentat de statiile de lucru ale utilizatorilor interni si externi. De pe aceste statii de lucru prin utilizarea unui browser Web standard utilizatorii acceseaza sistemul e-learning propus pentru realizare.
- **Nivelul prezentare**: este compus din urmatoarele servere:
  - Ferma servere portal educational Web: formata din trei servere Web (Server Web 1, 2 si 3) cu balansare a incarcarii pe care ruleaza serviciile de prezentare si acces pentru utilizatorii interni si externi;
  - Un server (Server comunicatie 1) cu rol de inregistrare si asigurare acces la continutul digital format audio si video;
  - Ferma de servere firewall si proxy: formata din doua servere (Server Firewall 1 si Server Firewall 2) in topologie cluster pentru disponibilitate ridicata pentru accesul controlat in portalul educational Web.

Obiectivele serverelor din nivelul de prezentare sunt:

- Sa permita accesul utilizatorilor interni si externi in portalul educational din clienti Web standard (exemplu: Mozilla, Netscape Navigator) cat si de pe dispozitive mobile (exemplu: PDA, Palm);
- Sa permita accesul utilizatorilor interni si externi la continutul digital, nelimitat in format audio si video, cu suport de conversatii in grup si indicatori de prezenta si spatiu de lucru comun;

frecventa operatiilor de tip crawl si performanta cautarilor prin distribuirea lor pe mai multe servere;

- Posibilitatea de a restrictiona rezultatele cautarilor la un anume numar de rezultate;
- Posibilitatea de a alerta administratorul atunci cand volumul de documente dintr-o unitate logica de stocare gen biblioteca de documente este atins.

- Server de integrare (Server Integrare)

  Obiectivele serverului de integrare sunt:
  Integrarea componentelor și a serviciilor prin arhitectură bazată pe mesaje, suport pentru atasarea de fisiere multiple la mesaje si configurarea retrimiterii automate de mesaje

- Un server de comunicatii (Server Comunicatii 2) cu rol de inregistrare si asigurare acces la continutul digital format audio si video.

  Obiectivele serverului de comunicatii sunt:

  - Sa permita accesul utilizatorilor interni si externi la continutul digital inclusiv in format audio si video, cu suport de conversatii in grup si indicatori de prezenta si spatiu de lucru comun.

- Serverul de securizare a infrastructurii folosind certificate digitale (Server CA) pe care ruleaza serviciul care asigura definirea si folosirea certificatelor digitale in cadrul sistemului e-learning propus spre realizare.

  Obiectivele serverului de securizare a infrastructurii folosind certificate digitale sunt:

  - asigura definirea si folosirea certificatelor digitale locale in cadrul sistemului e-learning pentru operatii de securizare a accesului la informatii, de criptare si semnatura digitala a datelor;
  - asigura securizarea mesajelor de tip e-mail atat in timpul in care sunt stocate cat si in timpul transmiterii acestora;
  - asigura securizarea de documente, atat locale cat si in timpul transmiterii acestora.

- Doua servere pentru serviciul director compatibil LDAP (Server LDAP 1 si Server LDAP 2). Servere dedicate stocarii informatiei despre profilul utilizatorilor si structura organizatorica.

- Consola de administrare a sistemului e-learning.

Nivel baze de date

Nivelul baze de date este compus din urmatoarele servere:

- Doua servere cu rol de servere baze de date (Server DB 1 si Server DB 2) in topologie de cluster pe care ruleaza componenta de gestiune a bazei de date. Cele doua servere sunt conectate la un echipament de stocare date extern. Pe echipamentul extern vor fi stocate instantele de baze de date de productie.

  Obiectivele serverelor de baza de date sunt:

  sistem performant de gestiune a bazelor de date de tip relational;

  asigura procesarea tranzactiilor si a datelor analitice;

  scalabilitate si securitate;

  Servicii de date prin care sa se asigure consisterta datelor in sisteme eterogene

  Compresie date cu suport Unicode

  Posibilitatea de stocare si gestiune a structurilor de date de tip XML utilizand mecanisme native ale bazei de date;

  Sa ofere posibilitatea de partitionare a tabelelor in scopul reducerii timpului de acces la date;

  Sa permita accesul cat mai rapid la informatii si prin utilizarea diferitelor tipuri le tadecsi;

  Sa ofere posibilitatea de limitare a accesului prin politici de securitate;

  Sa permita implementarea de sisteme de audit

- Framework tehnologie pentru implementarea solutiilor de business intelligence si datawarehouse.

- Acest framework furnizeaza o infrastructura cuprinzatoare, scalabila, extensibila pentru aplicatiile de business intelligence , asigurand o solutie care satisface cerintele la diverse niveluri de management incluzand :

  - Depozit de date relational si instrumente OLAP: sistemul sa ofere in mod nativ solutii OLAP si data warehouse:
  - Data warehouse sa permita lucru in mod partitionat pentru incarcarea rapida si mentenanta usoara a tabelelor foarte mari

    ETL (EXtract, transformation, load): functionalitati native de extragere a datelor din diferite surse de date (de ex:Oracle, SQL Server, Excel, Web services), realizarea de filtrari, agregari si diferite alte transformari asupra datelor si in final stocarea datelor in data warehouse.
  - Baza de date multidimensionale native: stocarea datelor intr-un cub cu mai multe dimensiuni, in vederea interogarii mai usoare a datelor si construirii rapoartelor relevante.

    Instrumente de data mining: functionalitati pentru construirea de modele analitice complexe precum si integrarea acestor modele cu operatiile de business.

    Interogare si analiza ad-hoc a datelor: facilitati de interogare a datelor in momentul solicitarii rapoartelor
  - Extragerea si editarea dinamica a rapoartelor

    Mediu de raportare

    Creare de rapoarte ad-hoc

Administrare de securitate

Nivel administrare configuratii

Componenta de administrare a configuratiilor are in componere doua servere:

Ministerul Comunicațiilor și Societății Informaționale
Organismul Intermediar pentru Promovarea Societății Informaționale

Prezenta cerere a fost completată în conformitate cu prevederile art. 292 din Codul Penal cu privire la fals în declarații.

Funcția ocupată în instituție

Secretar de stat – ordonator principal de credite

Nume și prenume (majuscule)

ALINA MIHAELA BICA

Semnătura și ștampila

	Prenume NUME	*Funcția*	*Direcția/Serviciul*	*Data*	*Semnătură*
Avizat	Diana Popescu	Director General	DGDM	14.06.2010	
Avizat	Alexandru Olaru	Director	DPE	14.06.2010	
Avizat	Răzvan Crăciunescu	Director	DTI	14.06.2010	