ORDIN nr. 553 din 5 iunie 2019 privind reglementarea procedurii de avizare a instrumentelor de plată electronică cu acces la distanţă

În temeiul art. 4 alin. (1) pct. 53 din Hotărârea Guvernului nr. **36/2017** privind organizarea şi funcţionarea Ministerului Comunicaţiilor şi Societăţii Informaţionale, cu modificările şi completările ulterioare,
având în vedere prevederile art. 129 alin. (1) pct. 2 lit. c) din Regulamentul Băncii Naţionale a României nr. **3/2018** privind monitorizarea infrastructurilor pieţei financiare şi a instrumentelor de plată şi prevederile Legii nr. **135/2007** privind arhivarea documentelor în formă electronică, republicată,
ministrul comunicaţiilor şi societăţii informaţionale emite prezentul ordin.

CAPITOLUL I: Dispoziţii generale

Art. 1
Prezentul ordin reglementează procedura de eliberare a avizului Ministerului Comunicaţiilor şi Societăţii Informaţionale pentru instrumentele de plată electronică cu acces la distanţă furnizate de către prestatorii de servicii de plată autorizaţi de Banca Naţională a României, de tip internet-banking, home-banking, phone-banking sau mobile-banking, necesar pentru notificarea acestora către BNR, precum şi înscrierea auditorilor IT, conform procedurii prevăzute în cap III.

Art. 2
Prezentul ordin stabileşte cerinţele minime de securitate ale sistemelor informatice pe care trebuie să le îndeplinească prestatorii de servicii de plată prevăzuţi la art. 1, prin intermediul cărora este furnizat instrumentul de plată electronică cu acces la distanţă.

Art. 3
În înţelesul prezentului ordin, termenii, expresiile şi abrevierile de mai jos au următoarele semnificaţii:
1.*ameninţare* - cauza potenţială a unui incident nedorit, care poate dăuna unui sistem sau unei organizaţii;
2.*administrator al arhivei electronice* - persoana fizică sau juridică acreditată de autoritatea de reglementare şi supraveghere specializată în domeniu să administreze sistemul electronic de arhivare şi documentele arhivate în cadrul arhivei electronice;
3.*arhivă electronică* - sistemul electronic de arhivare, împreună cu totalitatea documentelor în formă electronică arhivate;
4.*atac etic/test de penetrare* - un test direct al eficacităţii de apărare a securităţii prin mimarea acţiunilor atacatorilor reali/test al sistemelor informatice realizat printr-o simulare a unui atac real asupra reţelelor, sistemelor şi programelor informatice utilizate de entitatea testată sau auditată, după caz, efectuat cu acordul managementului prestatorului;
5.*audit IT* - activitatea de colectare şi evaluare a unor probe pentru a determina dacă sistemul informatic respectă parametrii de performanţe şi de lucru conform cerinţelor de proiectare, dacă asigură funcţionalităţii necesare cerinţelor de afaceri şi respectarea legislaţiei în domeniu, dacă este securizat, dacă menţine integritatea datelor prelucrate şi stocate, dacă permite atingerea obiectivelor strategice ale entităţii şi utilizarea eficientă a resurselor informaţionale;
6.*auditor IT* - persoana fizică autorizată care deţine certificat de auditor IT sau persoana juridică cu personal certificat care derulează o activitate de auditare a sistemelor informatice, conform reglementărilor şi bunelor practici în domeniu;
7.*autentificare* - procedură care permite prestatorului de servicii de plată să verifice identitatea unui utilizator al serviciilor de plată sau valabilitatea utilizării unui anumit instrument de plată şi care include utilizarea elementelor de securitate personalizate ale utilizatorului;
8.*aviz* - actul administrativ emis de către Ministerul Comunicaţiilor şi Societăţii Informaţionale în conformitate cu prevederile art. 129 alin. (1) pct. 2 lit. c) din Regulamentul Băncii Naţionale a României nr. **3/2018**;

9.*BNR* - Banca Naţională a României;
10.*centru de date* - spaţiu securizat, dotat cu tehnică de calcul şi echipamente de comunicaţii prin intermediul cărora se primesc, se stochează şi se transmit date în formă electronică;
11.*comunicaţii/telecomunicaţii* - sisteme de transmisie, precum şi orice alte resurse care permit transportul semnalelor prin fir, radio, fibră optică sau orice alte mijloace electromagnetice, precum şi tehnologiile utilizate în cadrul proceselor de comunicare, care presupun existenţa unui mediu informatic constituit din echipamente hardware, software specializat, precum şi dispozitive electronice de transmisie/recepţie date;
12.*continuitatea activităţii* - starea de funcţionare neîntreruptă a operaţiunilor, ce presupune măsuri organizaţionale, tehnice şi de personal utilizate pentru a asigura continuitatea serviciilor critice după o întrerupere cauzată de producerea unui eveniment perturbator şi pentru reluarea treptată a tuturor serviciilor în cazul unui eveniment perturbator major;
13.*controale informatice* - totalitatea politicilor, procedurilor, practicilor, ghidurilor, mijloacelor de gestionare a riscurilor şi a structurilor organizaţionale informatice proiectate să ofere o asigurare rezonabilă asupra faptului că obiectivele afacerii vor fi atinse, evenimentele nedorite vor fi prevenite sau detectate şi corectate;
14.*date (informatice)* - orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic, incluzându-se şi orice program informatic care poate determina realizarea unei funcţii similare de către un sistem informatic;
15.*disponibilitate* - capabilitatea unui serviciu IT sau a unui element de configuraţie IT de a efectua funcţiile agreate;
16.*emitent* - prestator de servicii de plată care emite şi pune la dispoziţia deţinătorului un instrument de plată electronică, în baza unui contract încheiat cu deţinătorul;
17.*externalizare servicii IT* - utilizarea de către o entitate a unui furnizor extern de servicii IT, în vederea desfăşurării de către aceasta, pe bază contractuală şi în mod continuu sau pentru o anumită perioadă, a operaţiunilor aferente suportului tehnic sau procesării, necesare desfăşurării activităţii efectuate în mod obişnuit de către entitatea în cauză;
18.*furnizor de servicii de arhivare electronică* - orice persoană fizică sau juridică acreditată să presteze servicii legate de arhivarea electronică;
19.*furnizor de servicii IT externalizate* - furnizori care oferă servicii de mentenanţă, administrare software (aplicaţii), servicii de administrare reţea, baze de date şi sisteme de operare, furnizori de software, servicii de hosting, co-locare şi cloud. Furnizorii de servicii de comunicaţii nu fac obiectul prezentei definiţii;
20.*incident operaţional sau de securitate* - un eveniment unic sau o serie de evenimente corelate, neprevăzute de către prestatorul serviciului de plată, care are un impact negativ asupra integrităţii, disponibilităţii, confidenţialităţii, autenticităţii şi/sau continuităţii serviciilor aferente plăţilor;
21.*instrument de plată electronică cu acces la distanţă* - set de proceduri, care se bazează pe o soluţie informatică, de tipul: internet-banking, home-banking, phone-banking, mobile-banking, care permite utilizatorului iniţierea de operaţiuni de plată;
22.*instrument de plată electronică cu acces la distanţă tip internet-banking* - acel instrument de plată cu acces la distanţă care se bazează pe tehnologia internet (world wide web) şi pe sistemele informatice ale emitentului;
23.*instrument de plată la distanţă tip home-banking* - acel instrument de plată cu acces la distanţă care se bazează pe o aplicaţie software a emitentului instalată la sediul deţinătorului, pe o staţie de lucru individuală sau în reţea;
24.*instrument de plată electronică cu acces la distanţă tip mobile-banking* - acel instrument de plată cu acces la distanţă care presupune utilizarea unui echipament mobil (telefon, tabletă, PDA - Personal Digital Assistant etc.) şi a unor servicii oferite de către operatorii de telecomunicaţii;
25.*instrument de plată electronică cu acces la distanţă tip phone-banking* - acel instrument de plată cu acces la distanţă care facilitează accesul clienţilor la produsele şi serviciile unui prestator de servicii de plată prin utilizarea telefonului drept canal alternativ de acces de la distanţă;
26.*MCSI* - Ministerul Comunicaţiilor şi Societăţii Informaţionale;

27.*operaţiune de plată* - acţiune iniţiată de plătitor sau de o altă persoană în numele şi pe seama plătitorului ori de beneficiarul plăţii cu scopul de a depune, de a transfera sau de a retrage fonduri, indiferent de orice obligaţii subsecvente între plătitor şi beneficiarul plăţii;
28.*ordin de autorizare centru de date* - document emis de MCSI care atestă că un centru de date îndeplineşte toate condiţiile cerute de legislaţia în vigoare în vederea desfăşurării operaţiunilor de arhivare electronică;
29.*prelucrarea datelor* - orice operaţiune sau set de operaţiuni efectuate asupra datelor sau asupra seturilor de date, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;
30.*procedură de autorizare a unui centru de date* - metodă de evaluare sistematică, documentată, periodică şi obiectivă a performanţei centrului de date, a sistemului de management şi a proceselor destinate protecţiei arhivelor electronice, în scopul verificării respectării cerinţelor prevăzute de legislaţia în vigoare;
31.*prestator de servicii de plată* - entitate autorizată să presteze servicii de plată pe teritoriul României, respectiv instituţii de credit, instituţii de plată şi instituţii emitente de monedă electronică;
32.*prestator* - prestator de servicii de plată specifice instrumentelor financiare de plată electronică cu acces la distanţă;
33.*plan de securitate* - documentul ce descrie totalitatea măsurilor tehnice şi administrative care sunt luate de către emitent pentru utilizarea în condiţii de siguranţă a instrumentului de plată electronică cu acces la distanţă;
34.*raport de audit IT* - instrumentul prin care se comunică scopul auditării, obiectivele urmărite, normele/standardele aplicate, perioada acoperită, natura, procedurile, constatările şi concluziile auditului, precum şi orice rezervă pe care auditorul IT o are asupra sistemului informatic auditat;
35.*raport de testare IT* - instrumentul prin care se comunică scopul testării, obiectivele urmărite, normele/standardele aplicate, perioada acoperită, natura, întinderea, procedurile, constatările şi concluziile testării, precum şi orice rezervă pe care echipa de testare o are asupra sistemului informatic testat;
36.*Regulamentul Băncii Naţionale a României nr.* ***3/2018*** - Regulamentul Băncii Naţionale a României nr. **3/2018** privind monitorizarea infrastructurilor pieţei financiare şi a instrumentelor de plată, publicat în Monitorul Oficial al României, Partea I, nr. 713 din 16 august 2018;
37.*risc de securitate* - riscul care rezultă din procesele interne sau evenimentele externe eşuate sau necorespunzătoare, care au sau ar putea avea un impact negativ asupra disponibilităţii, integrităţii, confidenţialităţii şi asupra sistemelor de tehnologie a informaţiei şi a comunicaţiilor şi/sau asupra informaţiilor utilizate pentru furnizarea serviciilor de plată;
38.*securitate informatică* - capacitatea unui sistem informatic, rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive, de a rezista, la un nivel de încredere dat, unei acţiuni accidentale sau răuvoitoare care ar putea compromite disponibilitatea, autenticitatea, integritatea sau confidenţialitatea datelor stocate sau transmise ori a serviciilor conexe oferite de reţeaua sau de sistemul informatic respectiv sau accesibile prin intermediul acestora;
39.*siguranţă în funcţionare* - modalitate de gestionare a riscurilor specifice infrastructurii pieţei financiare, respectiv a instrumentului de plată, în scopul asigurării funcţionării conform nivelurilor de calitate a serviciilor şi/sau orarului de funcţionare asumat, fără a afecta în mod negativ încrederea participanţilor şi a publicului;
40.*sistem informatic* - ansamblu de elemente intercorelate funcţional în scopul automatizării obţinerii informaţiilor necesare activităţilor operaţionale şi manageriale într-o entitate, prin intermediul serviciilor IT, al echipamentelor hardware şi produselor software, proceduri manuale, baze de date şi modele matematice pentru analiză, planificare, control şi luarea deciziilor, utilizând componente de introducere şi prelucrare date, componente de procesare precum servere, calculatoare, sisteme software de operare de bază, programe informatice, reţele de calculatoare şi telecomunicaţii, componente de stocare şi utilizatori, fără ca enumerarea să fie limitativă;

41.*vulnerabilitate* - este un punct slab (defect) în proiectarea, implementarea, operarea sau controlul intern al unui proces care ar putea expune sistemul la un risc de securitate.

Art. 4

Cerinţele minime de securitate ale sistemelor informatice pe care trebuie să le îndeplinească prestatorii de servicii de plată prevăzuţi la art. 1, prin intermediul cărora este furnizat instrumentul de plată electronică cu acces la distanţă, se referă la:

1.confidenţialitatea şi integritatea comunicaţiilor între emitent şi beneficiarul instrumentului financiar de plată electronică cu acces la distanţă;

2.mecanismele care să garanteze confidenţialitatea şi nerepudierea operaţiunilor efectuate utilizând instrumentul de plată electronică cu acces la distanţă;

3.autenticitatea părţilor care participă la tranzacţii şi existenţa metodelor de autentificare în concordanţă cu nivelul de securitate al platformei software, precum şi mijloacele de garantare a identităţii;

4.confidenţialitatea, autenticitatea şi integritatea informaţiilor/datelor aferente tranzacţiilor efectuate cu ajutorul instrumentului de plată electronică, prin sistemul informatic al emitentului, în timpul procesării, stocării şi arhivării acestora;

5.păstrarea secretului bancar;

6.trasabilitatea tranzacţiilor;

7.respectarea protecţiei datelor cu caracter personal în sistemele informatice;

8.controlul accesului fizic şi logic la sistemul informatic şi la platforma/aplicaţia software utilizate în procesul de furnizare a instrumentului financiar de plată electronică cu acces la distanţă;

9.stocarea, păstrarea datelor înregistrate şi jurnalizarea acestora, precum şi păstrarea în siguranţă a unor copii de rezervă ale datelor şi aplicaţiilor;

10.prevenirea/limitarea/înlăturarea impactului incidentelor de securitate informatică, reluarea în siguranţă a activităţii şi recuperarea informaţiilor afectate;

11.detectarea, înregistrarea şi gestionarea incidentelor de securitate informatică;

12.evaluarea riscurilor de securitate informatică şi măsuri de gestionare a acestora;

13.asigurarea unui proces formal şi continuu (cel puţin anual) de pregătire a resurselor umane implicate în operarea, mentenanţa şi administrarea instrumentelor de plată electronică cu acces la distanţă şi o evaluare anuală a acestora;

14.continuitatea serviciilor oferite clienţilor;

15.gestionarea şi administrarea sistemului informatic;

16.impactul operaţiilor de modificare a:

a)arhitecturii din cadrul sistemului informatic (componente hardware/software) şi aplicaţiilor software utilizate în ciclul de viaţă al instrumentului de plată electronică cu acces la distanţă; şi

b)planului de securitate specific securităţii aferente instrumentului de plată cu acces la distanţă;

17.orice alte activităţi sau măsuri tehnice întreprinse pentru exploatarea în siguranţă a sistemului informatic al emitentului.

Art. 5

Măsurile tehnice şi organizatorice întreprinse pentru îndeplinirea cerinţelor enumerate la art. 4 vor fi în concordanţă cu tehnologia utilizată şi cu riscurile potenţiale.

Art. 6

Prestatorii au obligaţia de a implementa măsuri de securitate informatică, de a monitoriza continuu şi de a evalua anual riscurile operaţionale generate de utilizarea sistemelor informatice prin intermediul cărora este furnizat instrumentul de plată electronică cu acces la distanţă, cu respectarea legislaţiei interne şi a reglementărilor comunitare.

Art. 7

Documentele elaborate în format electronic, aferente instrumentului de plată electronică cu acces la distanţă, vor fi arhivate conform legislaţiei naţionale privind arhivarea electronică, pe baza nomenclatorului arhivistic al prestatorului, în concordanţă cu cerinţele Legii Arhivelor Naţionale nr. **16/1996**, republicată.

Art. 8

(1) Prestatorii au obligaţia ca, anual, să efectueze teste de penetrare a aplicaţiilor software şi sistemelor informatice utilizate în ciclul de viaţă al instrumentului de plată electronică cu acces la distanţă.
(2) Testele de penetrare menţionate la alin. (1) se vor realiza de către echipe externe/interne, certificate în acest scop, care vor evalua securitatea informatică a aplicaţiilor şi sistemului informatic al prestatorului care furnizează instrumentul de plată electronică cu acces la distanţă şi vor fi finalizate cu un raport de testare.
(3) Raportul de testare pentru testele prevăzute la alin. (2) trebuie să fie aprobat de către reprezentantul legal al prestatorului şi păstrat la sediul acestuia, care are obligaţia să îl prezinte auditorului IT, precum şi MCSI, la solicitarea acestuia.

CAPITOLUL II: Eliberarea avizului

Art. 9

(1) Documentele necesare pentru eliberarea avizului sunt:
a)cererea adresată MCSI, conform modelului prevăzut în anexa nr. 1;
b)licenţa de funcţionare/autorizaţia acordată de BNR sau notificarea transmisă către BNR de autoritatea competentă din statul membru de origine;
c)descrierea funcţională a sistemului informatic şi a aplicaţiei software prin intermediul cărora este furnizat instrumentul de plată electronică cu acces la distanţă;
d)planul de securitate al sistemului informatic, semnat de către prestatorii de servicii de plată prevăzuţi la art. 1, cuprinzând descrierea măsurilor tehnice şi organizatorice prevăzute pentru asigurarea cerinţelor cuprinse la art. 4;
e)declaraţia reprezentantului legal din care să rezulte efectuarea testelor de penetrare menţionate la art. 8, perioada de efectuare a testelor, precum şi datele de identificare ale echipei de testare;
f)certificările profesionale ale echipei de testare, recunoscute internaţional. Certificările profesionale agreate pentru efectuarea testelor de penetrare acceptate trebuie să fie în termenul de valabilitate şi să se regăsească în lista prevăzută în anexa nr. 2;
g)raportul de audit, care trebuie să îndeplinească următoarele condiţii:
1.să cuprindă elementele prevăzute în raportul de audit prezentat în anexa nr. 3, fără a se limita la acestea;
2.să fie întocmit de către un auditor selectat din Lista auditorilor IT;
3.data de întocmire a raportului de audit nu trebuie să depăşească 180 de zile faţă de data depunerii documentaţiei de avizare;
h)declaraţia pe propria răspundere, din care să rezulte independenţa auditorului faţă de sistemul informatic auditat şi faţă de prestatorul auditat;
i)declaraţia pe propria răspundere a reprezentantului legal al prestatorului cu privire la respectarea, în cadrul procesului de furnizare a instrumentelor de plată electronică cu acces la distanţă, a cerinţelor Legii nr. **190/2018** privind măsuri de punere în aplicare a Regulamentului (UE) **2016/679** al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei **95/46/CE** (Regulamentul general privind protecţia datelor);
j)ordinul de acreditare ca administrator de arhivă electronică, în conformitate cu prevederile Legii nr. **135/2007** privind arhivarea documentelor în formă electronică, republicată, sau contractul încheiat cu un administrator de arhivă electronică acreditat.
(2)MCSI va retrage avizul eliberat prestatorului dacă contractul de externalizare sau ordinul de acreditare a serviciilor de arhivare este suspendat/retras sau îşi pierde valabilitatea.

Art. 10

(1) Documentele prevăzute la art. 9 alin. (1) se vor transmite către MCSI, în limba română, vor fi semnate de către reprezentantul legal al prestatorului de servicii de plată sau de către o persoană împuternicită de către acesta, în scris, şi vor avea menţiunea "Conform cu originalul".
(2) Documentaţia va fi paginată şi însoţită de un opis.

Art. 11

Documentaţia aferentă planului de securitate va avea următoarea structură:

1.informaţii de identificare:
a)denumirea prestatorului;
b)denumirea instrumentului de plată electronică cu acces la distanţă;
c)categoria (internet-banking, home-banking, mobile-banking, phone-banking);
d)statutul operaţional al sistemului prin intermediul căruia este oferit instrumentul de plată electronică cu acces la distanţă;
e)anul intrării în producţie;
f)descrierea generală a soluţiei tehnice şi dezvoltatorului aplicaţiei;
g)interconectarea sistemului;
h)aria geografică în care instrumentul de plată cu acces la distanţă poate fi utilizat;
i)datele de contact ale persoanelor responsabile;
2.senzitivitatea sistemului:
a)legislaţia aplicabilă;
b)descrierea generală a senzitivităţii informaţiilor gestionate de către sistem;
3.măsuri pentru securitatea sistemului:
a)evaluarea şi managementul riscurilor potenţiale;
b)identificarea, analizarea şi remedierea riscurilor de securitate în conformitate cu cele mai bune practici în gestionarea acestora;
c)măsurile tehnice de securitate implementate;
d)situaţia cu înregistrarea şi analizarea incidentelor de securitate informatică;
e)metodologia de recuperare a informaţiilor în caz de dezastru şi continuarea activităţii;
f)rapoartele de testare a funcţionalităţii instrumentului efectuate în ultimele 12 luni;
g)codurile de conduită/condiţiile de utilizare/contractul prin care este oferit instrumentul de plată electronică cu acces la distanţă;
h)procedurile operaţionale de exploatare;
i)măsurile aplicate pentru asigurarea securităţii fizice;
j)instruirea personalului propriu în legătură cu administrarea sistemului informatic;
k)instrucţiunile de utilizare a instrumentului de plată cu acces la distanţă (manual de utilizare oferit clienţilor);
l)suportul tehnic oferit clienţilor care utilizează instrumentul de plată electronică cu acces la distanţă;
4.orice alte informaţii relevante legate de măsurile luate de către emitent pentru a asigura exploatarea în siguranţă a instrumentului de plată electronică cu acces la distanţă.

CAPITOLUL III: Înscrierea în Lista auditorilor IT

Art. 12

Lista auditorilor IT este gestionată de către MCSI şi publicată pe site-ul acestuia.

Art. 13

Auditorul IT care intenţionează să presteze servicii de audit IT pentru prestatorii cărora le sunt incidente prevederile prezentului ordin are obligaţia înscrierii în Lista auditorilor IT prevăzuta la art. 12.

Art. 14

Auditorul IT înscris în lista menţionată la art. 9 poate întocmi şi raportul de audit în vederea autorizării centrelor de date, prevăzute în Legea nr. **135/2007**, republicată.

Art. 15

Documentele necesare pentru înscrierea în Lista auditorilor IT, prevăzută la art. 12, sunt următoarele:
1.cererea adresată MCSI, conform modelului prevăzut în anexa nr. 4;
2.datele de identificare ale auditorului IT:
a)numele complet/denumirea şi adresa/sediul - adresa completă;
b)adresa unde îşi desfăşoară activitatea;
c)telefon/fax, e-mail, adresa paginii de internet;
d)certificat de înregistrare la Oficiul Naţional al Registrului Comerţului;
3.pentru auditorul IT persoană fizică certificată şi pentru reprezentantul societăţii de audit IT, care vor semna raportul de audit, se depun următoarele documente:
a)actul de identitate al auditorului IT, în copie;

b)curriculum vitae al auditorului IT, datat şi semnat, cu prezentarea experienţei profesionale în auditarea IT a sistemelor informatice;
c)dovada deţinerii uneia dintre certificările profesionale specifice domeniului de audit al sistemelor informatice, menţionate în anexa nr. 5 (certificatul de auditor, în copie semnată şi cu menţiunea "Conform cu originalul");
d)dovada experienţei în audit IT, concretizată în participarea la minimum cinci misiuni de audit în domeniul securităţii sistemelor informatice aparţinând prestatorilor de servicii de plată, cu un total de cel puţin 30 de zile;
e)certificat constatator emis de Oficiul Naţional al Registrului Comerţului, cu starea la zi a persoanei juridice, nu mai vechi de 30 de zile, în original;
f)certificatul de cazier judiciar şi certificatul de cazier fiscal, aflate în termenul de valabilitate, în original;
g)contractul de asigurare de răspundere civilă profesională a auditorului IT, pentru suma asigurată de minimum 100.000 euro, valabil la data depunerii documentaţiei, în copie semnată şi cu menţiunea "Conform cu originalul".

Art. 16
Înscrierea auditorului IT în Lista auditorilor IT sau transmiterea refuzului motivat al înscrierii se efectuează de MCSI în termen de maximum 30 de zile de la primirea dosarului complet al solicitantului.

Art. 17
Orice modificare a documentaţiei prevăzute la art. 15 trebuie transmisă către MCSI în termen de maximum 30 de zile de la data efectuării modificării.

Art. 18
Radierea auditorilor IT din lista prevăzută la art. 12 se va efectua în oricare dintre următoarele situaţii:
a)la cererea acestora;
b)în cazul lichidării sau la declanşarea insolvenţei;
c)în cazul nerespectării prevederilor prezentului ordin;
d)la expirarea contractului de asigurare de răspundere civilă profesională;
e)la expirarea certificării profesionale.

Art. 19
MCSI va transmite auditorului IT o notificare prealabilă prin care i se aduc la cunoştinţă motivele pentru care se va proceda la iniţierea demersurilor pentru radierea din Lista auditorilor IT.

CAPITOLUL IV: Condiţii privind desfăşurarea auditului IT

Art. 20
(1) Auditarea se va efectua în baza unui contract încheiat între prestatorul care a solicitat auditarea şi un auditor înscris în Lista auditorilor IT.
(2) Prestatorul nu poate contracta auditarea cu acelaşi auditor IT pentru mai mult de 2 auditări consecutive.
(3) Prestatorul are obligaţia de a se asigura că în contractul de auditare sunt cuprinse în mod obligatoriu clauze cu privire la faptul că auditorul IT trebuie să respecte cerinţele impuse pentru efectuarea auditului sistemelor informatice, în conformitate cu prevederile prezentului ordin şi cu bunele practici în domeniu.
(4) Activitatea de auditare trebuie să respecte conduita etică şi profesională, nu presupune încălcarea secretului profesional impus prin clauze contractuale sau prin prevederi legale şi nu atrage niciun fel de răspundere asupra persoanei fizice şi/sau juridice în cauză ca urmare a respectării prevederilor prezentului ordin.

Art. 21
Perioada supusă auditării reprezintă perioada cuprinsă între două auditări consecutive.

Art. 22
Pe timpul auditării, auditorul IT are obligaţia de a analiza situaţia deficienţelor şi vulnerabilităţilor identificate, întocmită cu ocazia auditării precedente, precum şi măsurile întreprinse de către prestator.

Art. 23

Auditorul IT notifică MCSI, în scris, în maximum 10 zile de la constatare, orice fapt sau act care:
a)este de natură să afecteze utilizarea în siguranţă a instrumentului financiar de plată electronică cu acces la distanţă;
b)poate conduce la o opinie de audit cu rezerve, negativă sau imposibilitatea exprimării acesteia.

Art. 24

În termen de maximum 10 zile de la solicitarea scrisă a MCSI, auditorul IT trebuie să comunice următoarele, fără a se limita la acestea:
a)orice raport sau document care a fost adus la cunoştinţa prestatorului auditat;
b)motivaţia de încetare a contractului de audit, dacă aceasta a avut loc înainte de finalizarea auditării.

Art. 25

La finalizarea auditării, auditorii IT au obligaţia de a întocmi un raport de audit IT, care să cuprindă cel puţin elementele enumerate în raportul de audit prevăzut în anexa nr. 3, dar fără a se limita la acestea.

Art. 26

Pentru cazurile în care sistemul informatic şi platforma/aplicaţia software utilizate în procesul de furnizare a instrumentului financiar de plată electronică cu acces la distanţă sunt situate în afara ţării, auditarea sistemului se va face astfel:
- auditorul IT extern român va audita sistemele din străinătate; sau
- auditorul IT extern român agreează auditarea sistemului din străinătate de către un auditor cu o certificare cuprinsă în lista certificărilor menţionate în anexa nr. 5 şi preia responsabilitatea auditării.

Art. 27

MCSI poate verifica derularea procesului de auditare, atât prin participarea la activitatea de auditare a auditorului IT, cât şi prin prisma discuţiilor legate de dosarul de audit.

CAPITOLUL V: Cerinţe aplicabile furnizorilor de servicii IT externalizate pentru sistemele informatice ale prestatorului

Art. 28

Orice externalizare de servicii IT se realizează cu respectarea legislaţiei naţionale aplicabile Prestatorului.

Art. 29

(1) Prestatorul are obligaţia de a specifica în documentaţia de avizare următoarele informaţii şi documente, după caz:
a)descrierea serviciilor furnizate/externalizate;
b)datele de identificare ale furnizorului: adresa sediului social, telefon/fax, e-mail, pagina de internet;
c)certificat constatator emis de Oficiul Naţional al Registrului Comerţului, cu starea la zi a persoanei juridice, sau echivalentul acestuia pentru furnizorii externi înregistraţi în alte state, în original sau copie conformă cu originalul;
d)documente în funcţie de tipul serviciului sau activităţii desfăşurate, astfel:
1.SR ISO/IEC 27001 sau certificări pentru standarde echivalente - pentru toţi furnizorii de servicii IT externalizate;
2.certificări pentru furnizarea şi dezvoltarea de programe informatice software;
3.act doveditor de respectare a condiţiilor tehnice conform standardelor internaţionale privind serviciile de găzduire sau externalizare prin intermediul centrelor de date;
4.acreditare pentru furnizarea de servicii de arhivare electronică.
(2) Certificările trebuie să fie emise de entităţi/organisme recunoscute pe plan intern şi/sau internaţional.

Art. 30

(1) Prestatorul are obligaţia de a notifica MCSI încheierea contractului cu furnizorul de servicii IT externalizate în termen de maximum 14 zile de la data încheierii.

(2) Prestatorul are obligaţia ca, în cazul modificării unor informaţii şi/sau documente prevăzute la art. 29, să notifice MCSI şi să depună originalul sau copia documentelor modificate în termen de maximum 60 de zile de la data efectuării modificării.

Art. 31

(1) Prestatorul are obligaţia să se asigure că prevederile prezentului ordin sunt respectate de către toţi furnizorii de servicii IT externalizate, inclusiv în cazul externalizărilor în lanţ.

(2) Furnizorii de servicii IT externalizate vor permite MCSI şi auditorului IT să verifice şi/sau să auditeze sistemele sale informatice în contextul aplicării prevederilor prezentului ordin sau vor pune la dispoziţia auditorului IT un raport de audit IT întocmit în conformitate cu standardele internaţionale în domeniu.

CAPITOLUL VI: Cerinţe privind raportarea

Art. 32

(1) Prestatorul va raporta către MCSI, trimestrial, referitor la instrumentele de plată electronică cu acces la distanţă, următoarele: numărul de utilizatori, numărul de plăţi efectuate, valoarea plăţilor efectuate prin intermediul acestora, în formatul prezentat în anexa nr. 6.

(2) Raportările pot fi transmise prin poştă, pe adresa Ministerului Comunicaţiilor şi Societăţii Informaţionale, Bd. Libertăţii nr. 14, sectorul 5, cod 050706, sau prin e-mail, ca fişier ataşat, pe adresa e-banking@comunicaţii.gov.ro, până la sfârşitul lunii următoare trimestrului pentru care se face raportarea.

CAPITOLUL VII: Dispoziţii tranzitorii şi finale

Art. 33

(1) Documentele prevăzute la art. 9 se înaintează către MCSI cu minimum 40 de zile înaintea expirării avizului anterior şi vor fi întocmite într-un singur exemplar.

(2) Avizul acordat este valabil 1 an de la data eliberării acestuia.

(3) Avizul acordat este netransmisibil.

Art. 34

(1)MCSI va comunica solicitantului decizia sa cu privire la acordarea avizului, în termen de 40 de zile calendaristice de la data înregistrării cererii de eliberare a avizului.

(2)MCSI va remite solicitantului un exemplar al avizului, în termen de 3 zile calendaristice după acordarea acestuia.

(3) Forma avizului acordat este prevăzută în anexa nr. 7.

Art. 35

(1) Prestatorul va notifica MCSI orice dezvoltare, modificare a condiţiilor de exploatare şi a procedurilor operaţionale, precum şi a măsurilor tehnice de securitate aplicabile instrumentului, în termen de 30 de zile de la data când devin operaţionale.

(2) Prestatorul va notifica MCSI, în termen de maximum 10 zile, orice incident de securitate care a afectat în mod direct clienţii. Notificarea va cuprinde cauza şi măsurile ce urmează a fi luate în vederea remedierii situaţiei apărute.

(3)MCSI poate solicita un nou raport de audit pentru instrumentul financiar de plată electronică cu acces la distanţă, după analizarea notificărilor prevăzute la alin. (1) şi (2).

(4)MCSI poate retrage avizul şi informează BNR dacă în termen de 60 de zile prestatorul nu prezintă raportul de audit prevăzut la alin. (3).

Art. 36

(1)MCSI poate efectua verificări la sediul prestatorului avizat sau în curs de avizare prin personal desemnat prin ordin al ministrului comunicaţiilor şi societăţii informaţionale.

(2)În cazul în care, în urma verificărilor, se constată nerespectarea prevederilor conţinute în documentaţia de avizare, MCSI poate dispune neacordarea avizului sau, eventual, retragerea acestuia.

Art. 37

Eliberarea de către MCSI a avizului pentru furnizarea instrumentului de plată electronică cu acces la distanţă nu exonerează prestatorul şi utilizatorii acestuia de răspunderile asumate prin contractul încheiat între aceştia.

CAPITOLUL VIII: Măsuri tranzitorii

Art. 38

(1) Avizul eliberat de către MCSI conform Ordinului ministrului comunicaţiilor şi tehnologiei informaţiei nr. **389/2007** privind procedura de avizare a instrumentelor de plată cu acces la distanţă, de tipul aplicaţiilor internet-banking, home-banking sau mobile-banking, îşi prelungeşte valabilitatea cu 60 de zile de la data publicării prezentului ordin în Monitorul Oficial al României, Partea I.

(2)În perioada extinderii valabilităţii, prestatorul trebuie să depună documentaţia de avizare în condiţiile prezentului ordin.

(3) Documentaţiile întocmite şi depuse de către prestatori la MCSI, după data publicării în Monitorul Oficial al României, Partea I, a Regulamentului Băncii Naţionale a României nr. **3/2018**, pentru avizarea instrumentelor de plată electronică cu acces la distanţă, se vor completa în concordanţă cu cerinţele prezentului ordin.

(4) Raportul de audit deja întocmit sau în curs de realizare la data intrării în vigoare a prezentului ordin poate fi depus împreună cu documentaţia de avizare, cu respectarea prevederilor art. 9 alin. (1).

Art. 39

Anexele nr. 1-7 fac parte integrantă din prezentul ordin.

Art. 40

Prezentul ordin intră în vigoare la data publicării acestuia în Monitorul Oficial al României, Partea I.

Art. 41

Ordinul ministrului comunicaţiilor şi tehnologiei informaţiei nr. **389/2007** privind procedura de avizare a instrumentelor de plată cu acces la distanţă, de tipul aplicaţiilor internet-banking, home-banking sau mobile-banking, publicat în Monitorul Oficial al României, Partea I, nr. 485 din 19 iulie 2007, se abrogă la data publicării prezentului ordin în Monitorul Oficial al României, Partea I.

-****-

Ministrul comunicaţiilor şi societăţii informaţionale,
Alexandru Petrescu

ANEXA nr. 1: CERERE de eliberare a avizului

CERERE de eliberare a avizului

..... (denumirea prestatorului de servicii de plată) ....., având sediul în ..... (adresa completă, inclusiv telefon şi fax) ....., înmatriculat(ă)/înregistrat(ă) la oficiul registrului comerţului cu nr. ..... (numărul de înregistrare/codul unic de înregistrare) ....., cod fiscal ....., având Autorizaţia de funcţionare nr. ....., eliberată de Banca Naţională a României, reprezentat(ă) legal prin ..... (numele şi prenumele)....., domiciliat(ă) în ..... (adresa completă, inclusiv telefon) ....., identificat(ă) prin ..... (actul de identitate: seria, numărul şi emitentul, precum şi codul numeric personal) .....,

în conformitate cu prevederile Hotărârii Guvernului **36/2017** privind organizarea şi funcţionarea Ministerului Comunicaţiilor şi Societăţii Informaţionale, cu modificările şi completările ulterioare, prevederile art. 129 alin. (1) pct. 2 lit. c) din Regulamentul Băncii Naţionale a României nr. **3/2018** privind monitorizarea infrastructurilor pieţei financiare şi a instrumentelor de plată şi cu prevederile Ordinului ministrului comunicaţiilor şi societăţii informaţionale nr. 553/2019 privind reglementarea procedurii de avizare a instrumentelor de plată electronică cu acces la distanţă, vă solicităm eliberarea/menţinerea avizului pentru emiterea şi punerea în circulaţie a instrumentului de plată electronică cu acces la distanţă ...../menţinerea în circulaţie a instrumentului ..... cu următoarele caracteristici generale (scurtă descriere):

.....
.....
.....

Sistemul funcţionează (va funcţiona) la sediul din ..... .

Numele şi prenumele solicitantului

.....

Ştampila solicitantului

Data .....

ANEXA nr. 2: LISTA certificărilor profesionale agreate pentru efectuarea testelor de penetrare

Echipa de testare ce efectuează testele de penetrare trebuie să deţină cel puţin una din certificările menţionate mai jos.

Certificări recunoscute internaţional:

CEPT - Certified Expert Penetration Tester;
CPT - Certified Penetration Tester;
GPEN - GIAC Certified Penetration Tester;
GWAPT - GIAC Web Application;
LPT - Licensed Penetration Tester;
OPST - OSSTMM Professional Security Tester Aceredited Certification;
OSCE - Offensive Security Certified Expert;
OSCP - Offensive Security Certified Professional;
PTC - MILLE2 Certified Penetration Testing Consultant.

ANEXA nr. 3: RAPORT DE AUDIT

SECŢIUNEA I: "Raport"

Nr. crt.	Capitol	Observaţii
1.	Titlul raportului	
2.	Destinatarii raportului şi orice restricţii privind conţinutul şi circulaţia raportului	
3.	Paragraf introductiv	Identificarea prestatorului de servicii de plată auditat (denumire/numărul de înregistrare la Oficiul Naţional al Registrului Comerţului/adresă) Identificarea instrumentului de plată electronică cu acces la distanţă auditat (menţionarea denumirii instrumentului). Includerea afirmaţiei că sistemele/aplicaţiile informatice au fost auditate ca urmare a obligaţiei legale impuse de Ordinul ministrului comunicaţiilor şi societăţii informaţionale nr. 553/2019 privind reglementarea procedurii de avizare a instrumentelor de plată electronică cu acces la distanţă
4.	Asumarea responsabilităţii conducerii entităţii privind auditul efectuat asupra sistemelor informatice	
5.	Responsabilitatea auditorului IT	Raportul de audit IT va include cel puţin afirmaţiile: - că "este responsabilitatea auditorului IT să exprime o opinie cu privire la conformitatea sistemelor informatice cu prevederile Ordinului ministrului comunicaţiilor şi societăţii informaţionale nr. 553/2019"; - că "raportul de audit IT a fost elaborat în conformitate cu standardul de audit utilizat, respectiv ..... (menţionarea acestuia)".
6.	Datele de identificare ale coordonatorului certificat al echipei de audit IT/auditorului IT persoană fizică/auditorului IT intern certificat	Numele, prenumele, telefon, fax, adresa de e-mail şi adresa unde îşi desfăşoară activitatea
7.	Semnătura coordonatorului certificat al echipei de audit şi semnătura reprezentantului legal al auditorului persoană juridică/semnătura auditorului IT persoană fizică/semnătura auditorului IT certificat	
8.	Obiectivele activităţii de audit IT, perioada auditată	
9.	Sediul desfăşurării activităţii de audit IT, data întocmirii raportului de audit IT	Adresa sediului unde a avut loc activitatea de audit IT (sediu central/sucursală/filială), data întocmirii raportului de audit IT
10.	Descrierea ariei auditului IT	Identificarea sistemului informatic utilizat de către prestatorul de servicii de plată folosit în procesul de emitere/exploatare a instrumentului financiar de plată electronică cu acces la distantă ..... (menţionarea denumirii instrumentului de plată electronică) Raportarea componentelor sistemului informatic se va face într-un tabel care să cuprindă următoarele:

		Nr. crt.; Denumire echipament/aplicaţie; Descriere hardware/software; Serial number; Funcţia Îndeplinită; Administrarea sistemului informatic (internă/externalizată) Pentru sistemele informatice supuse auditului IT se vor menţiona următoarele: - măsurile organizatorice: politicile aplicabile şi procedurile implementate; - un sumar conţinând analiza riscurilor aferente activităţii, a posibilelor deficienţe ale sistemului informatic auditat şi a măsurilor de reducere a riscurilor asociate, în baza controalelor generale sau specifice implementate conform prevederilor Ordinului ministrului comunicaţiilor şi societăţii informaţionale nr. 553/2019.
11.	Referiri cu privire la implementarea planului de acţiune asumat de prestatorul de servicii de plată rezultat în urma activităţii de audit IT anterioare, dacă este cazul	Verificarea modului de implementare a măsurilor şi respectarea termenelor asumate prin raportul de audit anterior
12.	Referiri cu privire la modul de efectuare a evaluării anuale de către prestatorul de servicii de plată a riscurilor operaţionale generate de utilizarea sistemelor informatice importante (Entităţile au obligaţia să evalueze anual şi să monitorizeze continuu riscurile operaţionale generate de utilizarea sistemelor informatice importante, să prioritizeze resursele, să implementeze măsuri de securitate informatică şi să monitorizeze eficacitatea acestora prin aplicarea managementului de risc.)	Opinie cu privire la plauzibilitatea metodologiei/tehnicilor utilizate, precum şi asupra măsurilor de control implementate în vederea gestionării riscurilor operaţionale identificate
13.	Rezultatul obţinut în urma efectuării testului de penetrare	Conform raportului privind testul de penetrare se consemnează următoarele elemente: - nr. de înregistrare/data raportului privind testele de penetrare: - perioada în care s-au desfăşurat testele de penetrare; - descrierea metodologiei/tehnicilor utilizate; - menţionarea rezultatelor obţinute în urma testului; - concluziile raportului; - recomandările adresate entităţii şi răspunsul managementului entităţii.
14.	Afirmaţia de conformitate, reflectată prin opinia auditorului IT	Opinie pozitivă, opinie cu rezerve/calificată, opinie negativă, după caz

SECŢIUNEA II: "Anexe la raportul de audit IT"

1.Sumarul observaţiilor - anexa nr. R1

(1) Anexa este însuşită de către entitatea auditată prin semnarea acesteia de către reprezentantul legal şi conţine, fără a se limita la acestea:

a)descrierea neconformităţii/constatării;

b)importanţa neconformităţii/constatării;

c)riscurile asociate;

d)probabilitatea ca aceste constatări să aibă un impact semnificativ; recomandările auditorului IT pentru acţiuni corective şi răspunsul conducerii entităţii auditate pentru fiecare constatare din raport (inclusiv în urma testului de penetrare);

e)planul de acţiune asumat de către entitatea auditată care conţine măsurile efective, termenul de implementare şi persoanele responsabile de implementare.

2.Analiza internă a riscurilor operaţionale şi registrul riscurilor - anexa nr. R2

(1) Anexa conţine următoarele informaţii, fără a se limita la acestea:

a)descrierea politicii/metodologiei utilizate de către entitate;

b)rezultatele revizuirii riscurilor generate de utilizarea sistemelor informatice;

c)rezultatele evaluării de către auditorul IT a măsurilor de control implementate în vederea gestionării riscurilor operaţionale identificate (pentru riscuri semnificative).

3.Cerinţe referitoare la furnizorii de servicii IT externalizate pentru sistemele informatice auditate - anexa nr. R3

(Raportarea se efectuează prin completarea tabelului prezentat.)

Sisteme/Servicii externalizate	Funcţia sistemelor/serviciilor externalizate - descriere	Furnizor - date de identificare (denumire, sediul entităţii, datele de înregistrare fiscală, telefon/fax/website)	Certificare SR ISO/IEC 27001 sau echivalent (emitent, număr certificare, data emiterii, perioada de valabilitate)	Alte certificări	Concluzie - Conformitate Da/Nu/Parţial	Observaţii

4.Concluzii ale echipei de audit privind respectarea cerinţelor impuse de Ordinul ministrului comunicaţiilor şi societăţii informaţionale nr. 553/2019 - anexa nr. R4

5._

NOTĂ:

Anexele prevăzute la secţiunea II "Anexe la raportul de audit" R1-R4 fac parte integrantă din raport.

ANEXA nr. 4: CERERE de înscriere în Lista auditorilor IT

..... (denumirea auditorului IT) ....., având sediul în ..... (adresa completă, inclusiv telefon şi fax, adresa de e-mail, adresa paginii de internet) ....., înmatriculat(ă)/înregistrat(ă) la oficiul registrului comerţului cu nr. ..... (numărul de înregistrare/codul unic de înregistrare) ....., cod fiscal ....., reprezentat(ă) legal prin dl/dna ....., identificat(ă) prin ..... (actul de identitate: seria, numărul şi emitentul) .....,

intenţionez să prestez servicii de audit IT pentru prestatorii de servicii de plată care emit instrumente financiare de plată electronică cu acces la distanţă cărora le sunt incidente prevederile Ordinului ministrului comunicaţiilor şi societăţii informaţionale nr. 553/2019 privind reglementarea procedurii de avizare a instrumentelor de plată electronică cu acces la distanţă şi vă solicit înscrierea în Lista auditorilor IT publicată pe site-ul instituţiei dumneavoastră.

Anexez prezentei cereri documentaţia de calificare prevăzută la art. 15 din Ordinul ministrului comunicaţiilor şi societăţii informaţionale nr. 553/2019.

Numele şi prenumele reprezentantului legal

.....

Ştampila solicitantului

Data .....

ANEXA nr. 5: LISTA certificărilor profesionale agreate pentru auditorii IT

Raportul de audit se întocmeşte de către un auditor IT care trebuie să deţină cel puţin una din certificările menţionate mai jos.

Certificări recunoscute internaţional:

ISACA - CISA - Certified Information Systems Auditor (auditorul pentru sisteme informatice, certificat de ISACA);

GIAC(SANS) - GSNA Systems and Network Auditors;

GIAC - GCCC Critical Controls Certification;

CISSP - Certified Information Systems Security Professional.

ANEXA nr. 6:

Prestatorul de servicii de plată: .....

Instrumentul de plată electronică cu acces la distanţă	Numărul de utilizatorii	Numărul de plăţi/tranzacţii[2] - lei -	Numărul de tranzacţii - valută -	Valoarea plăţilor/tranzacţiilor[3] - lei -	Valoarea tranzacţiilor în valută (echivalent euro)	Perioada de raportare Trimestrul

Semnătură reprezentant legal

.....

[1]Numărul de utilizatori se referă la numărul de utilizatori cu care există încheiat un contract pentru utilizarea instrumentului de plată cu acces la distanţă, pe parcursul trimestrului pentru care se face raportarea. Se iau în considerare toate contractele în vigoare de la data lansării instrumentului de plată electronică cu acces la distanţă.

[2]Numărul de plăţi efectuate prin intermediul instrumentelor de plată cu acces la distanţă se referă la plăţile efectuate doar pe perioada trimestrului raportat şi care vor fi prezentate, defalcat, în numărul de plăţi în lei şi în numărul de plăţi în valută.

[3]Valoarea plăţilor efectuate prin intermediul instrumentelor de plată cu acces la distanţă în perioada trimestrului raportat va fi prezentată astfel: valoarea plăţilor efectuate în lei şi valoarea plăţilor efectuate în valută. Plăţile efectuate în valută vor fi exprimate în echivalent euro, la cursul de schimb BNR din ultima zi a trimestrului pentru care se face raportarea.

ANEXA nr. 7:

MINISTERUL COMUNICAŢIILOR ŞI SOCIETĂŢII INFORMAŢIONALE

Având în vedere prevederile Hotărârii Guvernului nr. **36/2017** privind organizarea şi funcţionarea Ministerului Comunicaţiilor şi Societăţii Informaţionale, cu modificările şi completările ulterioare,

având în vedere prevederile art. 129 alin. (1) pct. 2 lit. c) din Regulamentul Băncii Naţionale a României nr. **3/2018** privind monitorizarea infrastructurilor pieţei financiare şi a instrumentelor de plată şi ale Ordinului ministrului comunicaţiilor şi societăţii informaţionale nr. 553/2019 privind reglementarea procedurii de avizare a instrumentelor de plată electronică cu acces la distanţă,

ministrul comunicaţiilor şi societăţii informaţionale eliberează prezentul aviz.

....., având sediul în ..... (adresa completă, inclusiv telefon şi fax) ....., înmatriculat(ă)/înregistrat(ă) la oficiul registrului comerţului cu nr. ....., cod fiscal ....., având Autorizaţia de funcţionare, nr. ....., eliberată de Banca Naţională a României, reprezentat(ă) legal prin ..... (numele şi prenumele) .....,

a obţinut avizul pentru furnizarea instrumentului de plată cu acces la distanţă ..... cu următoarele caracteristici generale:

.....

.....

.....

Sistemul funcţionează (va funcţiona) la sediul din ..... .

Observaţii:

Prezentul document s-a eliberat prestatorului de servicii de plată în scopul acordării/menţinerii avizului Ministerului Comunicaţiilor şi Societăţii Informaţionale necesar pentru emiterea/punerea în circulaţie a instrumentului de plată electronică cu acces la distanţă şi are valabilitate un an de la data eliberării acestuia.

Ministrul comunicaţiilor şi societăţii informaţionale,

.....

Nr. .....

Data .....

Publicat în Monitorul Oficial cu numărul 485 din data de 14 iunie 2019