

ORDIN nr. 489 din 15 iunie 2009 privind normele metodologice de autorizare a centrelor de date

EMITENT: MINISTERUL COMUNICATIILOR SI SOCIETATII INFORMATIONALE

PUBLICAT: MONITORUL OFICIAL nr. 435 din 25 iunie 2009

În temeiul art. 4 alin. (1) pct. 58 și al <>art. 6 alin. (6) din Hotărârea Guvernului nr. 12/2009 privind organizarea și funcționarea Ministerului Comunicațiilor și Societății Informaționale, cu modificările și completările ulterioare, precum și al art. 17 alin. (2) și <>art. 27 alin. (2) din Legea nr. 135/2007 privind arhivarea documentelor în formă electronică,

ministrul comunicațiilor și societății informaționale emite următorul ordin:

ART. 1

(1) Prezentul ordin se aplică centrelor de date utilizate de către administratorii de arhive electronice, în conformitate cu prevederile <>Legii nr. 135/2007 privind arhivarea documentelor în formă electronică.

(2) Prezentul ordin stabilește procedura și condițiile privind acordarea, suspendarea și retragerea autorizării centrelor de date, emise de către Ministerul Comunicațiilor și Societății Informaționale, denumit în continuare MCSI, precum și conținutul, durata de valabilitate și efectele suspendării sau retragerii autorizării.

ART. 2

În înțelesul prezentului ordin, următorii termeni se definesc astfel:

- a) centru de date - spațiu securizat, dotat cu tehnică de calcul și echipamente de comunicații prin intermediul cărora se primesc, se stochează și se transmit date în formă electronică;
- b) procedură de autorizare - metodă de evaluare sistematică, documentată, periodică și obiectivă a performanței centrului de date, a sistemului de management și a proceselor destinate protecției arhivelor electronice, în scopul verificării respectării cerințelor prevăzute de legislația în vigoare;
- c) ordin de autorizare - document emis de MCSI care atestă că un centru de date îndeplinește toate condițiile cerute de legislația în vigoare în vederea desfășurării operațiunilor de arhivare electronică;
- d) backup - activitatea de copiere a unor fișiere sau baze de date în vederea conservării și recuperării acestora în cazul unei avarii sau al altui eveniment neprevăzut;
- e) UPS (Uninterruptible Power Supply) - dispozitiv care permite calculatorului să funcționeze pentru o perioadă scurtă de timp în cazul în care sursa principală de energie este întreruptă, respectiv care asigură protecție împotriva suprasarcinilor tranzitorii;
- f) firewall - dispozitiv hardware sau aplicație software care monitorizează și filtrează permanent transmisiile de date realizate între rețeaua protejată și alte rețele, pe baza unui set de reguli și criterii;
- g) router - dispozitiv hardware sau aplicație software care conectează două sau mai multe rețele de calculatoare;
- h) upgrade - proces de îmbunătățire a unui echipament tehnic sau a unei aplicații software;
- i) redundanță - introducerea de dispozitive suplimentare față de cel de bază, care să asigure funcționarea unui sistem în cazul în care unul dintre dispozitivele cu aceeași funcție a ieșit întâmplător din uz.

ART. 3

Centrele de date utilizate de către administratorii de arhive electronice trebuie să dispună de dotările tehnice și să aplice politicile și procedurile de management și de securitate necesare pentru a îndeplini condițiile prevăzute la <>art. 17 alin. (1) din Legea nr. 135/2007 .

ART. 4

(1) Persoana fizică sau juridică care intenționează să obțină autorizarea unui centru de date în vederea desfășurării activităților legate de arhivarea electronică a documentelor, denumită în continuare solicitant, va transmite MCSI o cerere scrisă în acest sens. Forma și conținutul acestei cereri sunt prevăzute în anexa nr. 1.

(2) Cererea prevăzută la alin. (1) va fi însoțită de următoarele documente:

a) descrierea politicilor și procedurilor de lucru, incluzând enumerarea posturilor și a funcțiilor personalului, precum și calificările/atestările profesionale ale acestuia;

b) descrierea generală a echipamentelor utilizate în procesul de arhivare;

c) procedurile pentru asigurarea disponibilității serviciului;

d) politica generală de securitate, politicile privind utilizatorii, parolele și accesul la sisteme.

(3) Cererea și documentele anexate se transmit la sediul MCSI în unul dintre următoarele moduri:

a) prin depunere, personal sau de către reprezentantul legal, cu luare de număr de înregistrare de la registratura generală a MCSI;

b) printr-un serviciu poștal;

c) ca înscris în formă electronică, căruia i s-a încorporat, i s-a atașat sau i s-a asociat logic o semnătură electronică extinsă, bazată pe un certificat calificat nesuspendat sau nerevocat la momentul respectiv și generată cu ajutorul unui dispozitiv securizat de creare a semnăturii electronice.

(4) Este considerată dată a transmiterii, după caz, data înscrierii în registrul general de intrare-ieșire a corespondenței al MCSI, data confirmării primirii documentelor la sediul MCSI printr-un serviciu poștal cu confirmare de primire sau data confirmării primirii înscrisului în formă electronică.

(5) În cazul în care documentația nu îndeplinește condițiile prevăzute de prezentul ordin, MCSI va solicita completarea acesteia, în termen de 10 zile de la transmiterea solicitării de completare.

(6) În cazul în care documentația transmisă potrivit alin. (1)-(3) este completă sau a fost completată în conformitate cu prevederile alin. (5), MCSI demarează procedura de autorizare a centrului de date.

ART. 5

(1) Verificarea îndeplinirii condițiilor în vederea autorizării se face de către personalul MCSI cu atribuții în acest sens, în cadrul procedurii de autorizare.

(2) Pe perioada desfășurării procedurii de autorizare, MCSI poate solicita orice documente referitoare la activitatea centrului de date care au legătură cu activitatea de arhivare electronică și poate efectua acțiuni de control pentru a verifica conformitatea dintre informațiile declarate în cursul procedurii de autorizare și realitate.

ART. 6

În vederea autorizării, centrul de date trebuie să îndeplinească condițiile prevăzute la <>art. 17 alin. (1) din Legea nr. 135/2007 , obiectivele principale urmărite de MCSI în cursul procedurii de autorizare pentru verificarea îndeplinirii acestor condiții fiind următoarele:

- a) asigurarea securității și integrității datelor, la nivel de securitate fizică și acces prin mijloace informatice;
- b) disponibilitatea serviciului de arhivare electronică și backupul informațiilor stocate.

ART. 7

În cursul procedurii de autorizare, MCSI va verifica îndeplinirea de către centrul de date, în mod cumulativ, a condițiilor prevăzute la art. 8-12.

ART. 8

Spațiul în care funcționează centrul de date trebuie să fie amenajat astfel încât să fie posibilă respectarea cerințelor de securitate specifice și să asigure funcționarea echipamentelor la parametri optimi prevăzuți de producătorii acestora. În acest sens, se vor asigura:

- a) instalarea unor sisteme de climatizare care să asigure valorile optime de temperatură și umiditate în vederea funcționării echipamentelor în condiții de siguranță;
- b) utilizarea de materiale ignifuge și instalarea unor sisteme de prevenire și stingere a incendiilor, concepute special pentru evitarea deteriorării echipamentelor;
- c) dimensionarea corespunzătoare a rețelei electrice, în funcție de consumurile echipamentelor folosite;
- d) garantarea siguranței la defecțiunile previzibile ale sistemelor de utilități (apă, gaze etc.) care deservește spațiul care găzduiește centrul de date.

ART. 9

Asigurarea redundanței și realizarea backupului trebuie să fie implementate prin următoarele măsuri:

- a) utilizarea de dispozitive UPS și/sau generatoare electrice, care să asigure funcționarea neîntreruptă a echipamentelor în cazul opririi alimentării cu curent electric de la rețeaua principală; timpul de asigurare a alimentării din sursa de urgență va fi calculat în funcție de timpii estimați pentru remedierea posibilelor avarii care ar surveni la rețeaua electrică principală;
- b) duplicarea tuturor elementelor rețelei electrice și asigurarea posibilității comutării automate de pe rețeaua principală pe rețeaua de rezervă;
- c) utilizarea procedurilor de lucru care să asigure efectuarea de backup periodic al tuturor informațiilor păstrate în centrul de date și stocarea acestora în alt spațiu, diferit de spațiul principal al centrului de date, cu asigurarea aceluiași condiții de securitate ca și cele ale spațiului principal, aflat la o distanță față de spațiul principal care să corespundă normelor europene în domeniu;
- d) asigurarea unor proceduri de mentenanță pentru echipamente și pentru infrastructură, respectând recomandările producătorilor echipamentelor respective, astfel încât să se minimizeze riscul apariției de probleme tehnice;

e) în cazul echipamentelor critice (a căror funcționare permanentă este esențială în asigurarea continuității funcționării centrului de date) se vor asigura echipamente de rezervă, care vor fi folosite pe perioada efectuării operațiunilor de mentenanță ce implică oprirea sau deconectarea respectivului echipament și pe perioada în care echipamentul principal este afectat de defecțiuni tehnice.

ART. 10

Centrul de date trebuie să aibă o structură scalabilă, atât în ceea ce privește echipamentele informatice utilizate, cât și în ceea ce privește infrastructura, cu scopul de a păstra performanțele sistemului la un nivel constant în cazul apariției de condiții noi (mărirea capacității centrului de date, facilități noi etc.).

ART. 11

(1) Centrul de date trebuie să asigure securitatea și integritatea informațiilor stocate, atât în ceea ce privește accesul fizic la echipamentele utilizate, cât și în ceea ce privește accesul prin mijloace electronice la documentele arhivate.

(2) Securitatea fizică presupune luarea următoarelor măsuri:

a) accesul controlat la echipamentele centrului de date utilizate pentru arhivarea electronică a documentelor, cu precizarea mai multor niveluri de drepturi de acces ale personalului care operează sistemele;

b) utilizarea echipamentelor speciale de evitare și detecție a intruziunilor fizice.

(3) Pentru asigurarea securității accesului prin mijloace electronice la documentele arhivate trebuie utilizate următoarele măsuri tehnice:

a) sisteme de detecție a intruziunilor (Intrusion Detection System - IDS);

b) firewall (software și/sau hardware), routere pentru filtrarea traficului;

c) sisteme antivirus;

d) securizarea proceselor de autentificare și de autorizare a accesului la date;

e) jurnalizarea automată a acțiunilor efectuate în sistem.

ART. 12

Operarea centrului de date trebuie realizată respectându-se strategii, politici și proceduri bine determinate în ceea ce privește managementul, controlul și securitatea sistemelor. În realizarea acestor politici și proceduri se vor respecta următoarele cerințe minimale:

- a) jurnalizarea cronologică a acțiunilor efectuate în sistem (accesul fizic la echipamente, comutări de pe un sistem pe altul, procese de mentenanță, acțiuni ale operatorului etc.);
- b) evaluarea la intervale regulate a infrastructurii centrului de date, a sistemului de securitate și a echipamentelor informatice folosite, inclusiv a sistemelor de backup;
- c) folosirea unui sistem de management al calității;
- d) evaluarea efectelor extinderilor și upgrade-urilor;
- e) realizarea auditului regulat al planului de securitate;
- f) evaluarea și perfecționarea periodică a personalului;
- g) implementarea unor politici de resurse umane care să asigure operarea centrului de date de către personal specializat care să dispună de certificări în domeniu.

ART. 13

(1) În termen de 30 de zile de la primirea documentației în conformitate cu prevederile art. 4 alin. (1)-(3) sau a completărilor solicitate în conformitate cu prevederile art. 4 alin. (5), MCSI emite ordinul de autorizare a centrului de date sau ordinul de respingere a cererii de autorizare, motivat în mod corespunzător.

(2) Forma și conținutul ordinului de autorizare a centrului de date sunt prevăzute în anexa nr. 2.

ART. 14

- (1) Ordinul de autorizare este valabil pentru o perioadă de 3 ani de la data emiterii acestuia.
- (2) Autorizarea poate fi reînnoită, procedura de reautorizare fiind identică cu cea de autorizare.
- (3) Pe durata valabilității autorizării, MCSI are dreptul de a efectua acțiuni de control periodice, pentru verificarea menținerii condițiilor de funcționare a centrului de date.

ART. 15

- (1) Constatarea de către personalul de control de specialitate din cadrul MCSI a neîndeplinirii condițiilor minime de funcționare a centrului de date atrage suspendarea ordinului de autorizare pe o perioadă de 30 de zile; în această perioadă, centrul de date nu poate primi spre stocare documente în formă electronică.
- (2) Dacă deficiențele survenite în funcționarea centrului de date nu sunt remediate în intervalul de timp prevăzut la alin. (1), autorizarea se retrage, prin ordin emis de ministrul comunicațiilor și societății informaționale.
- (3) În cazul expirării duratei de valabilitate a autorizării, precum și în cazul retragerii autorizării de către MCSI în condițiile alin. (2), centrul de date nu mai poate furniza servicii legate de arhivarea electronică în sensul <>Legii nr. 135/2007 .
- (4) În cazul intenției de încetare a activității centrului de date autorizat în condițiile prezentului ordin, MCSI va fi informat, cu cel puțin 30 de zile în avans, despre această intenție și despre existența și natura împrejurării care justifică imposibilitatea de continuare a activității. La data încetării activității centrului de date, autorizarea se retrage, prin ordin emis de ministrul comunicațiilor și societății informaționale.

ART. 16

Pentru funcționarea corespunzătoare a centrelor de date se recomandă aplicarea și respectarea următoarelor standarde sau a unor standarde echivalente:

- a) SR ISO/CEI 17799: 2006 Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației;

- b) SR ISO/IEC 27001: 2006 Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe;
- c) SR ISO/CEI 15408-1: 2004 Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 1: Introducere și model general;
- d) ISO/IEC 20000-1: 2005 Tehnologia informației - Managementul securității - Partea 1: Specificații;
- e) ISO/IEC 20000-2: 2005 Tehnologia informației - Managementul securității - Partea a 2-a: Cod de practică;
- f) TIA/EIA 942 2005 Standard privind infrastructura de telecomunicații a Centrului de date;
- g) SR EN 50173-5 2008 Tehnologia informației. Sisteme generice de cablare. Partea a 5-a: Centre de date;
- h) SR EN 50173-1 2008 Tehnologia informației. Sisteme generice de cablare. Partea 1: Cerințe generale.

ART. 17

Anexele nr. 1 și 2 fac parte integrantă din prezentul ordin.

ART. 18

(1) La data intrării în vigoare a prezentului ordin se abrogă <>Decizia președintelui Autorității Naționale pentru Comunicații nr. 1.131/2008 privind normele metodologice de autorizare a centrelor de date, publicată în Monitorul Oficial al României, Partea I, nr. 861 din 20 decembrie 2008.

(2) Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

ANEXA 1

CERERE pentru începerea procedurii de autorizare

Către:

Stimate domnule ministru,

Având în vedere prevederile <>Legii nr. 135/2007 privind arhivarea documentelor în formă electronică, precum și ale Ordinului ministrului comunicațiilor și societății informaționale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date, vă solicităm să dispuneți începerea procedurii de autorizare a centrului de date aparținând/(numele și prenumele/denumirea solicitantului)....., având domiciliul/sediul în/(adresa completă, inclusiv telefon și fax)....., înregistrat în Registrul Comerțului al Municipiului, cod numeric personal/cod unic de înregistrare/cod de identificare fiscală, reprezentat legal prin/(numele și prenumele).., domiciliat (ă) în/(adresa completă, inclusiv telefon)....., identificat (ă) prin/(actul de identitate: seria, numărul, codul numeric personal)

Numele și prenumele/Denumirea solicitantului

.....

Semnătura reprezentantului legal și ștampila solicitantului

.....

Data

.....

ANEXA 2

ORDIN de autorizare a centrului de date

Având în vedere dispozițiile <>Legii nr. 135/2007 privind arhivarea documentelor în formă electronică, precum și ale Ordinului ministrului comunicațiilor și societății informaționale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date,

în baza Referatului de aprobare al Direcției*1), înregistrat cu nr./.....,

în temeiul art. 4 alin. (1) pct. 58 și al <>art. 6 alin. (6) din Hotărârea Guvernului nr. 12/2009 privind organizarea și funcționarea Ministerului Comunicațiilor și Societății Informaționale, cu modificările și completările ulterioare,

ministrul comunicațiilor și societății informaționale emite prezentul ordin.

Art. 1. - Începând cu data comunicării prezentului ordin, centrul de date aparținând/(numele și prenumele/denumirea solicitantului autorizării)..... este autorizat să desfășoare operațiuni de arhivare electronică în condițiile <>Legii nr. 135/2007 privind arhivarea documentelor în formă electronică.

Art. 2. - Se certifică faptul că centrul de date îndeplinește condițiile stabilite de dispozițiile <>art. 17 din Legea nr. 135/2007 și prevederile art. 8-12 din Ordinul ministrului comunicațiilor și societății informaționale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date.

Art. 3. - Autorizarea se acordă pe o perioadă de 3 ani de la data comunicării prezentului ordin și poate fi reînnoită pe baza procedurii prevăzute în Ordinul ministrului comunicațiilor și societății informaționale nr. 489/2009.

Art. 4. - Prezentul ordin se comunică/(numele și prenumele/denumirea persoanei care operează centrul de date) atât pe suport de hârtie, cât și în formă electronică, semnată electronic.

*1) Se va menționa denumirea direcției de specialitate din cadrul Ministerului Comunicațiilor și Societății Informaționale care îndeplinește atribuțiile de punere în aplicare a <>Legii nr. 135/2007 privind arhivarea documentelor în formă electronică.

Ministru,

.....

Nr.