EXPUNERE DE MOTIVE

Secţiunea 1 **Titlul proiectului de act normativ**	
Lege privind aprobarea Ordonanţei de urgenţă pentru modificarea şi completarea Legii nr.362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice	
Secţiunea a 2-a **Motivul emiterii proiectului de act normativ**	
1. Descrierea situaţiei actuale	*Directiva (UE) 2016/1148 a Parlamentului European şi a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune*, denumită în continuare *Directiva NIS*, stabileşte la nivelul întregii Uniuni Europene un sistem unitar de creştere a nivelului de securitate a reţelelor şi sistemelor informatice care susţin furnizarea de servicii esenţiale şi servicii digitale de cea mai mare importanţă pentru activităţile economice şi societale, având drept scop creşterea încrederii cetăţenilor în Piaţa Unică Digitală. În data de 12 ianuarie 2019 a intrat în vigoare *Legea nr.362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice*, lege ce transpune în legislaţia naţională prevederile *Directivei NIS* şi care a transpus obiectivele Strategiei Europene de securitate cibernetică stabilite pentru pilonul NIS. Astfel, Legea nr. 362/2018 prevede: • stabilirea cadrului de cooperare la nivel naţional şi de participare la nivel european şi internaţional în domeniul asigurării securităţii reţelelor şi sistemelor informatice. • desemnarea autorităţilor şi entităţilor de drept public şi privat care deţin competenţe şi responsabilităţi în aplicarea prevederilor legii, a punctului unic de contact la nivel naţional şi a echipei naţionale de răspuns la incidente de securitate informatică. • stabilirea cerinţelor de securitate şi notificare pentru operatorii de servicii esenţiale şi pentru furnizorii de servicii digitale şi instituirea mecanismelor de actualizare a acestora în funcţie de evoluţia ameninţărilor la adresa securităţii reţelelor şi sistemelor informatice. Pentru aplicarea la nivel naţional a prevederilor sale,

	Legea nr.362/2018 desemnează ca autoritate competentă conform art.15 alin (1), punct unic de contact conform art.19 lit. a) şi echipă CSIRT naţională conform art.19 lit. b), Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, denumit în continuare *CERT-RO*, instituţie înfiinţată prin *Hotărârea Guvernului nr.494/2011 privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică – CERT-RO*, modificată şi completată prin *Hotărârea Guvernului nr.584/2019 şi prin Hotărârea Guvernului nr.256/2020.* Amploarea, frecvenţa şi impactul incidentelor de securitate sunt în creştere şi reprezintă o ameninţare gravă pentru funcţionarea reţelelor şi a sistemelor informatice, atât la nivelul Uniunii Europene, cât şi la nivelul României. Implementarea Directivei NIS este de o importanţă deosebită pentru România, prin prisma asigurării unui mediu cibernetic sigur şi desfăşurării activităţilor operatorilor de servicii esenţiale şi a furnizorilor de servicii digitale în condiţii de securitate cibernetică ridicată. Un prim impact naţional al implementării Directivei NIS în România este aplicabilitatea acesteia la nivelul a 7 (şapte) sectoare, respectiv la 12 (douăsprezece) subsectoare economice importante pe piaţa internă, aceleaşi stabilite şi de către Directiva NIS. Implementarea Directivei NIS, reglementarea continuă a domeniului securităţii cibernetice datorată dezvoltărilor tehnologice, impactul naţional a unor potenţiale atacuri cibernetice cu răspândire geografică globală şi necesitatea asigurării unor servicii de intervenţie rapidă pentru limitarea incidentelor, presupune adaptarea CERT-RO, inclusiv a legislaţiei necesare funcţionării acesteia. Pentru îndeplinirea acestor funcţionalităţi Legea nr.362/2018 conferă CERT-RO atribuţii noi, prevăzute detaliat în cuprinsul legii şi prevede totodată o serie de modificări la nivelul organizatoric, precum şi cu privire la finanţarea instituţiei, precum şi o serie de termene de îndeplinire a unui set de obligaţii care curg de la data intrării în vigoare a legii. Prin Legea nr.362/2018 sunt stabilite obligaţii de asigurare a securităţii informatice şi de notificare a incidentelor de securitate survenite la nivelul reţelelor şi sistemelor informatice către autoritatea competentă la nivel naţional desemnată pentru operatorii de servicii esenţiale, denumiţi în continuare *OSE*, o mdin

	sectoarele/subsectoarele de activitate economică prevăzute în anexa legii. Conform art.5 din Legea nr.362/2018 este prevăzută identificarea de către CERT-RO a operatorilor de servicii esențiale subsecvent stabilirii unui set de criterii și valori de prag aferente și înscrierea acestora în Registrul operatorilor de servicii esențiale. În procesul de identificare ca OSE, operatorii economici și celelalte entități care operează ori furnizează servicii în cadrul sectoarelor și subsectoarelor definite în anexa la Legea nr.362/2018 stabilesc calitatea de operator de servicii esențiale având la bază importanța serviciului esențial furnizat, iar pentru această fază a procesului este necesar să evalueze gradul de perturbare a furnizării serviciului esențial în funcție de criteriile intersectoriale și, după caz, de criteriile sectoriale specifice și valorile de prag corespunzătoare fiecărui sector și subsector de activitate. Legea nr.362/2018 prevede la art.6 alin.(3) că se stabilește prin hotărâre a Guvernului în termen de 5 luni de la intrarea în vigoare a legii: a) valorile de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale; b) valorile de prag corespunzătoare criteriilor intersectoriale stabilite potrivit dispozițiilor alin.(2); c) criteriile sectoriale specifice și valorile de prag corespunzătoare fiecărui sector și subsector de activitate prevăzut în anexă; d) normele tehnice de stabilire a impactului incidentelor. De asemenea, pentru stabilirea impactului unui incident Grupul de lucru interinstituțional pentru determinarea valorilor de prag necesare pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale prevăzut la art.6 alin.(4) elaborează și actualizează normele tehnice pentru categoriile de operatori și furnizori prevăzuți de prezenta lege, iar normele tehnice de stabilire a impactului incidentelor se aprobă prin hotărâre a Guvernului. În vederea stabilirii criteriilor și valorilor de prag, prin art.6 alin.(4) a fost este necesară înființarea un grup de lucru inter-instituțional, pentru care prin art.6 alin.(5) se stabilește în sarcina CERT-RO ca, în termen de 3 luni de

	la data intrării în vigoare a legii, să supună aprobării prin hotărâre a Guvernului componența, atribuțiile și modul de organizare a Grupului de lucru interinstituțional prevăzute la alin.(4). Prevederile art.6 alin.(3), (4) și (5) din Legea nr.362/2018, cu modificările și completările ulterioare, nu pot fi aplicabile, având în vedere că sunt unele inadvertențe în textul alin.(3), respectiv literele b) și c), care, în fapt reprezintă subpuncte ale literei a), fapt ce impune modificarea legislației primare. Obligativitatea operaționalizării Grupului de lucru interinstituțional (GdLINIS) este determinată inclusiv de necesitatea continuării implementării la nivel național a Directivei NIS, blocată de lipsa aprobării valorilor de prag și a normelor tehnice pentru stabilirea impactului unui incident, activități aflate în sarcina respectivului grup. *Prin Ordonanța de urgență a Guvernului nr.68/2019 privind stabilirea unor măsuri la nivelul administrației publice centrale și pentru modificarea și completarea unor acte normative, s-au stabilit următoarele:* • Se înființează Ministerul Transporturilor, Infrastructurii și Comunicațiilor prin reorganizarea Ministerului Transporturilor și prin comasarea cu Ministerul Comunicațiilor și Societății Informaționale, prin preluarea activităților și structurilor Ministerului Transporturilor și, respectiv, prin preluarea activităților și structurilor Ministerului Comunicațiilor și Societății Informaționale – art.5 alin.(1). • Ministerul Transporturilor, Infrastructurii și Comunicațiilor preia de la Ministerul Transporturilor și Ministerul Comunicațiilor și Societății Informaționale și exercită orice alte atribuții exercitate de aceste ministere, stabilite potrivit actelor normative în vigoare, acordurilor internaționale sau altor acte încheiate potrivit dispozițiilor legale aplicabile și corespunzătoare activităților preluate – art.5 alin.(3) lit.c). • În cuprinsul actelor normative în vigoare denumirea sintagmele „Ministerul Transporturilor" și „Ministerul Comunicațiilor și Societății Informaționale" se înlocuiesc cu sintagma „Ministerul Transporturilor, Infrastructurii și Comunicațiilor" – art.16 alin.(1) lit.b). Conform art.3 din Ordonanța de urgență a Guvernului

	nr.90/2019, Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, instituție publică cu personalitate juridică, structură independentă de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice, funcționează în coordonarea prim-ministrului. Prin art.II din Ordonanța de urgență a Guvernului nr.4/2020 au fost aprobate următoarele măsuri: ▪ SGG realizează politica Guvernului în domeniul securității cibernetice și stabilește la nivel național strategiile și politicile publice în domeniul securității cibernetice. ▪ CERT-RO va elabora propuneri de acte normative în domeniul său de activitate și le va înainta spre inițiere SGG. ▪ Resursele financiare necesare pentru funcționarea CERT-RO se asigură din venituri proprii și, în completare, din subvenții de la bugetul de stat prin bugetul SGG. *Legea nr.362/2018* conține mai multe prevederi conform cărora MCSI supune aprobării prin hotărâre a Guvernului sau aprobă prin ordin al ministrului comunicațiilor și societății informaționale o serie de reglementări în aplicarea Legii NIS, cu toate că respectivele atribuții au fost preluate de Secretariatul General al Guvernului în baza Ordonanței de urgență a Guvernului nr.4/2020.
2. Schimbări preconizate	Prin propunerea de act normativ se urmărește deblocarea și accelerarea implementării Directivei NIS în România prin operaționalizarea de urgență a Grupului de lucru interinstituțional fapt ce impune modificarea legislației primare. Prezenta Ordonanță de urgență a Guvernului stabilește normele necesare pentru funcționarea Grupului de lucru interinstituțional pentru asigurarea îndeplinirii cerințelor tehnice și obligațiilor stabilite prin Legea nr.362/2018. În vederea îndeplinirii atribuțiilor ce îi revin, Grupul de lucru interinstituțional, denumit în continuare *GdLINIS*, este compus din câte un expert/specialist din cadrul instituțiilor stabilite la art.15 alin.(2) și al autorităților și entităților de reglementare și administrare a sectoarelor și subsectoarelor prevăzute în anexa la Legea nr.362/2018. *GdLINIS* este abilitat să sprijine CERT-RO, autoritatea competentă la nivel național, în ceea ce privește: a) determinarea și actualizarea permanentă a

	valorilor de prag necesare pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul reţelelor şi sistemelor informatice ale operatorilor de servicii esenţiale; b) elaborarea şi actualizarea permanentă a normelor tehnice de stabilire a impactului incidentelor. *CERT-RO*, după consultarea *GdLINIS*, supune aprobării prin hotărâre a Guvernului acte referitoare la următoarele elemente: a) valorile de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul reţelelor şi sistemelor informatice ale operatorilor de servicii esenţiale, prin: i. valorile de prag corespunzătoare criteriilor intersectoriale stabilite potrivit dispoziţiilor alin.(2); ii. criteriile sectoriale specifice şi valorile de prag corespunzătoare fiecărui sector şi subsector de activitate prevăzut în anexă; b) normele tehnice de stabilire a impactului incidentelor. În vederea asigurării unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, în funcţie de necesităţile identificate, sectoarele şi subsectoarele de activitate prevăzute în anexa la Legea nr.362/2018 se pot modifica sau completa prin hotărâre a Guvernului iniţiată de Secretariatul General al Guvernului la propunerea CERT-RO. Totodată, este necesară înlocuirea în cadrul Legii nr.362/2019, a sintagmei „prin ordin al ministrului comunicaţiilor şi societăţii informaţionale" cu sintagma „prin ordin al secretarului general al Guvernului" şi a abrevierii „MCSI" cu sintagma „Secretariatul General al Guvernului", pentru punerea în acord cu arhitectura instituţională existentă în prezent.
3. Alte informaţii	Procesul de implementare a Legii nr. 362/2018 este unul complex, adaptat la nivel naţional şi mult diferit de cel stabilit prin Directiva NIS, care presupune înfiinţarea şi organizarea unor grupuri de lucru şi entităţi specifice, elaborarea actelor subsecvente, identificarea furnizorilor de servicii, stabilirea cerinţelor de securitate cibernetică şi, implicit, operaţionalizarea integrală a legii. La acest moment nu s-a încheiat procesul de aprobare a actelor subsecvente necesare implementării Legii nr.

	362/2018, cu modificările şi completările ulterioare, respectiv constituirea grupului de lucru interinstituţional – specific României ce are strânsă legătură cu identificarea operatorilor de servicii esenţiale, furnizorilor de servicii digitale. Mai mult, sub aspectul urgenţei, având în vedere scrisoarea adresată României de către Comisia Europeană în cauza nr. 2019/2214 (operatori servicii esenţiale) de punere în întârziere, Comisia reclamă încălcarea de către România a obligaţiilor care îi revin în temeiul articolului 5 alineatul (7) din Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune. Termenele stabilite prin Directiva (UE) 2016/1148 nu pot fi respectate de statul român, deşi Legea nr. 362/2018 transpune în totalitate a ceastă directivă. Cauza se datorează procesului greoi de implementare, proces stabilit prin Legea nr. 362/2018, şi a ne operaţionalizării totale a legii. Neîndeplinirea termenelor stabilite prin Directiva (UE) 2016/1148 duce la escaladarea procedurii de infringement, respectiv la trecerea la etapa de judecată la Curtea Europeană de Justiţie şi în final la amendarea României pentru neîndeplinirea obligaţiilor ce decurg din directiva menţionată. Comunicarea Comisiei (2019/C 70/01) privind modificarea metodei de calcul al plăţilor forfetare şi al plăţilor zilnice ale penalităţilor cu titlu cominatoriu propuse de Comisie în cadrul acţiunilor în constatarea neîndeplinirii obligaţiilor în faţa Curţii de Justiţie a Uniunii Europene prevede că în cazul în care România nu îşi îndeplineşte obligaţia de notificare a măsurilor de transpunere a unei directive adoptate sancţiunea financiară aplicată presupune plata unei sume forfetare minimă de 1592 mii EUR. Întârzierea unui singur pas din procesul aplicării legii duce la neimplementarea Directivei NIS la nivel naţional şi afectarea imaginii României pe plan european cauzată de posibilitatea aplicării unor sancţiuni din partea Comisiei Europene.

Secţiunea a 3-a
Impactul socioeconomic al proiectului de act normativ

1. Impactul macroeconomic	Proiectul de act normativ nu se refera la acest subiect.

1[1].Impactul asupra mediului concurențial și domeniului ajutoarelor de stat	Proiectul de act normativ nu se refera la acest subiect.
2. Impactul asupra mediului de afaceri	Proiectul de act normativ nu se refera la acest subiect.
3. Impactul social	Conformarea cu dispozițiile Legii nr.362/2018, precum și limitarea efectelor și a daunelor provocate de incidente sau atacuri cibernetice prin dimensionarea corespunzătoare a autorității.
4. Impactul asupra mediului (***)	Proiectul de act normativ nu se refera la acest subiect.

Secțiunea a 4-a
Impactul financiar asupra bugetului general consolidat, atât pe termen scurt, pentru anul curent, cât și pe termen lung (pe 5 ani)

- mii lei -

Indicatori	**Anul curent**	**Următorii 4 ani**				**Media pe 5 ani**
1	2	3	4	5	6	7
1. Modificări ale veniturilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta:						
(i) impozit pe profit						
(ii) impozit pe venit						
b) bugete locale:						
(i) impozit pe profit						
c) bugetul asigurărilor sociale de stat:						
(i) contribuții de asigurări						
2. Modificări ale cheltuielilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta:						
(i) cheltuieli de personal						
(ii) bunuri si servicii						
b) bugete locale:						
(i) cheltuieli de personal						
(ii) bunuri și servicii						
c) bugetul asigurărilor sociale de stat:						
(i) cheltuieli de personal						

(ii) bunuri si servicii						
3. Impact financiar, plus/minus, din care:						
a) buget de stat						
b) bugete locale						
4. Propuneri pentru acoperirea creşterii cheltuielilor bugetare						
5. Propuneri pentru a compensa reducerea veniturilor bugetare						
6. Calcule detaliate privind fundamentarea modificărilor veniturilor si/sau cheltuielilor bugetare						
7. Alte informaţii	Nu au fost identificate					

Secţiunea a 5-a
Efectele proiectului de act normativ asupra legislaţiei în vigoare

1. Măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ: a) acte normative în vigoare ce vor fi modificate sau abrogate, ca urmare a intrării în vigoare a proiectului de act normativ; b) acte normative ce urmează a fi elaborate în vederea implementării noilor dispoziţii.	Proiectul de act normativ nu se refera la acest subiect.
2. Conformitatea proiectului de act normativ cu legislaţia comunitară în cazul proiectelor ce transpun prevederi comunitare	Articolele aplicabile din Directiva (UE) 2016/1148 a Parlamentului European şi a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune. **Articolul 6 – Efect perturbator semnificativ** (1) La determinarea importanţei unui efect perturbator menţionat la articolul 5 alineatul (2) litera (c), statele membre ţin cont cel puţin de următorii factori transsectoriali: (a) numărul de utilizatori care se bazează pe serviciul furnizat de entitatea în cauză; (b) dependenţa altor sectoare menţionate în

	anexa II de serviciul furnizat de entitatea în cauză; (c) impactul pe care l-ar putea avea incidentele, în ceea ce priveşte intensitatea şi durata, asupra activităţilor economice şi societale sau asupra siguranţei publice; (d) cota de piaţă a entităţii în cauză; (e) distribuţia geografică în ceea ce priveşte zona care ar putea fi afectată de un incident; (f) importanţa entităţii pentru menţinerea unui nivel suficient al serviciului, ţinând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului respectiv. (2) Pentru a stabili dacă un incident ar avea un efect perturbator semnificativ, statele membre ţin cont, după caz, de factorii specifici fiecărui sector. **Articolul 8 – Autorităţile competente la nivel naţional şi punctul unic de contact** ... (2) Autorităţile competente monitorizează aplicarea prezentei directive la nivel naţional. ... (5) Statele membre se asigură că autorităţile competente şi punctele unice de contact dispun de resurse adecvate pentru a-şi îndeplini în mod eficace şi eficient atribuţiile şi a realiza astfel obiectivele prezentei directive. Statele membre asigură cooperarea eficace, eficientă şi sigură a reprezentanţilor desemnaţi în grupul de cooperare. (6) Autorităţile competente şi punctul unic de contact se consultă şi cooperează, după caz şi în conformitate cu dreptul intern, cu autorităţile naţionale de aplicare a legii şi cu autorităţile naţionale de protecţie a datelor relevante. **Articolul 15 – Punere în aplicare şi executare** (1) Statele membre se asigură că autorităţile competente deţin competenţele şi mijloacele necesare pentru a evalua măsura în care operatorii de servicii esenţiale se conformează obligaţiilor care le revin în temeiul articolului

	14, precum şi efectele acesteia asupra securităţii reţelelor şi a sistemelor informatice. (2) Statele membre garantează că autorităţile competente deţin competenţele şi mijloacele pentru a solicita operatorilor de servicii esenţiale să furnizeze: (a) informaţiile necesare pentru evaluarea securităţii reţelelor şi a sistemelor lor informatice, inclusiv politicile de securitate documentate;
3. Măsuri normative necesare aplicării directe a actelor normative comunitare	Proiectul de act normativ nu se refera la acest subiect
4. Hotărâri ale Curţii de Justiţie a Uniunii Europene	Proiectul de act normativ nu se refera la acest subiect
5. Alte acte normative şi/sau documente internaţionale din care decurg angajamente	Proiectul de act normativ nu se refera la acest subiect
6. Alte informaţii	Nu au fost identificate

Secţiunea a 6-a
Consultările efectuate în vederea elaborării proiectului de act normativ

1. Informaţii privind procesul de consultare cu organizaţii neguvernamentale, institute de cercetare şi alte organisme implicate	Nu este cazul.
2. Fundamentarea alegerii organizaţiilor cu care a avut loc consultarea, precum şi a modului în care activitatea acestor organizaţii este legată de obiectul proiectului de act normativ	Nu este cazul.
3. Consultările organizate cu autorităţile administraţiei publice locale, în situaţia în care proiectul de act normativ are ca obiect activităţi ale acestor autorităţi, în condiţiile Hotărârii Guvernului nr.521/2005 privind procedura de consultare a structurilor asociative ale autorităţilor administraţiei publice locale la elaborarea proiectelor de acte normative	Nu este cazul.
4. Consultările desfăşurate în cadrul consiliilor interministeriale, în conformitate cu prevederile Hotărârii Guvernului	Nu este cazul.

nr.750/2005 privind constituirea consiliilor interministeriale permanente	
5. Informaţii privind avizarea de către: a) Consiliul Legislativ b) Consiliul Suprem de Apărare a Ţării c) Consiliul Economic şi Social d) Consiliul Concurenţei e) Curtea de Conturi	Consiliul Legislativ a avizat favorabil proiectul de ordonanţă de urgenţă a Guvernului prin avizul nr. 701/2020.
6. Alte informaţii	Nu au fost identificate.

Secţiunea a 7-a
Activităţi de informare publică privind elaborarea si implementarea proiectului de act normativ

1. Informarea societăţii civile cu privire la necesitatea elaborării proiectului de act normativ	Proiectul a fost iniţiat cu respectarea dispoziţiilor art. 7 alin. (13) ale Legii nr.52/2003 privind transparenţa decizională în administraţia publică, republicată.
2. Informarea societăţii civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum şi efectele asupra sănătăţii şi securităţii cetăţenilor sau diversităţii biologice	Proiectul de act normativ nu se referă la acest subiect
3. Alte informaţii	

Secţiunea a 8-a
Măsuri de implementare

1. Măsurile de punere în aplicare a proiectului de act normativ de către autorităţile administraţiei publice centrale şi/sau locale - înfiinţarea unor noi organisme sau extinderea competentelor instituţiilor existente	
2. Alte informaţii	Nu au fost identificate.

Față de cele prezentate, a fost elaborat proiectul de Lege privind aprobarea Ordonanței de urgență a Guvernului pentru modificarea și completarea Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, pe care îl supunem Parlamentului spre adoptare.

PRIM-MINISTRU

LUDOVIC ORBAN