REGULAMENTUL (UE) 2023/1543 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 12 iulie 2023

privind ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice în cadrul procedurilor penale și pentru executarea pedepselor privative de libertate în urma unor proceduri penale

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 82 alineatul (1),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European ([1]),

hotărând în conformitate cu procedura legislativă ordinară ([2]),

întrucât:

(1) Uniunea și-a stabilit obiectivul de a menține și de a dezvolta un spațiu de libertate, securitate și justiție. În vederea instituirii progresive a unui astfel de spațiu, Uniunea trebuie să adopte măsuri privind cooperarea judiciară în materie penală bazată pe principiul recunoașterii reciproce a hotărârilor judecătorești și a deciziilor judiciare, care este considerat, începând cu Consiliul European de la Tampere din 15-16 octombrie 1999, ca fiind piatra de temelie a cooperării judiciare în materie penală în cadrul Uniunii.

(2) Măsurile care vizează obținerea și păstrarea probelor electronice sunt din ce în ce mai importante pentru anchetele penale și urmăririle penale în întreaga Uniune. Mecanismele eficace de obținere a probelor electronice sunt esențiale pentru combaterea criminalității, iar aceste mecanisme ar trebui să facă obiectul unor condiții și garanții care să asigure deplina conformitate cu drepturile fundamentale și cu principiile recunoscute la articolul 6 din Tratatul privind Uniunea Europeană (TUE) și în Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta"), în special principiile necesității și proporționalității, respectarea garanțiilor procedurale, protecția vieții private, precum și a datelor cu caracter personal și a confidențialității comunicațiilor.

(3) Declarația comună a miniștrilor justiției și afacerilor interne și a reprezentanților instituțiilor Uniunii cu privire la atentatele teroriste din 24 martie 2016 de la Bruxelles a subliniat necesitatea prioritară de a asigura și a obține mai rapid și mai eficient probele electronice și de a identifica măsuri concrete în acest sens.

(4) Concluziile Consiliului din 9 iunie 2016 au accentuat importanța tot mai mare a probelor electronice în cadrul procedurilor penale și importanța protejării spațiului cibernetic împotriva abuzurilor și a activităților infracționale în beneficiul economiilor și al societăților și, prin urmare, necesitatea ca autoritățile de aplicare a legii și autoritățile judiciare să dispună de instrumente eficace în vederea anchetării și a urmării penale a infracțiunilor legate de spațiul cibernetic.

(5) În Comunicarea comună a Comisiei și a Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate către Parlamentul European și Consiliu din 13 septembrie 2017 intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE", Comisia a subliniat că anchetarea și urmărirea penală eficace a infracțiunilor facilitate de calculator reprezintă un factor-cheie de descurajare a atacurilor cibernetice și că actualul cadru procedural trebuie să fie mai bine adaptat la era internetului. Rapiditatea atacurilor cibernetice poate depăși uneori procedurile actuale, creând astfel necesități deosebite de cooperare transfrontalieră rapidă.

(6) Rezoluția Parlamentului European din 3 octombrie 2017 privind combaterea criminalității cibernetice ([3]) a subliniat necesitatea de a găsi mijloace de asigurare și de obținere mai rapidă a probelor electronice, precum și importanța unei cooperări strânse între autoritățile de aplicare a legii, țările terțe și furnizorii de servicii care își desfășoară activitatea pe teritoriul european, în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([4]) și cu Directiva (UE) 2016/680 a Parlamentului European și a

([1]) JO C 367, 10.10.2018, p. 88.
([2]) Poziția Parlamentului European din 13 iunie 2023 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 27 iunie 2023.
([3]) JO C 346, 27.9.2018, p. 29.
([4]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

Consiliului ([5]) și cu acordurile de asistență judiciară reciprocă existente. Respectiva rezoluție a Parlamentului European a accentuat, de asemenea, că actualul cadru juridic fragmentat poate crea provocări pentru furnizorii de servicii care doresc să respecte cererile de aplicare a legii și a solicitat Comisiei să prezinte un cadru juridic al Uniunii privind probele electronice care să conțină garanții suficiente pentru drepturile și libertățile tuturor părților implicate, salutând totodată activitatea în curs a Comisiei în direcția unei platforme de cooperare cu un canal de comunicare securizat între autoritățile judiciare ale Uniunii pentru schimburile digitale de ordine europene de anchetă (OEA) pentru probele electronice și pentru răspunsuri.

(7) Serviciile în rețea pot fi furnizate de oriunde și nu necesită o infrastructură fizică, instalații sau personal în țara în care este oferit serviciul respectiv. Prin urmare, probele electronice relevante sunt adesea stocate în afara statului care desfășoară ancheta sau de către un furnizor de servicii stabilit în afara statului respectiv, ceea ce creează dificultăți legate de obținerea probelor electronice în cadrul procedurilor penale.

(8) Din cauza modului în care sunt furnizate serviciile în rețea, cererile de cooperare judiciară sunt adesea adresate statelor care găzduiesc un număr mare de furnizori de servicii. În plus, numărul de cereri a crescut, pentru că serviciile în rețea sunt utilizate din ce în ce mai mult. Directiva 2014/41/UE a Parlamentului European și a Consiliului ([6]) prevede posibilitatea de emitere a unui OEA pentru strângerea de probe în alt stat membru. În plus, Convenția elaborată de Consiliu în temeiul articolului 34 din Tratatul privind Uniunea Europeană, cu privire la asistența judiciară reciprocă în materie penală între statele membre ale Uniunii Europene ([7]) (denumită în continuare „Convenția privind asistența judiciară reciprocă în materie penală") prevede, de asemenea, posibilitatea de a solicita probe de la un alt stat membru. Cu toate acestea, procedurile și termenele prevăzute în Directiva 2014/41/UE de instituire a OEA și în Convenția privind asistența judiciară reciprocă în materie penală ar putea să nu fie adecvate pentru probele electronice, care sunt mai volatile și ar putea fi șterse mai ușor și mai rapid. Obținerea de probe electronice prin intermediul canalelor de cooperare judiciară necesită adesea un timp îndelungat, conducând adesea la situații în care este posibil ca eventualele indicii să nu mai fie disponibile. De asemenea, nu există un cadru armonizat de cooperare cu furnizorii de servicii, deși anumiți furnizori din țări terțe acceptă cereri directe referitoare la alte date decât cele care se referă la conținut, în măsura în care acest lucru este permis de dreptul lor intern aplicabil. În consecință, statele membre se bazează tot mai mult pe canalele de cooperare directă voluntară cu furnizorii de servicii atunci când acestea sunt disponibile și utilizează diferite instrumente, condiții și proceduri naționale. Pentru datele referitoare la conținut, unele state membre au luat măsuri unilaterale, în timp ce altele continuă să se bazeze pe cooperarea judiciară.

(9) Cadrul juridic fragmentat creează provocări pentru autoritățile de aplicare a legii și autoritățile judiciare, precum și pentru furnizorii de servicii care urmăresc să respecte cererile legale de probe electronice, în condițiile în care aceștia se confruntă tot mai mult cu insecuritate juridică și, eventual, cu conflicte de legi. Prin urmare, este necesar să se prevadă norme specifice în ceea ce privește cooperarea judiciară transfrontalieră pentru conservarea și divulgarea probelor electronice, care să abordeze natura specifică a probelor electronice. Astfel de norme ar trebui să includă o obligație pentru furnizorii de servicii cărora li se aplică prezentul regulament de a răspunde direct cererilor care provin din partea autorităților dintr-un alt stat membru. Prin urmare, prezentul regulament va completa dreptul existent al Uniunii și va clarifica normele aplicabile autorităților de aplicare a legii și autorităților judiciare, precum și furnizorilor de servicii în domeniul probelor electronice, asigurând, în același timp, respectarea deplină a drepturilor fundamentale.

(10) Prezentul regulament respectă drepturile fundamentale și principiile recunoscute la articolul 6 din TUE și în Cartă, în dreptul internațional și acordurile internaționale la care Uniunea sau toate statele membre sunt parte, inclusiv Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, și în constituțiile statelor membre în domeniile lor respective de aplicare. Printre aceste drepturi și principii se numără, în special, dreptul la libertate și la siguranță, respectarea vieții private și de familie, protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială, dreptul de proprietate, dreptul la o cale de atac eficientă și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare, principiile legalității și proporționalității, precum și dreptul de a nu fi judecat sau condamnat de două ori pentru aceeași infracțiune.

([5]) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

([6]) Directiva 2014/41/UE a Parlamentului European și a Consiliului din 3 aprilie 2014 privind ordinul european de anchetă în materie penală (JO L 130, 1.5.2014, p. 1).

([7]) Convenție elaborată de Consiliu în temeiul articolului 34 din Tratatul privind Uniunea Europeană, cu privire la asistența judiciară reciprocă în materie penală între statele membre ale Uniunii Europene (JO C 197, 12.7.2000, p. 3).

(11) Nicio dispoziție din prezentul regulament nu ar trebui interpretată ca o interdicție de a refuza un ordin european de divulgare a probelor electronice de către o autoritate de executare, în cazul în care există motive să se considere, pe baza unor elemente obiective, că ordinul european de divulgare a probelor electronice a fost emis cu scopul de a urmări penal o persoană sau de a-i impune sancțiuni din cauza unor motive precum genul, originea rasială sau etnică, religia, orientarea sexuală sau identitatea de gen, naționalitatea, limba sau opiniile politice sau în cazul în care există motive să se considere că s-ar putea aduce atingere situației persoanei din unul dintre aceste motive.

(12) Mecanismul privind ordinul european de divulgare a probelor electronice și ordinul european de păstrare a probelor electronice în cadrul procedurilor penale se bazează pe principiul asigurării încrederii reciproce între statele membre și pe prezumția de respectare de către statele membre a dreptului Uniunii, a statului de drept și, în special, a drepturilor fundamentale, care reprezintă elemente esențiale ale spațiului de libertate, securitate și justiție al Uniunii. Un astfel de mecanism permite autorităților naționale competente să trimită astfel de ordine direct furnizorilor de servicii.

(13) Respectarea vieții private și de familie și protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal sunt drepturi fundamentale. În conformitate cu articolul 7 și articolul 8 alineatul (1) din Cartă, orice persoană are dreptul la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor, precum și la protecția datelor cu caracter personal care o privesc.

(14) La punerea în aplicare a prezentului regulament, statele membre ar trebui să se asigure că datele cu caracter personal sunt protejate și prelucrate în conformitate cu Regulamentul (UE) 2016/679 și cu Directiva (UE) 2016/680, precum și cu Directiva 2002/58/CE a Parlamentului European și a Consiliului ([8]), inclusiv în cazul folosirii ulterioare, a transmiterii și a transferurilor ulterioare ale datelor obținute.

(15) Datele cu caracter personal obținute în temeiul prezentului regulament ar trebui prelucrate numai când acest lucru este necesar și în mod proporțional cu scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al aplicării pedepselor și al exercitării dreptului la apărare. În special, statele membre ar trebui să se asigure că se aplică politici adecvate de protecție a datelor în cazul transmiterii de date cu caracter personal din partea autorităților relevante către furnizorii de servicii în sensul prezentului regulament, inclusiv măsuri pentru a garanta securitatea datelor. Furnizorii de servicii ar trebui să se asigure că aceleași garanții se aplică pentru transmiterea de date cu caracter personal către autoritățile relevante. Numai persoanele autorizate ar trebui să aibă acces la informații care conțin date cu caracter personal, acces care poate fi obținut prin proceduri de autentificare.

(16) Drepturile procesuale în procedurile penale prevăzute în Directivele 2010/64/UE ([9]), 2012/13/UE ([10]), 2013/48/UE ([11]), (UE) 2016/343 ([12]), (UE) 2016/800 ([13]) și (UE) 2016/1919 ([14]) ale Parlamentului European și ale Consiliului ar trebui să se aplice, în limita domeniului de aplicare al directivelor respective, procedurilor penale care intră sub incidența prezentului regulament în ceea ce privește statele membre care au obligații în temeiul directivelor menționate. Garanțiile procedurale prevăzute de Cartă ar trebui, de asemenea, să se aplice.

(17) Pentru a garanta respectarea deplină a drepturilor fundamentale, valoarea probatorie a probelor obținute în aplicarea prezentului regulament ar trebui să fie evaluată în cadrul procesului de către autoritatea judiciară competentă, în conformitate cu dreptul intern și cu respectarea, în special, a dreptului la un proces echitabil și a dreptului la apărare.

([8]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

([9]) Directiva 2010/64/UE a Parlamentului European și a Consiliului din 20 octombrie 2010 privind dreptul la interpretare și traducere în cadrul procedurilor penale (JO L 280, 26.10.2010, p. 1).

([10]) Directiva 2012/13/UE a Parlamentului European și a Consiliului din 22 mai 2012 privind dreptul la informare în cadrul procedurilor penale (JO L 142, 1.6.2012, p. 1).

([11]) Directiva 2013/48/UE a Parlamentului European și a Consiliului din 22 octombrie 2013 privind dreptul de a avea acces la un avocat în cadrul procedurilor penale și al procedurilor privind mandatul european de arestare, precum și dreptul ca o persoană terță să fie informată în urma privării de libertate și dreptul de a comunica cu persoane terțe și cu autorități consulare în timpul privării de libertate (JO L 294, 6.11.2013, p. 1).

([12]) Directiva (UE) 2016/343 a Parlamentului European și a Consiliului din 9 martie 2016 privind consolidarea anumitor aspecte ale prezumției de nevinovăție și a dreptului de a fi prezent la proces în cadrul procedurilor penale (JO L 65, 11.3.2016, p. 1).

([13]) Directiva (UE) 2016/800 a Parlamentului European și a Consiliului din 11 mai 2016 privind garanțiile procedurale pentru copiii care sunt persoane suspectate sau acuzate în cadrul procedurilor penale (JO L 132, 21.5.2016, p. 1).

([14]) Directiva (UE) 2016/1919 a Parlamentului European și a Consiliului din 26 octombrie 2016 privind asistența juridică gratuită pentru persoanele suspectate și persoanele acuzate în cadrul procedurilor penale și pentru persoanele căutate în cadrul procedurilor privind mandatul european de arestare (JO L 297, 4.11.2016, p. 1).

(18) Prezentul regulament stabilește normele în temeiul cărora o autoritate judiciară competentă a unui stat membru poate, în cadrul procedurilor penale, inclusiv în cadrul anchetelor penale, sau în vederea executării unei pedepse privative de libertate sau a unei măsuri privative de libertate în urma unor proceduri penale în conformitate cu prezentul regulament, să îi ceară unui furnizor de servicii care oferă servicii în Uniune să divulge sau să păstreze probe electronice, prin intermediul unui ordin european de divulgare a probelor electronice sau a unui ordin european de păstrare a probelor electronice. Prezentul regulament ar trebui să se aplice în toate cazurile transfrontaliere în care furnizorul de servicii are sediul desemnat sau reprezentantul legal într-un alt stat membru. Prezentul regulament nu aduce atingere competențelor autorităților naționale de a aborda furnizorii de servicii stabiliți sau reprezentați pe teritoriul lor pentru ca aceștia să se conformeze unor măsuri naționale similare.

(19) Prezentul regulament ar trebui să reglementeze colectarea de date stocate de un furnizor de servicii exclusiv în momentul primirii unui ordin european de divulgare a probelor electronice sau a unui ordin european de păstrare a probelor electronice. Acesta nu ar trebui să prevadă o obligație generală de păstrare a datelor în sarcina furnizorilor de servicii și nu ar trebui să aibă ca efect păstrarea generală și nediferențiată a datelor. De asemenea, prezentul regulament nu ar trebui să autorizeze interceptarea datelor sau obținerea datelor care sunt stocate după primirea unui ordin european de divulgare a probelor electronice sau a unui ordin european de păstrare a probelor electronice.

(20) Aplicarea prezentului regulament nu ar trebui să aducă atingere utilizării criptării de către furnizorii de servicii sau de către utilizatorii acestora. Datele solicitate prin intermediul unui ordin european de divulgare a probelor electronice sau al unui ordin european de păstrare a probelor electronice ar trebui furnizate sau păstrate indiferent dacă sunt sau nu criptate. Cu toate acestea, prezentul regulament nu ar trebui să prevadă nicio obligație pentru furnizorii de servicii de a decripta datele.

(21) În multe cazuri, datele nu mai sunt stocate sau prelucrate în alt mod într-un dispozitiv al utilizatorului, ci sunt puse la dispoziție într-o infrastructură bazată pe „cloud”, care permit accesul de oriunde. Pentru a gestiona aceste servicii, nu este necesar ca furnizorii de servicii să fie stabiliți sau să aibă servere într-o anumită jurisdicție. Prin urmare, aplicarea prezentului regulament nu ar trebui să depindă de localizarea efectivă a formei de stabilire a furnizorului de servicii sau de unitatea de prelucrare sau de stocare a datelor.

(22) Prezentul regulament nu aduce atingere competențelor de anchetare ale autorităților în cadrul procedurilor civile sau administrative, inclusiv atunci când astfel de proceduri pot duce la aplicarea unor sancțiuni.

(23) Întrucât procedurile care vizează acordarea de asistență judiciară reciprocă ar putea fi considerate drept proceduri penale în conformitate cu dreptul intern aplicabil în statele membre, ar trebui să se clarifice faptul că ordinul european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice nu ar trebui emis în scopul furnizării de asistență judiciară reciprocă altui stat membru sau unei țări terțe. În astfel de cazuri, cererea de acordare a asistenței judiciară reciproce ar trebui adresată statului membru sau țării terțe care poate furniza asistența judiciară reciprocă în temeiul dreptului său intern.

(24) În cadrul procedurilor penale, ordinul european de divulgare a probelor electronice și ordinul european de păstrare a probelor electronice ar trebui să fie emise doar în cadrul unor proceduri penale specifice în privința unei infracțiuni concrete care a avut deja loc, în urma unei evaluări individuale a necesității și proporționalității ordinelor respective în fiecare caz în parte, ținând seama de drepturile suspectului sau ale inculpatului.

(25) Prezentul regulament ar trebui să se aplice, de asemenea, procedurilor inițiate de o autoritate emitentă pentru localizarea unei persoane condamnate care s-a sustras justiției, în vederea executării unei pedepse privative de libertate sau a unei măsuri privative de libertate în urma unor proceduri penale. Cu toate acestea, atunci când pedeapsa privativă de libertate sau măsura privativă de libertate a fost aplicată printr-o hotărâre pronunțată în lipsă, nu ar trebui să fie posibil să se emită un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice, întrucât dreptul intern al statelor membre privind hotărârile judecătorești pronunțate în lipsă variază considerabil pe teritoriul Uniunii.

(26) Prezentul regulament ar trebui să se aplice furnizorilor de servicii care oferă servicii în Uniune și ar trebui să fie posibil să se emită ordinele prevăzute în prezentul regulament doar pentru datele referitoare la serviciile oferite în Uniune. Serviciile oferite exclusiv în afara Uniunii nu ar trebui să fie incluse în domeniul de aplicare al prezentului regulament, chiar dacă furnizorul de servicii este stabilit în Uniune. Prin urmare, prezentul regulament nu ar trebui să permită accesul la alte date decât datele referitoare la serviciile oferite utilizatorului din Uniune de către respectivii furnizori de servicii.

(27) Furnizorii de servicii care prezintă cel mai mult interes pentru strângerea de probe în cadrul procedurilor penale sunt furnizorii de servicii de comunicații electronice și anumiți furnizori de servicii ale societății informaționale care facilitează interacțiunea dintre utilizatori. Prin urmare, ambelor categorii ar trebui să li se aplice prezentul regulament. Serviciile de comunicații electronice sunt definite în Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului ([15]) și includ comunicațiile interpersonale, cum ar fi telefonia VOIP, mesageria

([15]) Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (JO L 321, 17.12.2018, p. 36).

instantanee și serviciile de e-mail. Prezentul regulament ar trebui să se aplice totodată și furnizorilor de servicii ale societății informaționale în înțelesul Directivei (UE) 2015/1535 a Parlamentului European și a Consiliului ([16]) care nu se califică drept furnizori de servicii de comunicații electronice, dar care le oferă utilizatorilor lor capacitatea de a comunica între ei sau le oferă servicii care pot fi utilizate pentru a stoca sau prelucra în alt mod date în numele lor. Acest lucru ar fi în conformitate cu termenii utilizați în Convenția Consiliului Europei privind criminalitatea informatică (ETS nr. 185), încheiată la Budapesta la 23 noiembrie 2001 (denumită în continuare „Convenția de la Budapesta"). Prelucrarea datelor ar trebui înțeleasă în sens tehnic, drept crearea sau manipularea de date, cu alte cuvinte operații tehnice prin care se produc sau se modifică date cu ajutorul capacității de procesare a computerelor. Categoriile de furnizori de servicii cărora li se aplică prezentul regulament ar trebui să includă, de exemplu, piețele online care oferă consumatorilor și întreprinderilor posibilitatea de a comunica unii cu alții și alte servicii de găzduire, inclusiv în cazul în care serviciul este furnizat prin intermediul tehnologiei de tip cloud computing, precum și platformele online de jocuri și platformele online de jocuri de noroc. În cazul în care un furnizor de servicii ale societății informaționale nu oferă utilizatorilor săi capacitatea de a comunica între ei, ci numai cu furnizorul de servicii, sau nu oferă capacitatea de a stoca sau prelucra în alt mod date, sau în cazul în care stocarea datelor nu este o componentă definitorie, adică o parte esențială, a serviciului furnizat utilizatorilor, cum ar fi serviciile juridice, de arhitectură, de inginerie și de contabilitate furnizate online la distanță, acesta nu ar trebui să intre în domeniul de aplicare al definiției „furnizorului de servicii" prevăzute în prezentul regulament, chiar dacă serviciile furnizate de furnizorul de servicii respectiv sunt servicii ale societății informaționale în înțelesul Directivei (UE) 2015/1535.

(28) Furnizorii de servicii de infrastructură de internet legate de alocarea de nume și numere, cum ar fi registrele și operatorii de registre de nume de domenii și furnizorii de servicii de protecție a vieții private și de servicii de proxy sau registrele regionale de internet pentru adrese de protocol de internet (IP) sunt deosebit de importanți pentru identificarea actorilor din spatele site-urilor web rău-intenționate sau compromise. Acești furnizori dețin date care ar putea permite identificarea unei persoane sau a unei entități din spatele unui site web utilizat într-o activitate infracțională sau a victimei unei activități infracționale.

(29) Pentru a stabili dacă un furnizor de servicii oferă sau nu servicii în Uniune, este necesară o evaluare din care să reiasă dacă furnizorul de servicii le permite unor persoane fizice sau juridice din unul sau mai multe state membre să utilizeze serviciile sale. Cu toate acestea, simpla accesibilitate a unei interfețe online în Uniune, cum ar fi, de exemplu, accesibilitatea unui site web sau a unei adrese de e-mail sau a altor date de contact ale unui furnizor de servicii sau ale unui intermediar, ar trebui considerată, în sine, insuficientă pentru a stabili că un furnizor de servicii oferă servicii în Uniune în înțelesul prezentului regulament.

(30) O legătură substanțială cu Uniunea ar trebui, de asemenea, să fie relevantă pentru a stabili dacă un furnizor de servicii furnizează servicii în Uniune. Ar trebui să se considere că există o astfel de legătură substanțială cu Uniunea în cazul în care furnizorul de servicii dispune de un sediu în Uniune. În absența unui sediu în Uniune, criteriul privind legătura substanțială ar trebui să fie bazat pe criterii factuale specifice, precum existența unui număr semnificativ de utilizatori în unul sau mai multe state membre sau existența unor activități direcționate către unul sau mai multe state membre. Direcționarea activităților către unul sau mai multe state membre ar trebui stabilită pe baza tuturor circumstanțelor relevante, inclusiv pe baza unor factori precum utilizarea unei limbi sau a unei monede folosite în general în statul membru respectiv sau posibilitatea de a comanda bunuri sau servicii. Direcționarea activităților către un stat membru ar putea să reiasă, de asemenea, din disponibilitatea unei aplicații în magazinul de aplicații naționale relevante, din furnizarea de publicitate locală sau de publicitate în limba folosită în general în statul membru respectiv sau din gestionarea relațiilor cu clienții, de exemplu prin furnizarea de servicii pentru clienți în limba folosită în general în statul membru respectiv. Ar trebui să se considere că există o legătură substanțială și în cazul în care un furnizor de servicii își direcționează activitățile către unul sau mai multe state membre, astfel cum se prevede în Regulamentul (UE) nr. 1215/2012 al Parlamentului European și al Consiliului ([17]). Pe de altă parte, furnizarea unui serviciu în scopul simplei respectări a interdicției de discriminare prevăzute în Regulamentul (UE) 2018/302 al Parlamentului European și al Consiliului ([18]) nu ar trebui considerată, fără motive suplimentare, a fi direcționarea activităților către un anumit teritoriu din cadrul Uniunii. Aceleași considerente ar trebui să se aplice atunci când se stabilește dacă un furnizor de servicii oferă servicii într-un stat membru.

([16]) Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului din 9 septembrie 2015 referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale (JO L 241, 17.9.2015, p. 1).

([17]) Regulamentul (UE) nr. 1215/2012 al Parlamentului European și al Consiliului din 12 decembrie 2012 privind competența judiciară, recunoașterea și executarea hotărârilor în materie civilă și comercială (JO L 351, 20.12.2012, p. 1).

([18]) Regulamentul (UE) 2018/302 al Parlamentului European și al Consiliului din 28 februarie 2018 privind prevenirea geoblocării nejustificate și a altor forme de discriminare bazate pe cetățenia sau naționalitatea, domiciliul sau sediul clienților pe piața internă și de modificare a Regulamentelor (CE) nr. 2006/2004 și (UE) 2017/2394, precum și a Directivei 2009/22/CE (JO L 60I, 2.3.2018, p. 1).

(31) Prezentul regulament ar trebui să acopere categoriile de date constând în date privind abonații, date privind traficul și date referitoare la conținut. Această clasificare este în concordanță cu dreptul multor state membre și cu dreptul Uniunii, cum ar fi Directiva 2002/58/CE, și cu jurisprudența Curții de Justiție, precum și cu dreptul internațional, în special Convenția de la Budapesta.

(32) Adresele IP, precum și numerele de acces și informațiile conexe pot constitui un punct de plecare crucial pentru anchetele penale în care identitatea unui suspect nu este cunoscută. Acestea fac de obicei parte dintr-o înregistrare de evenimente, numită și log al serverului, care indică începerea și încheierea unei sesiuni de acces a unui utilizator la un serviciu. Este adesea o adresă IP individuală, statică sau dinamică, sau un identificator pentru interfața de rețea utilizată în cursul sesiunii de acces. Sunt necesare informații conexe privind începerea și terminarea unei sesiuni de acces a unui utilizator la un serviciu, cum ar fi portalurile-sursă și marca temporală, deoarece adresele IP sunt adesea partajate între utilizatori, de exemplu în cazul în care există o translatare a adreselor de rețea la scară largă (CGN) sau echivalente tehnice. Cu toate acestea, în conformitate cu acquis-ul Uniunii, este necesar ca adresele IP să fie considerate date cu caracter personal și să beneficieze de protecția deplină în temeiul acquis-ului Uniunii privind protecția datelor. În plus, în anumite circumstanțe, adresele IP pot fi considerate date privind traficul. De asemenea, numerele de acces și informațiile conexe sunt considerate date privind traficul în unele state membre. Cu toate acestea, în scopul desfășurării unei anchete penale specifice, s-ar putea ca autoritățile de aplicare a legii să trebuiască să solicite o adresă IP, precum și numere de acces și informații conexe, exclusiv în scopul identificării utilizatorului, înainte de a putea solicita furnizorului de servicii datele privind abonații aferente respectivului identificator. În astfel de cazuri, este oportun să se aplice același regim ca în cazul datelor privind abonații, astfel cum este definit în prezentul regulament.

(33) În cazul în care adresele IP, numerele de acces și informațiile conexe nu sunt solicitate exclusiv în scopul identificării utilizatorului în cadrul unei anchete penale specifice, acestea sunt, în general, solicitate pentru a obține informații mai intruzive asupra vieții private, cum ar fi datele de contact și locul unde se află utilizatorul. Ca atare, acestea ar putea servi la stabilirea unui profil cuprinzător al unei persoane vizate, dar în același timp acestea pot fi prelucrate și analizate mai ușor decât datele referitoare la conținut, deoarece sunt prezentate într-un format structurat și standardizat. Prin urmare, este esențial ca, în astfel de situații, adresele IP, numerele de acces și informațiile conexe care nu sunt solicitate exclusiv în scopul identificării utilizatorului în cadrul unei anchete penale specifice să fie tratate ca date privind traficul și să fie solicitate în cadrul aceluiași regim ca cel al datelor referitoare la conținut, astfel cum sunt definite în prezentul regulament.

(34) Toate categoriile de date conțin date cu caracter personal și, prin urmare, sunt acoperite de garanțiile acordate în temeiul acquis-ului Uniunii în materie de protecție a datelor. Cu toate acestea, intensitatea impactului asupra drepturilor fundamentale diferă între categorii, în special între datele privind abonații și datele solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, pe de o parte, și datele referitoare la trafic, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, și datele referitoare la conținut, pe de altă parte. În timp ce datele privind abonații și adresele IP, numerele de acces și informațiile conexe, atunci când sunt solicitate exclusiv în scopul identificării utilizatorului, ar putea fi utile pentru a obține primele indicii în cadrul unei anchete cu privire la identitatea unui suspect, date referitoare la trafic, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, și datele referitoare la conținut sunt adesea mai relevante ca element probatoriu. Prin urmare, este esențial ca toate aceste categorii de date să fie reglementate de prezentul regulament. Având în vedere gradul variabil de interferență cu drepturile fundamentale, ar trebui să fie prevăzute garanții și condiții adecvate pentru obținerea unor astfel de date.

(35) Situațiile în care există o amenințare iminentă la adresa vieții, a integrității fizice sau a siguranței unei persoane ar trebui să fie tratate ca fiind cazuri de urgență și să presupună termene mai scurte pentru furnizorul de servicii și pentru autoritatea de executare. În cazul în care întreruperea sau distrugerea unei infrastructuri critice, astfel cum este definită în Directiva 2008/114/CE a Consiliului ([19]), ar implica o astfel de amenințare, inclusiv prin prejudicierea gravă a aprovizionării de bază a populației sau a exercitării funcțiilor de bază ale statului, o astfel de situație ar trebui, de asemenea, tratată ca un caz de urgență, în conformitate cu dreptul Uniunii.

(36) Atunci când este emis un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice, ar trebui să intervină întotdeauna o autoritate judiciară fie în procesul de emitere, fie în procesul de validare a ordinului. Având în vedere natura mai sensibilă a datelor privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, și al datelor referitoare la conținut, emiterea sau validarea unui ordin european de divulgare a probelor electronice pentru obținerea acestor categorii de date necesită un control jurisdicțional din partea unui judecător. În plus,

([19]) Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora (JO L 345, 23.12.2008, p. 75).

întrucât datele privind abonații și datele solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, sunt mai puțin sensibile, un ordin european de divulgare a probelor electronice pentru a obține astfel de date poate fi, în plus, emis sau validat de un procuror competent. În conformitate cu dreptul la un proces echitabil, astfel cum este protejat de Cartă și de Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, procurorii își exercită responsabilitățile în mod obiectiv, luând decizii cu privire la emiterea sau validarea unui ordin european de divulgare a probelor electronice sau a unui ordin european de păstrare a probelor electronice numai pe baza elementelor de fapt din dosar și ținând seama de toate probele care incriminează și care dezincriminează.

(37) Pentru a asigura că drepturile fundamentale sunt protejate pe deplin, validarea ordinului european de divulgare a probelor electronice sau a ordinului european de păstrare a probelor electronice de către autoritățile judiciare ar trebui, în principiu, să fie obținută înainte de emiterea ordinului în cauză. Ar trebui să se facă excepții de la acest principiu numai în cazuri de urgență stabilite în mod valabil, atunci când se solicită prezentarea datelor privind abonații sau a datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, sau păstrarea datelor, în cazul în care nu este posibil să se obțină validarea prealabilă de către autoritatea judiciară în timp util, în special deoarece autoritatea de validare nu poate fi contactată pentru a obține validarea, iar amenințarea este atât de iminentă încât trebuie luate măsuri imediate. Cu toate acestea, astfel de excepții ar trebui făcute numai în cazul în care autoritatea care emite ordinul în cauză ar putea emite un ordin într-o cauză internă similară în temeiul dreptului intern fără validare prealabilă.

(38) Un ordin european de divulgare a probelor electronice ar trebui să fie emis doar dacă este necesar, proporțional, adecvat și aplicabil cazului vizat. Autoritatea emitentă ar trebui să țină seama de drepturile suspectului sau ale inculpatului în cadrul procedurilor referitoare la o infracțiune și ar trebui să emită un ordin european de divulgare a probelor electronice numai dacă un astfel de ordin ar fi putut fi emis în aceleași condiții într-o cauză internă similară. Evaluarea privind emiterea unui ordin european de divulgare a probelor electronice ar trebui să ia în considerare dacă ordinul respectiv se limitează la ceea ce este strict necesar pentru a atinge obiectivul legitim de obținere a datelor care sunt relevante și necesare ca mijloace de probă într-un caz individual.

(39) În cazurile în care un ordin european de divulgare a probelor electronice este emis pentru a se obține categorii de date diferite, autoritatea emitentă ar trebui să se asigure că condițiile și procedurile, cum ar fi notificarea autorității de executare, sunt îndeplinite pentru toate categoriile de date respective.

(40) Având în vedere natura mai sensibilă a datelor privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, și al datelor referitoare la conținut, ar trebui să se facă o distincție în ceea ce privește domeniul de aplicare material al prezentului regulament. Ar trebui să fie posibil să se emită un ordin european de divulgare a probelor electronice pentru a obține date privind abonații sau pentru a obține date solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, pentru orice infracțiune, întrucât un ordin european de divulgare a probelor electronice pentru a obține date privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, sau pentru a obține date referitoare la conținut ar trebui să facă obiectul unor cerințe mai stricte pentru a reflecta natura mai sensibilă a acestor date. Prezentul regulament ar trebui să prevadă un prag în ceea ce privește domeniul său de aplicare, care să permită o abordare proporțională, împreună cu o serie de alte condiții și garanții *ex ante* și *ex post* pentru a asigura respectarea proporționalității și a drepturilor persoanelor afectate. În același timp, un asemenea prag nu ar trebui să limiteze eficacitatea prezentului regulament și utilizarea sa de către practicieni. Faptul de a permite ca ordinele europene de divulgare a probelor electronice să fie emise doar în proceduri penale legate de infracțiuni pentru care se prevede o limită maximă a pedepsei privative de libertate de cel puțin trei ani va limita domeniul de aplicare a prezentului regulament la infracțiuni mai grave, fără a afecta excesiv posibilitățile sale de utilizare de către practicieni. Respectiva limitare ar exclude din domeniul de aplicare al prezentului regulament un număr semnificativ de infracțiuni care sunt considerate mai puțin grave de către statele membre, astfel cum reiese din aplicarea unei limite maxime a pedepsei mai reduse. De asemenea, respectiva limitare ar avea avantajul de a fi ușor de aplicat în practică.

(41) Pentru anumite infracțiuni, probele sunt în mod normal disponibile exclusiv în format electronic, care este deosebit de fluid prin natura sa. Acest lucru este valabil pentru infracțiunile conexe mediului informatic, chiar și pentru cele care ar putea să nu fie considerate grave în sine, dar care ar putea provoca pagube extinse sau considerabile, în special infracțiunile cu impact individual redus, dar cu volum ridicat și prejudiciu global. Pentru majoritatea cazurilor în care infracțiunea a fost săvârșită prin intermediul unui sistem informatic, aplicarea aceluiași prag ca și în cazul altor tipuri de infracțiuni ar conduce în mare măsură la impunitate. Acest lucru justifică aplicarea prezentului regulament pentru astfel de infracțiuni și în cazurile în care limita maximă a pedepsei privative de libertate este mai mică de trei ani. Infracțiunile legate de terorism, în înțelesul Directivei (UE) 2017/541 a Parlamentului European și a Consiliului ([20]), precum și infracțiunile de abuz sexual și exploatare

([20]) Directiva (UE) 2017/541 a Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului (JO L 88, 31.3.2017, p. 6).

sexuală a copiilor, în înțelesul Directivei 2011/93/UE a Parlamentului European și a Consiliului ([21]), nu ar trebui să necesite o limită maximă a pedepsei privative de libertate de cel puțin trei ani.

(42) În principiu, un ordin european de divulgare a probelor electronice ar trebui adresat furnizorului de servicii care acționează în calitate de operator. Cu toate acestea, în anumite circumstanțe, stabilirea faptului dacă un furnizor de servicii are rolul de operator sau de persoană împuternicită de operator se poate dovedi deosebit de dificilă, în special în cazul în care mai mulți furnizori de servicii sunt implicați în prelucrarea datelor sau în cazul în care furnizorii de servicii prelucrează datele în numele unei persoane fizice. Distincția între rolul operatorului și cel al persoanei împuternicite de operator în ceea ce privește un anumit set de date necesită nu numai cunoștințe specializate privind contextul juridic, ci ar putea necesita, de asemenea, interpretarea cadrelor contractuale adesea foarte complexe care prevăd, în cazuri specifice, alocarea către diverși furnizori de servicii a unor sarcini și roluri diferite în ceea ce privește un anumit set de date. În cazul în care furnizorii de servicii prelucrează date în numele unei persoane fizice, în unele cazuri poate fi dificil să se stabilească cine este operatorul, chiar și în cazul în care este implicat un singur furnizor de servicii. În cazul în care datele în cauză sunt stocate sau prelucrate în alt mod de către un furnizor de servicii și nu este clar cine este operatorul, în pofida eforturilor rezonabile din partea autorității emitente, ar trebui, prin urmare, să fie posibil să se adreseze un ordin european de divulgare a probelor electronice direct furnizorului de servicii respectiv. În plus, în unele cazuri, abordarea operatorului ar putea fi în detrimentul anchetei în cazul vizat, de exemplu pentru că operatorul are calitatea de suspect sau inculpat sau condamnat sau există indicii că operatorul ar putea acționa în interesul persoanei anchetate. De asemenea, în aceste cazuri, ar trebui să fie posibil să se adreseze un ordin european de divulgare a probelor electronice direct furnizorului de servicii care prelucrează datele în numele operatorului. Acest lucru nu ar trebui să aducă atingere dreptului autorității emitente de a-i impune furnizorului de servicii să păstreze datele.

(43) În conformitate cu Regulamentul (UE) 2016/679, persoana împuternicită de operator care stochează sau prelucrează în alt mod datele în numele operatorului are obligația de a informa operatorul cu privire la divulgarea datelor, cu excepția cazului în care autoritatea emitentă a solicitat furnizorului de servicii să se abțină de la informarea operatorului, atât timp cât este necesar și proporțional, pentru a nu obstrucționa procedurile penale relevante. În acest caz, autoritatea emitentă ar trebui să indice la dosarul cazului motivele pentru care operatorul a fost informat cu întârziere și ar trebui adăugată o scurtă justificare în certificatul asociat transmis destinatarului.

(44) În cazul în care datele sunt stocate sau prelucrate în alt mod ca parte a unei infrastructuri furnizate de un furnizor de servicii unei autorități publice, ar trebui să fie posibil să se emită un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice numai în cazul în care autoritatea publică pentru care datele sunt stocate sau prelucrate în alt mod se află în statul emitent.

(45) În cazurile în care date protejate de secretul profesional în temeiul dreptului statului emitent sunt stocate sau prelucrate în alt mod de către un furnizor de servicii ca parte a unei infrastructuri puse la dispoziția profesioniștilor obligați la păstrarea secretului profesional în considerarea calității lor, ar trebui să fie posibil doar să se emită un ordin european de divulgare a probelor electronice pentru a obține date privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, sau pentru a obține date referitoare la conținut în cazul în care profesionistul obligat la păstrarea secretului profesional își are reședința în statul emitent, în cazul în care adresarea profesionistului obligat la păstrarea secretului profesional ar putea fi în detrimentul anchetei sau în cazul în care privilegiile au fost ridicate în conformitate cu dreptul aplicabil.

(46) Principiul ne bis in idem reprezintă un principiu fundamental în dreptul Uniunii, astfel cum a fost recunoscut de Cartă și dezvoltat de jurisprudența Curții de Justiție a Uniunii Europene. În cazul în care autoritatea emitentă are motive să creadă că ar putea fi în curs proceduri penale paralele într-un alt stat membru, aceasta ar trebui să consulte autoritățile statului membru respectiv, în conformitate cu Decizia-cadru 2009/948/JAI a Consiliului ([22]). În orice caz, nu se emite un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice în cazul în care autoritatea emitentă are motive să creadă că acest lucru ar fi contrar principiului ne bis in idem.

(47) Imunitățile și privilegiile, care se pot referi la categorii de persoane cum ar fi diplomații, sau la raporturi juridice protejate în mod specific, cum ar fi secretul profesional al avocaților sau dreptul jurnaliștilor de a nu-și divulga sursele de informare, sunt menționate în alte instrumente de recunoaștere reciprocă, cum ar fi Directiva 2014/41/UE de instituire a OEA. Sfera de aplicare și impactul imunităților și privilegiilor diferă în funcție de dreptul intern aplicabil care ar trebui luat în considerare la momentul emiterii unui ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice, întrucât autoritatea emitentă ar trebui să poată emite ordinul doar dacă acesta ar fi putut fi emis în aceleași condiții într-o cauză internă similară. În dreptul Uniunii nu există o definiție comună a ceea ce constituie o imunitate sau un privilegiu.

([21]) Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului (JO L 335, 17.12.2011, p. 1).

([22]) Decizia-cadru 2009/948/JAI a Consiliului din 30 noiembrie 2009 privind prevenirea și soluționarea conflictelor referitoare la exercitarea competenței în cadrul procedurilor penale (JO L 328, 15.12.2009, p. 42).

Definiția exactă a acestor termeni este, prin urmare, lăsată la latitudinea dreptului intern, iar definiția poate include măsuri de protecție care se aplică, de exemplu, profesiilor medicale și juridice, inclusiv atunci când sunt utilizate platforme specializate în profesiile respective. Definiția precisă a imunităților și privilegiilor poate include, de asemenea, norme privind stabilirea și limitarea răspunderii penale legate de libertatea presei și libertatea de exprimare în alte mijloace de informare în masă.

(48) În cazul în care autoritatea emitentă urmărește să obțină date privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, sau să obțină date referitoare la conținut, prin emiterea unui ordin european de divulgare a probelor electronice și are motive întemeiate să creadă că datele solicitate sunt protejate de imunitățile sau privilegiile acordate în temeiul dreptului statului de executare sau că datele respective fac, în statul respectiv, obiectul unor norme privind stabilirea și limitarea răspunderii penale legate de libertatea presei și libertatea de exprimare în alte mijloace de informare în masă, autoritatea emitentă ar trebui să poată solicita clarificări înainte de emiterea ordinului european de divulgare a probelor electronice, inclusiv prin consultarea autorităților competente ale statului de executare, fie direct, fie prin intermediul Eurojust sau al Rețelei Judiciare Europene.

(49) Ar trebui să fie posibilă emiterea unui ordin european de păstrare a probelor electronice pentru orice infracțiune. Autoritatea emitentă ar trebui să țină seama de drepturile suspectului sau ale inculpatului în cadrul procedurilor referitoare la o infracțiune și ar trebui să emită un ordin european de păstrare a probelor electronice numai dacă un astfel de ordin ar fi putut fi emis în aceleași condiții într-o cauză internă similară și dacă este necesar, proporțional, adecvat și aplicabil în speță. Evaluarea privind emiterea unui ordin european de păstrare a probelor electronice ar trebui să ia în considerare dacă un astfel de ordin se limitează la ceea ce este strict necesar pentru a atinge obiectivul legitim de a împiedica eliminarea, ștergerea sau modificarea datelor care sunt relevante sau necesare ca probe într-o cauză individuală în situațiile în care ar putea dura mai mult timp obținerea divulgării datelor respective.

(50) Ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice ar trebui să se adreseze direct sediului desemnat sau reprezentantului legal desemnat sau numit de furnizorul de servicii în temeiul Directivei (UE) 2023/1544 a Parlamentului European și a Consiliului ([23]). În mod excepțional, în cazuri de urgență, astfel cum sunt definite în prezentul regulament, în cazul în care sediul desemnat sau reprezentantul legal al unui furnizor de servicii nu reacționează la certificatul de ordin european de divulgare a probelor electronice (EPOC) asociat sau la certificatul de ordin european de păstrare a probelor electronice (EPOC-PR) în termen sau nu a fost încă desemnat sau numit în termenele prevăzute în Directiva (UE) 2023/1544, ar trebui să fie posibil ca EPOC sau EPOC-PR să fie adresat oricărui alt sediu sau reprezentantului legal al furnizorului de servicii în Uniune în paralel cu continuarea executării ordinului inițial în temeiul prezentului regulament sau în locul acestei executări. Luând în considerare aceste diferite scenarii posibile, se utilizează termenul general „destinatar” în cadrul dispozițiilor prezentului Regulament.

(51) Având în vedere natura mai sensibilă a unui ordin european de divulgare a probelor electronice pentru a obține date privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, și pentru a obține date referitoare la conținut, este adecvat să se prevadă un mecanism de notificare aplicabil ordinelor europene de divulgare a probelor electronice pentru a obține respectivele categorii de date. Acest mecanism de notificare ar trebui să implice o autoritate de executare și să constea în transmiterea EPOC către autoritatea respectivă în același timp cu transmiterea EPOC către destinatar. Cu toate acestea, în cazul în care un ordin european de divulgare a probelor electronice este emis pentru a obține probe electronice în cadrul procedurilor penale cu legături substanțiale și puternice cu statul emitent, nu ar trebui să fie necesară notificarea autorității de executare. Ar trebui să se presupună astfel de legături în cazul în care, la momentul emiterii ordinului european de divulgare a probelor electronice, autoritatea emitentă are motive întemeiate să creadă că infracțiunea a fost săvârșită, este săvârșită sau că este probabil să fie săvârșită în statul emitent și dacă persoana ale cărei date sunt solicitate își are reședința în statul emitent.

(52) În sensul prezentului regulament, ar trebui să se considere că o infracțiune a fost săvârșită, este săvârșită sau este probabil să fie săvârșită în statul emitent dacă se consideră astfel în conformitate cu dreptul intern al statului emitent. În unele cazuri, în special în domeniul criminalității informatice, unele elemente de fapt, cum ar fi locul de reședință al victimei, sunt, de obicei, indicii importante care trebuie luate în considerare atunci când se stabilește unde a fost săvârșită infracțiunea. De exemplu, se poate adesea considera că infracțiunile de tip ransomware au fost comise în locul în care își are reședința victima unei astfel de infracțiuni, chiar și atunci când locul exact din care a fost lansat atacul ransomware este incert. Orice determinare a locului în care a fost săvârșită infracțiunea nu ar trebui să aducă atingere normelor privind competența în ceea ce privește infracțiunile relevante în temeiul dreptului intern aplicabil.

([23]) Directiva (UE) 2023/1544 a Parlamentului European și a Consiliului din 12 iulie 2023 de stabilire a unor norme armonizate privind desemnarea sediilor desemnate și numirea reprezentanților legali în scopul obținerii de probe electronice în cadrul procedurilor penale (a se vedea pagina 181 din prezentul Jurnal Oficial).

(53) Revine autorității emitente sarcina de a evalua, la momentul emiterii ordinului european de divulgare a probelor electronice pentru a obține date privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, sau pentru a obține date referitoare la conținut și pe baza elementelor de care dispune, dacă există motive întemeiate să se creadă că persoana ale cărei date sunt solicitate își are reședința în statul emitent. În această privință, pot fi relevante diferite împrejurări obiective care ar putea indica faptul că persoana în cauză și-a stabilit sau intenționează să își stabilească centrul obișnuit al intereselor într-un anumit stat membru. Din necesitatea aplicării uniforme a dreptului Uniunii și din principiul egalității rezultă că noțiunea „reședință” în acest context specific ar trebui să primească o interpretare uniformă în întreaga Uniune. Motive întemeiate pentru a crede că o persoană își are reședința într-un stat emitent ar putea exista, în special, în cazul în care o persoană este înregistrată ca rezident într-un stat emitent, astfel cum se indică prin deținerea unei cărți de identitate sau a un permis de ședere sau prin înregistrarea într-un registru oficial de rezidență. În lipsa înregistrării în statul emitent, reședința ar putea fi indicată prin faptul că o persoană și-a manifestat intenția de a se stabili în statul membru respectiv sau a dobândit, în urma unei prezențe stabile în statul membru respectiv, anumite legături cu acest stat care sunt similare celor care rezultă din stabilirea unei reședințe formale în statul membru respectiv. Pentru a stabili dacă, într-o situație concretă, există legături suficiente între persoana în cauză și statul emitent care dau naștere unor motive verosimile de a crede că persoana în cauză are reședința în acest stat, ar putea fi luate în considerare diferite elemente obiective care caracterizează situația persoanei respective, printre care figurează în special durata, natura și condițiile prezenței persoanei respective în statul emitent sau legăturile de familie sau legăturile economice pe care această persoană le are cu statul membru respectiv. Un vehicul înmatriculat, un cont bancar, faptul că șederea persoanei în statul emitent a fost neîntreruptă sau alți factori obiectivi ar putea fi relevanți pentru a stabili că există motive rezonabile pentru a crede că persoana în cauză își are reședința în statul emitent. O vizită de scurtă durată, o vacanță, inclusiv într-o casă de vacanță, sau o ședere similară în statul emitent fără nicio altă legătură substanțială nu este suficientă pentru a stabili existența unei reședințe în statul membru respectiv. În cazurile în care, la momentul emiterii ordinului european de divulgare a probelor electronice pentru a obține date privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, sau pentru a obține date referitoare la conținut, autoritatea emitentă nu are motive întemeiate să creadă că persoana ale cărei date sunt solicitate își are reședința în statul emitent, autoritatea emitentă ar trebui să notifice acest lucru autorității de executare.

(54) Pentru a asigura celeritatea procedurii, momentul potrivit pentru a se determina dacă este necesară notificarea autorității de executare ar trebui să fie momentul în care este emis ordinul european de divulgare a probelor electronice. Orice schimbare ulterioară a locului de reședință nu ar trebui să aibă niciun impact asupra procedurii. Persoana în cauză ar trebui să își poată invoca drepturile, precum și normele privind stabilirea și limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă, pe parcursul întregii proceduri penale, iar autoritatea de executare ar trebui să poată invoca un motiv de refuz în cazul în care, în situații excepționale, există motive întemeiate să se creadă, pe baza unor dovezi specifice și obiective, că executarea ordinului ar conduce, în circumstanțele specifice ale cazului, o încălcare vădită a unui drept fundamental aplicabil, prevăzut la articolul 6 din TUE și în Cartă. În plus, aceste motive ar trebui să poată fi invocate și în cursul procedurii de executare.

(55) Un ordin european de divulgare a probelor electronice ar trebui transmis prin intermediul unui EPOC, iar un ordin european de păstrare a probelor electronice ar trebui transmis prin intermediul unui EPOC-PR. Dacă este necesar, EPOC sau EPOC-PR ar trebui să fie traduse într-o limbă oficială a Uniunii acceptată de către destinatar. În cazul în care furnizorul de servicii nu a specificat nicio limbă, EPOC sau EPOC-PR ar trebui traduse într-o limbă oficială a statului membru în care se află sediul desemnat sau reprezentantul legal al furnizorului de servicii sau într-o altă limbă oficială pe care sediul desemnat sau reprezentantul legal al furnizorului de servicii a declarat că o va accepta. În cazul în care este necesară o notificare către autoritatea de executare în temeiul prezentului regulament, EPOC care urmează să fie transmis autorității respective ar trebui tradus într-o limbă oficială a statului de executare sau într-o altă limbă oficială a Uniunii acceptată de statul respectiv. În această privință, fiecare stat membru ar trebui încurajat să precizeze, în orice moment, într-o declarație scrisă transmisă Comisiei, dacă și în care limbă sau limbi oficiale ale Uniunii, pe lângă limba sau limbile oficiale ale statului membru respectiv, ar accepta traduceri ale EPOC și ale EPOC-PR. Comisia ar trebui să pună declarațiile respective la dispoziția tuturor statelor membre și a Rețelei Judiciare Europene.

(56) În cazul în care a fost emis un EPOC și nu este necesară o notificare către autoritatea de executare în temeiul prezentului regulament, destinatarul ar trebui să se asigure, la primirea EPOC, că datele solicitate sunt transmise direct autorității emitente sau autorităților de aplicare a legii, astfel cum sunt indicate în EPOC, în termen de cel mult 10 zile de la primirea EPOC. În cazul în care este necesară o notificare către autoritatea de executare în temeiul prezentului regulament, la primirea EPOC, furnizorul de servicii ar trebui să acționeze prompt pentru a asigura păstrarea datelor. În cazul în care autoritatea de executare nu a invocat niciun motiv de refuz în temeiul

prezentului regulament în termen de 10 zile de la primirea EPOC, destinatarul ar trebui să se asigure că datele solicitate sunt transmise direct autorității emitente sau autorităților de aplicare a legii indicate în EPOC, la sfârșitul perioadei de 10 zile. În cazul în care autoritatea de executare, înainte de sfârșitul perioadei de 10 zile, confirmă autorității emitente și destinatarului că nu va invoca niciun motiv de refuz, destinatarul ar trebui să acționeze cât mai curând posibil după o astfel de confirmare și cel târziu la sfârșitul respectivei perioade de 10 zile. Termenele mai scurte aplicabile în cazuri de urgență, astfel cum sunt definite în prezentul regulament, ar trebui să fie respectate de destinatar și, după caz, de autoritatea de executare. Destinatarul și, după caz, autoritatea de executare ar trebui să execute EPOC cât mai curând posibil și cel târziu în termenele stabilite în prezentul regulament, ținând seama cât mai mult posibil de termenele procedurale și de alte termene indicate de statul emitent.

(57) În cazul în care destinatarul consideră, exclusiv pe baza informațiilor conținute în EPOC sau în EPOC-PR, că executarea EPOC sau EPOC-PR ar putea afecta imunitățile sau privilegiile ori normele privind stabilirea sau limitarea răspunderii penale care se referă la libertatea presei sau la libertatea de exprimare în alte mijloace de informare în masă, în temeiul dreptului statului de executare, destinatarul ar trebui să informeze autoritatea emitentă și autoritatea de executare. În ceea ce privește EPOC, în cazul în care autoritatea de executare nu a fost notificată în temeiul prezentului regulament, autoritatea emitentă ar trebui să ia în considerare informațiile primite de la destinatar și să decidă, din proprie inițiativă sau la cererea autorității de executare, dacă retrage, adaptează sau menține ordinul european de divulgare a probelor electronice. În cazul în care autoritatea de executare a fost notificată în temeiul prezentului regulament, autoritatea emitentă ar trebui să ia în considerare informațiile primite de la destinatar și să decidă dacă retrage, adaptează sau menține ordinul european de divulgare a probelor electronice. Ar trebui să fie posibil, de asemenea, ca autoritatea de executare să invoce motivele de refuz prevăzute în prezentul regulament.

(58) Pentru a permite destinatarului să facă față unor probleme formale legate de un EPOC sau un EPOC-PR, este necesar să se instituie o procedură pentru comunicarea dintre destinatar și autoritatea emitentă, precum și, atunci când a fost notificată autoritatea de executare în temeiul prezentului regulament, între destinatar și autoritatea de executare, în cazurile în care EPOC sau EPOC-PR este incomplet, conține erori vădite sau nu conține informații suficiente pentru a executa ordinul în cauză. În plus, în cazul în care destinatarul nu oferă informațiile în mod exhaustiv sau la timp din orice alt motiv, de exemplu întrucât consideră că există un conflict cu o obligație în temeiul dreptului unei țări terțe sau întrucât consideră că ordinul european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice nu a fost emis în conformitate cu condițiile prevăzute în prezentul regulament, acesta ar trebui să informeze autoritatea emitentă, precum și, în cazul în care autoritatea de executare a fost notificată, autorității de executare, și să ofere justificarea pentru neexecutarea EPOC sau a EPOC-PR în timp util. Prin urmare, procedura de comunicare ar trebui să permită corectarea sau reconsiderarea ordinului european de divulgare a probelor electronice sau a ordinului european de păstrare a probelor electronice de către autoritatea emitentă într-un stadiu incipient. Pentru a garanta disponibilitatea datelor solicitate, destinatarul ar trebui să păstreze datele respective în cazul în care destinatarul respectiv poate identifica acele date.

(59) Destinatarul nu ar trebui să fie obligat să respecte ordinul european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice în cazul unei imposibilități de facto generate de împrejurări care nu îi pot fi imputate destinatarului sau, dacă este diferit, furnizorului de servicii la momentul primirii ordinului european de divulgare a probelor electronice sau a ordinului european de păstrare a probelor electronice. O imposibilitate de facto ar trebui prezumată în cazul în care persoana ale cărei date au fost solicitate nu este client al furnizorului de servicii sau nu poate fi identificată ca atare chiar și după transmiterea unei solicitări de informații suplimentare către autoritatea emitentă ori în cazul în care datele au fost șterse în mod legal înainte de primirea ordinului în cauză.

(60) |La primirea unui EPOC-PR, destinatarul ar trebui să păstreze datele solicitate pentru o perioadă maximă de 60 de zile, cu excepția cazului în care autoritatea emitentă confirmă că a fost emisă o solicitare ulterioară de divulgare, caz în care datele ar trebui păstrate în continuare. Autoritatea emitentă ar trebui să poată prelungi durata păstrării cu încă 30 de zile, dacă acest lucru este necesar pentru a permite emiterea unei cereri ulterioare de divulgare, utilizând formularul prevăzut în prezentul regulament. Atunci când autoritatea emitentă confirmă în timpul perioadei de păstrare că a fost emisă o cerere ulterioară de divulgare, destinatarul ar trebui să păstreze datele atât timp cât este necesar pentru a divulga datele, odată primită cererea ulterioară de divulgare. O astfel de confirmare ar trebui trimisă destinatarului în termenul relevant, într-o limbă oficială a statului de executare sau în orice altă limbă acceptată de destinatar, utilizând formularul prevăzut în prezentul regulament. Pentru a împiedica încetarea păstrării, ar trebui să fie suficient ca cererea ulterioară de divulgare să fi fost emisă și confirmarea să fi fost trimisă de către autoritatea emitentă; nu ar trebui să fie necesară îndeplinirea altor formalități necesare pentru transmitere, cum ar fi traducerea documentelor, la momentul respectiv. În cazul în care păstrarea datelor nu mai este necesară, autoritatea emitentă ar trebui să informeze destinatarul fără întârzieri nejustificate, iar obligația de a păstra datele, care decurge din ordinul european de păstrare a probelor electronice, ar trebui să înceteze.

(61) În pofida principiului încrederii reciproce, ar trebui să fie posibil ca autoritatea de executare să invoce motive de refuz al unui ordin european de divulgare a probelor electronice, în cazul în care a avut loc o notificare către autoritatea de executare în temeiul prezentului regulament, pe baza listei motivelor de refuz prevăzute în prezentul regulament. În cazul în care o notificare către autoritatea de executare sau executarea are loc în conformitate cu prezentul regulament, statul de executare ar putea prevedea în dreptul său intern ca executarea unui ordin european de divulgare a probelor electronice ar putea necesita implicarea procedurală a unei instanțe din statul de executare.

(62) În cazul în care autoritatea de executare este notificată cu privire la un ordin european de divulgare a probelor electronice pentru a obține date privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite în prezentul regulament, sau pentru a obține date referitoare la conținut, aceasta ar trebui să aibă dreptul de a evalua informațiile prevăzute în ordin și, după caz, de a le refuza în cazul în care, pe baza unei analize obligatorii și corespunzătoare a informațiilor conținute în ordinul respectiv și cu respectarea normelor aplicabile ale dreptului primar al Uniunii, în special Carta, ajunge la concluzia că ar putea fi invocat unul sau mai multe dintre motivele de refuz prevăzute în prezentul regulament. Necesitatea de a respecta independența autorităților judiciare impune ca acestora să li se acorde o anumită marjă de apreciere atunci când iau decizii cu privire la motivele de refuz.

(63) Ar trebui să fie posibil ca autoritatea de executare, atunci când este notificată în temeiul prezentului regulament, să refuze un ordin european de divulgare a probelor electronice în cazul în care datele solicitate sunt protejate de imunități sau privilegii acordate în temeiul dreptului statului de executare, care împiedică executarea sau asigurarea executării ordinului european de divulgare a probelor electronice, sau în cazul în care datele solicitate sunt reglementate de norme privind stabilirea sau limitarea răspunderii penale care se referă la libertatea presei sau la libertatea de exprimare în alte mijloace de informare în masă, care împiedică executarea sau asigurarea executării ordinului european de divulgare a probelor electronice.

(64) Ar trebui să fie posibil ca autoritatea de executare, în situații excepționale, atunci când există motive întemeiate să se creadă, pe baza unor dovezi specifice și obiective, că executarea ordinului european de divulgare a probelor electronice ar implica, în circumstanțele specifice ale cazului, o încălcare vădită a unui drept fundamental aplicabil, prevăzut la articolul 6 din TUE și în Cartă. În special, atunci când evaluează acest motiv de refuz, în cazul în care autoritatea de executare dispune de elemente de probă sau de elemente precum cele prezentate într-o propunere motivată a unei treimi dintre statele membre, a Parlamentului European sau a Comisiei Europene, adoptată în temeiul articolului 7 alineatul (1) din TUE, care indică existența unui risc clar, în cazul executării ordinului, de încălcare gravă a dreptului fundamental la o cale de atac eficientă și la un proces echitabil în temeiul articolului 47 din Cartă, ca urmare a unor deficiențe sistemice sau generalizate în ceea ce privește independența puterii judecătorești a statului emitent, autoritatea de executare ar trebui să stabilească în mod concret și precis dacă, având în vedere situația personală a persoanei în cauză, precum și natura infracțiunii în legătură cu care se desfășoară procedura penală și contextul de fapt care stă la baza ordinului și având în vedere informațiile furnizate de autoritatea emitentă, există motive serioase și întemeiate de a crede că există un risc de încălcare a dreptului unei persoane la un proces echitabil.

(65) Autoritatea de executare ar trebui să aibă posibilitatea de a refuza un ordin în cazul în care executarea unui astfel de ordin ar fi contrară principiului ne bis in idem.

(66) Ar trebui să fie posibil ca autoritatea de executare, atunci când este notificată în temeiul prezentului regulament, să refuze un ordin european de divulgare a probelor electronice, în cazul în care fapta pentru care a fost emis ordinul nu constituie o infracțiune în temeiul dreptului statului de executare, cu excepția cazului în care se referă la o infracțiune din categoriile de infracțiuni stabilite într-o anexă la prezentul regulament, astfel cum este indicată de autoritatea emitentă în EPOC, dacă fapta respectivă este sancționabilă în statul emitent cu o pedeapsă privativă de libertate sau cu o măsură privativă de libertate pentru o perioadă maximă de cel puțin trei ani.

(67) Întrucât informarea persoanei ale cărei date sunt solicitate este un element esențial al respectării drepturilor în materie de protecție a datelor și al dreptului la apărare, pentru că permite un control eficace și o cale de atac judiciară, în conformitate cu articolul 6 din TUE și cu Carta, autoritatea emitentă ar trebui să informeze persoana ale cărei date sunt solicitate, fără întârzieri nejustificate, cu privire la divulgarea datelor respective în temeiul unui ordin european de divulgare a probelor electronice. Cu toate acestea, autoritatea emitentă ar trebui să poată, în conformitate cu dreptul intern, să amâne sau să restricționeze informarea ori să nu informeze persoana ale cărei date sunt solicitate, în măsura în care și atât timp cât sunt îndeplinite condițiile din Directiva (UE) 2016/680, caz în care autoritatea emitentă ar trebui să indice în dosarul cauzei motivele întârzierii, restricționării sau neinformării și să adauge o justificare succintă în EPOC. Destinatarii și furnizorii de servicii, dacă aceștia sunt persoane diferite, ar trebui să ia măsurile operaționale și tehnice necesare cele mai avansate pentru a asigura confidențialitatea, caracterul secret și integritatea EPOC sau EPOC-PR și ale datelor divulgate sau păstrate.

(68) Ar trebui ca un furnizor de servicii să poată solicita statului emitent rambursarea costurilor suportate pentru a răspunde unui ordin european de divulgare a probelor electronice sau unui ordin european de păstrare a probelor electronice, dacă această posibilitate este prevăzută în dreptul intern al statului emitent pentru ordinele naționale în situații similare, în conformitate cu dispozițiile de drept intern ale statului respectiv. Statele membre ar trebui să informeze Comisia cu privire la normele lor interne de rambursare, iar Comisia ar trebui să le facă publice. Prezentul regulament prevede norme separate aplicabile rambursării costurilor legate de sistemul informatic descentralizat.

(69) Fără a aduce atingere legislațiilor naționale care prevăd impunerea de sancțiuni penale, statele membre ar trebui să stabilească normele privind sancțiunile pecuniare aplicabile în caz de nerespectare a prezentului regulament și să ia toate măsurile necesare pentru a se asigura că acestea sunt puse în aplicare. Statele membre ar trebui să se asigure că sancțiunile pecuniare prevăzute în dreptul intern sunt efective, proporționale și au efect de descurajare. Statele membre ar trebui să notifice Comisiei normele și măsurile respective fără întârziere și ar trebui să îi notifice, fără întârziere, orice modificare ulterioară a acestora.

(70) Atunci când, într-un caz individual, analizează care sunt sancțiunile pecuniare adecvate, autoritățile competente ar trebui să ia în considerare toate circumstanțele relevante, cum ar fi natura, gravitatea și durata încălcării, dacă aceasta a fost comisă intenționat sau din neglijență, dacă furnizorul de servicii a mai fost tras la răspundere pentru încălcări anterioare similare, precum și capacitatea financiară a furnizorului de servicii considerat răspunzător. În circumstanțe excepționale, analiza respectivă ar putea determina autoritatea de executare să decidă să se abțină de la impunerea oricăror sancțiuni pecuniare. În acest sens, se acordă o atenție deosebită microîntreprinderilor care nu respectă un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice într-un caz de urgență din cauza lipsei de resurse umane în afara orelor de program, dacă datele sunt transmise fără întârzieri nejustificate.

(71) Fără a aduce atingere obligațiilor de protecție a datelor, furnizorii de servicii nu ar trebui să fie considerați răspunzători în statele membre pentru prejudicii aduse utilizatorilor lor sau unor terți care rezultă exclusiv din respectarea cu bună-credință a unui EPOC sau a unui EPOC-PR. Responsabilitatea de a asigura legalitatea ordinului în cauză, în special în ceea ce privește caracterul său necesar și proporțional, ar trebui să revină autorității emitente.

(72) Atunci când destinatarul nu se conformează unui EPOC în termenul stabilit sau unui EPOC-PR, fără a oferi motive acceptate de autoritatea emitentă, și, după caz, atunci când autoritatea de executare nu a invocat niciunul dintre motivele de refuz prevăzute în prezentul regulament, autoritatea emitentă ar trebui să poată solicita autorității de executare să execute ordinul european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice. În acest scop, autoritatea emitentă ar trebui să transfere autorității de executare ordinul în cauză, formularul relevant prevăzut în prezentul regulament, astfel cum a fost completat de destinatar, precum și orice document relevant. Autoritatea emitentă ar trebui să traducă ordinul în cauză și orice document ce urmează să fie transferat într-una dintre limbile acceptate de statul de executare și ar trebui să informeze destinatarul cu privire la transfer. Statul respectiv ar trebui să execute ordinul în cauză în conformitate cu dreptul său intern.

(73) Procedura de executare ar trebui să permită destinatarului să invoce motive împotriva executării, pe baza unei liste de motive specifice prevăzute în prezentul regulament, inclusiv faptul că ordinul în cauză nu a fost emis sau validat de o autoritate competentă, astfel cum se prevede în prezentul regulament, sau atunci când ordinul nu privește date stocate de furnizorul de servicii sau în numele acestuia în momentul primirii certificatului relevant. Autoritatea de executare ar trebui să poată refuza să recunoască și să execute un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice pe baza acelorași motive și, de asemenea, în situații excepționale, din cauza încălcării vădite a unui drept fundamental relevant, astfel cum se prevede la articolul 6 din TUE și în Cartă. Autoritatea de executare ar trebui să se consulte autoritatea emitentă înainte de a decide să nu recunoască sau să nu execute ordinul, pe baza motivelor respective. Atunci când destinatarul nu respectă obligațiile care îi revin în temeiul unui ordin european de divulgare a probelor electronice recunoscut sau al unui ordin european de păstrare a probelor electronice recunoscut, al cărui caracter executoriu a fost confirmat de autoritatea de executare, autoritatea respectivă ar trebui să impună o sancțiune pecuniară. Sancțiunea respectivă ar trebui să fie proporțională mai ales ținând seama de circumstanțe specifice cum ar fi nerespectarea repetată sau sistemică a ordinelor.

(74) Respectarea unui ordin european de divulgare a probelor electronice ar putea intra în conflict cu o obligație în temeiul dreptului aplicabil al unei țări terțe. Pentru a garanta respectarea intereselor suverane ale țărilor terțe, pentru a proteja persoanele în cauză și pentru a face față obligațiilor contradictorii care le revin furnizorilor de servicii, prezentul regulament prevede un mecanism specific de control jurisdicțional în cazul în care respectarea unui ordin european de divulgare a probelor electronice ar împiedica un furnizor de servicii să respecte obligațiile legale ce rezultă din dreptul unei țări terțe.

(75) Atunci când destinatarul consideră că un ordin european de divulgare a probelor electronice într-un anume caz ar duce la încălcarea unei obligații legale care decurge din dreptul unei țări terțe, acesta ar trebui să informeze autoritatea emitentă și autoritatea de executare cu privire la motivele sale pentru neexecutarea ordinului prin intermediul unei obiecții motivate, utilizând formularul prevăzut în prezentul regulament. Autoritatea emitentă ar trebui să reexamineze ordinul european de divulgare a probelor electronice pe baza obiecției motivate și a oricărei contribuții prevăzute de statul de executare, luând în considerare aceleași criterii pe care ar trebui să le aibă în vedere instanța competentă din statul emitent. În cazul în care autoritatea emitentă intenționează să mențină ordinul, aceasta ar trebui să solicite o reexaminare de către instanța competentă din statul emitent, astfel cum a fost notificată de către statul membru în cauză, care ar trebui să reexamineze ordinul.

(76) În vederea stabilirii existenței unei obligații contradictorii în circumstanțele specifice ale cazului care face obiectul examinării, instanța competentă ar putea să se bazeze, dacă este necesar, pe o consultanță specializată externă adecvată, de exemplu cu privire la interpretarea dreptului din țara terță în cauză. În acest scop, instanța competentă ar putea, de exemplu, să consulte autoritatea centrală a țării terțe, ținând seama de Directiva (UE) 2016/680. Ar trebui, în special, ca statul emitent să solicite informații de la autoritatea competentă a țării terțe în cazul în care contradicția se referă la drepturile fundamentale sau la alte interese fundamentale ale țării terțe legate de securitatea și apărarea națională.

(77) Consultanța de specialitate în materie de interpretare ar putea fi furnizată, de asemenea, prin intermediul unor avize ale experților, în cazul în care acestea sunt disponibile. Informațiile și jurisprudența privind interpretarea dreptului unei țări terțe și privind procedurile în materie de conflicte de legi în statele membre ar trebui să fie puse la dispoziție pe o platformă centrală, cum ar fi proiectul SIRIUS sau Rețeaua Judiciară Europeană, pentru a putea beneficia de experiența și de cunoștințele de specialitate acumulate cu privire la aceleași aspecte sau la aspecte similare. Punerea la dispoziție a acestor informații pe o platformă centrală nu ar trebui să împiedice o nouă consultare a țării terțe, dacă este cazul.

(78) Atunci când evaluează dacă există obligații contradictorii, instanța competentă ar trebui să stabilească dacă dreptul țării terțe este aplicabil și, în caz afirmativ, dacă dreptul țării terțe interzice divulgarea datelor în cauză. În cazul în care instanța competentă stabilește că dreptul țării terțe interzice divulgarea datelor în cauză, instanța respectivă ar trebui să decidă dacă să se mențină sau să se revoce ordinul european de divulgare a probelor electronice, luând în considerare o serie de elemente care urmăresc să stabilească soliditatea legăturii cu una dintre cele două jurisdicții implicate, interesele privind obținerea, respectiv împiedicarea divulgării datelor și posibilele consecințe pentru destinatar sau pentru furnizorul de servicii ale respectării obligației de se conforma ordinului. Atunci când se efectuează evaluarea, ar trebui să se acorde o importanță și o greutate deosebite protecției drepturilor fundamentale de către dreptul țării terțe și altor interese fundamentale, cum ar fi interesele în materie de securitate națională ale țării terțe, precum și gradului de legătură dintre cauza penală și oricare dintre cele două jurisdicții. În cazul în care instanța decide să revoce ordinul, aceasta ar trebui să informeze autoritatea emitentă și destinatarul. Dacă instanța competentă stabilește că ordinul trebuie menținut, aceasta ar trebui să informeze autoritatea emitentă și destinatarul, iar destinatarul respectiv ar trebui să treacă la executarea ordinului. Autoritatea emitentă ar trebui să informeze autoritatea de executare cu privire la rezultatul procedurii de reexaminare.

(79) Condițiile prevăzute în prezentul regulament pentru executarea unui EPOC ar trebui să se aplice, de asemenea, în cazul în care există obligații contradictorii care derivă din dreptul unei țări terțe. Prin urmare, în cursul controlului jurisdicțional, în care respectarea unui ordin european de divulgare a probelor electronice ar împiedica furnizorii de servicii să respecte o obligație legală care decurge din dreptul unei țări terțe, datele solicitate prin ordinul respectiv ar trebui păstrate. În cazul în care, în urma controlului jurisdicțional, instanța competentă decide să revoce un ordin european de divulgare a probelor electronice, ar trebui să fie posibil să se emită un ordin european de păstrare a probelor electronice pentru a permite autorității emitente să solicite divulgarea datelor prin alte canale, cum ar fi asistența judiciară reciprocă.

(80) Este esențial ca toate persoanele ale căror date sunt solicitate în cursul anchetelor sau al procedurilor penale să aibă acces la o cale de atac eficientă, în conformitate cu articolul 47 din Cartă. În conformitate cu această cerință și fără a aduce atingere altor căi de atac disponibile în conformitate cu dreptul intern, orice persoană ale cărei date au fost solicitate printr-un ordin european de divulgare a probelor electronice ar trebui să aibă dreptul la căi de atac eficiente împotriva ordinului respectiv. În cazul în care persoana respectivă are calitatea de suspect sau inculpat, aceasta ar trebui să aibă dreptul la căi de atac eficiente în cursul procedurilor penale în care datele sunt folosite ca mijloace de probă. Dreptul la căi de atac eficiente ar trebui exercitat în fața unei instanțe din statul emitent în conformitate cu dreptul său intern și ar trebui să includă posibilitatea de a contesta legalitatea măsurii în cauză, inclusiv necesitatea și proporționalitatea sa, fără a se aduce atingere garanțiilor legate de drepturile fundamentale din statul de executare sau altor căi de atac existente în conformitate cu dreptul intern. Prezentul regulament nu ar trebui să limiteze motivele posibile pentru contestarea legalității unui ordin. Dreptul la căi de atac eficiente prevăzut în prezentul regulament nu ar trebui să aducă atingere dreptului de a recurge la căi de atac în temeiul Regulamentului (UE) 2016/679 și al Directivei (UE) 2016/680. Ar trebui furnizate informații în timp util cu privire la posibilitățile de a recurge la căi de atac în temeiul dreptului intern și ar trebui să se asigure faptul că acestea pot fi exercitate în mod eficient.

(81) Ar trebui dezvoltate canale adecvate pentru a se asigura faptul că toate părțile pot coopera eficient prin mijloace digitale, prin intermediul unui sistem informatic descentralizat care să permită schimbul electronic transfrontalier rapid, direct, interoperabil, durabil, fiabil și sigur de formulare, date și informații legate de cauze.

(82) Pentru a permite o comunicare scrisă eficientă și sigură între autoritățile competente și sediile desemnate sau reprezentanții legali ai furnizorilor de servicii în temeiul prezentului regulament, respectivelor sedii desemnate sau respectivilor reprezentanți legali ar trebui să li se pună la dispoziție mijloace electronice de acces la sistemele informatice naționale, care fac parte din sistemul informatic descentralizat, operate de statele membre.

(83) Sistemul informatic descentralizat ar trebui să fie alcătuit din sistemele informatice ale statelor membre și ale agențiilor și organelor Uniunii și din puncte de acces interoperabile prin care sistemele informatice respective să fie interconectate. Punctele de acces ale sistemului informatic descentralizat ar trebui să se bazeze pe sistemul e-CODEX, instituit prin Regulamentul (UE) 2022/850 al Parlamentului European și al Consiliului ([24]).

(84) Furnizorilor de servicii care folosesc soluții informatice personalizate în scopul schimbului de informații și de date legate de cererile de probe electronice ar trebui să li se pună la dispoziție mijloace automatizate de accesare a sistemelor informatice descentralizate prin intermediul unui standard comun de schimb de date.

(85) Ca regulă generală, orice comunicare în scris între autoritățile competente sau între autoritățile competente și sediile desemnate sau reprezentanții legali ar trebui să aibă loc prin intermediul sistemului informatic descentralizat. Ar trebui să fie posibilă utilizarea unor mijloace alternative numai atunci când utilizarea sistemului informatic descentralizat nu este posibilă, de exemplu din cauza unor cerințe specifice în materie de expertiză criminalistică, din cauză că transferul volumului de date în cauză este împiedicat de constrângeri legate de capacitatea tehnică sau din cauza faptului că un alt sediu care nu este conectat la sistemul informatic descentralizat trebuie să fie contactat într-o situație de urgență. În astfel de cazuri, transmiterea ar trebui efectuată prin cele mai adecvate mijloace alternative, ținând seama de necesitatea de a asigura un schimb de informații rapid, sigur și fiabil.

(86) Pentru a asigura faptul că sistemul informatic descentralizat conține o evidență completă a schimburilor scrise în temeiul prezentului regulament, orice transmitere efectuată prin mijloace alternative ar trebui înregistrată în sistemul informatic descentralizat fără întârzieri nejustificate.

(87) Ar trebui luată în calcul folosirea mecanismelor de asigurare a autenticității, astfel cum se prevede în Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului ([25]).

(88) Furnizorii de servicii, în special întreprinderile mici și mijlocii, nu ar trebui să fie expuși unor costuri disproporționate în ceea ce privește instituirea și funcționarea sistemului informatic descentralizat. Prin urmare, în cadrul creării, întreținerii și dezvoltării implementării de referință, Comisia trebuie, de asemenea, să pună la dispoziție o interfață web care să permită furnizorilor de servicii să comunice în siguranță cu autoritățile fără a trebui să își stabilească propria infrastructură specifică pentru a accesa sistemul informatic descentralizat.

(89) Ar trebui să fie posibil ca statele membre să folosească software-ul dezvoltat de Comisie, și anume software-ul de implementare de referință, în locul unui sistem informatic național. Este necesar ca respectivul software de implementare de referință să se bazeze pe o configurație modulară, și anume ca software-ul să fie structurat și livrat separat de componentele sistemului e-CODEX necesare pentru a-l conecta la sistemul informatic descentralizat. Configurația respectivă ar trebui să le permită statelor membre să reutilizeze sau să îmbunătățească infrastructurile lor naționale de comunicare judiciară existente în scopul utilizării transfrontaliere.

(90) Comisia ar trebui să fie responsabilă de crearea, întreținerea și dezvoltarea software-ului de implementare de referință. Comisia ar trebui să proiecteze, să dezvolte și să întrețină software-ul de implementare de referință respectând cerințele și principiile în materie de protecție a datelor stabilite în Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([26]), în Regulamentul (UE) 2016/679 și în Directiva (UE) 2016/680, în special principiul protecției datelor din faza de proiectare și principiul protecției datelor în mod implicit, precum și un nivel ridicat de securitate cibernetică. De asemenea, este important ca software-ul de implementare de referință să includă măsuri tehnice adecvate și să permită luarea măsurilor organizatorice necesare pentru asigurarea unui nivel adecvat de securitate și interoperabilitate.

([24]) Regulamentul (UE) 2022/850 al Parlamentului European și al Consiliului din 30 mai 2022 privind un sistem informatizat pentru schimbul electronic transfrontalier de date în domeniul cooperării judiciare în materie civilă și penală (sistemul e-CODEX) și de modificare a Regulamentului (UE) 2018/1726 (JO L 150, 1.6.2022, p. 1).

([25]) Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73).

([26]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

(91) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, ar trebui conferite competențe de executare Comisiei. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([27]).

(92) Pentru schimburile de date efectuate prin intermediul sistemului informatic descentralizat sau înregistrate în sistemul informatic descentralizat, statele membre ar trebui să poată colecta statistici pentru a-și îndeplini obligațiile de monitorizare și de raportare care le revin în temeiul prezentului regulament prin intermediul portalurilor lor naționale.

(93) Pentru a monitoriza realizările, rezultatele și impactul prezentului regulament, Comisia ar trebui să publice un raport anual cu privire la anul calendaristic precedent, pe baza datelor obținute de la statele membre. În acest scop, statele membre ar trebui să colecteze și să furnizeze Comisiei statistici cuprinzătoare privind diferite aspecte ale prezentului regulament, în funcție de tipul de date solicitate, de destinatari și de tipul situației, precum și de existența sau nu a unui caz de urgență.

(94) Utilizarea de formulare pretraduse și standardizate ar înlesni cooperarea și schimbul de informații în temeiul prezentului regulament, permițând astfel o comunicare mai rapidă și mai eficace într-un mod ușor de utilizat. Astfel de formulare ar reduce costurile de traducere și ar contribui la un nivel ridicat de calitate a comunicării. În mod similar, formularele de răspuns ar face posibil un schimb standardizat de informații, în special în cazul în care furnizorii de servicii nu sunt în măsură să se conformeze, întrucât contul respectiv de utilizator nu există sau datele nu sunt disponibile. De asemenea, formularele prevăzute în prezentul regulament ar înlesni colectarea de statistici.

(95) Pentru a răspunde în mod eficace unei posibile necesități de îmbunătățire în ceea ce privește conținutul formularelor EPOC și EPOC-PR și al formularelor care trebuie folosite pentru a furniza informații cu privire la imposibilitatea de a executa un EPOC sau un EPOC-PR, pentru a confirma emiterea unei cereri de divulgare în urma unui ordin european de păstrare a probelor electronice și pentru a prelungi termenul de păstrare a probelor electronice, competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene (TFUE) ar trebui delegată Comisiei în ceea ce privește modificarea formularelor prevăzute în prezentul regulament. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare ([28]). În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(96) Prezentul regulament nu ar trebui să aducă atingere altor instrumente, acorduri și înțelegeri ale Uniunii și internaționale privind strângerea de probe care intră sub incidența prezentului regulament. Autoritățile statelor membre ar trebui să aleagă instrumentul cel mai adaptat cazului vizat. În unele cazuri, acestea ar putea prefera să utilizeze instrumente, acorduri și înțelegeri ale Uniunii și internaționale atunci când solicită o serie de diferite tipuri de măsuri de anchetare, care nu se limitează la divulgarea de probe electronice din partea unui alt stat membru. În termen de cel mult trei ani de la data intrării în vigoare a prezentului regulament, statele membre ar trebui să informeze Comisia cu privire la instrumentele, acordurile și înțelegerile existente menționate în prezentul regulament pe care vor continua să le aplice. De asemenea, statele membre ar trebui să informeze Comisia în termen de trei luni cu privire la semnarea oricărui nou acord sau a oricărei noi înțelegeri menționate în prezentul regulament.

(97) Având în vedere evoluțiile tehnologice, în câțiva ani ar putea prevala noi forme de instrumente de comunicare sau ar putea apărea lacune în ceea ce privește aplicarea prezentului regulament. Prin urmare, este important să se prevadă o evaluare a aplicării sale.

(98) Comisia ar trebui să efectueze o evaluare a prezentului regulament care ar trebui să se bazeze pe cinci criterii, și anume eficiența, eficacitatea, relevanța, coerența și valoarea adăugată pentru Uniune, iar evaluarea respectivă ar trebui să servească drept bază pentru evaluările impactului unor eventuale măsuri suplimentare. Raportul de evaluare ar trebui să includă o evaluare a aplicării prezentului regulament și a rezultatelor obținute în ceea ce privește obiectivele sale, precum și o evaluare a impactului prezentului regulament asupra drepturilor fundamentale. Comisia ar trebui să colecteze în mod regulat informații care să servească la evaluarea prezentului regulament.

([27]) Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

([28]) JO L 123, 12.5.2016, p. 1.

(99) Întrucât obiectivul prezentului regulament, și anume îmbunătățirea asigurării și obținerii de probe electronice la nivel transfrontalier, nu poate fi realizat în mod satisfăcător de către statele membre, dar, având în vedere natura sa transfrontalieră, acesta poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din TUE. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivului respectiv.

(100) În conformitate cu articolul 3 din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la TUE și la TFUE, Irlanda a notificat intenția sa de a participa la adoptarea și la aplicarea prezentului regulament.

(101) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la TUE și la TFUE, Danemarca nu participă la adoptarea prezentului regulament, acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică.

(102) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 și a emis un aviz la 6 noiembrie 2019 ([29]),

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

OBIECT, DOMENIU DE APLICARE ȘI DEFINIȚII

Articolul 1

Obiect

(1) Prezentul regulament stabilește normele în temeiul cărora o autoritate a unui stat membru poate, în cadrul procedurilor penale, să emită un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice și astfel să ceară unui furnizor de servicii care oferă servicii în Uniune și care este stabilit în alt stat membru sau, dacă nu este stabilit, este reprezentat de un reprezentant legal în alt stat membru, să divulge sau să păstreze probe electronice, indiferent de locul în care se află datele.

Prezentul regulament nu aduce atingere competențelor autorităților naționale de a se adresa furnizorilor de servicii stabiliți sau reprezentați pe teritoriul lor pentru a se asigura că aceștia respectă măsurile naționale similare celor menționate în primul paragraf.

(2) Emiterea unui ordin european de divulgare a probelor electronice sau a unui ordin european de păstrare a probelor electronice poate fi solicitată și de către un suspect sau inculpat sau de către un avocat în numele respectivei persoane, în cadrul drepturilor la apărare aplicabile în conformitate cu dreptul procesual penal intern.

(3) Prezentul regulament nu are ca efect modificarea obligației de respectare a drepturilor fundamentale și a principiilor juridice astfel cum sunt consacrate în Cartă și la articolul 6 din TUE și nu aduce atingere obligațiilor aplicabile autorităților de aplicare a legii sau autorităților judiciare în această privință. Prezentul regulament se aplică fără a aduce atingere principiilor fundamentale, în special libertății de exprimare și de informare, inclusiv libertății și pluralismului mass-mediei, respectării vieții private și de familie, protecției datelor cu caracter personal, precum și dreptului la protecție jurisdicțională efectivă.

Articolul 2

Domeniu de aplicare

(1) Prezentul regulament se aplică furnizorilor de servicii care oferă servicii în Uniune.

(2) Ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice pot fi emise doar în cadrul și în scopul procedurilor penale și pentru executarea unei pedepse privative de libertate sau a unei măsuri privative de libertate de cel puțin patru luni, în urma unei proceduri penale, impuse printr-o hotărâre care nu a fost pronunțată în lipsă, în cazurile în care persoana condamnată s-a sustras justiției. De asemenea, astfel de ordine pot fi emise în proceduri referitoare la o infracțiune pentru care o persoană juridică ar putea răspunde penal sau ar putea fi sancționată în statul emitent.

(3) Ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice pot fi emise doar pentru datele referitoare la serviciile menționate la articolul 3 punctul 3, oferite în Uniune.

(4) Prezentul regulament nu se aplică procedurilor inițiate cu scopul de a oferi asistență judiciară reciprocă unui alt stat membru sau unei țări terțe.

([29]) JO C 32, 31.1.2020, p. 11.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „ordin european de divulgare a probelor electronice” înseamnă o decizie prin care se dispune divulgarea probelor electronice, emisă sau validată de o autoritate judiciară dintr-un stat membru în conformitate cu articolul 4 alineatele (1), (2), (4) și (5) și adresată unui sediu desemnat sau unui reprezentant legal al unui furnizor de servicii care oferă servicii în Uniune, atunci când sediul desemnat respectiv sau reprezentantul legal respectiv se află într-un alt stat membru care are obligații în temeiul prezentului regulament;

2. „ordin european de păstrare a probelor electronice” înseamnă o decizie prin care se dispune păstrarea probelor electronice în scopul formulării unei cereri ulterioare de divulgare și care este emisă sau validată de o autoritate judiciară dintr-un stat membru în conformitate cu articolul 4 alineatele (3), (4) și (5) și este adresată unui sediu desemnat sau unui reprezentant legal al unui furnizor de servicii care oferă servicii în Uniune, atunci când sediul desemnat respectiv sau reprezentantul legal respectiv se află într-un alt stat membru care are obligații în temeiul prezentului regulament;

3. „furnizor de servicii” înseamnă orice persoană fizică sau juridică care furnizează una sau mai multe dintre următoarele categorii de servicii, cu excepția serviciilor financiare menționate la articolul 2 alineatul (2) litera (b) din Directiva 2006/123/CE a Parlamentului European și a Consiliului ([30]):

   (a) servicii de comunicații electronice, astfel cum sunt definite la articolul 2 punctul 4 din Directiva (UE) 2018/1972;

   (b) servicii legate de numele de domenii de internet și de numerotarea IP, cum ar fi servicii de atribuire de adrese IP, de registru de nume de domenii, de operator de registru de nume de domenii, de protecție a vieții private și de proxy legate de numele de domenii;

   (c) alte servicii ale societății informaționale, astfel cum sunt menționate la articolul 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535, care:

      (i) le permit utilizatorilor lor să comunice între ei; sau

      (ii) fac posibilă stocarea sau prelucrarea în alt mod a datelor în numele utilizatorilor cărora le este furnizat serviciul, cu condiția ca stocarea datelor să fie o componentă definitorie a serviciului furnizat utilizatorului;

4. „oferirea de servicii în Uniune” înseamnă:

   (a) a permite persoanelor fizice sau juridice dintr-un stat membru să utilizeze serviciile enumerate la punctul 3; și

   (b) a avea o legătură substanțială, bazată pe criterii factuale specifice, cu statul membru menționat la litera (a); se consideră că există o astfel de legătură substanțială atunci când furnizorul de servicii dispune de un sediu într-un stat membru sau, în absența unui astfel de sediu, atunci când există un număr semnificativ de utilizatori în unul sau mai multe state membre sau atunci când există o direcționare a activităților către unul sau mai multe state membre;

5. „sediu” înseamnă o entitate care exercită efectiv o activitate economică pentru o perioadă nedeterminată prin intermediul unei infrastructuri stabile de unde este exercitată activitatea de furnizare de servicii sau este gestionată activitatea;

6. „sediu desemnat” înseamnă un sediu cu personalitate juridică desemnat în scris de un furnizor de servicii stabilit într-un stat membru care participă la un instrument juridic menționat la articolul 1 alineatul (2) din Directiva (UE) 2023/1544, în scopurile menționate la articolul 1 alineatul (1) și la articolul 3 alineatul (1) din directiva respectivă;

7. „reprezentant legal” înseamnă o persoană fizică sau juridică numită în scris de un furnizor de servicii care nu este stabilit într-un stat membru care participă la un instrument juridic menționat la articolul 1 alineatul (2) din Directiva (UE) 2023/1544, în scopurile menționate la articolul 1 alineatul (1) și la articolul 3 alineatul (1) din directiva respectivă;

8. „probe electronice” înseamnă date privind abonații, date privind traficul sau date referitoare la conținut stocate de către un furnizor de servicii sau în numele acestuia, în format electronic, în momentul primirii unui certificat de ordin european de divulgare a probelor electronice (EPOC) sau a unui certificat de ordin european de păstrare a probelor electronice (EPOC-PR);

([30]) Directiva 2006/123/CE a Parlamentului European și a Consiliului din 12 decembrie 2006 privind serviciile în cadrul pieței interne (JO L 376, 27.12.2006, p. 36).

9. „date privind abonații” înseamnă orice date deținute de către un furnizor de servicii legate de abonamentul la serviciile sale, cu privire la:

   (a) identitatea unui abonat sau client, cum ar fi numele furnizat, data nașterii, adresa poștală sau adresa geografică, datele privind facturarea și plata, numărul de telefon sau adresa de e-mail;

   (b) tipul de serviciu și durata sa, inclusiv datele tehnice și datele de identificare a măsurilor tehnice conexe sau a interfețelor utilizate de către abonat sau client sau furnizate abonatului sau clientului în momentul primei înregistrări sau activări, precum și date privind validarea utilizării serviciului, cu excepția parolelor sau a altor mijloace de autentificare utilizate în locul unei parole care sunt furnizate de către un utilizator sau create la cererea unui utilizator;

10. „date solicitate exclusiv în scopul identificării utilizatorului” înseamnă adrese IP și, după caz, porturile sursă și marca temporală relevante, și anume data și ora, sau echivalentele tehnice ale identificatorilor respectivi și informațiile conexe, atunci când sunt solicitate de autoritățile de aplicare a legii sau de autoritățile judiciare exclusiv în scopul identificării utilizatorului în cadrul unei anchete penale specifice;

11. „date privind traficul” înseamnă date legate de furnizarea unui serviciu oferit de un furnizor de servicii, care servesc la a oferi informații contextuale sau suplimentare cu privire la un astfel de serviciu și sunt generate sau prelucrate de un sistem informatic al furnizorului de servicii, cum ar fi originea și destinația unui mesaj sau ale oricărui alt tip de interacțiune, poziția dispozitivului, data, ora, durata, dimensiunea, ruta, formatul, protocolul utilizat și tipul de compresie, precum și alte metadate privind comunicațiile electronice și date, altele decât datele privind abonații, legate de începerea și terminarea unei sesiuni de acces al utilizatorului, cum ar fi data și ora utilizării, conectarea la serviciu și deconectarea de la acesta;

12. „date referitoare la conținut” înseamnă orice date în format digital, cum ar fi mesajele scrise, mesajele vocale, înregistrările video, imaginile și sunetele, altele decât datele privind abonații sau datele privind traficul;

13. „sistem informatic” înseamnă un sistem informatic astfel cum este definit la articolul 2 litera (a) din Directiva 2013/40/UE a Parlamentului European și a Consiliului ([31]);

14. „stat emitent” înseamnă statul membru în care este emis ordinul european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice;

15. „autoritate emitentă” înseamnă autoritatea competentă din statul emitent, care, în conformitate cu articolul 4, poate emite un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice;

16. „stat de executare” înseamnă statul membru în care este stabilit sediul desemnat sau reprezentantul legal și căruia autoritatea emitentă îi transmite, în vederea notificării sau a executării în conformitate cu prezentul regulament, un ordin european de divulgare a probelor electronice și un EPOC sau un ordin european de păstrare a probelor electronice și un EPOC-PR;

17. „autoritate de executare” înseamnă autoritatea din statul de executare care, în conformitate cu dreptul intern al statului respectiv, este competentă să primească un ordin european de divulgare a probelor electronice și un EPOC sau un ordin european de păstrare a probelor electronice și un EPOC-PR transmis de autoritatea emitentă spre notificare sau spre executare în conformitate cu prezentul regulament;

18. „caz de urgență” înseamnă o situație în care există o amenințare iminentă la adresa vieții, a integrității fizice sau a siguranței unei persoane sau la adresa unei infrastructuri critice, astfel cum este definită la articolul 2 litera (a) din Directiva 2008/114/CE, atunci când perturbarea sau distrugerea unei astfel de infrastructuri critice ar duce la un pericol iminent pentru viața, integritatea fizică sau siguranța unei persoane, inclusiv prin afectarea gravă a aprovizionării cu produse de bază a populației sau a exercitării funcțiilor de bază ale statului;

19. „operator” înseamnă operator astfel cum este definit la articolul 4 punctul 7 din Regulamentul (UE) 2016/679;

20. „persoană împuternicită de operator” înseamnă persoană împuternicită de operator astfel cum este definită la articolul 4 punctul 8 din Regulamentul (UE) 2016/679;

([31]) Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (JO L 218, 14.8.2013, p. 8).

21. „sistem informatic descentralizat” înseamnă o rețea de sisteme informatice și de puncte de acces interoperabile care funcționează sub responsabilitatea și gestionarea individuală a fiecărui stat membru, a fiecărei agenții a Uniunii sau a fiecărui organ al Uniunii și permite ca schimbul transfrontalier de informații să aibă loc într-un mod securizat și fiabil.

CAPITOLUL II

ORDINUL EUROPEAN DE DIVULGARE A PROBELOR ELECTRONICE, ORDINUL EUROPEAN DE PĂSTRARE A PROBELOR ELECTRONICE ȘI CERTIFICATELE AFERENTE

Articolul 4

Autoritatea emitentă

(1) Un ordin european de divulgare a probelor electronice pentru a obține date privind abonații sau pentru a obține date solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite la articolul 3 punctul 10, poate fi emis doar de către:

(a) un judecător, o instanță judecătorească, un judecător de instrucție sau un procuror competent în cazul vizat; sau

(b) orice altă autoritate competentă, astfel cum este definită de către statul emitent, care acționează, în cazul respectiv, în calitatea sa de autoritate de anchetă în cadrul procedurilor penale și care are competența să dispună strângerea de probe în conformitate cu dreptul intern; într-un astfel de caz, ordinul european de divulgare a probelor electronice este validat, după examinarea conformității sale cu condițiile pentru emiterea unui ordin european de divulgare a probelor electronice în temeiul prezentului regulament, de către un judecător, o instanță judecătorească, un judecător de instrucție sau un procuror din statul emitent.

(2) Un ordin european de divulgare a probelor electronice pentru a obține date privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite la articolul 3 punctul 10, sau pentru a obține date referitoare la conținut poate fi emis doar de către:

(a) un judecător, o instanță judecătorească sau un judecător de instrucție competent în cazul vizat; sau

(b) orice altă autoritate competentă, astfel cum este definită de către statul emitent, care acționează, în cazul respectiv, în calitatea sa de autoritate de anchetă în cadrul procedurilor penale și care are competența să dispună strângerea de probe în conformitate cu dreptul intern; într-un astfel de caz, ordinul european de divulgare a probelor electronice este validat, după examinarea conformității sale cu condițiile pentru emiterea unui ordin european de divulgare a probelor electronice în temeiul prezentului regulament, de către un judecător, o instanță judecătorească sau un judecător de instrucție din statul emitent.

(3) Un ordin european de păstrare a probelor electronice pentru datele din orice categorie poate fi emis doar de către:

(a) un judecător, o instanță judecătorească, un judecător de instrucție sau un procuror competent în cazul vizat; sau

(b) orice altă autoritate competentă, astfel cum este definită de către statul emitent, care acționează, în cazul respectiv, în calitatea sa de autoritate de anchetă în cadrul procedurilor penale și care are competența să dispună strângerea de probe în conformitate cu dreptul intern; într-un astfel de caz, ordinul european de păstrare a probelor electronice este validat, după examinarea conformității sale cu condițiile pentru emiterea unui ordin european de păstrare a probelor electronice în temeiul prezentului regulament, de către un judecător, o instanță judecătorească, un judecător de instrucție sau un procuror din statul emitent.

(4) În cazul în care un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice a fost validat de către o autoritate judiciară în temeiul alineatului (1) litera (b), al alineatului (2) litera (b) sau al alineatului (3) litera (b), autoritatea respectivă poate fi considerată, de asemenea, drept autoritate emitentă în contextul transmiterii EPOC și a EPOC-PR.

(5) Într-un caz de urgență a cărui existență a fost stabilită în mod valabil, astfel cum este definit la articolul 3 punctul 18, autoritățile competente menționate la alineatul (1) litera (b) și la alineatul (3) litera (b) de la prezentul articol pot emite, în mod excepțional, un ordin european de divulgare a probelor electronice pentru datele referitoare la abonați sau pentru datele solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite la articolul 3 punctul 10, sau un ordin european de păstrare a probelor electronice, fără validarea prealabilă a ordinului în cauză, atunci când validarea nu poate fi obținută la timp și când autoritățile respective ar putea emite un ordin într-o cauză internă similară fără validare prealabilă. Autoritatea emitentă solicită validarea *ex post* a ordinului în cauză fără întârzieri nejustificate, în termen de cel mult 48 de ore. În cazul în care nu se acordă o astfel de validare *ex post* a ordinului în cauză, autoritatea emitentă retrage imediat ordinul și șterge orice date care au fost obținute sau restricționează în alt mod utilizarea acestora.

(6) Fiecare stat membru poate desemna una sau mai multe autorități centrale ca fiind responsabile cu transmiterea administrativă a EPOC și a EPOC-PR, a ordinelor europene de divulgare a probelor electronice, a ordinelor europene de păstrare a probelor electronice și a notificărilor, precum și cu primirea datelor și a notificărilor și cu transmiterea altor tipuri de corespondență oficială referitoare la astfel de certificate sau ordine.

Articolul 5

Condițiile pentru emiterea unui ordin european de divulgare a probelor electronice

(1) O autoritate emitentă poate emite un ordin european de divulgare a probelor electronice doar în cazul în care sunt îndeplinite condițiile prevăzute în prezentul articol.

(2) Un ordin european de divulgare a probelor electronice trebuie să fie necesar și proporțional în scopul procedurilor menționate la articolul 2 alineatul (3), ținând seama de drepturile suspectului sau inculpatului, și poate fi emis doar dacă un ordin similar ar fi putut fi emis în aceleași condiții într-o cauză internă similară.

(3) Un ordin european de divulgare a probelor electronice pentru a obține date privind abonații sau pentru a obține date solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite la articolul 3 punctul 10, poate fi emis pentru toate infracțiunile și pentru executarea unei pedepse privative de libertate sau a unei măsuri privative de libertate de cel puțin patru luni, în urma unei proceduri penale, impuse printr-o hotărâre care nu a fost pronunțată în lipsă, în cazurile în care persoana condamnată s-a sustras justiției.

(4) Un ordin european de divulgare a probelor electronice pentru a obține date privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite la articolul 3 punctul 10 din prezentul regulament, sau pentru a obține date referitoare la conținut este emis doar:

(a) pentru infracțiuni care se pedepsesc în statul emitent cu o pedeapsă privativă de libertate a cărei limită maximă este de cel puțin trei ani; sau

(b) pentru următoarele infracțiuni, dacă sunt în întregime sau parțial săvârșite prin intermediul unui sistem informatic:

(i) infracțiunile definite la articolele 3-8 din Directiva (UE) 2019/713 a Parlamentului European și a Consiliului ([32]);

(ii) infracțiunile definite la articolele 3-7 din Directiva 2011/93/UE;

(iii) infracțiunile definite la articolele 3-8 din Directiva 2013/40/UE;

(c) pentru infracțiunile definite la articolele 3-12 și la articolul 14 din Directiva (UE) 2017/541;

(d) pentru executarea unei pedepse privative de libertate sau a unei măsuri privative de libertate de cel puțin patru luni, în urma unei proceduri penale, impuse printr-o hotărâre care nu a fost pronunțată în lipsă, în cazurile în care persoana condamnată s-a sustras justiției, pentru infracțiunile menționate la literele (a), (b) și (c) de la prezentul alineat.

(5) Un ordin european de divulgare a probelor electronice include următoarele informații:

(a) autoritatea emitentă și, după caz, autoritatea de validare;

(b) destinatarul ordinului european de divulgare a probelor electronice, astfel cum se menționează la articolul 7;

(c) utilizatorul, cu excepția cazului în care unicul scop al ordinului este de a identifica utilizatorul, sau orice alt identificator unic, cum ar fi numele de utilizator, ID-ul de conectare sau denumirea contului, pentru a stabili datele care sunt solicitate;

(d) categoria de date solicitate astfel cum sunt definite la articolul 3 punctele 9-12;

(e) după caz, intervalul de timp al datelor pentru care se solicită divulgarea;

(f) dispozițiile de drept penal aplicabile ale statului emitent;

(g) în cazuri de urgență astfel cum sunt definite la articolul 3 punctul 18, motivele justificate în mod corespunzător ale situației de urgență;

(h) în cazurile în care ordinul european de divulgare a probelor electronice este adresat direct furnizorului de servicii care stochează sau prelucrează în alt mod datele în numele operatorului, o confirmare că sunt îndeplinite condițiile prevăzute la alineatul (6) de la prezentul articol;

(i) motivele pentru care s-a stabilit că ordinul european de divulgare a probelor electronice îndeplinește condițiile de necesitate și proporționalitate prevăzute la alineatul (2) de la prezentul articol;

(j) o descriere succintă a cazului.

([32]) Directiva (UE) 2019/713 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar și de înlocuire a Deciziei-cadru 2001/413/JAI a Consiliului (JO L 123, 10.5.2019, p. 18).

(6) Un ordin european de divulgare a probelor electronice se adresează furnizorului de servicii care acționează în calitate de operator în conformitate cu Regulamentul (UE) 2016/679.

Prin excepție, ordinul european de divulgare a probelor electronice poate fi adresat direct furnizorului de servicii care stochează sau prelucrează în alt mod datele în numele operatorului, atunci când:

(a) operatorul nu poate fi identificat în ciuda eforturilor rezonabile din partea autorității emitente; sau

(b) contactarea operatorului ar putea dăuna anchetei.

(7) În conformitate cu Regulamentul (UE) 2016/679, persoana împuternicită de operator care stochează sau prelucrează în alt mod datele în numele operatorului informează operatorul cu privire la divulgarea datelor, cu excepția cazului în care autoritatea emitentă a solicitat furnizorului de servicii să se abțină de la a informa operatorul, atât timp cât este necesar și proporțional, pentru a nu obstrucționa procedurile penale relevante. În acest caz, autoritatea emitentă indică în dosarul cauzei motivele pentru informarea cu întârziere a operatorului. În EPOC se adaugă, de asemenea, o justificare succintă.

(8) Atunci când datele sunt stocate sau prelucrate în alt mod ca parte a unei infrastructuri furnizate de un furnizor de servicii unei autorități publice, poate fi emis un ordin european de divulgare a probelor electronice numai în cazul în care autoritatea publică pentru care datele sunt stocate sau prelucrate în alt mod se află în statul emitent.

(9) În cazurile în care datele protejate de secretul profesional în temeiul dreptului statului emitent sunt stocate sau prelucrate în alt mod de către un furnizor de servicii ca parte a unei infrastructuri puse la dispoziția profesioniștilor obligați la păstrarea secretului profesional, în considerarea calității lor, un ordin european de divulgare a probelor electronice pentru a obține date privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului astfel cum sunt definite la articolul 3 punctul 10, sau pentru a obține date referitoare la conținut poate fi emis doar:

(a) atunci când profesionistul obligat la păstrarea secretului profesional își are reședința în statul emitent;

(b) atunci când contactarea profesionistului obligat la păstrarea secretului profesional ar putea dăuna anchetei; sau

(c) atunci când privilegiile au fost ridicate în conformitate cu dreptul aplicabil.

(10) În cazul în care autoritatea emitentă are motive să considere că datele privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite la articolul 3 punctul 10, sau datele referitoare la conținut solicitate prin ordinul european de divulgare a probelor electronice sunt protejate de imunitățile sau privilegiile acordate în temeiul dreptului statului de executare, sau că datele respective fac, în statul în cauză, obiectul unor norme privind stabilirea și limitarea răspunderii penale legate de libertatea presei sau de libertatea de exprimare în alte mijloace de informare în masă, autoritatea emitentă poate solicita clarificări înainte de a emite ordinul european de divulgare a probelor electronice, inclusiv prin consultarea autorităților competente ale statului de executare, fie direct, fie prin intermediul Eurojust sau al Rețelei Judiciare Europene.

Autoritatea emitentă nu emite un ordin european de divulgare a probelor electronice dacă constată că datele privind traficul solicitate, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite la articolul 3 punctul 10, sau datele referitoare la conținut sunt protejate prin imunități sau privilegii acordate în temeiul dreptului statului de executare, sau că datele respective fac, în statul respectiv, obiectul unor norme privind stabilirea și limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă.

Articolul 6

Condițiile pentru emiterea unui ordin european de păstrare a probelor electronice

(1) O autoritate emitentă poate emite un ordin european de păstrare a probelor electronice doar în cazul în care sunt îndeplinite condițiile prevăzute în prezentul articol. Articolul 5 alineatul (8) se aplică *mutatis mutandis*.

(2) Un ordin european de păstrare a probelor electronice este necesar și proporțional în scopul de a preveni eliminarea, ștergerea sau modificarea datelor în vederea efectuării unei solicitări ulterioare de divulgare a respectivelor date prin intermediul asistenței judiciare reciproce, al unui ordin european de anchetă sau al unui ordin european de divulgare a probelor electronice, ținând cont de drepturile suspectului sau inculpatului.

(3) Un ordin european de păstrare a probelor electronice poate fi emis pentru toate infracțiunile, dacă ar fi putut fi emis în aceleași condiții într-o cauză internă similară, și pentru executarea unei pedepse privative de libertate sau a unei măsuri privative de libertate de cel puțin patru luni, în urma unei proceduri penale, impuse printr-o hotărâre care nu a fost pronunțată în lipsă, în cazurile în care persoana condamnată s-a sustras justiției.

(4) Un ordin european de păstrare a probelor electronice include următoarele informații:

(a) autoritatea emitentă și, după caz, autoritatea de validare;

(b) destinatarul ordinului european de păstrare a probelor electronice, astfel cum se menționează la articolul 7;

(c) utilizatorul, cu excepția cazului în care unicul scop al ordinului este de a identifica utilizatorul, sau orice alt identificator unic, cum ar fi numele de utilizator, ID-ul de conectare sau denumirea contului, pentru a stabili datele pentru care se solicită păstrarea;

(d) categoria de date solicitate astfel cum sunt definite la articolul 3 punctele 9-12;

(e) după caz, intervalul de timp al datelor pentru care se solicită păstrarea;

(f) dispozițiile de drept penal aplicabile ale statului emitent;

(g) motivele pentru care s-a stabilit că ordinul european de păstrare a probelor electronice îndeplinește condițiile de necesitate și proporționalitate prevăzute la alineatul (2) de la prezentul articol.

Articolul 7

Destinatarii ordinelor europene de divulgare a probelor electronice și ai ordinelor europene de păstrare a probelor electronice

(1) Ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice se adresează în mod direct unui sediu desemnat sau unui reprezentant legal al furnizorului de servicii în cauză.

(2) În mod excepțional, în cazuri de urgență, astfel cum sunt definite la articolul 3 punctul 18, atunci când sediul desemnat sau reprezentantul legal al unui furnizor de servicii nu reacționează la un EPOC sau la un EPOC-PR în termenele stabilite, respectivul EPOC sau EPOC-PR poate fi adresat oricărui alt sediu sau oricărui alt reprezentant legal al furnizorului de servicii din Uniune.

Articolul 8

Notificarea autorității de executare

(1) Atunci când un ordin european de divulgare a probelor electronice este emis pentru a obține date privind traficul, cu excepția datelor solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite la articolul 3 punctul 10, sau pentru a obține date referitoare la conținut, autoritatea emitentă notifică acest lucru autorității de executare prin transmiterea EPOC către autoritatea respectivă în același timp cu transmiterea EPOC către destinatar în conformitate cu articolul 9 alineatele (1) și (2).

(2) Alineatul (1) nu se aplică dacă, la momentul emiterii ordinului, autoritatea emitentă are motive întemeiate să considere că:

(a) infracțiunea a fost săvârșită, este săvârșită sau este probabil să fie săvârșită în statul emitent; și

(b) persoana ale cărei date sunt solicitate își are reședința în statul emitent.

(3) Atunci când transmite EPOC astfel cum se menționează la alineatul (1) de la prezentul articol autorității de executare, autoritatea emitentă include, după caz, orice informații suplimentare care ar putea fi necesare pentru evaluarea posibilității de a invoca un motiv de refuz în conformitate cu articolul 12.

(4) Notificarea către autoritatea de executare menționată la alineatul (1) de la prezentul articol are un efect suspensiv asupra obligațiilor destinatarului, astfel cum sunt prevăzute la articolul 10 alineatul (2), cu excepția cazurilor de urgență, astfel cum sunt definite la articolul 3 punctul 18.

Articolul 9

Certificatul de ordin european de divulgare a probelor electronice (EPOC) și certificatul de ordin european de păstrare a probelor electronice (EPOC-PR)

(1) Un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice se transmite destinatarului astfel cum este definit la articolul 7 prin intermediul unui EPOC sau al unui EPOC-PR.

Autoritatea emitentă sau, după caz, autoritatea de validare completează EPOC prevăzut în anexa I sau EPOC-PR prevăzut în anexa II, îl semnează și certifică faptul că conținutul acestuia este exact și corect.

(2) Un EPOC conține informațiile menționate la articolul 5 alineatul (5) literele (a)-(h), inclusiv informații suficiente care să îi permită destinatarului să identifice și să contacteze autoritatea emitentă și autoritatea de executare, dacă este nevoie.

Atunci când este necesară o notificare către autoritatea de executare în temeiul articolului 8, EPOC transmis autorității respective conține informațiile enumerate la articolul 5 alineatul (5) literele (a)-(j).

(3) Un EPOC-PR conține informațiile menționate la articolul 6 alineatul (4) literele (a)-(f), inclusiv informații suficiente care să îi permită destinatarului să identifice și să contacteze autoritatea emitentă.

(4) Dacă este necesar, EPOC sau EPOC-PR se traduce într-o limbă oficială a Uniunii acceptată de către destinatar astfel cum se prevede la articolul 4 din Directiva (UE) 2023/1544. În cazul în care nicio limbă nu a fost specificată de către furnizorul de servicii, EPOC sau EPOC-PR se traduce într-o limbă oficială a statului membru în care se află sediul desemnat sau reprezentantul legal al furnizorului de servicii.

În cazul în care este necesară o notificare către autoritatea de executare în temeiul articolului 8, EPOC care urmează să fie transmis autorității respective este tradus într-o limbă oficială a statului de executare sau într-o altă limbă oficială a Uniunii acceptată de către statul respectiv.

Articolul 10

Executarea unui EPOC

(1) După primirea unui EPOC, destinatarul acționează cu promptitudine în vederea păstrării datelor solicitate.

(2) În cazul în care este necesară o notificare către autoritatea de executare în temeiul articolului 8, iar autoritatea respectivă nu a invocat niciun motiv de refuz în conformitate cu articolul 12 în termen de 10 zile de la primirea EPOC, destinatarul se asigură că datele solicitate sunt transmise direct autorității emitente sau autorităților de aplicare a legii, astfel cum se specifică în EPOC, la sfârșitul perioadei de 10 zile. În cazul în care autoritatea de executare confirmă autorității emitente și destinatarului, încă înainte de sfârșitul perioadei de 10 zile, că nu va invoca niciun motiv de refuz, destinatarul acționează în cel mai scurt timp posibil după o astfel de confirmare și cel târziu la sfârșitul respectivei perioade de 10 zile.

(3) În cazul în care nu este necesară o notificare către autoritatea de executare în temeiul articolului 8, după primirea unui EPOC, destinatarul se asigură că datele solicitate sunt transmise direct autorității emitente sau autorităților de aplicare a legii, astfel cum se specifică în EPOC, în termen de cel mult 10 zile de la primirea EPOC.

(4) În cazuri de urgență, destinatarul transmite datele solicitate fără întârzieri nejustificate, cel târziu în termen de opt ore după primirea EPOC. În cazul în care este necesară o notificare către autoritatea de executare în temeiul articolului 8, autoritatea de executare poate, dacă decide să invoce un motiv de refuz în conformitate cu articolul 12 alineatul (1), fără întârziere și cel târziu în termen de 96 de ore de la primirea notificării, să notifice autorității emitente și destinatarului că se opune utilizării datelor sau că datele pot fi utilizate numai în condițiile pe care le precizează. În cazul în care autoritatea de executare invocă un motiv de refuz, dacă datele au fost deja transmise de către destinatar autorității emitente, autoritatea emitentă șterge sau restricționează în alt mod utilizarea datelor sau, în cazul în care autoritatea de executare a precizat condiții, autoritatea emitentă respectă condițiile respective atunci când utilizează datele.

(5) În cazul în care destinatarul consideră, exclusiv pe baza informațiilor conținute în EPOC, că executarea EPOC ar putea afecta imunitățile sau privilegiile ori normele privind stabilirea sau limitarea răspunderii penale legate de libertatea presei sau libertatea de exprimare în alte mijloace de informare în masă în temeiul dreptului statului de executare, destinatarul informează autoritatea emitentă și autoritatea de executare, utilizând formularul prevăzut în anexa III.

În cazul în care autoritatea de executare nu a fost notificată în temeiul articolului 8, autoritatea emitentă ia în considerare informațiile menționate la primul paragraf de la prezentul alineat și decide, din proprie inițiativă sau la cererea autorității de executare, dacă retrage, adaptează sau menține ordinul european de divulgare a probelor electronice.

În cazul în care autoritatea de executare a fost notificată în temeiul articolului 8, autoritatea emitentă ia în considerare informațiile menționate la primul paragraf de la prezentul alineat și decide dacă retrage, adaptează sau menține ordinul european de divulgare a probelor electronice. Autoritatea de executare poate decide să invoce motivele de refuz prevăzute la articolul 12.

(6) În cazul în care destinatarul nu își poate îndeplini obligația de divulgare a datelor solicitate întrucât EPOC este incomplet, conține erori vădite sau nu conține suficiente informații pentru executarea acestuia, destinatarul informează fără întârzieri nejustificate autoritatea emitentă și, în cazul în care autoritatea de executare a fost notificată în temeiul articolului 8, autoritatea de executare menționată în EPOC și solicită clarificări, utilizând formularul prevăzut în anexa III. În același timp, destinatarul informează autoritatea emitentă dacă au fost posibile identificarea datelor solicitate și păstrarea datelor respective, astfel cum se prevede la alineatul (9) de la prezentul articol.

Autoritatea emitentă reacționează cu promptitudine în termen de cel mult cinci zile de la primirea formularului. Destinatarul se asigură că poate primi clarificările necesare sau eventualele corecții transmise de către autoritatea emitentă pentru ca destinatarul să-și poată îndeplini obligațiile prevăzute la alineatele (1)-(4). Obligațiile prevăzute la alineatele (1)-(4) nu se aplică până când nu se furnizează astfel de clarificări sau corecții de către autoritatea emitentă sau de către autoritatea de executare.

(7) În cazul în care destinatarul nu își poate îndeplini obligația de a divulga datele solicitate din cauza unei imposibilități *de facto* generate de împrejurări care nu îi pot fi imputate destinatarului, destinatarul informează fără întârzieri nejustificate autoritatea emitentă și, în cazul în care autoritatea de executare a fost notificată în temeiul articolului 8, autoritatea de executare menționată în EPOC, explicând motivele acestei imposibilități *de facto*, utilizând formularul prevăzut în anexa III. În cazul în care ajunge la concluzia că există o astfel de imposibilitate, autoritatea emitentă informează destinatarul și, în cazul în care autoritatea de executare a fost notificată în temeiul articolului 8, autoritatea de executare că EPOC nu mai trebuie executat.

(8) În toate cazurile în care destinatarul nu furnizează datele solicitate, nu furnizează datele solicitate în mod exhaustiv sau nu furnizează datele solicitate în termenul specificat, din alte motive decât cele menționate la alineatele (5), (6) și (7) de la prezentul articol, destinatarul informează, fără întârzieri nejustificate și cel târziu în termenele prevăzute la alineatele (2), (3) și (4) de la prezentul articol, autoritatea emitentă și, în cazul în care a avut loc o notificare către autoritatea de executare în temeiul articolului 8, autoritatea de executare menționată în EPOC cu privire la motivele respective, utilizând formularul prevăzut în anexa III. Autoritatea emitentă revizuiește ordinul european de divulgare a probelor electronice ținând seama de informațiile furnizate de destinatar și, dacă este necesar, stabilește un nou termen pentru divulgarea datelor de către destinatar.

(9) Datele sunt păstrate, în măsura posibilului, până în momentul în care sunt divulgate, indiferent dacă divulgarea este solicitată în cele din urmă pe baza unui ordin european de divulgare a probelor electronice clarificat și a EPOC aferent sau prin intermediul altor canale, cum ar fi asistența judiciară reciprocă, sau până la retragerea ordinului european de divulgare a probelor electronice.

În cazul în care divulgarea datelor și păstrarea acestora nu mai sunt necesare, autoritatea emitentă și, după caz, în temeiul articolului 16 alineatul (8), autoritatea de executare informează destinatarul fără întârzieri nejustificate.

Articolul 11

Executarea unui EPOC-PR

(1) După primirea unui EPOC-PR, destinatarul păstrează datele solicitate, fără întârzieri nejustificate. Obligația de a păstra datele încetează după 60 de zile, cu excepția cazului în care autoritatea emitentă confirmă, utilizând formularul prevăzut în anexa V, că a fost emisă o cerere ulterioară de divulgare. În cursul acestei perioade de 60 de zile, autoritatea emitentă poate prelungi durata obligației de păstrare a datelor cu o perioadă suplimentară de 30 de zile, utilizând formularul prevăzut în anexa VI, dacă acest lucru este necesar pentru a permite emiterea unei cereri ulterioare de divulgare.

(2) În cazul în care, în termenul de păstrare prevăzut la alineatul (1), autoritatea emitentă confirmă că a fost emisă o cerere ulterioară de divulgare, destinatarul păstrează datele atâta timp cât este necesar pentru a divulga datele odată primită cererea ulterioară de divulgare.

(3) În cazul în care păstrarea datelor nu mai este necesară, autoritatea emitentă informează destinatarul fără întârzieri nejustificate, iar obligația de a păstra datele, care decurge din ordinul european de păstrare a probelor electronice corespunzător, încetează.

(4) În cazul în care destinatarul consideră, exclusiv pe baza informațiilor conținute în EPOC-PR, că executarea EPOC-PR ar putea afecta imunitățile sau privilegiile ori normele privind stabilirea sau limitarea răspunderii penale care se referă la libertatea presei sau la libertatea de exprimare în alte mijloace de informare în masă, în temeiul dreptului statului de executare, destinatarul informează autoritatea emitentă și autoritatea de executare, utilizând formularul prevăzut în anexa III.

Autoritatea emitentă ia în considerare informațiile menționate la primul paragraf și decide, din proprie inițiativă sau la cererea autorității de executare, dacă retrage, adaptează sau menține ordinul european de păstrare a probelor electronice.

(5) În cazul în care destinatarul nu își poate îndeplini obligația de păstrare a datelor solicitate întrucât EPOC-PR este incomplet, conține erori vădite sau nu conține suficiente informații pentru executarea acestuia, destinatarul informează fără întârzieri nejustificate autoritatea emitentă menționată în EPOC-PR și solicită clarificări, utilizând formularul prevăzut în anexa III.

Autoritatea emitentă reacționează cu promptitudine în termen de cel mult cinci zile de la primirea formularului. Destinatarul se asigură că poate primi clarificările necesare sau eventualele corecții transmise de către autoritatea emitentă pentru ca destinatarul să-și poată îndeplini obligațiile prevăzute la alineatele (1), (2) și (3). În absența unei reacții din partea autorității emitente în termenul de cinci zile, furnizorul de servicii este exonerat de obligațiile prevăzute la alineatele (1) și (2).

(6) În cazul în care destinatarul nu își poate îndeplini obligația de a păstra datele solicitate din cauza unei imposibilități de facto generate de împrejurări care nu îi pot fi imputate destinatarului, destinatarul informează fără întârzieri nejustificate autoritatea emitentă menționată în EPOC-PR, explicând motivele acestei imposibilități de facto, utilizând formularul prevăzut în anexa III. În cazul în care autoritatea emitentă ajunge la concluzia că o astfel de imposibilitate este reală, aceasta informează destinatarul că EPOC-PR nu mai trebuie executat.

(7) În toate cazurile în care destinatarul nu păstrează datele solicitate, din alte motive decât cele menționate la alineatele (4), (5) și (6), destinatarul informează fără întârzieri nejustificate autoritatea emitentă cu privire la motivele respective, utilizând formularul prevăzut în anexa III. Autoritatea emitentă revizuiește ordinul european de păstrare a probelor electronice ținând seama de justificările oferite de destinatar.

Articolul 12

Motive pentru refuzul unui ordin european de divulgare a probelor electronice

(1) În cazul în care autoritatea emitentă a notificat autoritatea de executare în temeiul articolului 8, și fără a aduce atingere articolului 1 alineatul (3), autoritatea de executare analizează, cât mai curând posibil, dar nu mai târziu de 10 de zile de la primirea notificării sau, în cazuri de urgență, în termen de cel mult 96 de ore de la primirea notificării, informațiile incluse în ordin și, după caz, invocă unul sau mai multe dintre următoarele motive de refuz:

(a) datele solicitate sunt protejate de imunități sau privilegii acordate în temeiul dreptului statului de executare, care împiedică executarea sau asigurarea executării ordinului, sau datele solicitate sunt reglementate de norme privind stabilirea sau limitarea răspunderii penale care se referă la libertatea presei sau la libertatea de exprimare în alte mijloace de informare în masă, care împiedică executarea sau asigurarea executării ordinului;

(b) în situații excepționale, există motive întemeiate să se considere, pe baza unor dovezi concrete și obiective, că executarea ordinului ar implica, în circumstanțele specifice ale cazului, o încălcare vădită a unui drept fundamental aplicabil, prevăzut la articolul 6 din TUE și în Cartă;

(c) executarea ordinului ar fi contrară principiului *ne bis in idem*;

(d) fapta pentru care a fost emis ordinul nu constituie o infracțiune în temeiul dreptului statului de executare, cu excepția cazului în care se referă la o infracțiune din categoriile de infracțiuni stabilite în anexa IV, astfel cum este indicată de autoritatea emitentă în EPOC, dacă fapta respectivă este sancționabilă în statul emitent cu o pedeapsă privativă de libertate sau cu o măsură privativă de libertate pentru o perioadă maximă de cel puțin trei ani.

(2) În cazul în care autoritatea de executare invocă un motiv de refuz în temeiul alineatului (1), aceasta informează destinatarul și autoritatea emitentă. Destinatarul încetează executarea ordinului european de divulgare a probelor electronice și nu transferă datele, iar autoritatea emitentă retrage ordinul.

(3) Înainte de a decide să invoce un motiv de refuz, autoritatea de executare notificată în temeiul articolului 8 contactează autoritatea emitentă prin orice mijloace corespunzătoare, pentru a discuta măsurile care trebuie luate. Pe această bază, autoritatea emitentă poate decide să adapteze sau să retragă ordinul european de divulgare a probelor electronice. În cazul în care, în urma acestor discuții, nu se ajunge la nicio soluție, autoritatea de executare notificată în temeiul articolului 8 poate decide să invoce motive de refuz al ordinului european de divulgare a probelor electronice și să informeze autoritatea emitentă și destinatarul în consecință.

(4) În cazul în care decide să invoce motive de refuz în temeiul alineatului (1), autoritatea de executare poate indica dacă se opune transferului tuturor datelor solicitate în ordinul european de divulgare a probelor electronice sau dacă datele pot fi transferate sau utilizate doar parțial, în condițiile specificate de autoritatea de executare.

(5) Atunci când competența pentru ridicarea imunității sau a privilegiului prevăzut la alineatul (1) litera (a) de la prezentul articol îi revine unei autorități a statului de executare, autoritatea emitentă îi poate cere autorității de executare notificate în temeiul articolului 8 să contacteze autoritatea respectivă a statului de executare pentru a-i solicita să exercite competența respectivă fără întârziere. Atunci când ridicarea imunității sau privilegiului ține de competența unei autorități a unui alt stat membru sau a unei țări terțe ori de competența unei organizații internaționale, autoritatea emitentă îi poate solicita autorității în cauză să își exercite această competență.

Articolul 13

Informații privind utilizatorii și confidențialitatea

(1) Autoritatea emitentă informează, fără întârzieri nejustificate, persoana ale cărei date sunt solicitate cu privire la divulgarea datelor respective în temeiul unui ordin european de divulgare a probelor electronice.

(2) Autoritatea emitentă poate, în conformitate cu dreptul intern al statului emitent, să amâne sau să restricționeze informarea, ori să nu informeze persoana ale cărei date sunt solicitate, în măsura în care și atât timp cât sunt îndeplinite condițiile de la articolul 13 alineatul (3) din Directiva (UE) 2016/680, caz în care autoritatea emitentă indică în dosarul cazului motivele amânării, restricționării sau neinformării. În EPOC se adaugă, de asemenea, o justificare succintă.

(3) Atunci când informează persoana ale cărei date sunt solicitate, astfel cum se menționează la alineatul (1) de la prezentul articol, autoritatea emitentă include informații cu privire la căile de atac disponibile în temeiul articolului 18.

(4) Destinatarii și furnizorii de servicii, dacă aceștia sunt persoane diferite, iau măsurile operaționale și tehnice necesare cele mai avansate pentru a asigura confidențialitatea, caracterul secret și integritatea EPOC sau EPOC-PR și a datelor divulgate sau păstrate.

Articolul 14

Rambursarea cheltuielilor

(1) Furnizorul de servicii poate solicita rambursarea cheltuielilor sale de către statul emitent, dacă această posibilitate este prevăzută în dreptul intern al statului emitent pentru ordinele naționale în situații similare, în conformitate cu dispozițiile de drept intern ale statului respectiv. Statele membre informează Comisia cu privire la normele lor interne de rambursare, iar Comisia le publică.

(2) Prezentul articol nu se aplică rambursării costurilor sistemului informatic descentralizat, menționat la articolul 25.

CAPITOLUL III

SANCȚIUNI ȘI EXECUTARE

Articolul 15

Sancțiuni

(1) Fără a aduce atingere legislațiilor naționale care prevăd aplicarea de sancțiuni penale, statele membre stabilesc normele privind sancțiunile pecuniare aplicabile în caz de încălcare a articolelor 10 și 11 și a articolului 13 alineatul (4), în conformitate cu articolul 16 alineatul (10), și iau toate măsurile necesare pentru a se asigura că acestea sunt puse în aplicare. Sancțiunile pecuniare prevăzute trebuie să fie efective, proporționale și cu efect de descurajare. Statele membre asigură posibilitatea de a se aplica sancțiuni pecuniare de până la 2 % din cifra de afaceri anuală totală înregistrată de furnizorul de servicii la nivel mondial în exercițiul financiar precedent. Statele membre notifică normele și măsurile respective Comisiei fără întârziere și îi comunică acesteia, fără întârziere, orice modificare ulterioară a acestora.

(2) Fără a aduce atingere obligațiilor de protecție a datelor, furnizorii de servicii nu sunt considerați răspunzători în statele membre pentru prejudiciile aduse utilizatorilor lor sau unor terți care rezultă exclusiv din respectarea cu bună-credință a unui EPOC sau a unui EPOC-PR.

Articolul 16

Procedura de executare

(1) În cazul în care destinatarul nu se conformează unui EPOC în termenul stabilit sau unui EPOC-PR, fără a oferi motive acceptate de autoritatea emitentă, și, după caz, dacă autoritatea de executare nu a invocat niciunul dintre motivele de refuz prevăzute la articolul 12, autoritatea emitentă poate solicita autorității de executare să pună în executare ordinul european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice.

În scopul punerii în executare astfel cum se menționează în primul paragraf, autoritatea emitentă transferă ordinul în cauză, formularul prevăzut în anexa III completat de către destinatar și orice document relevant în conformitate cu articolul 19. Autoritatea emitentă traduce ordinul în cauză și orice document ce urmează să fie transferat într-una dintre limbile acceptate de statul de executare și informează destinatarul cu privire la transfer.

(2) În momentul primirii, autoritatea de executare recunoaște fără formalități suplimentare și ia măsurile necesare pentru punerea în executare a:

(a) unui ordin european de divulgare a probelor electronice, cu excepția cazului în care autoritatea de executare consideră că se aplică unul din motivele prevăzute la alineatul (4); sau

(b) unui ordin european de păstrare a probelor electronice, cu excepția cazului în care autoritatea de executare consideră că se aplică unul dintre motivele prevăzute la alineatul (5).

Autoritatea de executare ia decizia de a recunoaște ordinul în cauză fără întârzieri nejustificate și cel târziu în termen de cinci zile lucrătoare de la primirea ordinului respectiv.

(3) Autoritatea de executare solicită în mod oficial destinatarului să își îndeplinească obligațiile relevante și îl informează pe destinatar cu privire la următoarele:

(a) posibilitatea de a formula obiecții împotriva executării ordinului în cauză invocând unul sau mai multe dintre motivele enumerate la alineatul (4) literele (a)-(f) sau la alineatul (5) literele (a)-(e);

(b) sancțiunile aplicabile în caz de neconformare; și

(c) termenul pentru conformare sau pentru obiecție.

(4) Executarea ordinului european de divulgare a probelor electronice poate fi refuzată doar invocând unul sau mai multe din următoarele motive:

(a) ordinul european de divulgare a probelor electronice nu a fost emis sau validat de o autoritate emitentă astfel cum se prevede la articolul 4;

(b) ordinul european de divulgare a probelor electronice nu a fost emis pentru o infracțiune prevăzută la articolul 5 alineatul (4);

(c) destinatarul nu a putut să se conformeze EPOC din cauza unei imposibilități *de facto* generate de împrejurări care nu îi pot fi imputate destinatarului sau deoarece EPOC conține erori vădite;

(d) ordinul european de divulgare a probelor electronice nu vizează date stocate de către furnizorul de servicii sau în numele acestuia în momentul primirii EPOC;

(e) serviciul nu intră sub incidența prezentului regulament;

(f) datele solicitate sunt protejate de imunități sau privilegii acordate în temeiul dreptului statului de executare sau datele solicitate sunt reglementate de norme privind stabilirea sau limitarea răspunderii penale care se referă la libertatea presei sau la libertatea de exprimare în alte mijloace de informare în masă, care împiedică executarea sau asigurarea executării ordinului european de divulgare a probelor electronice;

(g) în situații excepționale, exclusiv pe baza informațiilor conținute în EPOC, reiese că există motive întemeiate să se considere, pe baza unor dovezi concrete și obiective, că executarea ordinului european de divulgare a probelor electronice ar implica, în circumstanțele specifice ale cazului, o încălcare vădită a unui drept fundamental aplicabil, prevăzut la articolul 6 din TUE și în Cartă.

(5) Executarea ordinului european de păstrare a probelor electronice poate fi refuzată doar invocând unul sau mai multe din următoarele motive:

(a) ordinul european de păstrare a probelor electronice nu a fost emis sau validat de o autoritate emitentă astfel cum se prevede la articolul 4;

(b) destinatarul nu a putut să se conformeze EPOC-PR din cauza unei imposibilități *de facto* generate de împrejurări care nu îi pot fi imputate destinatarului sau deoarece EPOC-PR conține erori vădite;

(c) ordinul european de păstrare a probelor electronice nu vizează date stocate de către furnizorul de servicii sau în numele acestuia în momentul primirii EPOC-PR;

(d) serviciul nu intră sub incidența prezentului regulament;

(e) datele solicitate sunt protejate de imunități sau privilegii acordate în temeiul dreptului statului de executare sau datele solicitate sunt reglementate de norme privind stabilirea sau limitarea răspunderii penale care se referă la libertatea presei sau la libertatea de exprimare în alte mijloace de informare în masă, care împiedică executarea sau asigurarea executării ordinului european de păstrare a probelor electronice;

(f) în situații excepționale, exclusiv pe baza informațiilor conținute în EPOC-PR, reiese că există motive întemeiate să se considere, pe baza unor dovezi concrete și obiective, că executarea ordinului european de păstrare a probelor electronice ar implica, în circumstanțele specifice ale cazului, o încălcare vădită a unui drept fundamental aplicabil, prevăzut la articolul 6 din TUE și în Cartă.

(6) În cazul unei obiecții formulate de către destinatar astfel cum se menționează la alineatul (3) litera (a), autoritatea de executare decide dacă va executa sau nu ordinul european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice pe baza informațiilor furnizate de către destinatar și, dacă este necesar, pe baza informațiilor suplimentare obținute de la autoritatea emitentă în conformitate cu alineatul (7).

(7) Înainte de a decide să nu recunoască sau să nu execute ordinul european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice în conformitate cu alineatul (2) sau, respectiv, (6), autoritatea de executare se consultă cu autoritatea emitentă prin orice mijloace adecvate. După caz, aceasta solicită informații suplimentare din partea autorității emitente. Autoritatea emitentă răspunde la orice cerere de acest tip în termen de cinci zile lucrătoare.

(8) Autoritatea de executare notifică imediat toate deciziile sale autorității emitente și destinatarului.

(9) În cazul în care autoritatea de executare obține de la destinatar datele solicitate de un ordin european de divulgare a probelor electronice, aceasta le transmite autorității emitente fără întârzieri nejustificate.

(10) În cazul în care destinatarul nu se conformează obligațiilor care îi revin în temeiul unui ordin european recunoscut de divulgare a probelor electronice sau al unui ordin european recunoscut de păstrare a probelor electronice, al cărui caracter executoriu a fost confirmat de către autoritatea de executare, autoritatea respectivă impune o sancțiune pecuniară în conformitate cu articolul 15. Împotriva unei decizii de aplicare a unei sancțiuni pecuniare trebuie să fie disponibilă o cale de atac eficientă.

CAPITOLUL IV

CONFLICTUL DE LEGI ȘI CĂI DE ATAC

Articolul 17

Procedura de control jurisdicțional în cazul unor obligații contradictorii

(1) În cazul în care un destinatar consideră că respectarea unui ordin european de divulgare a probelor electronice ar intra în conflict cu o obligație în temeiul dreptului aplicabil al unei țări terțe, acesta informează autoritatea emitentă și autoritatea de executare cu privire la motivele sale de a nu executa ordinul european de divulgare a probelor electronice, în conformitate cu procedura prevăzută la articolul 10 alineatele (8) și (9), utilizând formularul prevăzut în anexa III (denumită în continuare „obiecția motivată”).

(2) Obiecția motivată include toate detaliile relevante cu privire la dreptul țării terțe, la aplicabilitatea sa în cazul vizat și la natura obligațiilor contradictorii. Obiecția motivată nu poate fi întemeiată pe:

(a) faptul că nu există dispoziții similare privind condițiile, formalitățile și procedurile de emitere a unui ordin de divulgare în dreptul aplicabil al țării terțe; sau

(b) simplul fapt că datele sunt stocate într-o țară terță.

Obiecția motivată se depune în termen de cel mult 10 zile de la data la care destinatarul a primit EPOC.

(3) Autoritatea emitentă revizuiește ordinul european de divulgare a probelor electronice pe baza obiecției motivate și a informațiilor transmise de statul de executare. În cazul în care autoritatea emitentă intenționează să mențină ordinul european de divulgare a probelor electronice, aceasta solicită un control jurisdicțional din partea instanței competente din statul emitent. Executarea ordinului european de divulgare a probelor electronice este suspendată până la finalizarea controlului jurisdicțional.

(4) Instanța competentă evaluează mai întâi dacă există obligații contradictorii, examinând:

(a) dacă, pe baza circumstanțelor specifice ale cauzei respective, se aplică dreptul țării terțe; și

(b) dacă, atunci când este aplicabilă astfel cum se menționează la litera (a), dreptul țării terțe interzice divulgarea datelor în cauză atunci când se aplică circumstanțelor specifice ale cauzei respective.

(5) În cazul în care instanța competentă consideră că nu există nicio contradicție relevantă între obligații în înțelesul alineatelor (1) și (4), aceasta menține ordinul european de divulgare a probelor electronice.

(6) În cazul în care instanța competentă consideră, pe baza examinării efectuate în temeiul alineatului (4) litera (b), că dreptul țării terțe interzice divulgarea datelor în cauză, instanța competentă decide menținerea sau revocarea ordinului european de divulgare a probelor electronice. Această examinare se bazează mai ales pe următorii factori, o importanță deosebită fiind acordată factorilor menționați la literele (a) și (b):

(a) interesul protejat de dreptul relevant al țării terțe, inclusiv drepturile fundamentale, precum și alte interese fundamentale care împiedică divulgarea datelor, în special interesele de securitate națională ale țării terțe;

(b) gradul de legătură dintre cauza penală pentru care a fost emis ordinul european de divulgare a probelor electronice și oricare dintre cele două jurisdicții, astfel cum reiese din analizarea, printre altele, a următorilor factori:

(i) localizarea, cetățenia și reședința persoanei ale cărei date sunt solicitate sau ale victimei sau victimelor infracțiunii respective;

(ii) locul în care a fost săvârșită infracțiunea în cauză;

(c) gradul de legătură dintre furnizorul de servicii și țara terță în cauză; în acest context, doar locul de stocare a datelor nu este suficient pentru stabilirea unei legături substanțiale;

(d) interesele statului care desfășoară ancheta în obținerea probelor în cauză, pe baza gravității infracțiunii și a importanței obținerii de probe în mod rapid;

(e) posibilele consecințe ale respectării ordinului european de divulgare a probelor electronice pentru destinatar sau pentru furnizorul de servicii, inclusiv eventualele sancțiuni.

(7) Instanța competentă poate solicita informații din partea autorității competente a țării terțe, ținând seama de Directiva (UE) 2016/680, în special de capitolul V din aceasta, și în măsura în care această solicitare nu obstrucționează procedurile penale relevante. Informațiile sunt solicitate, în special, de la autoritatea competentă a țării terțe de către statul emitent în cazul în care obligațiile contradictorii se referă la drepturile fundamentale sau la alte interese fundamentale ale țării terțe legate de securitatea și apărarea națională.

(8) În cazul în care instanța competentă decide să revoce ordinul european de divulgare a probelor electronice, aceasta informează autoritatea emitentă și destinatarul. În cazul în care instanța competentă stabilește că ordinul european de divulgare a probelor electronice trebuie menținut, aceasta informează autoritatea emitentă și destinatarul, iar acesta din urmă execută ordinul european de divulgare a probelor electronice.

(9) În sensul procedurilor prevăzute la prezentul articol, termenele se calculează în conformitate cu dreptul intern al autorității emitente.

(10) Autoritatea emitentă informează autoritatea de executare cu privire la rezultatul procedurii de control jurisdicțional.

Articolul 18

Căi de atac eficiente

(1) Fără a aduce atingere altor căi de atac disponibile în conformitate cu dreptul intern, orice persoană ale cărei date au fost solicitate prin intermediul unui ordin european de divulgare a probelor electronice are dreptul la căi de atac eficiente împotriva ordinului respectiv. În cazul în care persoana respectivă are calitatea de suspect sau inculpat, aceasta are dreptul la căi de atac eficiente în cursul procedurilor penale în cadrul cărora sunt folosite datele. Dreptul la căi de atac eficiente menționat la prezentul alineat nu aduce atingere dreptului de a introduce căi de atac în temeiul Regulamentului (UE) 2016/679 și al Directivei (UE) 2016/680.

(2) Dreptul la căi de atac eficiente se exercită în fața unei instanțe din statul emitent în conformitate cu dreptul său intern și include posibilitatea de a contesta legalitatea măsurii, inclusiv necesitatea și proporționalitatea acesteia, fără a se aduce atingere garanțiilor legate de drepturile fundamentale în statul de executare.

(3) În sensul articolului 13 alineatul (1), sunt furnizate informații în timp util cu privire la posibilitățile de a introduce căi de atac în temeiul dreptului intern și se asigură faptul că acestea pot fi exercitate în mod eficient.

(4) În sensul prezentului regulament se aplică aceleași termene sau alte condiții ca în cazul introducerii unor căi de atac în cauze interne similare, într-un mod care să garanteze că persoanele vizate își pot exercita efectiv dreptul la respectivele căi de atac.

(5) Fără a aduce atingere normelor procedurale interne, statul emitent și orice alt stat membru căruia i-au fost transmise probe electronice în temeiul prezentului regulament se asigură că se respectă dreptul la apărare și la echitatea procedurilor în cadrul evaluării probelor obținute prin intermediul ordinului european de divulgare a probelor electronice.

CAPITOLUL V

SISTEMUL INFORMATIC DESCENTRALIZAT

Articolul 19

Securitatea comunicării digitale și a schimburilor de date între autoritățile competente și furnizorii de servicii și între autoritățile competente însele

(1) Comunicarea scrisă între autoritățile competente și sediile desemnate sau reprezentanții legali desemnați în temeiul prezentului regulament, inclusiv schimbul de formulare prevăzut în prezentul regulament și transmiterea datelor solicitate în temeiul unui ordin european de divulgare a probelor electronice sau al unui ordin european de păstrare a probelor electronice, se efectuează prin intermediul unui sistem informatic descentralizat securizat și fiabil (denumit în continuare „sistemul informatic descentralizat").

(2) Fiecare stat membru se asigură că sediile desemnate sau reprezentanții legali ai furnizorilor de servicii situați în statul membru respectiv beneficiază de acces la sistemul informatic descentralizat prin intermediul sistemului său informatic intern.

(3) Furnizorii de servicii se asigură că sediile lor desemnate sau reprezentanții lor legali pot utiliza sistemul informatic descentralizat prin intermediul sistemului informatic național respectiv pentru a primi EPOC și EPOC-PR, pentru a trimite datele solicitate autorității emitente și pentru a comunica în orice alt mod cu autoritatea emitentă și cu autoritatea de executare, astfel cum se prevede în prezentul regulament.

(4) Comunicarea scrisă între autoritățile competente în temeiul prezentului regulament, inclusiv schimbul de formulare prevăzut în prezentul regulament și transmiterea datelor solicitate în cadrul procedurii de executare prevăzute la articolul 16, precum și comunicarea scrisă cu agențiile sau organele competente ale Uniunii se efectuează prin intermediul sistemului informatic descentralizat.

(5) În cazul în care comunicarea prin intermediul sistemului informatic descentralizat în conformitate cu alineatul (1) sau (4) nu este posibilă, de exemplu din cauza perturbării sistemului informatic descentralizat, a naturii materialelor transmise, a limitărilor tehnice, cum ar fi volumul datelor, constrângerile juridice legate de admisibilitatea ca probe a datelor solicitate ori cerințele criminalistice aplicabile datelor solicitate, sau din cauza unor circumstanțe excepționale, transmiterea se efectuează prin cele mai potrivite mijloace alternative, ținându-se seama de necesitatea de a se asigura un schimb de informații care este rapid, sigur și fiabil și permite destinatarului să stabilească autenticitatea.

(6) În cazul în care o transmitere se efectuează prin mijloace alternative, astfel cum se prevede la alineatul (5), emitentul transmiterii înregistrează în sistemul informatic descentralizat transmiterea, inclusiv, după caz, data și ora transmiterii, expeditorul și destinatarul, denumirea și dimensiunea fișierului, fără întârzieri nejustificate.

Articolul 20

Efectele juridice ale documentelor electronice

Documentele transmise în cadrul comunicării electronice nu pot fi lipsite de efecte juridice sau considerate inadmisibile în contextul procedurilor judiciare transfrontaliere desfășurate în temeiul prezentului regulament pentru motivul exclusiv că acestea sunt în format electronic.

Articolul 21

Semnăturile și sigiliile electronice

(1) În cazul comunicării electronice efectuate în temeiul prezentului regulament este aplicabil cadrul juridic general pentru utilizarea serviciilor de încredere, prevăzut în Regulamentul (UE) nr. 910/2014.

(2) În cazul în care un document transmis în cadrul comunicării electronice efectuate în temeiul articolului 19 alineatul (1) sau (4) din prezentul regulament necesită un sigiliu sau o semnătură, în conformitate cu prezentul regulament, documentul respectiv trebuie să poarte un sigiliu electronic calificat sau o semnătură electronică calificată, astfel cum sunt definite în Regulamentul (UE) nr. 910/2014.

Articolul 22

Software-ul de implementare de referință

(1) Comisia este responsabilă cu elaborarea, întreținerea și dezvoltarea unui software de implementare de referință, pe care statele membre pot opta să îl aplice drept sistem back-end propriu în locul unui sistem informatic național. Elaborarea, întreținerea și dezvoltarea software-ului de implementare de referință se finanțează din bugetul general al Uniunii.

(2) Comisia furnizează, întreține și sprijină în mod gratuit software-ul de implementare de referință.

Articolul 23

Costurile sistemului informatic descentralizat

(1) Fiecare stat membru suportă costurile de instalare, de funcționare și de întreținere a punctelor de acces ale sistemului informatic descentralizat care se află în responsabilitatea sa.

(2) Fiecare stat membru suportă costurile de creare și de ajustare a sistemelor sale informatice naționale relevante, pentru a asigura interoperabilitatea acestora cu punctele de acces, și suportă costurile de administrare, de funcționare și de întreținere a sistemelor respective.

(3) Agențiile și organele Uniunii suportă costurile de instalare, de funcționare și de întreținere a componentelor sistemului informatic descentralizat care se află în responsabilitatea lor.

(4) Agențiile și organele Uniunii suportă costurile de creare și de ajustare a sistemelor lor de gestionare a dosarelor, pentru a asigura interoperabilitatea acestora cu punctele de acces, și suportă costurile de administrare, de funcționare și de întreținere a sistemelor respective.

(5) Furnizorii de servicii suportă toate costurile necesare pentru a se integra cu succes în sistemul informatic descentralizat sau pentru a interacționa în alt mod cu acesta.

Articolul 24

Perioada de tranziție

Înainte ca obligația de a efectua comunicarea scrisă prin intermediul sistemului informatic descentralizat menționat la articolul 19 să devină aplicabilă (denumită în continuare „perioada de tranziție"), comunicarea scrisă între autoritățile competente și sediile desemnate sau reprezentanții legali desemnați în temeiul prezentului regulament are loc prin cele mai potrivite mijloace alternative, ținându-se seama de necesitatea de a se asigura un schimb de informații rapid, sigur și fiabil. În cazul în care furnizorii de servicii, statele membre sau agențiile și organele Uniunii au instituit platforme specializate sau alte canale securizate pentru tratarea cererilor de date din partea autorităților de aplicare a legii și a autorităților judiciare, autoritățile emitente pot alege, de asemenea, să transmită în cursul perioadei de tranziție sediilor desemnate sau reprezentanților legali desemnați un EPOC sau un EPOC-PR prin intermediul acestor canale.

Articolul 25

Acte de punere în aplicare:

(1) Comisia adoptă actele de punere în aplicare necesare pentru crearea și utilizarea sistemului informatic descentralizat în sensul prezentului regulament, stabilind următoarele:

(a) specificațiile tehnice care definesc metodele de comunicare prin mijloace electronice pentru sistemul informatic descentralizat;

(b) specificațiile tehnice ale protocoalelor de comunicare;

(c) obiectivele în materie de securitate a informațiilor și măsurile tehnice relevante care să asigure standarde minime de securitate a informațiilor și un nivel ridicat de securitate cibernetică pentru prelucrarea și comunicarea informațiilor în cadrul sistemului informatic descentralizat;

(d) obiectivele minime de disponibilitate și eventuale cerințe tehnice conexe pentru serviciile asigurate de sistemul informatic descentralizat.

(2) Actele de punere în aplicare menționate la alineatul (1) de la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 26.

(3) Actele de punere în aplicare menționate la alineatul (1) se adoptă până la 18 august 2025.

Articolul 26

Procedura comitetului

(1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

CAPITOLUL VI

DISPOZIȚII FINALE

Articolul 27

Aspecte lingvistice

Fiecare stat membru poate decide, în orice moment, că va accepta traduceri ale EPOC și ale EPOC-PR într-una sau mai multe limbi oficiale ale Uniunii, în plus față de limba sau limbile lor oficiale, și indică adoptarea acestei decizii într-o declarație scrisă transmisă Comisiei. Comisia pune declarațiile respective la dispoziția tuturor statelor membre și a Rețelei Judiciare Europene.

Articolul 28

Monitorizarea și raportarea

(1) Până la 18 august 2026, Comisia stabilește un program detaliat de monitorizare a realizărilor, a rezultatelor și a impactului prezentului regulament. Programul de monitorizare stabilește mijloacele care vor fi utilizate și intervalele care vor fi aplicate pentru colectarea de date. Acesta precizează măsurile pe care trebuie să le ia Comisia și statele membre pentru colectarea și analizarea datelor.

(2) În orice caz, începând cu 18 august 2026, statele membre colectează de la autoritățile relevante statistici cuprinzătoare și păstrează o evidență a unor astfel de date statistice. Datele colectate pentru anul calendaristic precedent sunt trimise Comisiei în fiecare an până la data de 31 martie și includ:

(a) numărul de EPOC și de EPOC-PR emise în funcție de tipul de date solicitate, în funcție de destinatari și în funcție de situație (cazuri de urgență sau nu);

(b) numărul de EPOC emise în temeiul derogărilor în cazuri de urgență;

(c) numărul de EPOC și de EPOC-PR executate și neexecutate în funcție de tipul de date solicitate, în funcție de destinatari și în funcție de situație (cazuri de urgență sau nu);

(d) numărul de notificări transmise autorităților de executare în temeiul articolului 8 și numărul de EPOC care au fost refuzate, în funcție de tipul de date solicitate, de destinatari, de situație (cazuri de urgență sau nu) și de motivul de refuz invocat;

(e) pentru EPOC executate, perioada medie scursă între momentul emiterii EPOC și momentul obținerii datelor solicitate, în funcție de tipul de date solicitate, în funcție de destinatari și în funcție de situație (cazuri de urgență sau nu);

(f) pentru EPOC-PR executate, perioada medie scursă între momentul emiterii EPOC-PR și momentul emiterii cererii ulterioare de divulgare, în funcție de tipul de date solicitate și de destinatari;

(g) numărul de ordine europene de divulgare a probelor electronice sau de ordine europene de păstrare a probelor electronice transmise unui stat de executare și primite de un stat de executare în vederea executării, în funcție de tipul de date solicitate, în funcție de destinatari și în funcție de situație (cazuri de urgență sau nu) și numărul de ordine de acest tip care au fost executate;

(h) numărul de căi de atac introduse împotriva ordinelor europene de divulgare a probelor electronice în statul emitent și în statul de executare, în funcție de tipul de date solicitate;

(i) numărul de cazuri în care nu a fost acordată validarea *ex post* în conformitate cu articolul 4 alineatul (5);

(j) o prezentare generală a costurilor declarate de furnizorii de servicii în legătură cu executarea EPOC și EPOC-PR și a costurilor rambursate de autoritățile emitente.

(3) Începând cu 18 august 2026, pentru schimburile de date efectuate prin intermediul sistemului informatic descentralizat în temeiul articolului 19 alineatul (1), statisticile menționate la alineatul (2) de la prezentul articol pot fi colectate de către portalurile naționale în mod automat. Software-ul de implementare de referință menționat la articolul 22 este dotat cu capacități tehnice pentru asigurarea acestei funcționalități.

(4) Furnizorii de servicii pot colecta, păstra o evidență a statisticilor și publica statistici în conformitate cu principiile existente privind protecția datelor. În cazul în care se colectează astfel de statistici pentru anul calendaristic precedent, acestea pot fi transmise Comisiei până la 31 martie și pot include, pe cât posibil:

(a) numărul de EPOC și de EPOC-PR primite, în funcție de tipul de date solicitate, de statul emitent și de situație (cazuri de urgență sau nu);

(b) numărul de EPOC și de EPOC-PR executate și neexecutate, în funcție de tipul de date solicitate, de statul emitent și de situație (cazuri de urgență sau nu);

(c) pentru EPOC executate, perioada medie de transmitere a datelor solicitate din momentul în care a fost primit EPOC și până în momentul transmiterii datelor, în funcție de tipul de date solicitate, de statul emitent și de situație (cazuri de urgență sau nu);

(d) pentru EPOC-PR executate, perioada medie scursă între momentul emiterii EPOC-PR și momentul emiterii cererii ulterioare de divulgare, în funcție de tipul de date solicitate și de statul emitent.

(5) Începând cu 18 august 2027, Comisia publică, până la data de 30 iunie a fiecărui an, un raport care conține datele menționate la alineatele (2) și (3), în formă compilată, defalcate pe statele membre și pe tipurile de furnizori de servicii.

Articolul 29

Modificarea certificatelor și a formularelor

Comisia adoptă acte delegate în conformitate cu articolul 30 de modificare a anexelor I, II, III, V și VI, pentru a aborda în mod eficient o eventuală nevoie de îmbunătățire în ceea ce privește conținutul formularelor EPOC și EPOC-PR și al formularelor care trebuie utilizate pentru a furniza informații cu privire la imposibilitatea de a executa un EPOC sau un EPOC-PR, pentru a confirma emiterea unei cereri de divulgare în urma unui ordin european de păstrare a probelor electronice și pentru a prelungi termenul de păstrare a probelor electronice.

Articolul 30

Exercitarea delegării de competențe

(1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.

(2) Competența de a adopta acte delegate menționată la articolul 29 se conferă Comisiei pe o perioadă nedeterminată de la 18 august 2026.

(3) Delegarea de competențe menționată la articolul 29 poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

(4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare.

(5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(6) Un act delegat adoptat în temeiul articolului 29 intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 31

Notificarea Comisiei

(1) Până la 18 august 2025, fiecare stat membru notifică Comisiei următoarele:

(a) autoritatea sau autoritățile care, în conformitate cu dreptul lor intern, sunt competente în temeiul articolului 4 să emită, să valideze sau să transmită ordine europene de divulgare a probelor electronice și ordine europene de păstrare a probelor electronice sau notificări despre acestea;

(b) autoritatea sau autoritățile care sunt competente să primească notificări în temeiul articolului 8 și să execute ordine europene de divulgare a probelor electronice și ordine europene de păstrare a probelor electronice în numele unui alt stat membru, în conformitate cu articolul 16;

(c) autoritatea sau autoritățile care sunt competente să soluționeze obiecțiile motivate transmise de către destinatari în conformitate cu articolul 17;

(d) limbile acceptate pentru notificarea și transmiterea unui EPOC, a unui EPOC-PR, a unui ordin european de divulgare a probelor electronice sau a unui ordin european de păstrare a probelor electronice, în cazul executării, în conformitate cu articolul 27.

(2) Comisia pune la dispoziția publicului informațiile primite în temeiul prezentului articol, fie pe un site web specific, fie pe site-ul web al Rețelei Judiciare Europene în materie penală menționat la articolul 9 din Decizia 2008/976/JAI a Consiliului ([33]).

Articolul 32

Relația cu alte instrumente, acorduri și înțelegeri

(1) Prezentul regulament nu aduce atingere altor instrumente, acorduri și înțelegeri ale Uniunii și internaționale privind strângerea de probe care intră sub incidența prezentului regulament.

(2) Până la 18 august 2026, statele membre informează Comisia cu privire la toate instrumentele, acordurile și înțelegerile menționate la alineatul (1), pe care vor continua să le aplice. De asemenea, statele membre informează Comisia, în termen de trei luni, cu privire la semnarea oricărui nou acord sau a oricărei noi înțelegeri menționate la alineatul (1).

Articolul 33

Evaluare

Până la 18 august 2029, Comisia efectuează o evaluare a prezentului regulament. Comisia transmite un raport de evaluare Parlamentului European, Consiliului, Autorității Europene pentru Protecția Datelor și Agenției pentru Drepturi Fundamentale a Uniunii Europene. Raportul de evaluare respectiv include o evaluare a aplicării prezentului regulament și a rezultatelor obținute în ceea ce privește obiectivele sale, precum și o evaluare a impactului prezentului regulament asupra drepturilor fundamentale. Evaluarea este efectuată în conformitate cu orientările Comisiei privind o mai bună legiferare. Statele membre furnizează Comisiei informațiile necesare pentru întocmirea raportului de evaluare.

Articolul 34

Intrarea în vigoare și aplicarea

(1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

([33]) Decizia 2008/976/JAI a Consiliului din 16 decembrie 2008 privind Rețeaua Judiciară Europeană (JO L 348, 24.12.2008, p. 130).

(2) Se aplică de la 18 august 2026.

Cu toate acestea, obligația autorităților competente și a furnizorilor de servicii de a utiliza sistemul informatic descentralizat instituit prin articolul 19 pentru comunicarea scrisă în temeiul prezentului regulament se aplică începând cu un an de la adoptarea actelor de punere în aplicare menționate la articolul 25.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în statele membre în conformitate cu tratatele.

Adoptat la Strasbourg, 12 iulie 2023.

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*
R. METSOLA	P. NAVARRO RÍOS

ANEXA I

CERTIFICATUL DE ORDIN EUROPEAN DE DIVULGARE A PROBELOR ELECTRONICE (EPOC)

În temeiul Regulamentului (UE) 2023/1543 al Parlamentului European și al Consiliului [1], destinatarul certificatului de ordin european de divulgare (EPOC) trebuie să execute prezentul EPOC și să transmită datele solicitate în conformitate cu termenul sau termenele specificate la secțiunea C din prezentul EPOC autorității indicate la litera (a) din secțiunea L a prezentului EPOC.

În orice situație, la primirea EPOC, destinatarul trebuie să acționeze prompt pentru a păstra datele solicitate, cu excepția cazului în care informațiile din EPOC nu îi permit să identifice respectivele date. Datele trebuie păstrate în continuare până la momentul în care sunt divulgate sau până când autoritatea emitentă sau, după caz, autoritatea de executare, precizează că datele nu mai trebuie păstrate și divulgate.

Destinatarul trebuie să ia măsurile necesare pentru a asigura confidențialitatea, caracterul secret și integritatea EPOC și a datelor divulgate sau păstrate.

SECȚIUNEA A: Autoritatea emitentă/de validare

Statul emitent: ....

Autoritatea emitentă: ....

Autoritatea de validare (dacă este cazul): ....

NB: detaliile despre autoritatea emitentă și de validare se prezintă la sfârșit (secțiunile I și J) .....

Numărul de dosar al autorității emitente: ....

Numărul de dosar al autorității de validare: ....

SECȚIUNEA B: Destinatarul

Destinatarul: ....

☐ Sediul desemnat

☐ Reprezentantul legal

☐ Prezentul ordin este emis într-un caz de urgență destinatarului specificat deoarece sediul desemnat sau reprezentantul legal al unui furnizor de servicii nu a reacționat la EPOC în termenele prevăzute la articolul 10 din Regulamentul (UE) 2023/1543 sau nu a fost desemnat sau numit în termenele stabilite în Directiva (UE) 2023/1544 a Parlamentului European și a Consiliului [2]

Adresa: ....

Tel./Fax/e-mail (dacă se cunoaște): ....

Persoana de contact (dacă este cunoscută): ....

Numărul de dosar al destinatarului (dacă se cunoaște): ....

Furnizorul de servicii vizat (dacă este diferit de destinatar): ....

Orice alte informații utile: ....

[1] Regulamentul (UE) 2023/1543 al Parlamentului European și al Consiliului din 12 iulie 2023 privind ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice în cadrul procedurilor penale și pentru executarea pedepselor privative de libertate în urma unor proceduri penale (JO L 191, 28.7.2023, p. 118).

[2] Directiva (UE) 2023/1544 a Parlamentului European și a Consiliului din 12 iulie 2023 de stabilire a unor norme armonizate privind desemnarea sediilor desemnate și numirea reprezentanților legali în scopul obținerii de probe electronice în cadrul procedurilor penale (JO L 191, 28.7.2023, p. 181).

SECȚIUNEA C: Termene (a se bifa și completa căsuța corespunzătoare dacă este cazul)

La primirea EPOC, datele solicitate trebuie divulgate:

☐ cât mai curând posibil și cel târziu în termen de 10 de zile (fără notificarea autorității de executare)

☐ dacă este notificată autoritatea de executare: la sfârșitul celor 10 zile, dacă autoritatea de executare nu invocă un motiv de refuz în termenul respectiv, sau cât mai curând posibil și cel târziu la sfârșitul celor 10 zile, dacă autoritatea de executare confirmă înainte de scurgerea celor 10 zile că nu va invoca un motiv de refuz

☐ fără întârzieri nejustificate și cel târziu în termen de opt ore într-un caz de urgență care implică:

☐ o amenințare iminentă la adresa vieții sau integrității fizice a unei persoane

☐ o amenințare iminentă la adresa unei infrastructuri critice, astfel cum este definită la articolul 2 litera (a) din Directiva 2008/114/CE a Consiliului ([3]), dacă întreruperea sau distrugerea unei astfel de infrastructuri critice ar duce la o amenințare iminentă la adresa vieții, integrității fizice sau siguranței unei persoane, inclusiv dacă este afectată grav aprovizionarea cu produse de bază a populației sau exercitarea funcțiilor de bază ale statului.

Vă rugăm să precizați dacă există termene procedurale sau de altă natură de care ar trebui ținut cont pentru executarea prezentului EPOC: ....

Vă rugăm să furnizați informații suplimentare, dacă este cazul: ....

SECȚIUNEA D: Legătura cu o cerere anterioară de divulgare/păstrare (bifați și completați dacă este cazul și dacă este disponibilă)

☐ Datele solicitate au fost păstrate integral/parțial în conformitate cu o cerere anterioară de păstrare

emisă de .... (indicați autoritatea și numărul dosarului)

în data de .... (indicați data la care a fost emisă cererea)

și transmisă în data de ..... (indicați data la care a fost transmisă cererea)

către ..... (indicați furnizorul de servicii/reprezentantul legal/sediul desemnat/autoritatea competentă căreia i-a fost transmisă cererea și, dacă este disponibil, numărul de dosar dat de destinatar).

☐ Datele solicitate sunt legate de o cerere anterioară de divulgare

emisă de .... (indicați autoritatea și numărul de dosar)

în data de .... (indicați data la care a fost emisă cererea)

și transmisă în data de ..... (indicați data la care a fost transmisă cererea)

către ..... (indicați furnizorul de servicii/reprezentantul legal/sediul desemnat/autoritatea competentă căreia i-a fost transmisă și, dacă este disponibil, numărul de dosar dat de destinatar).

Orice alte informații utile: ....

([3]) Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora (JO L 345, 23.12.2008, p. 75).

SECȚIUNEA E: Informații care să sprijine identificarea datelor solicitate (a se completa în măsura în care aceste informații sunt cunoscute și necesare pentru identificarea datelor)

Adresa (adresele) IP și înregistrarea datei și orei (inclusiv fusul orar): .....

Nr. tel.: ....

Adresa (adresele) de e-mail: ....

numărul (numerele) IMEI: ....

Adresa (adresele) MAC: ....

Utilizatorul (utilizatorii) sau alt (alți) identificator(i) unic(i), cum ar fi numele de utilizator, ID-ul de conectare sau denumirea contului: ....

Numele serviciului (serviciilor) relevant(e): ....

Altele: ....

Dacă este cazul, intervalul de timp pentru care se solicită divulgarea:

....

☐ Informații suplimentare, dacă este necesar: ....

SECȚIUNEA F: Probele electronice care urmează să fie divulgate

Prezentul EPOC vizează (a se bifa căsuța (căsuțele) corespunzătoare):

(a) ☐ date despre abonați:

☐ numele, data nașterii, adresa poștală sau geografică, datele de contact (adresă de e-mail, număr de telefon) și alte informații relevante referitoare la identitatea utilizatorului/abonatului

☐ data și ora înregistrării inițiale, tipul de înregistrare, o copie a unui contract, mijloace de verificare a identității la momentul înregistrării, copii ale documentelor furnizate de abonat

☐ tipul de serviciu și durata acestuia, inclusiv identificatorul (identificatorii) utilizat (utilizați) de abonat sau furnizat acestuia în momentul înregistrării sau activării inițiale (de exemplu, numărul de telefon, numărul cardului SIM, adresa MAC) și dispozitivul (dispozitivele) asociat(e)

☐ informații despre profil (de exemplu, nume de utilizator, pseudonim, fotografie de profil)

☐ date de validare a utilizării serviciului, cum ar fi o adresă de e-mail alternativă furnizată de utilizator/titularul abonamentului

☐ datele de pe cardul de debit sau de credit (furnizate de utilizator pentru facturare), inclusiv alte mijloace de plată

☐ coduri PUK

☐ altele: .....

(b) ☐ date solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite la articolul 3 punctul 10 din Regulamentul (UE) 2023/1543:

☐ înregistrări ale conexiunii IP, cum ar fi adrese/jurnale/numere de acces IP, împreună cu alți identificatori tehnici, cum ar fi porturi sursă și mărci temporale sau date echivalente, datele de identificare ale utilizatorului și interfața utilizată în contextul utilizării serviciului, vă rugăm să precizați, dacă este necesar: .....

☐ dacă este cazul, intervalul de timp pentru care se solicită divulgarea (dacă este diferit față de secțiunea E): ...

☐ altele: .....

(c) ☐ date de trafic

(i) pentru telefonie (mobilă):

☐ identificatori de ieșire (A) și de intrare (B) (număr de telefon, IMSI, IMEI)

☐ ora și durata conexiunii (conexiunilor)

☐ apel(uri) pierdute

☐ identificatorul stației de bază, inclusiv informații geografice (coordonatele X/Y), în momentul inițierii și încheierii conexiunii

☐ rețeaua/serviciul de telecomunicații utilizat (de exemplu, UMTS, GPRS)

☐ altele: .....

(ii) pentru internet:

☐ informațiile de rutare (adresa IP a sursei, adresa (adresele) IP ale destinatarului, numărul (numerele) de port, browser-ul, informații privind antetul e-mailului, identificatorul de mesaj)

☐ identificatorul stației de bază, inclusiv informații geografice (coordonatele X/Y), în momentul inițierii și încheierii conexiunii (conexiunilor)

☐ volumul de date

☐ data și ora conexiunii (conexiunilor)

☐ durata sesiunii (sesiunilor) de conectare sau de acces

☐ altele: .....

(iii) pentru găzduire:

☐ fișiere jurnal

☐ tichete

☐ altele: .....

(iv) altele:

☐ istoricul cumpărăturilor

☐ istoricul încărcărilor cartelelor preplătite

☐ altele: .....

(d) ☐ date de conținut:

☐ dump-ul căsuței de (web)mail

☐ dump-ul stocării online (datele generate de utilizator)

☐ dump-ul paginilor

☐ jurnalul/backup-ul mesajelor

☐ dump-ul mesageriei vocale

☐ conținuturi de pe server

☐ backup-ul dispozitivului

☐ lista contactelor

☐ altele: .....

☐ Informații suplimentare, dacă trebuie precizat sau limitat (mai bine) ansamblul de date solicitate: .....

SECȚIUNEA G: Informații privind condițiile aplicabile

(a) Prezentul EPOC vizează (a se bifa căsuța (căsuțele) corespunzătoare):

☐ proceduri penale referitoare la o infracțiune (infracțiuni);

☐ executarea unei pedepse privative de libertate sau a unei măsuri privative de libertate de cel puțin patru luni, în urma unei proceduri penale, impuse printr-o hotărâre care nu a fost pronunțată în lipsă și în cazurile în care persoana condamnată s-a sustras justiției.

(b) Natura și încadrarea juridică a infracțiunii (infracțiunilor) în legătură cu care a fost emis EPOC și dispozițiile legale aplicabile ([4]):

....

(c) Prezentul EPOC este emis pentru date de trafic care nu sunt solicitate exclusiv în scopul identificării utilizatorului sau pentru date de conținut sau ambele și se referă la (a se bifa căsuța(ele) relevantă(e), dacă este cazul):

☐ o infracțiune (infracțiuni) care se pedepsește (pedepsesc) în statul emitent cu o pedeapsă privativă de libertate a cărei limită maximă este de cel puțin trei ani;

([4]) Pentru executarea unei pedepse sau a unei măsuri privative de libertate în cazul datelor de trafic care nu sunt necesare doar pentru a identifica utilizatorul, sau al datelor de conținut, vă rugăm să indicați la punctele (b) și (c) infracțiunea pentru care a fost aplicată pedeapsa.

☐ una sau mai multe din următoarele infracțiuni, dacă este (sunt) în întregime sau parțial săvârșită (săvârșite) prin intermediul unui sistem informatic:

☐ infracțiune (infracțiuni) definită (definite) la articolele 3-8 din Directiva (UE) 2019/713 a Parlamentului European și a Consiliului ([5]);

☐ infracțiune (infracțiuni) definită (definite) la articolele 3-7 din Directiva 2011/93/UE a Parlamentului European și a Consiliului ([6]);

☐ infracțiune (infracțiuni) definită (definite) la articolele 3-8 din Directiva 2013/40/UE a Parlamentului European și a Consiliului ([7]);

☐ infracțiuni definite la articolele 3-12 și 14 din Directiva (UE) 2017/541 a Parlamentului European și a Consiliului ([8]).

(d) Operator/persoană împuternicită de operator:

Ordinele europene de divulgare a probelor electronice se adresează furnizorilor de servicii care acționează în calitate de operatori. În mod excepțional, ordinul european de divulgare a probelor electronice poate fi adresat direct furnizorului de servicii care prelucrează datele în numele operatorului.

Bifați căsuța corespunzătoare:

☐ Prezentul EPOC se adresează furnizorului de servicii care acționează în calitate de operator.

☐ Prezentul EPOC se adresează furnizorului de servicii care prelucrează sau, când operatorul nu poate fi identificat, este posibil să prelucreze datele în numele operatorului, deoarece:

☐ operatorul nu poate fi identificat în ciuda eforturilor rezonabile depuse de autoritatea emitentă

☐ contactarea operatorului ar putea dăuna anchetei

Dacă prezentul EPOC se adresează furnizorului de servicii care prelucrează date în numele operatorului:

☐ persoana împuternicită de operator informează operatorul despre divulgarea datelor

☐ persoana împuternicită de operator nu informează operatorul despre divulgarea datelor până la noi dispoziții, deoarece ar dăuna anchetei. Vă rugăm să prezentați o scurtă justificare ([9]):

(e) Orice alte informații utile: ....

SECȚIUNEA H: Informații pentru utilizator

Destinatarul nu informează în niciun caz persoana ale cărei date sunt solicitate. Este responsabilitatea autorității emitente să informeze persoana respectivă, fără întârzieri nejustificate, despre divulgarea datelor.

([5]) Directiva (UE) 2019/713 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar și de înlocuire a Deciziei-cadru 2001/413/JAI a Consiliului (JO L 123, 10.5.2019, p. 18).

([6]) Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului (JO L 335, 17.12.2011, p. 1).

([7]) Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (JO L 218, 14.8.2013, p. 8).

([8]) Directiva (UE) 2017/541 a Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului (JO L 88, 31.3.2017, p. 6).

([9]) Autoritatea emitentă trebuie să indice motivele întârzierii în dosarul cauzei; în EPOC trebuie anexată doar o justificare succintă.

Vă rugăm să rețineți că (a se bifa, după caz):

☐ autoritatea emitentă va amâna informarea persoanei ale cărei date sunt solicitate, cât timp sunt îndeplinite una sau mai multe dintre următoarele condiții:

☐ este necesar pentru a evita obstrucționarea investigațiilor, anchetelor sau procedurilor oficiale sau judiciare;

☐ este necesar pentru a nu zădărnici prevenirea, depistarea, anchetarea sau urmărirea penală a infracțiunilor sau executarea pedepselor penale;

☐ este necesar pentru a proteja siguranța publică;

☐ este necesar pentru a proteja securitatea națională;

☐ este necesar pentru a proteja drepturile și libertățile altor persoane.

SECȚIUNEA I: Datele de contact ale autorității emitente

Tipul de autoritate emitentă (a se bifa căsuța (căsuțele) corespunzătoare):

☐ un judecător, o instanță judecătorească sau un judecător de instrucție

☐ un procuror

☐ altă autoritate competentă, definită de statul emitent

Dacă este nevoie de validare, vă rugăm să completați și secțiunea J.

Vă rugăm să rețineți că (a se bifa, după caz):

☐ Prezentul EPOC a fost emis pentru date despre abonați sau pentru date solicitate exclusiv în scopul identificării utilizatorului, într-un caz de urgență stabilit în mod valabil, fără validare prealabilă, deoarece validarea nu s-ar fi putut obține la timp, sau ambele. Autoritatea emitentă confirmă că ar putea emite un ordin pentru o cauză internă similară fără validare și că validarea *ex-post* va fi solicitată fără întârzieri nejustificate, cel târziu în termen de 48 de ore (vă rugăm să rețineți că destinatarul nu va fi informat).

Datele de contact ale autorității emitente care atestă exactitatea și corectitudinea conținutului EPOC sau ale reprezentatului acesteia sau ale ambelor:

Denumirea autorității: ....

Numele reprezentantului acesteia: ....

Funcția deținută (titlu/grad): ....

Numărul de dosar: ....

Adresa: ....

Numărul de telefon: (prefixul țării) (prefixul regiunii/localității) .....

Numărul de fax: (prefixul țării) (prefixul regiunii/localității) ....

Adresa de e-mail: ....

Limba (limbile) vorbită (vorbite): ....

Dacă diferă de cea de mai sus, autoritatea/punctul de contact (de exemplu, autoritatea centrală) care poate fi contactată pentru orice întrebare legată de executarea EPOC:

Denumirea autorității/numele: ....

Adresa: ....

Numărul de telefon: (prefixul țării) (prefixul regiunii/localității) .....

Numărul de fax: (prefixul țării) (prefixul regiunii/localității) ....

Adresa de e-mail: ....

Semnătura autorității emitente care atestă exactitatea și corectitudinea conținutului EPOC sau a reprezentatului său:

Data: ....

Semnătura ([10]): ....

SECȚIUNEA J: Datele de contact ale autorității de validare (a se completa dacă este cazul)

Tipul autorității de validare

☐ un judecător, o instanță judecătorească sau un judecător de instrucție

☐ un procuror

Datele de contact ale autorității de validare care atestă exactitatea și corectitudinea conținutului EPOC sau ale reprezentatului acesteia sau ale ambelor:

Denumirea autorității: ....

Numele reprezentantului acesteia: ....

Funcția deținută (titlu/grad): ....

Numărul de dosar: ....

Adresa: ....

Numărul de telefon: (prefixul țării) (prefixul regiunii/localității) .....

Numărul de fax: (prefixul țării) (prefixul regiunii/localității) ....

Adresa de e-mail: ....

Limba (limbile) vorbită (vorbite): ....

([10]) Dacă nu se folosește sistemul informatic descentralizat, vă rugăm să adăugați o ștampilă oficială, un sigiliu electronic sau o metodă de autentificare echivalentă.

Data: ....

Semnătura ([11]): ....

SECȚIUNEA K: Notificarea și datele de contact ale autorității de executare notificate (dacă este cazul)

☐ Prezentul EPOC este notificat următoarei autorități de executare:
....

Vă rugăm să furnizați datele de contact ale autorității de executare notificate (dacă sunt disponibile):

Denumirea autorității de executare: ....

Adresa: ....

Numărul de telefon: (prefixul țării) (prefixul regiunii/localității) .....

Numărul de fax: (prefixul țării) (prefixul regiunii/localității) ....

Adresa de e-mail: ....

SECȚIUNEA L: Transferarea datelor

(a) Autoritatea căreia trebuie să îi se transfere datele

☐ autoritatea emitentă

☐ autoritatea de validare

☐ altă autoritate competentă (de exemplu, o autoritare centrală)

Denumire și date de contact: ....

(b) Formatul preferat sau mijloacele prin care trebuie transferate datele (dacă este cazul): .....

SECȚIUNEA M: Informații suplimentare care trebuie incluse (a nu se trimite destinatarului – a se furniza autorității de executare dacă este obligatorie notificarea autorității de executare)

Motivele pentru care s-a stabilit că ordinul european de păstrare a probelor electronice îndeplinește condițiile de necesitate și proporționalitate:

....

O descriere succintă a cauzei:

....

([11]) Dacă nu se folosește sistemul informatic descentralizat, vă rugăm să adăugați o ștampilă oficială, un sigiliu electronic sau o metodă de autentificare echivalentă.

Infracțiunea pentru care s-a emis ordinul european de divulgare a probelor electronice se pedepsește în statul emitent cu o pedeapsă privativă de libertate sau o măsură privative de libertate pentru o perioadă maximă de cel puțin trei ani și figurează aceasta pe lista infracțiunilor prezentată mai jos? (bifați căsuța/căsuțele corespunzătoare)

☐ participare la un grup infracțional organizat;

☐ terorism;

☐ trafic de ființe umane;

☐ exploatarea sexuală a copiilor și pornografia infantilă;

☐ traficul ilicit de stupefiante și de substanțe psihotrope,

☐ traficul ilicit de arme, muniție și materiale explozive;

☐ corupție;

☐ fraudă, inclusiv frauda și alte infracțiuni care prejudiciază interesele financiare ale Uniunii, definite în Directiva (UE) 2017/1371 a Parlamentului European și a Consiliului ([12]);

☐ spălarea banilor proveniți din infracțiuni;

☐ falsificarea bancnotelor, inclusiv falsificarea bancnotelor euro;

☐ criminalitatea informatică;

☐ infracțiunile împotriva mediului, inclusiv traficul ilicit de specii de animale pe cale de dispariție și traficul ilicit de specii și soiuri de plante pe cale de dispariție;

☐ facilitarea intrării și șederii neautorizate;

☐ omorul sau vătămarea corporală gravă;

☐ traficul ilicit de organe și țesuturi umane;

☐ răpirea, lipsirea de libertate ilegală sau luarea de ostatici;

☐ rasismul și xenofobia;

☐ furtul organizat sau tâlhăria;

☐ traficul ilicit de bunuri culturale, inclusiv antichități și opere de artă;

☐ înșelăciunea;

☐ tâlhăria și extorcarea de fonduri;

☐ contrafacerea și piratarea de produse;

☐ falsul și uzul de fals în înscrisuri oficiale;

☐ falsificarea mijloacelor de plată;

☐ trafic ilicit de substanțe hormonale și alți factori de creștere;

([12]) Directiva (UE) 2017/1371 a Parlamentului European și a Consiliului din 5 iulie 2017 privind combaterea fraudelor îndreptate împotriva intereselor financiare ale Uniunii prin mijloace de drept penal (JO L 198, 28.7.2017, p. 29).

☐ traficul ilicit de materiale nucleare sau radioactive;

☐ traficul de vehicule furate;

☐ violul;

☐ incendierea;

☐ infracțiuni de competența Curții Penale Internaționale;

☐ capturarea ilicită a aeronavelor sau a navelor;

☐ acte de sabotaj.

Dacă este cazul, vă rugăm să adăugați orice alte informații de care autoritatea de executare ar putea avea nevoie pentru a evalua posibilitatea de a invoca motive de refuz:

… ....

ANEXA II

CERTIFICATUL DE ORDIN EUROPEAN DE PĂSTRARE A PROBELOR ELECTRONICE (EPOC-PR)

În temeiul Regulamentului (UE) 2023/1543 al Parlamentului European și al Consiliului ([1]), destinatarul prezentului certificat de ordin european de păstrare (EPOC-PR) trebuie să păstreze, fără întârzieri nejustificate după primirea EPOC-PR, datele solicitate. Perioada de păstrare încetează după 60 de zile, dacă autoritatea emitentă nu o prelungește cu încă 30 de zile sau dacă autoritatea emitentă nu confirmă că a fost lansată o cerere ulterioară de divulgare. Dacă autoritatea emitentă confirmă în aceste perioade de timp că a fost emisă o cerere ulterioară de divulgare, destinatarul trebuie să păstreze datele atât timp cât este necesar pentru a divulga datele, după primirea cererii ulterioare de divulgare.

Destinatarul trebuie să ia măsurile necesare pentru a asigura confidențialitatea, caracterul secret și integritatea EPOC-PR și a datelor păstrate.

SECȚIUNEA A: Autoritatea emitentă/de validare

Statul emitent:..... .....

Autoritatea emitentă:..... .....

Autoritatea de validare (dacă este cazul):..... .....

NB: datele de contact ale autorității emitente și de validare se prezintă la sfârșit (secțiunile F și G)

Numărul de dosar al autorității emitente:..... .....

Numărul de dosar al autorității de validare: ....

SECȚIUNEA B: Destinatarul

Destinatarul:..... .....

☐ Sediul desemnat

☐ Reprezentantul legal

☐ Prezentul ordin este emis într-un caz de urgență destinatarului specificat deoarece sediul desemnat sau reprezentantul legal al unui furnizor de servicii nu a reacționat la EPOC-PR în termenele prevăzute sau nu a fost desemnat sau numit în termenele stabilite în Directiva (UE) 2023/1544 a Parlamentului European și a Consiliului ([2])

([1]) Regulamentul (UE) 2023/1543 al Parlamentului European și al Consiliului din 12 iulie 2023 privind ordinul european de divulgare a probelor electronice și ordinul european de păstrare a probelor electronice în cadrul procedurilor penale și pentru executarea pedepselor privative de libertate în urma unor proceduri penale (JO L 191, 28.7.2023, p. 118).

([2]) Directiva (UE) 2023/1544 a Parlamentului European și a Consiliului din 12 iulie 2023 de stabilire a unor norme armonizate privind desemnarea sediilor desemnate și numirea reprezentanților legali în scopul obținerii de probe electronice în cadrul procedurilor penale (JO L 191, 28.7.2023, p. 181).

Adresa: .....

Tel./Fax/e-mail (dacă se cunoaște): .....

Persoana de contact (dacă este cunoscută): .....

Numărul de dosar al destinatarului (dacă se cunoaște): .....

Furnizorul de servicii vizat (dacă este diferit de destinatar): .....

Orice alte informații utile: .....

SECȚIUNEA C: Informații care să sprijine identificarea datelor care se solicită să fie păstrate (a se completa în măsura în care aceste informații sunt cunoscute și necesare pentru identificarea datelor)

☐ Adresa (adresele) IP și înregistrarea datei și orei (inclusiv fusul orar): .....

☐ Nr. tel.: .....

☐ Adresa (adresele) de e-mail: .....

☐ Numărul (numerele) IMEI: .....

☐ Adresa (adresele) MAC: .....

☐ Utilizatorul (utilizatorii) serviciului sau alt (alți) identificator(i) unic(i), cum ar fi numele de utilizator, ID-ul de conectare sau denumirea contului: .....

☐ Numele serviciului (serviciilor) în cauză: .....

☐ Altele: .....

Dacă este cazul, intervalul de timp pentru care se solicită păstrarea: .....

☐ Informații suplimentare, dacă este necesar: .....

SECȚIUNEA D: Probele electronice care urmează să fie păstrate

Prezentul EPOC-PR vizează [a se bifa căsuța (căsuțele) corespunzătoare]:

(a) ☐ date despre abonați:

☐ numele, data nașterii, adresa poștală sau geografică, datele de contact (adresă de e-mail, număr de telefon) și alte informații relevante referitoare la identitatea utilizatorului/abonatului

☐ data și ora înregistrării inițiale, tipul de înregistrare, o copie a unui contract, mijloace de verificare a identității la momentul înregistrării, copii ale documentelor furnizate de abonat

☐ tipul de serviciu și durata acestuia, inclusiv identificatorul (identificatorii) utilizat (utilizați) de abonat sau furnizat acestuia în momentul înregistrării sau activării inițiale (de exemplu, numărul de telefon, numărul cardului SIM, adresa MAC) și dispozitivul (dispozitivele) asociat(e)

☐ informații despre profil (de exemplu, nume de utilizator, pseudonim, fotografie de profil)

☐ date de validare a utilizării serviciului, de exemplu o adresă de e-mail alternativă furnizată de utilizator/titularul abonamentului

☐ datele de pe cardul de debit sau de credit (furnizate de utilizator pentru facturare), inclusiv alte mijloace de plată

☐ coduri PUK

☐ altele:..... .....

(b) ☐ date solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite la articolul 3 punctul 10 din Regulamentul (UE) 2023/1543:

☐ înregistrări ale conexiunii IP, cum ar fi adrese/jurnale/numere de acces IP, împreună cu alți identificatori tehnici, cum ar fi porturi sursă și mărci temporale sau date echivalente, datele de identificare ale utilizatorului și interfața utilizată, în contextul utilizării serviciului care sunt strict necesare în scopuri de identificare: vă rugăm să precizați, dacă este necesar:..... .....

☐ dacă este cazul, intervalul de timp pentru care se solicită păstrarea (dacă este diferit față de secțiunea C)...

☐ altele:..... .....

(c) ☐ date de trafic:

(i) pentru telefonie (mobilă):

☐ identificatori de ieșire (A) și de intrare (B) (număr de telefon, IMSI, IMEI)

☐ ora și durata conexiunii (conexiunilor)

☐ apel(uri) pierdute

☐ identificatorul stației de bază, inclusiv informații geografice (coordonatele X/Y), în momentul inițierii și încheierii conexiunii

☐ rețeaua/serviciul de telecomunicații utilizat (de exemplu, UMTS, GPRS)

☐ altele:..... .....

(ii) pentru internet:

☐ informațiile de rutare (adresa IP a sursei, adresa (adresele) IP ale destinatarului, numărul (numerele) de port, browser-ul, informații privind antetul e-mailului, identificatorul de mesaj)

☐ identificatorul stației de bază, inclusiv informații geografice (coordonatele X/Y), în momentul inițierii și încheierii conexiunii (conexiunilor)

☐ volumul de date

☐ data și ora conexiunii (conexiunilor)

☐ durata sesiunii (sesiunilor) de conectare sau de acces

☐ altele:..... .....

(iii) pentru găzduire:

☐ fișiere jurnal

☐ tichete

☐ altele:..... .....

(iv) altele

☐ istoricul cumpărăturilor

☐ istoricul încărcărilor cartelelor preplătite

☐ altele:..... .....

(d) ☐ date de conținut:

☐ dump-ul căsuței de (web)mail

☐ dump-ul stocării online (datele generate de utilizator)

☐ dump-ul paginilor

☐ jurnalul/backup-ul mesajelor

☐ dump-ul mesageriei vocale

☐ conținuturi de pe server

☐ backup-ul dispozitivului

☐ lista contactelor

☐ altele:..... .....

☐ Informații suplimentare, dacă trebuie precizat sau limitat (mai bine) ansamblul de date solicitate:.....

SECȚIUNEA E: Informații privind condițiile aplicabile

(a) Prezentul EPOC-PR vizează (a se bifa căsuța (căsuțele) corespunzătoare):

☐ proceduri penale referitoare la o infracțiune;

☐ executarea unei pedepse privative de libertate sau a unei măsuri privative de libertate de cel puțin patru luni, în urma unei proceduri penale, impuse printr-o hotărâre care nu a fost pronunțată în lipsă și în cazurile în care persoana condamnată s-a sustras justiției.

(b) Natura și încadrarea juridică a infracțiunii (infracțiunilor) pentru care a fost emis EPOC-PR și dispozițiile legale aplicabile ([3]): ....

SECȚIUNEA F: Datele de contact ale autorității emitente

Tipul de autoritate emitentă (a se bifa căsuța (căsuțele) corespunzătoare):

☐ un judecător, o instanță judecătorească sau un judecător de instrucție

☐ un procuror

☐ altă autoritate competentă, definită de dreptul statului emitent

Dacă este nevoie de validare, vă rugăm să completați și secțiunea G.

Vă rugăm să rețineți că (a se bifa, după caz):

☐ Prezentul EPOC-PR a fost emis pentru date despre abonați sau pentru date solicitate exclusiv în scopul identificării utilizatorului într-un caz de urgență stabilit în mod valabil, fără validare prealabilă, deoarece validarea nu s-ar fi putut obține la timp, sau ambele. Autoritatea emitentă confirmă că ar putea emite un ordin pentru o cauză internă similară fără validare și că validarea ex-post va fi solicitată fără întârzieri nejustificate, cel târziu în termen de 48 de ore (vă rugăm să rețineți că destinatarul nu va fi informat).

Acest caz de urgență se referă la o situație în care există o amenințare iminentă la adresa vieții, a integrității fizice sau a siguranței unei persoane sau la adresa unei infrastructuri critice, astfel cum este definită la articolul 2 litera (a) din Directiva 2008/114/CE a Consiliului ([4]), atunci când perturbarea sau distrugerea unei astfel de infrastructuri critice ar provoca un pericol iminent pentru viața, integritatea fizică sau siguranța unei persoane, inclusiv prin afectarea gravă a aprovizionării cu produse de bază a populației sau a exercitării funcțiilor de bază ale statului.

Datele de contact ale autorității emitente care atestă exactitatea și corectitudinea conținutului EPOC-PR și/sau ale reprezentatului acesteia:

Denumirea autorității: ....

Numele reprezentantului acesteia: ....

Funcția deținută (titlu/grad): ....

([3]) Pentru executarea unei pedepse sau a unei măsuri privative de libertate, vă rugăm să indicați infracțiunea pentru care a fost impusă pedeapsa.

([4]) Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene (JO L 345, 23.12.2008, p. 75).

Numărul de dosar:.....

Adresa:.....

Numărul de telefon: (prefixul țării) (prefixul regiunii/localității).....

Numărul de fax: (prefixul țării) (prefixul regiunii/localității).....

Adresa de e-mail:.....

Limba (limbile) vorbită (vorbite):.....

Dacă diferă de cea de mai sus, autoritatea/punctul de contact (de exemplu, autoritatea centrală) care poate fi contactată pentru orice întrebare legată de executarea EPOC-PR:

Denumirea autorității/numele:.....

Adresa:.....

Numărul de telefon: (prefixul țării) (prefixul regiunii/localității).....

Numărul de fax: (prefixul țării) (prefixul regiunii/localității).....

Adresa de e-mail:.....

Semnătura autorității emitente care atestă exactitatea și corectitudinea conținutului EPOC-PR sau a reprezentatului său:

Data:.....

Semnătura ([5]):.....

SECȚIUNEA G: Datele de contact ale autorității de validare (a se completa dacă este cazul)

Tipul de autoritate de validare

☐ un judecător, o instanță judecătorească sau un judecător de instrucție

☐ un procuror

Datele de contact ale autorității de validare care atestă exactitatea și corectitudinea conținutului EPOC-PR sau ale reprezentatului acesteia, sau ambele:

Denumirea autorității:.....

Numele reprezentantului acesteia:.....

Funcția deținută (titlu/grad):.....

([5]) Dacă nu se folosește sistemul informatic descentralizat, vă rugăm să adăugați o ștampilă oficială, un sigiliu electronic sau o metodă de autentificare echivalentă.

Numărul de dosar:.....

Adresa:.....

Numărul de telefon: (prefixul țării) (prefixul regiunii/localității).....

Numărul de fax: (prefixul țării) (prefixul regiunii/localității).....

Adresa de e-mail:.....

Limba (limbile) vorbită (vorbite):.....

Data:.....

Semnătura ([6]):.....

([6]) Dacă nu se folosește sistemul informatic descentralizat, vă rugăm să adăugați o ștampilă oficială, un sigiliu electronic sau o metodă de autentificare echivalentă.

ANEXA III

INFORMAȚII DESPRE IMPOSIBILITATEA DE A EXECUTA UN EPOC/EPOC-PR

În temeiul Regulamentului (UE) 2023/1543 al Parlamentului European și al Consiliului ([1]), în cazurile în care destinatarul nu își poate respecta obligația de a păstra datele solicitate în temeiul unui EPOC-PR sau de a le divulga în temeiul unui EPOC, nu poate respecta termenul specificat sau nu furnizează date complete, prezentul formular ar trebui completat de către destinatar și trimis înapoi autorității emitente, precum și, în cazul în care a avut loc o notificare și, în alte cazuri dacă este aplicabil, autorității de executare menționate în EPOC, fără întârzieri nejustificate.

În funcție de posibilități, destinatarul păstrează datele solicitate chiar și atunci când sunt necesare informații suplimentare pentru a le identifica cu precizie, cu excepția cazului în care informațiile din EPOC/EPOC-PR nu sunt suficiente în acest scop. Dacă sunt necesare clarificări din partea autorității emitente, destinatarul le solicită fără întârzieri nejustificate, utilizând prezentul formular.

SECȚIUNEA A: Certificatul în cauză

Următoarele informații se referă la:

☐ un certificat de ordin european de divulgare (EPOC)

☐ un certificat de ordin european de păstrare (EPOC-PR)

SECȚIUNEA B: Autoritatea (autoritățile) relevantă (relevante)

Autoritatea emitentă:.....

Numărul de dosar al autorității emitente:.....

După caz, autoritatea de validare:.....

Dacă este cazul, numărul de dosar al autorității de validare: .....

Data emiterii EPOC/EPOC-PR: .....

Data primirii EPOC/EPOC-PR: .....

După caz, autoritatea de executare:.....

Dacă este disponibil, numărul de dosar al autorității de executare:.....

SECȚIUNEA C: Destinatarul EPOC/EPOC-PR

Destinatarul EPOC/EPOC-PR: .....

Numărul de dosar al destinatarului: .....

([1]) Regulamentul (UE) 2023/1543 al Parlamentului European și al Consiliului din 12 iulie 2023 privind ordinul european de divulgare a probelor electronice și ordinul european de păstrare a probelor electronice în cadrul procedurilor penale și pentru executarea pedepselor privative de libertate în urma unor proceduri penale (JO L 191, 28.7.2023, p. 118).

SECȚIUNEA D: Motivele neexecutării

(a) EPOC/EPOC-PR nu poate fi executat sau nu poate fi executat în termenul specificat din următorul (următoarele) motiv(e):

☐ este incomplet

☐ conține erori vădite

☐ nu conține suficiente informații

☐ nu privește date stocate de către furnizorul de servicii sau în numele său în momentul primirii EPOC/EPOC-PR

☐ alte motive de imposibilitate *de facto* generate de împrejurări care nu îi pot fi imputate destinatarului sau a furnizorului de servicii în momentul primirii EPOC/EPOC-PR

☐ ordinul european de divulgare/ordinul european de păstrare nu a fost emis sau validat de o autoritate emitentă așa cum se prevede la articolul 4 din Regulamentul (UE) 2023/1543.

☐ ordinul european de divulgare a probelor electronice pentru a obține date de trafic care nu sunt solicitate exclusiv în scopul identificării utilizatorului, astfel cum sunt definite la articolul 3 punctul 10 din Regulamentul (UE) 2023/1543, sau pentru a obține date despre conținut a fost emis pentru o infracțiune care nu intră sub incidența articolului 5 alineatul (4) din Regulamentul (UE) 2023/1543.

☐ serviciul nu intră sub incidența Regulamentului (UE) 2023/1543.

☐ datele solicitate sunt protejate de imunități sau privilegii acordate în temeiul dreptului statului de executare sau datele solicitate sunt reglementate de norme privind stabilirea sau limitarea răspunderii penale care se referă la libertatea presei sau la libertatea de exprimare în alte mijloace de informare în masă, care împiedică executarea ordinului european de divulgare a probelor electronice/ordinului european de păstrare a probelor electronice;

☐ executarea ordinului european de divulgare ar intra în conflict cu dreptul aplicabil al unei țări terțe. Vă rugăm să completați și secțiunea E.

(b) Vă rugăm să detaliați motivele neexecutării menționate la litera (a) și, dacă este necesar, indicați și justificați orice alte motive care nu sunt enumerate la litera (a):

… ....

SECȚIUNEA E: Obligații contradictorii care rezultă din dreptul unei țări terțe

În cazul obligațiilor contradictorii determinate de aplicabilitatea dreptului unei țări terțe, vă rugăm să includeți următoarele informații:

— titlul legii (legilor) țării terțe:

… ....

— dispoziția sau dispozițiile legale aplicabile și textul dispoziției sau dispozițiilor relevante:

… ....

— natura obligației conflictuale, inclusiv interesul protejat prin dreptul țării terțe:

☐ drepturile fundamentale ale persoanelor (vă rugăm să precizați):

… ....

☐ interese fundamentale ale țării terțe legate de securitatea și apărarea națională (vă rugăm să precizați):

… ....

☐ alte interese (vă rugăm să precizați):

… ....

— explicați de ce legea este aplicabilă în acest caz:

… ....

— explicați de ce considerați că există un conflict în acest caz:

… ....

— explicați legătura dintre furnizorul de servicii și țara terță în cauză:

… ....

— care ar putea fi consecințele pentru destinatar dacă respectă ordinul european de divulgare, inclusiv sancțiunile care ar putea fi aplicate:

… ....

Vă rugăm să adăugați orice alte informații pertinente: ....

SECȚIUNEA F: Cerere de informații/clarificări suplimentare (a se completa, dacă este cazul)

Sunt necesare informații suplimentare de la autoritatea emitentă pentru a fi executat EPOC/EPOC-PR

… ....

SECȚIUNEA G: Păstrarea datelor

Datele solicitate (a se bifa și completa căsuța corespunzătoare):

☐ sunt păstrate până în momentul în care sunt divulgate sau până când autoritatea emitentă sau, după caz, autoritatea de executare, precizează că datele nu mai trebuie păstrate și divulgate sau până când autoritatea emitentă a furnizat informațiile necesare pentru a permite restrângerea datelor care trebuie păstrate/divulgate

☐ nu sunt păstrate (ar trebui să fie doar un caz excepțional, de exemplu dacă furnizorul de servicii nu deține datele în momentul primirii solicitării sau nu poate identifica suficient de bine datele solicitate)

SECȚIUNEA H: Datele de contact ale sediului desemnat/reprezentantului legal al furnizorului de servicii

Denumirea sediului desemnat/reprezentantului legal al furnizorului de servicii:
.....

Numele persoanei de contact: ....

Funcția ocupată: .....

Adresa: .....

Numărul de telefon: (prefixul țării) (prefixul regiunii/localității) ....

Numărul de fax: (prefixul țării) (prefixul regiunii/localității) .....

Adresa de e-mail: .....

Numele persoanei autorizate: .....

Data .....

Semnătura ([2]): .....

([2]) Dacă nu se folosește sistemul informatic descentralizat, vă rugăm să adăugați o ștampilă oficială, un sigiliu electronic sau o metodă de autentificare echivalentă.

ANEXA IV

CATEGORII DE INFRACȚIUNI MENȚIONATE LA ARTICOLUL 12 ALINEATUL (1) LITERA (D)

1. participare la un grup infracțional organizat;

2. terorism;

3. trafic de ființe umane;

4. exploatarea sexuală a copiilor și pornografia infantilă;

5. traficul ilicit de stupefiante și de substanțe psihotrope;

6. traficul ilicit de arme, muniție și materiale explozive;

7. corupție;

8. frauda, inclusiv fraudă și alte infracțiuni care aduc atingere intereselor financiare ale Uniunii, definite în Directiva (UE) 2017/1371 a Parlamentului European și a Consiliului ([1]);

9. spălarea banilor obținuți din infracțiuni;

10. falsificarea bancnotelor, inclusiv falsificarea bancnotelor euro;

11. criminalitatea informatică;

12. infracțiunile împotriva mediului, inclusiv traficul ilicit de specii de animale pe cale de dispariție și traficul ilicit de specii și soiuri de plante pe cale de dispariție;

13. facilitarea intrării și șederii neautorizate;

14. omorul sau vătămarea corporală gravă;

15. traficul ilicit de organe și țesuturi umane;

16. răpirea, lipsirea de libertate în mod ilegal sau luarea de ostatici;

17. rasismul și xenofobia;

18. furtul organizat sau tâlhăria;

19. traficul ilicit de bunuri culturale, inclusiv antichități și opere de artă;

20. înșelăciunea;

21. tâlhăria și extorcarea de fonduri;

22. contrafacerea și piratarea de produse;

([1]) Directiva (UE) 2017/1371 a Parlamentului European și a Consiliului din 5 iulie 2017 privind combaterea fraudelor îndreptate împotriva intereselor financiare ale Uniunii prin mijloace de drept penal (JO L 198, 28.7.2017, p. 29).

23. falsul și uzul de fals în înscrisuri oficiale;

24. falsificarea mijloacelor de plată;

25. trafic ilicit de substanțe hormonale și alți factori de creștere;

26. traficul ilicit de materiale nucleare sau radioactive;

27. traficul de vehicule furate;

28. violul;

29. incendierea;

30. infracțiuni care țin de competența Curții Penale Internaționale;

31. capturarea ilicită a aeronavelor sau a navelor;

32. acte de sabotaj.

ANEXA V

CONFIRMAREA EMITERII UNEI CERERI DE DIVULGARE ÎN URMA UNUI ORDIN EUROPEAN DE PĂSTRARE

În temeiul Regulamentului (UE) 2023/1543 al Parlamentului European și al Consiliului ([1]), atunci când primește un ordin european de păstrare (EPOC-PR) destinatarul trebuie să păstreze, fără întârzieri nejustificate, datele solicitate. Perioada de păstrare încetează după 60 de zile, dacă autoritatea emitentă nu o prelungește cu încă 30 de zile sau dacă autoritatea emitentă nu confirmă că a fost lansată o cerere ulterioară de divulgare folosind formularul prevăzut în prezenta anexă.

După această confirmare, destinatarul trebuie să păstreze datele cât timp este necesar pentru a divulga datele, după ce primește cererea ulterioară de divulgare.

SECȚIUNEA A: Autoritatea emitentă EPOC-PR

Statul emitent:..... .....

Autoritatea emitentă:..... .....

Dacă diferă de punctul de contact indicat în EPOC-PR, autoritatea/punctul de contact (de exemplu, autoritatea centrală) care poate fi contactat pentru orice întrebare legată de executarea EPOC-PR:

Denumire și date de contact: ....

SECȚIUNEA B: Destinatarul EPOC-PR

Destinatarul:..... .....

Adresa: ....

Tel./Fax/e-mail (dacă se cunoaște): ....

Persoana de contact (dacă este cunoscută): ....

Numărul de dosar al destinatarului (dacă se cunoaște):..... .....

Furnizorul de servicii vizat (dacă este diferit de destinatar):.....

Orice alte informații relevante: ....

([1]) Regulamentul (UE) 2023/1543 al Parlamentului European și al Consiliului din 12 iulie 2023 privind ordinul european de divulgare a probelor electronice și ordinul european de păstrare a probelor electronice în cadrul procedurilor penale și pentru executarea pedepselor privative de libertate în urma unor proceduri penale (JO L 191, 28.7.2023, p. 118).

SECȚIUNEA C: Informații despre EPOC-PR

Datele sunt păstrate în conformitate cu EPOC-PR emis la ..... (indicați data emiterii cererii) și transmise în data de ..... (indicați data la care a fost transmisă cererea) cu numărul de dosar ..... (indicați numărul dosarului).

☐ a fost prelungită cu 30 de zile de autoritatea emitentă ...., numărul de dosar .... la ..... (bifați căsuța și indicați, dacă este cazul).

SECȚIUNEA D: Confirmare

Prin prezenta se confirmă că a fost emisă următoarea cerere de divulgare (bifați căsuța corespunzătoare și completați, dacă este necesar):

☐ Certificatul de ordin european de divulgare a probelor electronice emis de ..... (indicați autoritatea) în data de ..... (indicați data emiterii cererii) și transmis în data de ..... (indicați data la care a fost transmisă cererea) cu numărul de dosar ..... (indicați numărul dosarului) și transmis către ..... (indicați furnizorul de servicii/sediul desemnat/reprezentantul legal/autoritatea competentă către care a fost transmis și, dacă este disponibil, numărul de dosar dat de destinatar).

☐ Ordinul european de anchetă emis de ..... (indicați autoritatea) în data de ..... (indicați data emiterii cererii) și transmis în data de ..... (indicați data la care a fost transmisă cererea) cu numărul de dosar ..... (indicați numărul dosarului) și transmis către..... (indicați statul și autoritatea competentă către care a fost transmis și, dacă este disponibil, numărul de dosar dat de autoritățile solicitate).

☐ Cerere de acordare a asistenței judiciare reciproce emisă de ..... (indicați autoritatea) în data de..... (indicați data emiterii cererii) și transmisă în data de ..... (indicați data la care a fost transmisă cererea) cu numărul de dosar ..... (indicați numărul dosarului) și transmisă către ..... (indicați statul și autoritatea competentă către care a fost transmis și, dacă este disponibil, numărul de dosar dat de autoritățile solicitate).

Semnătura autorității emitente și/sau a reprezentantului acesteia

Nume: .....

Data: .....

Semnătura ([2]): .....

([2]) Dacă nu se folosește sistemul informatic descentralizat, vă rugăm să adăugați o ștampilă oficială, un sigiliu electronic sau o metodă de autentificare echivalentă.

ANEXA VI

PRELUNGIREA PERIOADEI DE PĂSTRARE A PROBELOR ELECTRONICE

În temeiul Regulamentului (UE) 2023/1543 al Parlamentului European și al Consiliului ([1]), atunci când primește un ordin european de păstrare (EPOC-PR) destinatarul trebuie să păstreze, fără întârzieri nejustificate, datele solicitate. Perioada de păstrare încetează după 60 de zile, cu excepția cazului în care autoritatea emitentă confirmă că a fost lansată o cerere ulterioară de divulgare. În această perioadă de 60 de zile, autoritatea emitentă poate prelungi durata de păstrare cu încă 30 de zile, dacă este necesar, pentru a permite emiterea unei cereri ulterioare de divulgare, utilizând formularul prevăzut în prezenta anexă.

SECȚIUNEA A: Autoritatea emitentă a EPOC-PR

Statul emitent:..... .....

Autoritatea emitentă:.....

Numărul de dosar al autorității emitente:..... .

Dacă diferă de punctul de contact indicat în EPOC-PR, autoritatea/punctul de contact (de exemplu, autoritatea centrală) care poate fi contactat pentru orice întrebare legată de executarea EPOC-PR:

Denumire și date de contact ....

SECȚIUNEA B: Destinatarul EPOC-PR

Destinatarul:..... .....

Adresa:..... .....

Tel./Fax/e-mail (dacă se cunoaște): ....

Persoana de contact (dacă este cunoscută):..... .....

Numărul de dosar al destinatarului (dacă se cunoaște):.....

Furnizorul de servicii vizat (dacă este diferit de destinatar):.....

Orice alte informații utile:..... .....

SECȚIUNEA C: Informații despre EPOC-PR precedent

Datele sunt păstrate în conformitate cu EPOC-PR emis în data de …..... (indicați data emiterii cererii) și transmis în data de …..... (indicați data transmiterii cererii) cu numărul de dosar …..... (indicați numărul dosarului) și transmis către ….....

([1]) Regulamentul (UE) 2023/1543 al Parlamentului European și al Consiliului din 12 iulie 2023 privind ordinul european de divulgare a probelor electronice și ordinul european de păstrare a probelor electronice în cadrul procedurilor penale și pentru executarea pedepselor privative de libertate în urma unor proceduri penale (JO L 191, 28.7.2023, p. 118).

SECȚIUNEA D: Prelungirea ordinului de păstrare precedent

Obligația de a păstra datele în temeiul EPOC-PR, precizată în secțiunea C, se prelungește cu încă 30 de zile.

Semnătura autorității emitente și/sau a reprezentantului acesteia

Nume: … .....

Data: ….....

Semnătura ([2]): ….....

([2]) Dacă nu se folosește sistemul informatic descentralizat, vă rugăm să adăugați o ștampilă oficială, un sigiliu electronic sau o metodă de autentificare echivalentă.