REGULAMENTUL (UE) 2018/1807 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 14 noiembrie 2018

privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 114,

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]),

după consultarea Comitetului Regiunilor,

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

întrucât:

(1) Digitalizarea economiei se accelerează. Tehnologiile informației și comunicațiilor nu mai reprezintă un sector specific, ci fundamentul tuturor sistemelor economice și al societăților inovatoare moderne. Datele electronice se află în centrul acestor sisteme și pot genera o valoare semnificativă atunci când sunt analizate sau utilizate împreună cu servicii și produse. În același timp, dezvoltarea rapidă a economiei bazate pe date și a tehnologiilor emergente, cum ar fi inteligența artificială, produsele și serviciile legate de internetul obiectelor, sistemele autonome și 5G, prezintă noi aspecte juridice privind accesul la date și reutilizarea acestora, răspunderea, etica și solidaritatea. Ar trebui să se lucreze în ceea ce privește chestiunea răspunderii, în special prin implementarea unor coduri de autoreglementare și a altor bune practici, având în vedere recomandările, deciziile și acțiunile adoptate fără interacțiune umană de-a lungul întregului lanț valoric de prelucrare a datelor. Această muncă ar putea să privească de asemenea mecanismele adecvate pentru stabilirea răspunderii, pentru transferul responsabilității între serviciile care cooperează, pentru asigurări și pentru audit.

(2) Lanțurile valorice ale datelor se bazează pe diferite activități legate de date: crearea și colectarea datelor; agregarea și organizarea datelor; prelucrarea datelor; analiza, comercializarea și distribuirea datelor; utilizarea și reutilizarea datelor. Funcționarea eficace și eficientă a prelucrării datelor este o componentă fundamentală a oricărui lanț valoric al datelor. Cu toate acestea, funcționarea eficace și eficientă a prelucrării datelor și dezvoltarea economiei bazate pe date în Uniune sunt afectate, în special, de două tipuri de obstacole în calea mobilității datelor și a pieței interne: cerințele stabilite de către autoritățile statelor membre privind localizarea datelor și practicile privind dependența de furnizor („vendor lock-in”) în sectorul privat.

(3) Libertatea de stabilire și libertatea de a furniza servicii în temeiul Tratatului privind funcționarea Uniunii Europene (TFUE) se aplică serviciilor de prelucrare a datelor. Totuși, furnizarea acestor servicii este îngreunată sau uneori împiedicată de anumite cerințe naționale, regionale sau locale de localizare a datelor într-un anumit teritoriu.

(4) Aceste obstacole în calea liberei circulații a serviciilor de prelucrare a datelor și a dreptului de stabilire a furnizorilor de servicii sunt generate de cerințele prevăzute de legislațiile statelor membre de a localiza datele într-o anumită zonă geografică sau într-un anumit teritoriu în scopul prelucrării datelor. Alte norme sau practici administrative au un efect echivalent prin impunerea unor cerințe specifice care fac mai dificilă prelucrarea datelor în afara unei anumite zone geografice sau a unui anumit teritoriu din Uniune, cum ar fi cerințele de a utiliza mijloacele tehnologice care sunt certificate sau aprobate într-un anumit stat membru. Securitatea juridică, în măsura în care privește cerințele legitime și ilegitime de localizare a datelor, limitează și mai mult opțiunile aflate la dispoziția actorilor de pe piață și a sectorului public în ceea ce privește localizarea prelucrării datelor. Prezentul regulament nu limitează în niciun fel libertatea întreprinderilor de a încheia contracte care precizează locul în care trebuie să se afle datele. Prezentul regulament urmărește doar să protejeze această libertate, prin garantarea faptului că locul convenit poate fi situat oriunde în Uniune.

([1]) JO C 227, 28.6.2018, p. 78.
([2]) Poziția Parlamentului European din 4 octombrie 2018 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 6 noiembrie 2018.

(5) În același timp, mobilitatea datelor în Uniune este împiedicată, de asemenea, de restricții private: aspecte juridice, contractuale și tehnice care îi stânjenesc sau îi împiedică pe utilizatorii de servicii de prelucrare a datelor să își porteze datele de la un furnizor de servicii la altul sau înapoi către propriile sisteme informatice, în special la încetarea contractului lor cu un furnizor de servicii.

(6) Combinarea acestor obstacole a dus la o lipsă a concurenței între furnizorii de servicii de cloud din Uniune, la diferite probleme legate de dependența de furnizor și la o gravă lipsă de mobilitate a datelor. În mod similar, politicile de localizare a datelor au subminat capacitatea întreprinderilor din domeniul cercetării și dezvoltării de a facilita colaborarea între întreprinderi, universități și alte organizații de cercetare pentru a stimula inovarea.

(7) Din motive de securitate juridică și datorită necesității unor condiții de concurență echitabile în Uniune, un set unic de norme pentru toți participanții la piață reprezintă un element-cheie pentru funcționarea pieței interne. Pentru a elimina obstacolele din calea schimburilor comerciale și denaturările concurenței generate de divergențele dintre legislațiile naționale și pentru a împiedica apariția unor noi astfel de obstacole în calea schimburilor comerciale și denaturări semnificative ale concurenței, este necesar să se adopte norme uniforme aplicabile în toate statele membre.

(8) Cadrul juridic privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice, în special Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([1]) și Directivele (UE) 2016/680 ([2]) și 2002/58/CE ([3]) ale Parlamentului European și ale Consiliului nu sunt afectate de prezentul regulament.

(9) Internetul obiectelor, inteligența artificială și învățarea automatizată, aflate în expansiune, constituie surse importante de date fără caracter personal, de exemplu ca urmare a utilizării acestora în procesele automatizate de producție industrială. Exemple specifice de date fără caracter personal includ seturile de date agregate și anonimizate utilizate pentru analiza volumelor mari de date, datele privind agricultura de precizie, care pot contribui la monitorizarea și optimizarea utilizării pesticidelor și a apei sau date privind necesitățile de întreținere a mașinilor industriale. Dacă progresele tehnologice fac posibilă transformarea datelor anonimizate în date cu caracter personal, astfel de date urmează să fie tratate ca date cu caracter personal, iar Regulamentul (UE) 2016/679 urmează să se aplice în mod corespunzător.

(10) În temeiul Regulamentului (UE) 2016/679, statele membre nu pot nici să limiteze, nici să interzică libera circulație a datelor cu caracter personal în cadrul Uniunii din motive legate de protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal. Prezentul regulament stabilește același principiu al liberei circulații în cadrul Uniunii pentru datele fără caracter personal, cu excepția cazului în care o restricție sau o interdicție este justificată din motive de securitate publică. Regulamentul (UE) 2016/679 și prezentul regulament prevăd o serie coerentă de norme care reglementează libera circulație a diferitelor tipuri de date. În plus, prezentul regulament nu impune obligația de a stoca separat diferitele tipuri de date.

(11) În vederea creării unui cadru pentru libera circulație a datelor fără caracter personal în Uniune și a fundamentului pentru dezvoltarea unei economii bazate pe date și sporirea competitivității industriei Uniunii, este necesar să se definească un cadru juridic clar, cuprinzător și previzibil pentru prelucrarea datelor, altele decât datele cu caracter personal, în piața internă. O abordare bazată pe principii care prevede cooperarea dintre statele membre, precum și autoreglementarea ar trebui să asigure o flexibilitate suficientă a cadrului încât acesta să poată ține seama de nevoile în continuă evoluție ale utilizatorilor, ale furnizorilor de servicii și ale autorităților naționale din Uniune. Pentru a evita riscul de suprapunere cu mecanismele existente și, prin urmare, o sporire a sarcinii suportate atât de statele membre, cât și de întreprinderi, nu ar trebui stabilite norme tehnice detaliate.

(12) Prezentul regulament nu ar trebui să afecteze prelucrarea datelor, în măsura în care se desfășoară ca parte dintr-o activitate care nu intră sub incidența dreptului Uniunii. În special, ar trebui reamintit faptul că, în conformitate cu articolul 4 din Tratatul privind Uniunea Europeană (TUE), securitatea națională ține de responsabilitatea exclusivă a fiecărui stat membru.

([1]) 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).

([2]) 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).

([3]) 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).

(13) Libera circulație a datelor în Uniune va juca un rol important în realizarea creșterii și a inovării bazate pe date. La fel ca întreprinderile și consumatorii, autoritățile publice și organismele de drept public ale statelor membre urmează să beneficieze de o libertate mai mare de alegere în ceea ce privește furnizorii de servicii bazate pe date, de prețuri mai competitive și de furnizarea mai eficientă a serviciilor pentru cetățeni. Având în vedere cantitățile mari de date pe care le gestionează, este extrem de important ca autoritățile publice și organismele de drept public să dea un exemplu prin utilizarea serviciilor de prelucrare a datelor și să nu impună restricții în materie de localizare a datelor când folosesc servicii de prelucrare a datelor. Prin urmare, autoritățile publice și organismele de drept public ar trebui să facă obiectul prezentului regulament. În această privință, principiul liberei circulații a datelor fără caracter personal prevăzut de prezentul regulament ar trebui să se aplice, de asemenea, practicilor administrative generale și consecvente și altor cerințe în materie de localizare a datelor în domeniul achizițiilor publice, fără a aduce atingere Directivei 2014/24/UE a Parlamentului European și a Consiliului ([1]).

(14) La fel ca în cazul Directivei 2014/24/UE, prezentul regulament nu aduce atingere actelor cu putere de lege și actelor administrative referitoare la organizarea internă a statelor membre și care atribuie, în rândul autorităților publice și organismelor de drept public, competențe și responsabilități pentru procesarea datelor, fără remunerarea contractuală a părților private, precum și actelor cu putere de lege și actelor administrative ale statelor membre care reglementează punerea în aplicare a acestor competențe și responsabilități. Chiar dacă autoritățile publice și organismele de drept public sunt încurajate să ia în considerare avantajele economice și alte beneficii ale externalizării către furnizori externi de servicii, aceștia pot avea motive legitime pentru a alege furnizarea internă a serviciilor sau internalizarea. În consecință, nicio dispoziție din prezentul regulament nu obligă statele membre să contracteze sau să externalizeze furnizarea serviciilor pe care doresc să le presteze ele însele sau să le organizeze prin alte mijloace decât prin contracte de achiziții publice.

(15) Prezentul regulament ar trebui să se aplice persoanelor fizice sau juridice care furnizează servicii de prelucrare a datelor pentru utilizatori care își au reședința sau sunt stabiliți în Uniune, inclusiv celor care furnizează servicii de prelucrare a datelor pe teritoriul Uniunii fără a fi stabiliți în Uniune. Prezentul regulament nu ar trebui să se aplice, așadar, serviciilor de prelucrare a datelor care sunt furnizate în afara Uniunii și cerințelor de localizare a datelor referitoare la astfel de date.

(16) Prezentul regulament nu prevede normele referitoare la stabilirea legii aplicabile în materie comercială și, prin urmare, nu aduce atingere dispozițiilor din Regulamentul (CE) nr. 593/2008 al Parlamentului European și al Consiliului ([2]). În special, în măsura în care legea aplicabilă unui contract nu a fost aleasă în conformitate cu regulamentul respectiv, un contract de furnizare de servicii este, în principiu, reglementat de dreptul țării în care își are sediul obișnuit furnizorul de servicii.

(17) Prezentul regulament ar trebui să se aplice prelucrării datelor în sensul cel mai larg, cuprinzând utilizarea tuturor tipurilor de sisteme informatice, indiferent dacă acestea se află la sediul utilizatorului sau sunt externalizate către un furnizor de servicii. Prezentul regulament ar trebui să acopere prelucrarea datelor la diferite niveluri de intensitate, de la stocarea datelor [infrastructura ca serviciu (IaaS)] la prelucrarea datelor pe platforme [platforma ca serviciu (PaaS)] sau în aplicații [software-ul ca serviciu (SaaS)].

(18) Cerințele de localizare a datelor reprezintă un obstacol clar în calea liberei furnizări a serviciilor de prelucrare a datelor în Uniune și în calea pieței interne. Prin urmare, acestea ar trebui interzise, cu excepția cazului în care sunt justificate din motive de siguranță publică, astfel cum sunt definite de dreptul Uniunii, în special în sensul articolului 52 din TFUE, și respectă principiul proporționalității, prevăzut la articolul 5 din TUE. Pentru a pune în aplicare principiul liberei circulații a datelor fără caracter personal la nivel transfrontalier, pentru a asigura eliminarea rapidă a cerințelor existente de localizare a datelor și pentru a permite, din motive operaționale, prelucrarea datelor în mai multe locuri din Uniune și deoarece prezentul regulament prevede măsuri de asigurare a disponibilității datelor în scopuri de control de reglementare, statele membre ar trebui să poată invoca numai siguranța publică drept justificare pentru cerințele de localizare a datelor.

(19) Conceptul de „siguranță publică”, în sensul articolului 52 din TFUE și conform interpretării date de Curtea de Justiție, cuprinde atât securitatea internă, cât și cea externă a unui stat membru, precum și aspectele siguranței publice, în special pentru a facilita investigarea, depistarea și urmărirea penală a infracțiunilor. Aceasta presupune existența unei amenințări reale și suficient de grave care afectează unul dintre interesele fundamentale ale societății, cum ar fi o amenințare la adresa funcționării instituțiilor și a serviciilor publice esențiale și la adresa supraviețuirii populației, precum și riscul unei perturbări grave a relațiilor externe sau a conviețuirii pașnice a națiunilor ori un risc la adresa intereselor militare. În conformitate cu principiul proporționalității, cerințele privind localizarea datelor care sunt justificate din motive de siguranță publică ar trebui să fie adecvate pentru îndeplinirea obiectivului urmărit și nu ar trebui să depășească ceea ce este necesar pentru atingerea acestui obiectiv.

([1]) Directiva 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE (JO L 94, 28.3.2014, p. 65).

([2]) Regulamentul (CE) nr. 593/2008 al Parlamentului European și al Consiliului din 17 iunie 2008 privind legea aplicabilă obligațiilor contractuale (Roma I) (JO L 177, 4.7.2008, p. 6).

(20) Pentru a se asigura aplicarea eficace a principiului liberei circulații a datelor fără caracter personal la nivel transfrontalier și pentru a preveni apariția unor noi bariere în calea bunei funcționări a pieței interne, statele membre ar trebui să comunice imediat Comisiei orice proiect de act care introduce o nouă cerință de localizare a datelor sau modifică o cerință existentă de localizare a datelor. Aceste proiecte de acte ar trebui să fie prezentate și evaluate în conformitate cu Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului ([1]).

(21) În plus, pentru a elimina potențialele bariere existente, în decursul unei perioade de tranziție de 24 de luni de la data aplicării prezentului regulament, statele membre ar trebui să efectueze o examinare a actelor cu putere de lege și a actelor administrative cu caracter general care stabilesc cerințele existente de localizare a datelor și să comunice Comisiei orice astfel de cerință de localizare a datelor pe care o consideră ca fiind conformă cu prezentul regulament, împreună cu o justificare pentru aceasta. Acest fapt ar trebui să permită Comisiei să examineze conformitatea oricăror cerințe rămase de localizare a datelor. Comisia ar trebui să poată, după caz, să trimită observații statului membru în cauză. Astfel de observații ar putea include o recomandare de modificare sau de abrogare a cerinței de localizare a datelor.

(22) Obligația stabilită prin prezentul regulament de a comunica Comisiei cerințele existente de localizare a datelor și proiectele de acte ar trebui să se aplice cerințelor normative de localizare a datelor și proiectelor de acte cu caracter general, dar nu deciziilor adresate unei anumite persoane fizice sau juridice.

(23) În vederea asigurării transparenței cerințelor de localizare a datelor în statele membre stabilite într-un act cu putere de lege sau act administrativ cu caracter general pentru persoanele fizice și juridice, cum ar fi furnizorii de servicii și utilizatorii de servicii de prelucrare a datelor, statele membre ar trebui să publice informații privind astfel de cerințe la un punct național unic de informare online și să actualizeze periodic aceste informații. În mod alternativ, statele membre ar trebui să ofere informații actualizate cu privire la astfel de cerințe la un punct de informare central stabilit în temeiul altui act al Uniunii. Pentru a informa în mod corespunzător persoanele fizice și juridice cu privire la cerințele de localizare a datelor la nivelul întregii Uniuni, statele membre ar trebui să notifice Comisiei adresele acestor puncte unice de informare. Comisia ar trebui să publice aceste informații pe propriul site web, împreună cu o listă consolidată actualizată periodic a tuturor cerințelor de localizare a datelor în vigoare în statele membre, care include și informații pe scurt referitoare la respectivele cerințe.

(24) Cerințele de localizare a datelor decurg în mod frecvent dintr-o lipsă de încredere în prelucrarea datelor la nivel transfrontalier, care rezultă din presupusa indisponibilitate a datelor pentru scopurile autorităților competente din statele membre, cum ar fi inspecția și auditul sau controlul de reglementare sau de supraveghere. Această lipsă de încredere nu poate fi depășită numai prin nulitatea clauzelor contractuale care interzic accesul legal la date din partea autorităților competente pentru îndeplinirea atribuțiilor lor oficiale. Prin urmare, prezentul regulament ar trebui să stipuleze în mod clar faptul că nu aduce atingere competențelor autorităților competente de a solicita și de a obține accesul la date, în conformitate cu dreptul Uniunii sau cu dreptul intern, și că autorităților competente nu le poate fi refuzat accesul la date pe motiv că datele sunt prelucrate în alt stat membru. Autoritățile competente pot impune cerințe funcționale pentru a sprijini accesul la date, cum ar fi obligația ca descrierile sistemului să fie păstrate în statul membru în cauză.

(25) Persoanele fizice sau juridice care sunt supuse obligațiilor de a furniza date autorităților competente se pot conforma acestor obligații prin furnizarea și garantarea accesului electronic eficace și în timp util la date pentru autoritățile competente, indiferent de statul membru pe teritoriul căruia datele sunt prelucrate. Acest acces poate fi asigurat prin intermediul termenilor și clauzelor concrete prevăzute în contractele încheiate între persoanele fizice sau juridice supuse obligației de a oferi acces și furnizorii de servicii.

(26) În cazul în care o persoană fizică sau juridică este supusă obligației de a furniza date și nu respectă obligația respectivă, autoritatea competentă ar trebui să fie în măsură să solicite asistență din partea autorităților competente din alte state membre. În astfel de cazuri, autoritățile competente ar trebui să utilizeze instrumentele de cooperare specifice prevăzute în dreptul Uniunii sau în acordurile internaționale, în funcție de obiectul specific fiecărui caz, de exemplu, în domeniul cooperării polițienești, al justiției penale sau civile sau, respectiv, în materie

([1]) 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).

administrativă, Decizia-cadru 2006/960/JAI a Consiliului ([1]), Directiva 2014/41/UE a Parlamentului European și a Consiliului ([2]), Convenția Consiliului Europei privind criminalitatea informatică ([3]), Regulamentul (CE) nr. 1206/2001 al Consiliului ([4]), Directiva 2006/112/CE a Consiliului ([5]) și Regulamentul (UE) nr. 904/2010 al Consiliului ([6]). În absența unor astfel de mecanisme de cooperare specifice, autoritățile competente ar trebui să coopereze pentru a oferi acces la datele solicitate, prin intermediul punctelor unice de contact desemnate.

(27) În cazul în care o cerere de asistență implică obținerea accesului la orice spațiu al unei persoane fizice sau juridice, inclusiv la orice echipamente și mijloace de prelucrare a datelor, de către autoritatea solicitată, acest acces trebuie să fie conform cu dreptul Uniunii sau cu dreptul procedural intern, inclusiv orice obligație de a obține o autorizație judiciară prealabilă.

(28) Prezentul regulament nu ar trebui să permită utilizatorilor să încerce să eludeze aplicarea dreptului intern. Prin urmare, statele membre ar trebui să prevadă sancțiuni eficace, proporționale și disuasive pentru utilizatorii care împiedică autoritățile competente să primească acces la datele lor necesare pentru îndeplinirea sarcinilor oficiale ale autorităților competente în conformitate cu dreptul Uniunii și dreptul intern. În cazuri urgente, atunci când un utilizator abuzează de dreptul său, statele membre ar trebui să aibă capacitatea să impună măsuri strict proporționale și provizorii. Orice măsură provizorie care necesită relocalizarea datelor pentru o perioadă mai lungă de 180 de zile de la relocalizare s-ar îndepărta de principiul liberei circulații a datelor pentru o perioadă semnificativă și, așadar, ar trebui să fie comunicată Comisiei pentru verificarea compatibilității sale cu dreptul Uniunii.

(29) Capacitatea de a porta datele fără obstacole este un factor esențial în facilitarea posibilității de alegere a utilizatorului și a concurenței eficace pe piețele de servicii de prelucrare a datelor. Dificultățile reale sau percepute de a porta datele la nivel transfrontalier subminează, de asemenea, încrederea utilizatorilor profesioniști atunci când acceptă ofertele transfrontaliere și, prin urmare, încrederea acestora în piața internă. În timp ce consumatorii individuali beneficiază de dreptul existent al Uniunii, capacitatea de a schimba furnizorii de servicii nu este facilitată pentru utilizatori în cadrul activităților comerciale sau profesionale ale acestora. Existența unor cerințe tehnice consecvente pe întreg teritoriul Uniunii, fie în legătură cu armonizarea tehnică, fie prin recunoaștere reciprocă sau armonizare voluntară contribuie, de asemenea, la dezvoltarea unei piețe interne competitive a serviciilor de prelucrare a datelor.

(30) Pentru a beneficia pe deplin de mediul concurențial, utilizatorii profesioniști ar trebui să fie în măsură să facă alegeri în cunoștință de cauză și să compare cu ușurință componentele individuale ale diverselor servicii de prelucrare a datelor oferite pe piața internă, inclusiv în ceea ce privește termenii și clauzele contractuale de portare a datelor la încheierea unui contract. În vederea alinierii la potențialul de inovare al pieței și pentru a lua în considerare experiența și cunoștințele de specialitate ale furnizorilor de servicii și ale utilizatorilor profesioniști de servicii de prelucrare a datelor, informațiile detaliate și cerințele operaționale pentru portarea datelor ar trebui să fie definite de actorii de pe piață prin autoreglementare, încurajată, facilitată și monitorizată de Comisie, sub formă de coduri de conduită ale Uniunii care ar putea include un model de termeni și clauze contractuale.

(31) Pentru a fi eficiente și pentru a facilita schimbarea furnizorului de servicii și portarea datelor, astfel de coduri de conduită ar trebui să fie cuprinzătoare și să includă cel puțin aspectele esențiale importante în cadrul procesului de portare a datelor, precum procesele folosite pentru copiile de siguranță ale datelor și locația acestora; formatele și suporturile disponibile ale datelor; configurația informatică necesară și lărgimea minimă de bandă; perioada de timp necesară înainte de a începe procesul de portare și perioada de timp pe parcursul căreia datele vor rămâne disponibile pentru portare; și garanțiile privind accesarea datelor în cazul falimentului furnizorului de servicii. De asemenea, codurile de conduită ar trebui să precizeze clar că dependența de furnizor nu este o practică comercială acceptabilă, să prevadă tehnologii care să mărească încrederea clienților și să fie actualizate periodic pentru a ține pasul cu evoluțiile tehnologice. Comisia ar trebui să se asigure că toate părțile interesate relevante, inclusiv asociațiile de întreprinderi mici și mijlocii (IMM-uri) și de întreprinderi nou-înființate, utilizatorii și furnizorii de servicii de tip cloud să fie consultate în acest proces. Comisia ar trebui să evalueze elaborarea și eficacitatea aplicării unor astfel de coduri de conduită.

([1]) Decizia-cadru 2006/960/JAI a Consiliului din 18 decembrie 2006 privind simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii ale statelor membre ale Uniunii Europene (JO L 386, 29.12.2006, p. 89).

([2]) 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).

([3]) Convenția Consiliului Europei privind criminalitatea informatică, STCE nr. 185.

([4]) Regulamentul (CE) nr. 1206/2001 al Consiliului din 28 mai 2001 privind cooperarea între instanțele statelor membre în domeniul obținerii de probe în materie civilă sau comercială (JO L 174, 27.6.2001, p. 1).

([5]) Directiva 2006/112/CE a Consiliului din 28 noiembrie 2006 privind sistemul comun al taxei pe valoarea adăugată (JO L 347, 11.12.2006, p. 1).

([6]) Regulamentul (UE) nr. 904/2010 al Consiliului din 7 octombrie 2010 privind cooperarea administrativă și combaterea fraudei în domeniul taxei pe valoarea adăugată (JO L 268, 12.10.2010, p. 1).

(32) În cazul în care o autoritate competentă dintr-un stat membru solicită asistență din partea unui alt stat membru pentru a obține acces la date în temeiul prezentului regulament, aceasta ar trebui ca, printr-un punct unic de contact desemnat, să transmită punctului unic de contact desemnat din cel din urmă stat membru o cerere motivată în mod corespunzător, care ar trebui să includă o explicație scrisă a motivelor și temeiurile juridice pentru solicitarea accesului la date. Punctul unic de contact desemnat de statul membru a cărui asistență este solicitată ar trebui să faciliteze transmiterea cererii către autoritatea competentă relevantă din statul membru solicitat. Pentru a se asigura o cooperare eficace, autoritatea căreia îi este transmisă cererea ar trebui să ofere asistență fără întârzieri nejustificate ca răspuns la o anumită cerere sau să furnizeze informații privind dificultățile întâmpinate în soluționarea unei astfel de cereri sau privind motivele de refuz al acesteia.

(33) Consolidarea încrederii în securitatea prelucrării datelor la nivel transfrontalier ar trebui să reducă tendința actorilor de pe piață și a sectorului public de a utiliza localizarea datelor ca un indicator pentru securitatea datelor. De asemenea, aceasta ar trebui să îmbunătățească securitatea juridică pentru întreprinderi cu privire la îndeplinirea cerințelor de securitate aplicabile atunci când își externalizează activitățile de prelucrare a datelor către furnizorii de servicii, inclusiv către cei din alte state membre.

(34) Orice cerințe de securitate legate de prelucrarea datelor care se aplică în mod justificat și proporțional în temeiul dreptului Uniunii sau al dreptului intern în conformitate cu dreptul Uniunii în statul membru de ședere sau de stabilire al persoanelor fizice sau juridice ale căror date sunt vizate ar trebui să continue să se aplice pentru prelucrarea acestor date în alt stat membru. Respectivele persoane fizice sau juridice ar trebui să fie în măsură să îndeplinească aceste cerințe fie direct, fie prin intermediul unor clauze contractuale prevăzute în contractele încheiate cu furnizorii de servicii.

(35) Cerințele de securitate stabilite la nivel național ar trebui să fie necesare și proporționale cu riscurile la adresa securității prelucrării datelor din domeniul de aplicare al dreptului intern în care sunt stabilite aceste cerințe.

(36) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului ([1]) prevede măsuri juridice pentru sporirea nivelului global al securității cibernetice în Uniune. Serviciile de prelucrare a datelor se numără printre serviciile digitale care intră sub incidența directivei menționate. Conform directivei menționate, statele membre urmează să se asigure că furnizorii de servicii digitale identifică și iau măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care le utilizează. Aceste măsuri ar trebui să asigure un nivel de securitate adecvat riscului existent și să țină cont de securitatea sistemelor și a instalațiilor, de gestionarea incidentelor, de gestionarea continuității activității, de monitorizare, auditare și testare, precum și de conformitatea cu standardele internaționale. Aceste elemente urmează să fie precizate de către Comisie în actele de punere în aplicare în temeiul directivei menționate.

(37) Comisia ar trebui să prezinte un raport cu privire la punerea în aplicare a prezentului regulament, în special pentru a stabili dacă este necesar să se efectueze modificări ca urmare a evoluțiilor tehnologice sau ale pieței. Acest raport ar trebui să evalueze îndeosebi punerea în aplicare a prezentului regulament în ceea ce privește seturile de date compuse din date cu caracter personal și date fără caracter personal, precum și punerea în aplicare a excepției privind siguranța publică. Înainte ca prezentul regulament să înceapă să se aplice, Comisia ar trebui de asemenea să publice orientări cu caracter informativ cu privire la modalitatea de gestionare a seturilor de date compuse din date cu caracter personal și date fără caracter personal, pentru ca întreprinderile, inclusiv IMM-urile, să înțeleagă mai bine interacțiunea dintre prezentul regulament și Regulamentul (UE) 2016/679 și să asigure conformitatea cu ambele.

(38) Prezentul regulament respectă drepturile fundamentale și principiile recunoscute, în special, de Carta drepturilor fundamentale a Uniunii Europene, și ar trebui să fie interpretat și aplicat în conformitate cu aceste drepturi și principii, inclusiv dreptul la protecția datelor cu caracter personal, libertatea de expresie și de informare și libertatea de a desfășura o activitate comercială.

(39) Deoarece obiectivul prezentului regulament, și anume asigurarea liberei circulații a datelor, altele decât datele cu caracter personal în Uniune, nu poate fi realizat în mod satisfăcător de către statele membre, dar, având în vedere amploarea și efectele sale, 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 definit la articolul menționat, prezentul regulament nu depășește ceea ce este necesar pentru realizarea acestui obiectiv,

([1]) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Obiect

Prezentul regulament urmărește să asigure libera circulație a datelor, altele decât datele cu caracter personal, în cadrul Uniunii, prin stabilirea de norme privind cerințele de localizare a datelor, disponibilitatea datelor pentru autoritățile competente și portarea datelor pentru utilizatorii profesioniști.

Articolul 2

Domeniul de aplicare

(1) Prezentul regulament se aplică prelucrării datelor electronice, altele decât datele cu caracter personal, în Uniune, care:

(a) este furnizată ca serviciu utilizatorilor ce își au reședința ori au sunt stabiliți în Uniune, indiferent dacă furnizorul de servicii este stabilit sau nu în Uniune; sau

(b) este efectuată de o persoană fizică sau juridică ce își are reședința ori este stabilită în Uniune pentru propriile sale nevoi.

(2) În cazul unui set de date compus atât din date cu caracter personal, cât și din date fără caracter personal, prezentul regulament se aplică părții din set cu date fără caracter personal. În cazul în care datele cu caracter personal și cele fără caracter personal dintr-un set de date sunt legate între ele în mod indisolubil, prezentul regulament nu aduce atingere aplicării Regulamentului (UE) 2016/679.

(3) Prezentul regulament nu se aplică

unei activități care nu intră sub incidența dreptului Uniunii. Prezentul regulament nu aduce atingere actelor cu putere de lege și actelor administrative referitoare la organizarea internă a statelor membre și care atribuie în rândul autorităților publice și al organismelor de drept public, astfel cum sunt definite la articolul 2 alineatul (1) punctul 4 din Directiva 2014/24/UE, competențe și responsabilități în materie de prelucrare a datelor, fără remunerarea contractuală a părților private, și nici actelor cu putere de lege și actelor administrative ale statelor membre care reglementează punerea în aplicare a acestor competențe și responsabilități.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „date” înseamnă date, altele decât datele cu caracter personal definite la articolul 4 punctul 1 din Regulamentul (UE) 2016/679;

2. „prelucrare” înseamnă orice operațiune sau serie de operațiuni efectuate asupra datelor sau a seturilor de date în format electronic, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

3. „proiect de act” înseamnă un text redactat în vederea adoptării ca act cu putere de lege sau act administrativ cu caracter general, textul respectiv fiind în stadiul de elaborare în care i se pot încă aduce modificări de fond;

4. „furnizor de servicii” înseamnă o persoană fizică sau juridică ce furnizează servicii de prelucrare a datelor;

5. „cerință de localizare a datelor” înseamnă orice obligație, interdicție, condiție, limită sau altă cerință prevăzută în actele cu putere de lege sau actele administrative ale unui stat membru sau care rezultă din practicile administrative generale și consecvente ale unui stat membru și ale organismelor de drept public, inclusiv în domeniul achizițiilor publice, fără a aduce atingere Directivei 2014/24/UE, care impune prelucrarea datelor pe teritoriul unui anumit stat membru sau împiedică prelucrarea datelor în orice alt stat membru;

6. „autoritate competentă” înseamnă o autoritate a unui stat membru sau orice altă entitate autorizată în temeiul dreptului intern să exercite o funcție publică sau autoritate oficială, care are competența de a obține acces la datele prelucrate de o persoană fizică ori juridică în exercitarea atribuțiilor sale oficiale, în conformitate cu dreptul Uniunii sau dreptul intern;

7. „utilizator” înseamnă o persoană fizică sau juridică, inclusiv o autoritate publică sau un organism de drept public, ce utilizează ori solicită un serviciu de prelucrare a datelor;

8. „utilizator profesionist” înseamnă o persoană fizică sau juridică, inclusiv o autoritate publică sau un organism de drept public, care utilizează ori solicită un serviciu de prelucrare a datelor în scopuri legate de activitatea sa comercială, industrială, artizanală sau profesională ori de sarcinile sale.

Articolul 4

Libera circulație a datelor în cadrul Uniunii

(1) Cerințele de localizare a datelor sunt interzise, cu excepția cazului în care acestea sunt justificate din motive de siguranță publică, în conformitate cu principiul proporționalității.

Primul paragraf de la prezentul alineat nu aduce atingere alineatului (3) și cerințelor de localizare a datelor stabilite în temeiul legislației existente a Uniunii.

(2) Statele membre comunică imediat Comisiei orice proiect de act care introduce o nouă cerință de localizare a datelor sau care aduce modificări unei cerințe existente de localizare a datelor, în conformitate cu procedurile stabilite la articolele 5, 6 și 7 din Directiva (UE) 2015/1535.

(3) Până la 30 mai 2021, statele membre se asigură că orice cerință de localizare a datelor existentă, care este prevăzută într-un act cu putere de lege sau dispoziție act administrativ cu caracter general și care nu respectă alineatul (1) de la prezentul articol este eliminată.

Până la 30 mai 2021, dacă un stat membru consideră că o măsură existentă care conține o cerință de localizare a datelor respectă alineatul (1) de la prezentul articol și poate, prin urmare, să rămână în vigoare, acesta comunică Comisiei măsura respectivă, împreună cu o justificare pentru menținerea sa în vigoare. Fără a aduce atingere dispozițiilor articolului 258 din TFUE, Comisia, în termen de șase luni de la data primirii unei astfel de comunicări, examinează conformitatea măsurii respective cu alineatul (1) de la prezentul articol și, dacă este cazul, trimite observații statului membru în cauză, inclusiv, dacă este necesar, recomandând modificarea sau abrogarea măsurii respective.

(4) Statele membre se asigură că informațiile referitoare la orice cerință de localizare a datelor prevăzută într-un act cu putere de lege sau într-un act administrativ cu caracter general și care este aplicabilă pe teritoriul lor sunt disponibile publicului prin intermediul unui punct unic de informare online național, pe care îl actualizează periodic, sau furnizează informații actualizate cu privire la orice astfel de cerințe de localizare unui punct central de informare creat în temeiul unui alt act al Uniunii.

(5) Statele membre informează Comisia cu privire la adresa punctului unic de informare menționat la alineatul (4). Comisia publică linkurile către aceste puncte pe site-ul său web, împreună cu o listă consolidată, actualizată periodic, a tuturor cerințelor de localizare a datelor menționate la alineatul (4), inclusiv informații de sinteză despre cerințele respective.

Articolul 5

Disponibilitatea datelor pentru autoritățile competente

(1) Prezentul regulament nu aduce atingere competențelor autorităților competente de a solicita sau de a obține acces la date pentru îndeplinirea atribuțiilor lor oficiale în conformitate cu dreptul Uniunii sau cu dreptul intern. Accesul la date al autorităților competente nu poate fi refuzat pe motiv că datele sunt prelucrate în alt stat membru.

(2) În cazul în care o autoritate competentă nu obține acces la datele unui utilizator după ce a solicitat acest lucru și dacă, în temeiul dreptului Uniunii sau al acordurilor internaționale, nu există un mecanism specific de cooperare pentru schimbul de date între autoritățile competente din diferite state membre, respectiva autoritate competentă poate solicita asistență autorității competente dintr-un alt stat membru, în conformitate cu procedura prevăzută la articolul 7.

(3) În cazul în care o cerere de asistență implică obținerea accesului autorității solicitate la orice spațiu al unei persoane fizice sau juridice, inclusiv la orice echipamente și mijloace de prelucrare a datelor, acest acces trebuie să fie conform cu dreptul Uniunii sau cu dreptul procedural intern.

(4) Statele membre pot impune sancțiuni eficace, proporționale și disuasive pentru nerespectarea unei obligații de a furniza date, în conformitate cu legislația Uniunii și cu cea națională.

În cazul unui abuz de drept din partea unui utilizator, un stat membru poate să îi impună acestui utilizator măsuri provizorii strict proporționale, atunci când acest lucru este justificat de urgența accesului la date și ținând seama de interesele părților în cauză. În cazul în care o măsură provizorie impune relocalizarea datelor pentru o perioadă care depășește 180 de zile de la relocalizare, acest lucru este comunicat Comisiei în decursul respectivei perioade de 180 de zile. Comisia examinează măsura în cauză și compatibilitatea sa cu dreptul Uniunii în cel mai scurt timp posibil și ia măsurile necesare, acolo unde este cazul. Comisia face schimb de informații cu punctele unice de contact din statele membre prevăzute la articolul 7, cu privire la experiența dobândită în această privință.

Articolul 6

Portarea datelor

(1) Comisia încurajează și facilitează elaborarea unor coduri de conduită de autoreglementare la nivelul Uniunii („coduri de conduită"), pentru a contribui la o economie competitivă a datelor, care să fie bazate pe principiile transparenței și interoperabilității, să țină seama în mod corespunzător de standardele deschise și să acopere, printre altele, următoarele aspecte:

(a) cele mai bune practici pentru a facilita schimbarea furnizorilor de servicii și portarea datelor într-un format structurat, utilizat în mod curent și care poate fi prelucrat electronic, inclusiv formate de standarde deschise dacă sunt impuse sau solicitate de furnizorul de servicii care primește datele;

(b) cerințe minime în materie de informare, pentru a asigura că utilizatorilor profesioniști li se oferă, înainte de încheierea unui contract de prelucrare a datelor, informații suficient de detaliate, clare și transparente, cu privire la procesele, cerințele tehnice, termenele și tarifele care se aplică în cazul în care un utilizator profesionist dorește să schimbe un furnizor de servicii sau să își porteze datele înapoi către propriile sisteme informatice;

(c) abordări în materie de sisteme de certificare care să faciliteze compararea produselor și serviciilor de prelucrare a datelor pentru utilizatorii profesioniști, ținând seama de normele internaționale sau naționale stabilite, pentru a facilita comparabilitatea acestor produse și servicii. Aceste abordări pot include, printre altele, managementul calității, al securității informațiilor, al continuității activității și managementul de mediu;

(d) foile de parcurs de comunicare concentrate asupra unei abordări multidisciplinare pentru a sensibiliza într-o mai mare măsură părțile interesate cu privire la codurile de conduită.

(2) Comisia se asigură că codurile de conduită sunt elaborate în strânsă cooperare cu toate părțile interesate relevante, inclusiv asociațiile de IMM-uri și de întreprinderi nou-înființate, utilizatorii și furnizorii de servicii de tip cloud.

(3) Comisia încurajează furnizorii de servicii să finalizeze redactarea codurilor de conduită până la 29 noiembrie 2019 și să le aplice efectiv până la 29 mai 2020.

Articolul 7

Procedura de cooperare între autorități

(1) Fiecare stat membru desemnează un punct unic de contact care asigură legătura cu punctele unice de contact din celelalte state membre și cu Comisia în ceea ce privește aplicarea prezentului regulament. Statele membre notifică Comisiei punctele unice de contact desemnate și orice modificare ulterioară a acestora.

(2) În cazul în care o autoritate competentă dintr-un stat membru solicită asistență din partea unui alt stat membru, în temeiul articolului 5 alineatul (2), pentru a obține acces la date, aceasta transmite punctului unic de contact desemnat din cel din urmă stat membru o cerere motivată în mod corespunzător. Cererea include o explicație scrisă a motivelor și temeiurile juridice pentru solicitarea accesului la date.

(3) Punctul unic de contact identifică autoritatea competentă relevantă din statul său membru și transmite cererea primită în temeiul alineatului (2) către respectiva autoritate competentă.

(4) Fără întârzieri nejustificate și într-un interval de timp proporțional cu urgența cererii, autoritatea competentă relevantă răspunde fie comunicând datele solicitate, fie informând autoritatea competentă solicitantă că nu consideră că au fost îndeplinite condițiile pentru solicitarea asistenței în temeiul prezentului regulament.

(5) Orice informație transmisă în contextul asistenței solicitate și acordate în temeiul articolului 5 alineatul (2) se utilizează numai în scopul pentru care a fost solicitată.

(6) Punctele unice de contact le oferă utilizatorilor informații generale referitoare la dispozițiile prezentului regulament, inclusiv cu privire la codurile de conduită.

Articolul 8

Evaluare și orientări

(1) Până la 29 noiembrie 2022, Comisia prezintă Parlamentului European, Consiliului și Comitetului Economic și Social European un raport de evaluare a punerii în aplicare a prezentului regulament, în special în ceea ce privește:

(a) aplicarea prezentului regulament, în special cu privire la seturile de date compuse din date cu caracter personal și date fără caracter personal, având în vedere evoluțiile tehnologiei și ale pieței care ar putea înmulți posibilitățile de dezanonimizare a datelor;

(b) punerea în aplicare de către statele membre a articolului 4 alineatul (1), și în special a excepției privind siguranța publică; și

(c) elaborarea și aplicarea efectivă a codurilor de conduită și furnizarea efectivă de informații de către furnizorii de servicii.

(2) Statele membre furnizează Comisiei informațiile necesare pentru elaborarea raportului menționat la alineatul (1).

(3) Până la 29 mai 2019, Comisia publică orientări informative privind interacțiunea dintre prezentul regulament și Regulamentul (UE) 2016/679, în special în ce privește seturile de date compuse din date cu caracter personal și date fără caracter personal.

Articolul 9

Dispoziții finale

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

Prezentul regulament se aplică la șase luni de la data publicării.

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

Adoptat la Strasbourg, 14 noiembrie 2018.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*
A. TAJANI	K. EDTSTADLER