COMISIA
EUROPEANĂ

Bruxelles, 23.6.2026
COM(2026) 314 final

2026/0173 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

de modificare a Regulamentului (UE) 2018/1725 al Parlamentului European și al Consiliului 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

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

• Motivele și obiectivele propunerii

Regulamentul (UE) 2018/1725 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile UE (RPDUE) a fost conceput pentru a institui un regim coerent și modernizat de protecție a datelor pentru toate instituțiile, organele, oficiile și agențiile UE. Capitolul IX din Regulamentul (UE) 2018/1725 a fost destinat în mod specific să reglementeze prelucrarea „datelor operaționale cu caracter personal” (și anume datele cu caracter personal prelucrate pentru desfășurarea activităților care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE) de către agențiile și organele UE din domeniul justiției și afacerilor interne (JAI), inclusiv Europol, Eurojust, Parchetul European (EPPO) și, într-o măsură limitată, Frontex.

În pofida adoptării RPDUE, cadrul de protecție a datelor aplicabil agențiilor și organelor JAI ale UE rămâne fragmentat. În special, capitolul IX nu se aplică EPPO, al cărui regulament de instituire este anterior RPDUE. Prin urmare, anumite dispoziții ale Regulamentului privind EPPO diferă în esență de dispozițiile corespunzătoare prevăzute în capitolul IX din RPDUE sau sunt formulate diferit față de acestea. În plus, RPDUE prevede că, în ceea ce privește prelucrarea datelor operaționale cu caracter personal, se aplică numai articolul 3 (definiții) și capitolul IX. Pe de o parte, acest lucru a dus la menținerea dispozițiilor care reglementează anumite aspecte legate de prelucrarea datelor operaționale cu caracter personal în actele de înființare ale organelor, oficiilor sau agențiilor respective. Pe de altă parte, aceasta a dat naștere unei incertitudini juridice cu privire la aspectul dacă și în ce măsură dispozițiile cuprinse în capitolele II-VIII, cum ar fi cele referitoare la evidențele activităților de prelucrare sau la sarcinile responsabilului cu protecția datelor, se aplică în situațiile în care nu există dispoziții similare nici în capitolul IX, nici în actele de înființare ale organelor, oficiilor sau agențiilor relevante. Această fragmentare nu numai că subminează securitatea juridică, ci creează și obstacole practice în calea unei cooperări eficace între organele, oficiile și agențiile UE atunci când fac schimb de date. În primul său raport privind aplicarea RPDUE din 2022, Comisia a recunoscut aceste deficiențe și a luat în considerare o intervenție legislativă pentru a le remedia.

În acest context, prezenta propunere urmărește obiectivele de simplificare și de asigurare a coerenței cadrului aplicabil privind protecția datelor, în special prin alinierea normelor relevante la nivelul tuturor organelor și agențiilor UE. Se preconizează că această aliniere va reduce sarcinile administrative și va facilita schimburile de date dintre acestea, sporind în același timp securitatea juridică. Din motive de coerență și în conformitate cu obiectivul general de reducere la minimum a fragmentării normelor de protecție a datelor, propunerea se bazează pe patru obiective principale:

Asigurarea aplicării consecvente a protecției datelor în cazul tuturor instituțiilor, organelor, oficiilor și agențiilor UE

Capitolul IX trebuie să aibă un domeniu de aplicare extins pentru a se asigura că se aplică în mod consecvent în cazul tuturor agențiilor, organelor și oficiilor UE din sectorul justiției penale și al asigurării respectării legii. Acesta va integra EPPO în cadrul RPDUE. Acest lucru se va realiza fără a aduce atingere posibilității de a menține, în Regulamentul privind EPPO, normele specifice de protecție a datelor necesare pentru a reflecta caracterul unic al EPPO în calitate de parchet independent al Uniunii. Normele din capitolul IX sunt deja aliniate la normele corespunzătoare din Directiva (UE) 2016/680 privind protecția datelor în materie de

asigurare a respectării legii și vor avea ca rezultat un set unic și armonizat de norme pentru toate părțile afectate, pentru a reduce fragmentarea și a asigura coerența normelor aplicate.

Consolidarea securității juridice

În prezent, capitolul IX nu conține dispoziții cu privire la mai multe aspecte importante, inclusiv rolul responsabililor cu protecția datelor (RPD), păstrarea evidențelor activităților de prelucrare, colaborarea dintre autoritățile de supraveghere și transferul internațional de date operaționale cu caracter personal. Propunerea urmărește să consolideze normele într-un singur loc, raționalizând cerințele în materie de conformitate fără a impune un impact operațional semnificativ. Acest lucru va oferi, de asemenea, o mai mare claritate operatorilor, persoanelor împuternicite de operatori și persoanelor vizate.

Raționalizarea competențelor Autorității Europene pentru Protecția Datelor

În prezent, competențele de supraveghere ale AEPD sunt reglementate în actele de instituire a Europol, Eurojust și EPPO, fiecare conținând dispoziții divergente, ceea ce duce la incertitudine și ineficiență. Actul de înființare a Frontex nu reglementează supravegherea AEPD în ceea ce privește prelucrarea datelor operaționale, ceea ce duce la o asimetrie importantă.

Propunerea urmărește să clarifice faptul că AEPD i se acordă competențe de supraveghere care sunt în conformitate cu cele prevăzute la articolul 58 din RPDUE, însă sunt adaptate la contextul prelucrării datelor operaționale, în special pentru EPPO în contextul activităților de investigare și urmărire penală. În acest sens, propunerea urmează modelul competențelor AEPD din reforma Europol din 2022, asigurând în același timp coerența cu capitolul VI din RPDUE și cu Directiva privind protecția datelor în materie de asigurare a respectării legii. Propunerea elimină din actele de instituire dispozițiile specifice agențiilor privind sarcinile și competențele AEPD.

Raționalizare generală

În cele din urmă, propunerea vizează raționalizarea dispozițiilor pentru a elimina redundanțele, duplicările și inconsecvențele în domeniul protecției datelor pentru organele, oficiile și agențiile JAI ale Uniunii atunci când desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 și capitolul 5 din TFUE. De asemenea, aliniază dispozițiile privind prelucrarea datelor operaționale la propunerea Omnibus în domeniul digital[1], după caz.

- **Coerența cu dispozițiile de politică deja existente în domeniul de politică vizat**

Propunerea urmărește să alinieze dispozițiile RPDUE la politicile existente în materie de protecție a datelor, consolidând principiile stabilite în Regulamentul general privind protecția datelor (RGPD) și în Directiva privind protecția datelor în materie de asigurare a respectării legii. Aceasta asigură alinierea la modificările aduse cadrului de protecție a datelor propus în cadrul pachetului Omnibus în domeniul digital, după caz.

- **Coerența cu alte politici ale Uniunii**

Propunerea face parte dintr-un pachet de inițiative în materie de justiție penală care urmăresc un obiectiv coerent și complementar: consolidarea capacității Uniunii de a preveni, a depista,

[1] Propunere de Regulament al Parlamentului European și al Consiliului de modificare a Regulamentelor (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 și a Directivelor 2002/58/CE, (UE) 2022/2555 și (UE) 2022/2557 în ceea ce privește simplificarea cadrului legislativ în domeniul digital și de abrogare a Regulamentelor (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 și a Directivei (UE) 2019/1024 (Regulamentul omnibus în domeniul digital), 19.11.2025, COM(2025) 837 final.

a investiga și a urmări penal formele grave de criminalitate transfrontalieră într-un mediu de securitate din ce în ce mai complex. Prin modernizarea cadrelor juridice care reglementează cooperarea dintre autoritățile de aplicare a legii, autoritățile judiciare și alte autorități relevante, pachetul urmărește să consolideze eficacitatea, coerența și interoperabilitatea arhitecturii de securitate internă a Uniunii.

Revizuirile propuse ale regulamentelor privind Europol și Eurojust constituie nucleul acestui efort. Europol și Eurojust îndeplinesc funcții distincte, dar complementare, în cadrul spațiului de libertate, securitate și justiție: în timp ce Europol sprijină prevenirea, depistarea și investigarea activităților infracționale, Eurojust facilitează cooperarea judiciară și asigură o urmărire penală și măsuri judiciare eficace. Prin urmare, pachetul urmărește să consolideze cooperarea și complementaritatea dintre cele două agenții, precum și cu alți actori relevanți ai Uniunii din domeniile justiției și afacerilor interne și arhitecturii antifraudă, în vederea asigurării unei continuități fluide între acțiunile de asigurare a respectării legii și măsurile judiciare ulterioare în toate etapele lanțului justiției penale.

În acest context, modificările aduse cadrului privind ordinul european de anchetă și prezenta propunere contribuie și mai mult la acest obiectiv prin facilitarea unei cooperări transfrontaliere eficace, prin îmbunătățirea condițiilor pentru schimbul de informații și prin asigurarea unui cadru juridic coerent, adaptat la realitățile operaționale și la evoluțiile tehnologice. Luate împreună, măsurile propuse în acest pachet vor consolida capacitatea Uniunii de a răspunde amenințărilor în continuă evoluție la adresa securității, respectând totodată pe deplin drepturile fundamentale, statul de drept și repartizarea responsabilităților între diferiții actori implicați.

În particular, prezenta propunere identifică toate elementele comune ale normelor de protecție a datelor aplicabile Europol și Eurojust și le regrupează în RPDUE, eliminând astfel fragmentarea și duplicarea. Acest lucru permite ca în actele de instituire a organelor, oficiilor și agențiilor Uniunii care își desfășoară activitatea în domeniul asigurării respectării legii și al justiției penale să se păstreze numai normele de protecție a datelor adaptate entităților menționate, norme elaborate pentru a reflecta nevoile operaționale și natura specifică a acestora.

Propunerea este adoptată în paralel cu revizuirile Regulamentelor privind Europol și Eurojust, asigurând coerența și alinierea cadrelor juridice respective. De asemenea, aceasta anticipează viitoarea revizuire a Regulamentului (UE) 2017/1939 de instituire a EPPO[2], ținând seama de evoluțiile sale viitoare și fără a aduce atingere evaluării posibilelor opțiuni de politică pentru revizuirea Regulamentului privind EPPO. Această abordare coordonată contribuie la un cadru cuprinzător și coerent pentru prelucrarea datelor operaționale de către organele și agențiile Uniunii.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

• Temeiul juridic

Protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal este un drept fundamental prevăzut la articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene.

Prezenta propunere se bazează pe articolul 16 din TFUE, care este temeiul juridic pentru adoptarea normelor în materie de protecție a datelor. Articolul susmenționat permite

[2] Regulamentul (UE) 2017/1939 al Consiliului din 12 octombrie 2017 de punere în aplicare a unei forme de cooperare consolidată în ceea ce privește instituirea Parchetului European (EPPO) (JO L 283, 31.10.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj).

adoptarea de norme privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii în exercitarea activităților care fac parte din domeniul de aplicare al dreptului Uniunii. Acesta permite, de asemenea, adoptarea de norme privind libera circulație a datelor cu caracter personal, inclusiv a datelor cu caracter personal prelucrate de aceste instituții, organe, oficii și agenții.

- **Subsidiaritatea (în cazul competențelor neexclusive)**

Nu se aplică

- **Proporționalitatea**

Nu se aplică

- **Alegerea instrumentului**

Nu se aplică

3. REZULTATELE EVALUĂRILOR *EX POST*, ALE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRILOR IMPACTULUI

- **Evaluările *ex post*/verificarea adecvării legislației existente**

Primul raport al Comisiei din 2022 privind aplicarea RPDUE a concluzionat că, în general, RPDUE funcționează bine și este adecvat scopului. În același timp, a identificat necesitatea unei intervenții legislative pentru a reduce la minimum fragmentarea normelor de protecție a datelor pentru instituțiile și organele UE care prelucrează date operaționale cu caracter personal atunci când desfășoară activități în domeniul cooperării polițienești și al cooperării judiciare în materie penală (capitolul IX din RPDUE, „capitolul privind asigurarea respectării legii”).

- **Consultarea cu părțile interesate**

Au fost efectuate consultări specifice cu părțile interesate în cadrul tuturor entităților care fac în prezent sau care vor face în viitor obiectul capitolului IX din RPDUE (și anume Europol, Eurojust, EPPO, Frontex), precum și cu Autoritatea Europeană pentru Protecția Datelor, care este responsabilă cu supravegherea conformității.

- **Obținerea și utilizarea cunoștințelor de specialitate**

Nu se aplică

- **Evaluarea impactului**

O evaluare a impactului nu este considerată adecvată pentru această inițiativă din cauza domeniului său de aplicare limitat și a naturii în mare măsură tehnice a modificărilor propuse. Propunerea vizează dispoziții specifice ale RPDUE, afectând doar un grup mic de entități ale UE din domeniul cooperării judiciare în materie penală și al cooperării polițienești, fără a modifica cadrul general. Modificările vizează asigurarea unui regim mai bine armonizat, nu implică noi opțiuni de politică și se preconizează că vor avea un impact minim, necuantificabil asupra drepturilor fundamentale și nici nu vor avea implicații economice, sociale sau de mediu. În plus, agențiile relevante fac deja obiectul unor evaluări separate și al unor evaluări ale impactului, inclusiv în ceea ce privește normele de protecție a datelor care le sunt aplicabile. O evaluare separată în temeiul RPDUE ar duplica acest exercițiu. Propunerea se aliniază la angajamentul anterior al Comisiei din primul său raport privind aplicarea RPDUE din 2022, iar o evaluare suplimentară a RPDUE este prevăzută pentru 2027. În cele din urmă, nu apar preocupări legate de subsidiaritate, deoarece RPDUE se aplică exclusiv organismelor UE, care nu pot fi reglementate de statele membre.

- **Adecvarea reglementărilor și simplificarea**

Propunerea armonizează și simplifică normele de protecție a datelor aplicabile agențiilor, oficiilor și organelor Uniunii care își desfășoară activitatea în domeniul asigurării respectării dreptului penal și al justiției penale. Prin raționalizarea normelor existente, aceasta sporește claritatea și coerența juridică în întregul cadru instituțional, facilitând astfel aplicarea acestora și reducând complexitatea administrativă. Deși beneficiile nu sunt ușor cuantificabile, se preconizează că propunerea va reduce costurile de asigurare a conformității și sarcinile administrative asociate parcurgerii unor cerințe diferite sau care se suprapun. Propunerea sprijină, de asemenea, elaborarea oricărui potențial mecanism de schimb între actorii vizați luat în considerare în contextul revizuirii arhitecturii antifraudă.

- **Drepturile fundamentale**

Caracterul specific al modificărilor asigură menținerea nivelului existent de protecție a datelor, asigurând, în același timp, îmbunătățiri în ceea ce privește coerența normelor aplicabile și o mai bună armonizare.

4. IMPLICAȚII BUGETARE

Nu se aplică

5. ALTE ELEMENTE

- **Planurile de punere în aplicare și măsurile de monitorizare, evaluare și raportare**

Nu se aplică

- **Explicarea detaliată a dispozițiilor specifice ale propunerii**

Articolul 1 se referă la modificările aduse Regulamentului (UE) 2018/1725 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile UE.

Alineatul (1) înlocuiește alineatul (2) al articolului 2 și extinde domeniul de aplicare al articolelor 43, 44 și 45 și al capitolelor VII și VIII din Regulamentul (UE) 2018/1725 la prelucrarea datelor operaționale cu caracter personal de către organele, oficiile și agențiile Uniunii, fără a aduce atingere normelor specifice privind protecția datelor aplicabile organelor, oficiilor sau agențiilor Uniunii. Acesta elimină, de asemenea, alineatul (3) al articolului 2, extinzând astfel aplicarea RPDUE la EPPO, fără a submina însă necesitatea de a menține, în Regulamentul privind EPPO, norme specifice de protecție a datelor care să țină seama de caracterul distinct al EPPO ca autoritate independentă de investigare și urmărire penală a Uniunii.

Alineatul (2) prevede adaptări tehnice ale formulării articolului 45 privind sarcinile responsabilului cu protecția datelor, asigurându-se faptul că sarcinile respective acoperă, de asemenea, prelucrarea datelor operaționale.

Alineatul (3) asigură faptul că competența Autorității Europene pentru Protecția Datelor în temeiul articolului 66 din Regulamentul (UE) 2018/1725 de a impune amenzi administrative se extinde la prelucrarea datelor operaționale cu caracter personal de către organele, oficiile și agențiile Uniunii.

Alineatul (4) elimină articolul 70 din Regulamentul (UE) 2018/1725, care devine caduc având în vedere definirea dispozițiilor aplicabile prelucrării datelor operaționale de la articolul 2 alineatul (2).

Alineatul (5) modifică articolul 77 din Regulamentul (UE) 2018/1725 pentru a asigura alinierea la propunerea Omnibus în domeniul digital și pentru a spori securitatea juridică, precizând că deciziile bazate exclusiv pe prelucrarea automată a datelor operaționale cu caracter personal sunt permise în cazul în care sunt îndeplinite condiții specifice.

Alineatul (6) modifică articolul 78 din Regulamentul (UE) 2018/1725 pentru a asigura alinierea la propunerea Omnibus în domeniul digital prin clarificarea noțiunii de cereri abuzive în contextul dreptului de acces. În special, acesta precizează că o cerere poate fi considerată vădit nefondată în cazul în care persoana vizată se bazează pe dreptul de acces în alte scopuri decât protecția datelor sale. În astfel de cazuri, operatorul poate refuza să dea curs cererii, rămânând totodată supus obligației de a demonstra că cererea este în mod vădit nefondată sau excesivă.

Alineatul (7) introduce un nou articol 87a în Regulamentul (UE) 2018/1725 privind păstrarea evidențelor pentru datele operaționale cu caracter personal, în conformitate cu normele Directivei privind protecția datelor în materie de asigurare a respectării legii.

Alineatele (8) și (9) adaugă garanții suplimentare la articolul 88 din Regulamentul (UE) 2018/1725 privind înregistrarea.

Alineatul (10) modifică articolul 92 alineatul (1) din Regulamentul (UE) 2018/1725 pentru a asigura alinierea la propunerea Omnibus în domeniul digital prin prelungirea termenului de notificare a unei încălcări a securității datelor cu caracter personal către Autoritatea Europeană pentru Protecția Datelor de la 72 de ore la 96 de ore. De asemenea, acesta ridică pragul de notificare, prevăzând că notificarea este necesară numai în cazul în care încălcarea securității datelor cu caracter personal este de natură să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice.

Alineatele (11) și (12) simplifică cadrul juridic care reglementează transferurile de date operaționale cu caracter personal către țări terțe și organizații internaționale, prin alinierea acestora la cadrul instituit prin Directiva (UE) 2016/680. Modificările prevăd un set uniform de norme aplicabile organelor, oficiilor și agențiilor Uniunii care își desfășoară activitatea în domeniul asigurării respectării dreptului penal și al justiției penale, ținând seama, în același timp, de contextul lor operațional și juridic specific, inclusiv de acordurile de cooperare. Acestea prevăd că transferurile către țări cu o decizie privind caracterul adecvat al nivelului de protecție sunt permise fără o autorizație suplimentară; în absența unei decizii privind caracterul adecvat al nivelului de protecție, transferurile sunt permise dacă există garanții adecvate prin intermediul unui instrument obligatoriu din punct de vedere juridic sau al unei evaluări a operatorului; și în scenarii specifice în care nu există nici o decizie privind caracterul adecvat al nivelului de protecție, nici garanții adecvate, se aplică anumite derogări. În cele din urmă, acestea prevăd, de asemenea, transferuri de date operaționale cu caracter personal către destinatari care nu sunt autorități competente stabilite în țări terțe în cazuri specifice, dacă condițiile enumerate la articolul respectiv sunt îndeplinite, inclusiv atunci când contactarea unei autorități competente din țara terță poate fi ineficace sau inadecvată iar transferul este strict necesar pentru îndeplinirea sarcinilor operatorului.

Alineatul (13) simplifică competențele Autorității Europene pentru Protecția Datelor în ceea ce privește datele operaționale cu caracter personal pentru toate organele, oficiile și agențiile Uniunii care își desfășoară activitatea în domeniul asigurării respectării dreptului penal și al

justiției penale, în conformitate cu competențele Autorității Europene pentru Protecția Datelor aplicabile Europol începând din 2022.

Articolul 2 clarifică momentul în care intră în vigoare noile dispoziții.

2026/0173 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

de modificare a Regulamentului (UE) 2018/1725 al Parlamentului European și al Consiliului 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

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16 alineatul (2),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene și articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc. De asemenea, acest drept este garantat și în temeiul articolului 8 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale.

(2) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului[1] stabilește cadrul juridic pentru prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii. Cu toate acestea, normele de protecție a datelor aplicabile prelucrării datelor operaționale cu caracter personal de către organele, oficiile și agențiile Uniunii atunci când desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE rămân stabilite în mod fragmentat în capitolul IX din Regulamentul (UE) 2018/1725 și alte acte juridice ale Uniunii. Articolul 98 din regulamentul respectiv prevede obligația Comisiei de a revizui normele aplicabile prelucrării datelor operaționale cu caracter personal, în vederea identificării posibilelor inconsecvențe, lacune și discrepanțe. Acesta prevede, de asemenea, că, dacă este cazul, Comisia abordează deficiențele identificate printr-o propunere legislativă, în special pentru a extinde aplicarea capitolului IX la Parchetul European (EPPO) instituit prin Regulamentul (UE) 2017/1939 al Consiliului[2], în

[1] 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

[2] Regulamentul (UE) 2017/1939 al Consiliului din 12 octombrie 2017 de punere în aplicare a unei forme de cooperare consolidată în ceea ce privește instituirea Parchetului European (EPPO) (JO L 283, 31.10.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj).

funcție de necesități, și pentru a introduce adaptările necesare ale capitolului respectiv. În primul său raport privind aplicarea Regulamentului (UE) 2018/1725, Comisia a confirmat eficacitatea generală a regulamentului în ceea ce privește asigurarea unui nivel ridicat de protecție a datelor cu caracter personal, subliniind în același timp o serie de inconsecvențe, discrepanțe și situații de fragmentare juridică care decurg din interacțiunea dintre capitolul IX și celelalte dispoziții ale Regulamentului (UE) 2018/1725, precum și existența unui regim de sine stătător de protecție a datelor pentru EPPO.

(3) În prezent, numai articolul 3 și capitolul IX din Regulamentul (UE) 2018/1725 se aplică prelucrării datelor operaționale cu caracter personal, împreună cu o serie de norme specifice privind protecția datelor prevăzute în actele de instituire a Agenției Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și a Agenției Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust). În același timp, EPPO are propriul său regim de protecție a datelor, de sine stătător, în actul său de instituire. Prin urmare, Regulamentul (UE) 2018/1725 ar trebui modificat pentru a extinde aplicarea capitolului IX la toate organele, oficiile și agențiile Uniunii care prelucrează date operaționale cu caracter personal în sectorul asigurării respectării legii și al justiției penale, pentru a asigura securitatea juridică prin abordarea lacunelor din actualul regim de protecție a datelor, în special pentru Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă, și pentru a raționaliza normele privind transferurile internaționale de date cu caracter personal, precum și normele privind competențele Autorității Europene pentru Protecția Datelor. Acest lucru nu ar trebui să afecteze posibilitatea de a menține, în Regulamentul (UE) 2017/1939, normele specifice de protecție a datelor necesare pentru a reflecta caracterul unic al EPPO în calitate de parchet independent al Uniunii.

(4) Pentru a crea un cadru juridic armonizat, coerent, simplificat și complet pentru prelucrarea datelor operaționale cu caracter personal de către organele, oficiile și agențiile Uniunii, definițiile (capitolul I), normele privind responsabilii cu protecția datelor (capitolul IV secțiunea 6), normele privind cooperarea și coerența (capitolul VII), normele privind căile de atac, răspunderea și sancțiunile (capitolul VIII) și normele privind prelucrarea datelor operaționale cu caracter personal [care ar trebui aliniate la Directiva (UE) 2016/680 a Parlamentului European și a Consiliului[3]– capitolul IX] prevăzute în Regulamentul (UE) 2018/1725 ar trebui să se aplice organelor, oficiilor și agențiilor Uniunii atunci când desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE. Aceste norme ar trebui să se aplice atunci când se desfășoară astfel de activități în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor. Aceste norme ar trebui să se aplice, de asemenea, prelucrării datelor operaționale cu caracter personal de către Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă, și nu doar capitolul IX din Regulamentul (UE) 2018/1725. Normele Regulamentului (UE) 2018/1725 ar trebui să se aplice fără a aduce atingere normelor specifice aplicabile prelucrării datelor operaționale cu caracter personal de către organele, oficiile și agențiile Uniunii atunci când desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE, în special normelor prevăzute în actele

[3] 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, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

de instituire a Europol, Eurojust și EPPO. Astfel de norme specifice ar trebui considerate *lex specialis* față de dispozițiile Regulamentului (UE) 2018/1725 privind prelucrarea datelor operaționale cu caracter personal.

(5) În cadrul tuturor instituțiilor și organelor Uniunii, un responsabil cu protecția datelor ar trebui să se asigure că sunt aplicate toate normele de protecție a datelor, inclusiv Regulamentul (UE) 2018/1725. Responsabilii ar trebui, de asemenea, să consilieze operatorii și persoanele împuternicite de operatori cu privire la obligațiile care le revin. Pentru a asigura coerența și a preveni duplicarea, atât în ceea ce privește datele administrative cu caracter personal, precum și cele operaționale, ar trebui să existe un singur set de norme pentru responsabilii cu protecția datelor.

(6) Autoritatea Europeană pentru Protecția Datelor ar trebui să aibă, ca măsură de ultimă instanță, competența de a impune amenzi administrative, inclusiv pentru prelucrarea datelor operaționale cu caracter personal de către organele, oficiile și agențiile Uniunii care își desfășoară activitatea în domeniul asigurării respectării legii și al justiției penale.

(7) Pentru a se evita suprapunerile în cadrul Regulamentului (UE) 2018/1725, articolul 70 din acesta ar trebui eliminat, întrucât domeniul de aplicare al capitolului IX este deja reglementat la articolul 2 din Regulamentul (UE) 2018/1725.

(8) Pentru a asigura alinierea la Regulamentul (UE).../... [*propunerea Omnibus în domeniul digital*], la articolul 77 din Regulamentul (UE) 2018/1725 ar trebui să se clarifice faptul că deciziile bazate exclusiv pe prelucrarea automată a datelor operaționale cu caracter personal sunt permise atunci când sunt îndeplinite anumite condiții specifice.

(9) Pentru a asigura alinierea la Regulamentul (UE).../... [*propunerea Omnibus în domeniul digital*], la articolul 78 din Regulamentul (UE) 2018/1725 ar trebui să se clarifice faptul că persoanele vizate nu ar trebui să utilizeze în mod abuziv dreptul de acces, care le este de la bun început favorabil, în alte scopuri decât protecția datelor lor.

(10) Pentru a demonstra conformitatea cu Regulamentul (UE) 2018/1725, organele, oficiile și agențiile Uniunii care își desfășoară activitatea în domeniul asigurării respectării legii și al justiției penale ar trebui să aibă norme uniforme privind păstrarea evidențelor referitoare la toate categoriile de activități de prelucrare aflate în responsabilitatea lor. Fiecare operator și fiecare persoană împuternicită de operator ar trebui să aibă obligația de a coopera cu Autoritatea Europeană pentru Protecția Datelor și de a își pune evidențele la dispoziția acesteia, la cerere, pentru a putea fi utilizate în scopul monitorizării operațiunilor de prelucrare respective.

(11) Organele, oficiile și agențiile Uniunii nu ar trebui să poată modifica înregistrările. În cazul în care organele, oficiile și agențiile Uniunii primesc date operaționale cu caracter personal de la autoritățile naționale competente, organele, oficiile și agențiile Uniunii ar trebui să comunice înregistrările autorităților respective, atunci când acestea sunt necesare pentru investigațiile interne de asigurare a conformității în materie de protecție a datelor.

(12) Pentru a asigura alinierea la Regulamentul (UE).../... [*propunerea Omnibus în domeniul digital*], pragul pentru notificarea Autorității Europene pentru Protecția Datelor cu privire la o încălcare a securității datelor cu caracter personal ar trebui să fie mai ridicat, iar termenul de notificare ar trebui prelungit.

(13) Organele, oficiile și agențiile Uniunii care își desfășoară activitatea în domeniul asigurării respectării legii și al justiției penale ar trebui să beneficieze de un set uniform de norme privind transferurile internaționale de date operaționale cu caracter personal, aliniat la Directiva (UE) 2016/680.

(14) Comisia poate să decidă, în temeiul articolului 36 din Directiva (UE) 2016/680, că o țară terță, un teritoriu sau un sector determinat dintr-o țară terță ori o organizație internațională asigură un nivel adecvat de protecție a datelor. În aceste cazuri, transferurile de date operaționale cu caracter personal efectuate de organe, oficii și agenții ale Uniunii către țara terță sau organizația internațională respectivă pot avea loc fără a fi necesar să se obțină autorizări suplimentare.

(15) Transferurile care nu se întemeiază pe o astfel de decizie privind caracterul adecvat al nivelului de protecție ar trebui să fie permise numai în cazul în care au fost prezentate garanții corespunzătoare într-un instrument obligatoriu din punct de vedere juridic, care să asigure protecția datelor cu caracter personal, sau în cazul în care operatorul a evaluat toate circumstanțele legate de datele transferate și, pe baza acestei evaluări, consideră că există garanții adecvate în ceea ce privește protecția datelor cu caracter personal. Astfel de instrumente obligatorii din punct de vedere juridic ar putea fi, de exemplu, acordurile de cooperare între Eurojust și o țară terță încheiate înainte de 12 decembrie 2019 în conformitate cu articolul 26a din Decizia 2002/187/JAI, acordurile de cooperare între Europol și o țară terță încheiate înainte de 1 mai 2017 în conformitate cu articolul 23 din Decizia 2009/371/JAI sau acordurile internaționale încheiate între Uniune și o țară terță în temeiul articolului 218 din TFUE.

(16) În cazul în care nu există o decizie privind caracterul adecvat al nivelului de protecție sau garanții adecvate, un transfer sau o categorie de transferuri ar putea avea loc numai în situații specifice, pe baza unei derogări. Derogările ar trebui interpretate în mod restrictiv și nu ar trebui să permită transferuri frecvente, masive și structurale de date cu caracter personal sau transferuri la scară largă de date, ci ar trebui să se limiteze la datele strict necesare. Astfel de transferuri ar trebui să fie documentate și să fie puse la dispoziția Autorității Europene pentru Protecția Datelor la cerere, în scopul monitorizării legalității transferului.

(17) În cazuri individuale specifice, procedurile obișnuite care necesită contactarea unei autorități competente dintr-o țară terță pot fi ineficace sau inadecvate, în special din cauză că transferul nu a putut fi efectuat în timp util sau din cauză că autoritatea din țara terță nu respectă statul de drept sau normele și standardele internaționale privind drepturile omului. Acest lucru poate fi valabil în cazul în care există o nevoie urgentă de a transfera date cu caracter personal către o societate privată dintr-o țară terță pentru a primi informații cu privire la un autor necunoscut al unei infracțiuni online sau pentru a salva viața unei persoane care se află în pericol de a deveni victimă a unei infracțiuni sau în interesul prevenirii săvârșirii iminente a unei infracțiuni, inclusiv a terorismului. În astfel de cazuri, în condiții specifice, organele, oficiile și agențiile Uniunii ar putea decide să transfere date operaționale cu caracter personal direct către destinatari care nu sunt autorități competente, stabiliți în țările terțe respective.

(18) Autoritatea Europeană pentru Protecția Datelor ar trebui să dispună de un set uniform de competențe aplicabile prelucrării datelor operaționale cu caracter personal de către organele, oficiile și agențiile Uniunii care își desfășoară activitatea în domeniul asigurării respectării legii și al justiției penale. Astfel de competențe se aplică deja Europol din 2022, de exemplu prin obligarea operatorului de date să asigure respectarea Regulamentului (UE) 2018/1725, prin dispunerea suspendării fluxurilor de

date către un destinatar dintr-un stat membru, o țară terță sau o organizație internațională sau prin impunerea unei amenzi administrative în cazul nerespectării acestei dispuneri.

(19) 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 XX XX 2026,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Modificări aduse Regulamentului (UE) 2018/1725

Regulamentul (UE) 2018/1725 se modifică după cum urmează:

1. Articolul 2 se modifică după cum urmează:

   (a) alineatul (2) se înlocuiește cu următorul text:

   „(2) Numai articolele 3, 43, 44, 45 și capitolele VII, VIII și IX din prezentul regulament se aplică prelucrării datelor operaționale cu caracter personal efectuate de organele, oficiile și agențiile Uniunii atunci când acestea desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE, fără a aduce atingere normelor specifice de protecție a datelor aplicabile unui astfel de organ, oficiu sau agenție a Uniunii.”

   (b) alineatul (3) se elimină.

2. La articolul 45 alineatul (1), literele (d), (e) și (f) se înlocuiesc cu următorul text:

   „(d) furnizarea de consiliere, la cerere, în ceea ce privește necesitatea unei notificări sau a unei comunicări a unei încălcări a datelor cu caracter personal, în temeiul articolelor 34 și 35 sau al articolelor 92 și 93;

   (e) furnizarea de consiliere, la cerere, în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea realizării acestei evaluări în temeiul articolului 39 sau al articolului 89 și consultarea Autorității Europene pentru Protecția Datelor în cazul în care există îndoieli cu privire la necesitatea efectuării unei evaluări a impactului asupra protecției datelor;

   (f) furnizarea de consiliere, la cerere, în ceea ce privește necesitatea consultării prealabile a Autorității Europene pentru Protecția Datelor, în temeiul articolului 40 sau al articolului 90; consultarea Autorității Europene pentru Protecția Datelor în cazul în care există îndoieli cu privire la necesitatea unei consultări prealabile;”.

3. La articolul 66 alineatul (1), prima teză se înlocuiește cu următorul text:

   „(1) Autoritatea Europeană pentru Protecția Datelor poate aplica amenzi administrative instituțiilor și organelor Uniunii, în funcție de circumstanțele fiecărui caz în parte, în cazul în care o instituție sau un organ al Uniunii nu se supune unui ordin al Autorității Europene pentru Protecția Datelor în temeiul articolului 58 alineatul (2) literele (d)-(h) și (j) sau în temeiul articolului 95a alineatul (3) literele (c), (e), (f), (j) și (k).”

4. Articolul 70 se elimină.

5. La articolul 77, alineatul (1) se înlocuiește cu următorul text:

„(1) O decizie care produce efecte juridice pentru o persoană vizată sau o afectează în mod similar într-o măsură semnificativă se poate baza exclusiv pe prelucrarea automată, inclusiv pe crearea de profiluri, numai în cazul în care decizia respectivă este autorizată de dreptul Uniunii care se aplică operatorului și care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, a libertăților și a intereselor legitime ale persoanei vizate, cel puțin dreptul de a obține intervenția umană din partea operatorului.”

6. La articolul 78, alineatul (4) se înlocuiește cu următorul text:

„(4) Operatorul transmite gratuit informațiile vizate la articolul 79 și realizează gratuit comunicările și măsurile prevăzute la articolele 80-84 și la articolul 92. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv sau, pentru cererile formulate în temeiul articolului 80, în cazul în care persoana vizată abuzează de dreptul de acces în alte scopuri decât protecția datelor sale, operatorul poate refuza să dea curs cererii. Operatorului îi revine sarcina de a demonstra caracterul vădit nefondat al cererii sau că există motive întemeiate să se considere că aceasta este excesivă.”

7. Se introduce următorul articol 87a:

„Articolul 87a

Evidențe ale categoriilor de activități de prelucrare a datelor operaționale cu caracter personal

(1) Fiecare operator păstrează o evidență a tuturor categoriilor de activități de prelucrare a datelor operaționale cu caracter personal desfășurate sub responsabilitatea sa. Evidența cuprinde toate informațiile următoare:

(a) datele de contact ale operatorului, numele și datele de contact ale responsabilului cu protecția datelor și, după caz, datele de contact ale operatorului asociat;

(b) scopurile prelucrării;

(c) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv părți private și destinatari din țări terțe sau organizații internaționale;

(d) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;

(e) atunci când este cazul, utilizarea creării de profiluri;

(f) atunci când este cazul, categoriile de transferuri de date cu caracter personal către o parte privată, o țară terță sau o organizație internațională;

(g) indicarea temeiului juridic al operațiunii de prelucrare, inclusiv transferurile, pentru care sunt destinate datele cu caracter personal;

(h) atunci când este posibil, termenele preconizate pentru ștergerea diferitelor categorii de date;

(i) atunci când este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 91 alineatul (1).

(2) Persoana împuternicită de operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprinde:

(a) datele de contact ale persoanei sau persoanelor împuternicite de operator, ale fiecărui operator în numele căruia acționează persoana împuternicită de operator și datele de contact ale responsabilului cu protecția datelor;

(b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;

(c) atunci când este cazul, transferurile de date cu caracter personal către o parte privată, către o țară terță sau către o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective, atunci când au primit instrucțiuni explicite în acest sens de la operator;

(d) atunci când este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 91 alineatul (1).

(3) Evidențele menționate la alineatele (1) și (2) se păstrează în scris, inclusiv în format electronic. Operatorul și persoana împuternicită de operator pun aceste evidențe la dispoziția Autorității Europene pentru Protecția Datelor, la cerere."

8. La articolul 88 alineatul (1), se adaugă următoarea teză:

„Înregistrările nu pot fi modificate."

9. La articolul 88 alineatul (3), se adaugă următoarea teză:

„În cazul în care autoritatea națională competentă solicită acest lucru pentru o investigație specifică legată de respectarea normelor de protecție a datelor, înregistrările menționate la alineatul (1) se comunică autorității respective."

10. La articolul 92, alineatul (1) se înlocuiește cu următorul text:

„(1) În cazul în care are loc o încălcare a securității datelor cu caracter personal care este de natură să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul notifică acest lucru Autorității Europene pentru Protecția Datelor fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 96 de ore după ce a luat cunoștință de aceasta. În cazul în care notificarea Autorității Europene pentru Protecția Datelor nu are loc în termen de 96 de ore, aceasta este însoțită de o explicație privind motivele întârzierii."

11. Articolul 94 se înlocuiește cu următorul text:

„Articolul 94

Principiile generale ale transferurilor de date operaționale cu caracter personal către țări terțe și către organizații internaționale

(1) Operatorul poate transfera date operaționale cu caracter personal către o țară terță sau către o organizație internațională sub rezerva respectării normelor aplicabile privind protecția datelor și a celorlalte dispoziții din prezentul regulament și numai în cazul în care sunt îndeplinite următoarele condiții:

(a) transferul este necesar pentru îndeplinirea sarcinilor operatorului;

(b) autoritatea din țara terță sau organizația internațională către care sunt transferate datele operaționale cu caracter personal are competențe de aplicare a legii sau competențe în materie de justiție penală;

(c) în cazul în care datele operaționale cu caracter personal care urmează să fie transferate au fost transmise sau puse la dispoziția operatorului de către un stat membru sau un organ, un oficiu sau o agenție a Uniunii, operatorul trebuie să obțină o autorizație prealabilă pentru transfer din partea autorității competente

relevante a statului membru respectiv sau din partea organului, oficiului sau agenției Uniunii, în conformitate cu dreptul său aplicabil, cu excepția cazului în care statul membru ori organul, oficiul sau agenția Uniunii în cauză a autorizat astfel de transferuri în termeni generali sau sub rezerva unor condiții specifice;

(d) în cazul unui transfer ulterior de către o țară terță sau o organizație internațională către o altă țară terță sau organizație internațională, operatorul cere țării terțe sau organizației internaționale care efectuează transferul să obțină o autorizație prealabilă din partea operatorului pentru respectivul transfer ulterior;

(e) operatorul furnizează autorizația conform literei (d) doar cu autorizarea prealabilă a statului membru ori a organului, oficiului sau agenției Uniunii de unde provin datele, după caz, și numai după ce a luat în considerare în mod corespunzător toți factorii relevanți, inclusiv gravitatea infracțiunii, scopul pentru care datele operaționale cu caracter personal au fost transferate inițial și nivelul de protecție a datelor cu caracter personal din țara terță sau din organizația internațională către care urmează să fie transferate ulterior datele operaționale cu caracter personal.

(2) Sub rezerva condițiilor prevăzute la alineatul (1) de la prezentul articol, operatorul poate transfera date operaționale cu caracter personal către o țară terță sau către o organizație internațională în cazul în care sunt îndeplinite condițiile prevăzute la articolul 94a, 94b, 94c sau 94d.

(3) Fără a aduce atingere articolului 94c, operatorul poate transfera date operaționale cu caracter personal unei autorități competente dintr-o țară asociată la punerea în aplicare, asigurarea respectării și dezvoltarea acquis-ului Schengen care a transpus și aplică efectiv dispozițiile Directivei (UE) 2016/680 și dispozițiile privind schimbul de informații prevăzute în Directiva (UE) 2023/977.

(4) În cazuri urgente, operatorul poate transfera date operaționale cu caracter personal fără autorizarea prealabilă din partea unui stat membru sau a unui organ, oficiu sau agenție a Uniunii, în conformitate cu alineatul (1) litera (c). Operatorul procedează astfel numai dacă transferul de date operaționale cu caracter personal este necesar pentru prevenirea unei amenințări imediate și grave la adresa securității publice a unui stat membru sau a unei țări terțe sau la adresa intereselor fundamentale ale unui stat membru, iar autorizarea prealabilă nu poate fi obținută în timp util. Autoritatea responsabilă pentru acordarea unei autorizări prealabile trebuie să fie informată fără întârziere.

(5) Toate dispozițiile privind transferurile internaționale din prezentul capitol se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice asigurat prin prezentul regulament nu este subminat.”

12. Se introduc următoarele articole:

„Articolul 94a

Transferuri în temeiul unei decizii privind caracterul adecvat al nivelului de protecție

Operatorul poate transfera date operaționale cu caracter personal către o țară terță sau către o organizație internațională în cazul în care Comisia a decis, în conformitate cu articolul 36 din Directiva (UE) 2016/680, că țara terță, un teritoriu ori unul sau mai multe sectoare determinate din țara terță respectivă sau organizația internațională în cauză asigură un nivel de protecție adecvat.

Articolul 94b

Transferuri în baza unor garanții adecvate

(1) În absența unei decizii privind caracterul adecvat al nivelului de protecție, operatorul poate transfera date operaționale cu caracter personal către o țară terță sau către o organizație internațională în cazul în care:

(a) sunt prevăzute garanții adecvate în ceea ce privește protecția datelor operaționale cu caracter personal într-un act obligatoriu din punct de vedere juridic;

(b) sau operatorul a evaluat toate circumstanțele aferente transferului de date operaționale cu caracter personal și a concluzionat că există garanții adecvate în ceea ce privește protecția datelor operaționale cu caracter personal.

(2) Instrumentul obligatoriu din punct de vedere juridic prevăzut la alineatul (1) litera (a) trebuie să fie:

(a) un acord internațional încheiat între Uniune și țara terță sau organizația internațională în temeiul articolului 218 din TFUE care prevede garanții adecvate în ceea ce privește protecția vieții private, protecția datelor și a altor drepturi și libertăți fundamentale ale persoanelor;

(b) un acord de cooperare care permite schimbul de date operaționale cu caracter personal și care a fost încheiat înainte de 12 decembrie 2019 între Eurojust și țara terță sau organizația internațională respectivă, în conformitate cu articolul 26a din Decizia 2002/187/JAI sau

(c) un acord de cooperare care permite schimbul de date operaționale cu caracter personal încheiat înainte de 1 mai 2017 între Europol și țara terță sau organizația internațională respectivă în conformitate cu articolul 23 din Decizia 2009/371/JAI.

(3) Organele, oficiile și agențiile Uniunii pot încheia acorduri de lucru pentru a stabili modalitățile de punere în aplicare a acordurilor menționate la alineatul (2).

(4) Operatorul informează Autoritatea Europeană pentru Protecția Datelor cu privire la categoriile de transferuri prevăzute la alineatul (1) litera (b).

(5) Atunci când un transfer se întemeiază pe alineatul (1) litera (b), un astfel de transfer se documentează, iar documentația se pune la dispoziția Autorității Europene pentru Protecția Datelor, la cerere. Documentația trebuie să includă o înregistrare a datei și orei transferului, informații cu privire la autoritatea competentă destinatară, cu privire la justificarea transferului și cu privire la datele operaționale cu caracter personal transferate.

Articolul 94c

Derogări pentru situații specifice

(1) În absența unei decizii privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate în temeiul articolului 94b, operatorul poate transfera date operaționale cu caracter personal către o țară terță sau către o organizație internațională numai în condițiile în care transferul este necesar:

(a) pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane;

(b) pentru protejarea unor interese legitime ale persoanei vizate;

(c) pentru prevenirea unei amenințări imediate și grave la adresa securității publice a unui stat membru sau a unei țări terțe;

(d) sau în cazuri individuale, pentru îndeplinirea sarcinilor operatorului, cu excepția cazului în care operatorul stabilește că drepturile și libertățile fundamentale ale persoanei vizate în cauză prevalează asupra interesului public în ceea ce privește transferul.

(2) Atunci când un transfer se întemeiază pe alineatul (1), un astfel de transfer se documentează, iar documentația se pune la dispoziția Autorității Europene pentru Protecția Datelor la cerere. Documentația trebuie să includă o înregistrare a datei și orei transferului, informații cu privire la autoritatea competentă destinatară, cu privire la justificarea transferului și cu privire la datele operaționale cu caracter personal transferate.

Articolul 94d

Transferul de date operaționale cu caracter personal către destinatari stabiliți în țări terțe

(1) Prin derogare de la articolul 94 alineatul (1) litera (b) și fără a afecta niciun acord internațional menționat la alineatul (2) de la prezentul articol, operatorul, în cazuri individuale și specifice, poate transfera date operaționale cu caracter personal direct către destinatari stabiliți în țări terțe numai dacă sunt îndeplinite toate condițiile următoare:

(a) transferul este strict necesar pentru îndeplinirea sarcinilor operatorului, în scopurile pentru care i se permite să prelucreze date operaționale cu caracter personal;

(b) operatorul stabilește că niciunul dintre drepturile și libertățile fundamentale ale persoanei vizate în cauză nu prevalează asupra interesului public care necesită transferul în cazul respectiv;

(c) operatorul consideră că transferul către o autoritate competentă din țara terță este ineficient sau inadecvat, în special deoarece transferul nu poate fi realizat în timp util;

(d) autoritatea competentă din țara terță este informată fără întârzieri nejustificate, cu excepția cazului în care această măsură este ineficientă sau inadecvată;

(e) operatorul informează destinatarul cu privire la scopul sau scopurile determinate în care numai acesta din urmă poate să prelucreze datele operaționale cu caracter personal, cu condiția ca o astfel de prelucrare să fie necesară.

(2) Un acord internațional menționat la alineatul (1) este orice acord internațional bilateral sau multilateral în vigoare între Uniune și țări terțe în domeniul cooperării judiciare în materie penală și al cooperării polițienești.

(3) Atunci când un transfer se întemeiază pe alineatul (1), un astfel de transfer se documentează, iar documentația se pune la dispoziția Autorității Europene pentru Protecția Datelor la cerere, incluzând data și ora transferului, informații cu privire la autoritatea competentă destinatară, cu privire la justificarea transferului și cu privire la datele operaționale cu caracter personal transferate.”

13. Se introduce următorul articol 95a:

„Articolul 95a

Supravegherea de către Autoritatea Europeană pentru Protecția Datelor

(1) Autoritatea Europeană pentru Protecția Datelor răspunde de monitorizarea și asigurarea aplicării dispozițiilor prezentului regulament referitoare la protecția drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor operaționale cu caracter personal efectuată de organele, oficiile și agențiile Uniunii, precum și de consilierea acestora și a persoanelor vizate asupra tuturor aspectelor privind prelucrarea de date operaționale cu caracter personal. În acest scop, Autoritatea Europeană pentru Protecția Datelor îndeplinește atribuțiile prevăzute la alineatul (2) și exercită competențele prevăzute la alineatul (3), cooperând strâns cu autoritățile naționale de supraveghere.

(2) Autoritatea Europeană pentru Protecția Datelor are următoarele atribuții:

(a) de a primi și a investiga plângeri și de a informa persoana vizată cu privire la soluționarea plângerii într-un termen rezonabil; de a efectua investigații fie din proprie inițiativă, fie pe baza unei plângeri, și de a informa persoana vizată cu privire la soluționarea plângerii într-un termen rezonabil;

(b) de a monitoriza și a asigura aplicarea prezentului regulament și a oricărui alt act al Uniunii referitor la protecția persoanelor fizice în ceea ce privește prelucrarea datelor operaționale cu caracter personal de către organele, oficiile și agențiile Uniunii;

(c) de a consilia organele, oficiile și agențiile Uniunii, fie din proprie inițiativă, fie ca răspuns la o consultare, cu privire la toate aspectele care au legătură cu prelucrarea datelor cu caracter personal, în special înainte ca acestea să elaboreze norme interne referitoare la protecția drepturilor și libertăților fundamentale în ceea ce privește prelucrarea datelor cu caracter personal;

(d) de a ține un registru al noilor tipuri de operațiuni de prelucrare care i-au fost notificate;

(e) de a efectua o consultare prealabilă privind prelucrarea care i-a fost notificată.

(3) În temeiul prezentului regulament, Autoritatea Europeană pentru Protecția Datelor poate:

(a) să consilieze persoanele vizate cu privire la exercitarea drepturilor lor;

(b) să sesizeze un organ, un oficiu sau o agenție a Uniunii în cazul unei presupuse încălcări a dispozițiilor care reglementează prelucrarea datelor operaționale cu caracter personal și, după caz, să formuleze propuneri de remediere a încălcării, precum și de îmbunătățire a protecției persoanelor vizate;

(c) să dispună să se dea curs cererilor de exercitare a anumitor drepturi în ceea ce privește datele operaționale cu caracter personal în cazul în care astfel de cereri au fost refuzate cu încălcarea normelor aplicabile privind drepturile persoanelor vizate;

(d) să avertizeze sau să admonesteze organul, oficiul sau agenția Uniunii;

(e) să dispună rectificarea, restricționarea, ștergerea sau distrugerea de către organul, oficiul sau agenția Uniunii a datelor cu caracter personal care au fost prelucrate cu încălcarea dispozițiilor care reglementează prelucrarea datelor operaționale cu caracter personal și notificarea unor astfel de acțiuni părților terțe cărora le-au fost divulgate aceste date;

(f) să impună o interdicție temporară sau definitivă asupra operațiunilor de prelucrare efectuate de organul, oficiul sau agenția Uniunii care încalcă dispozițiile care reglementează prelucrarea datelor operaționale cu caracter personal;

(g) să sesizeze organul, oficiul sau agenția Uniunii și, dacă este necesar, Parlamentul European, Consiliul și Comisia;

(h) să sesizeze Curtea de Justiție a Uniunii Europene în condițiile prevăzute de TFUE;

(i) să intervină în acțiunile introduse la Curtea de Justiție a Uniunii Europene;

(j) să dispună ca operatorul sau persoana împuternicită de operator să asigure conformitatea operațiunilor de prelucrare cu prezentul regulament și, după caz, cu normele privind protecția datelor prevăzute în actul de instituire a organului, oficiului sau agenției Uniunii, după caz, într-un mod specificat și într-un termen specificat;

(k) să dispună suspendarea fluxurilor de date către un destinatar dintr-un stat membru, dintr-o țară terță sau către o organizație internațională;

(l) să aplice o amendă administrativă în temeiul articolului 66 în cazul nerespectării de către organul, oficiul sau agenția Uniunii a uneia dintre măsurile menționate la literele (c), (e), (f), (j) și (k) de la prezentul alineat, în funcție de circumstanțele fiecărui caz în parte.

(4) Autoritatea Europeană pentru Protecția Datelor este împuternicită:

(a) să obțină din partea organului, oficiului sau agenției Uniunii acces la toate datele operaționale cu caracter personal și la toate informațiile necesare pentru anchetele sale;

(b) să obțină accesul în orice sediu în care organul, oficiul sau agenția Uniunii își desfășoară activitățile atunci când există motive întemeiate pentru a presupune că o activitate reglementată de prezentul capitol se desfășoară acolo.

(5) Autoritatea Europeană pentru Protecția Datelor întocmește un raport anual privind activitățile sale de supraveghere în legătură cu operatorii efectuate în temeiul prezentului capitol. Raportul respectiv face parte din raportul anual al Autorității Europene pentru Protecția Datelor menționat la articolul 60.

AEPD invită autoritățile naționale de supraveghere să prezinte observații cu privire la respectiva parte din raportul anual înainte ca raportul anual să fie adoptat. AEPD ține cont în cea mai mare măsură de respectivele observații și le menționează în raportul anual.

Partea din raportul anual menționată la al doilea paragraf trebuie să includă informații statistice privind plângeri, anchete și investigații, precum și privind transferurile de date operaționale cu caracter personal către țări terțe și organizații internaționale, cazurile de consultări prealabile ale Autorității Europene pentru Protecția Datelor și recurgerea la competențele prevăzute la alineatul (3) de la prezentul articol.

(6) Autoritatea Europeană pentru Protecția Datelor, funcționarii și ceilalți membri ai personalului secretariatului Autorității Europene pentru Protecția Datelor sunt supuși obligației de confidențialitate, în conformitate cu articolul 95.”

Articolul 2

Intrare în vigoare

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

2. Cu toate acestea, prezentul regulament se aplică prelucrării datelor operaționale cu caracter personal de către Parchetul European începând cu [*data intrării în vigoare a noului Regulament privind EPPO*].

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

Adoptat la Bruxelles,

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*
[...]	*[...]*