

# Declarație



## Declarație referitoare la pachetul privind serviciile digitale și la strategia privind datele Adoptată la 18 noiembrie 2021

### Comitetul european pentru protecția datelor a adoptat următoarea declarație:

Începând din noiembrie 2020, Comisia Europeană a prezentat mai multe propuneri legislative în cadrul strategiei sale digitale și strategiei sale privind datele, în special Actul legislativ privind serviciile digitale (*Digital Services Act – DSA*), Actul legislativ privind piețele digitale (*Digital Markets Act – DMA*), Legea privind guvernarea datelor (*Data Governance Act – DGA*) și Regulamentul privind o abordare europeană în domeniul inteligenței artificiale (AIR). Se preconizează că o a cincea propunere de „act legislativ privind datele” va fi prezentată foarte curând, făcând parte dintr-o serie de inițiative prevăzute în Strategia europeană privind datele<sup>1</sup>.

Propunerile urmăresc să faciliteze utilizarea și partajarea într-o mai mare măsură a datelor (cu caracter personal) între mai multe părți publice și private în cadrul „economiei datelor”, să sprijine utilizarea unor tehnologii specifice, cum ar fi Big Data și IA, precum și să reglementeze platformele online și controlorii fluxului de informație (gatekeeperi). Prelucrarea datelor cu caracter personal este deja sau va fi o activitate de bază a entităților, a modelelor de afaceri și a tehnologiilor reglementate de propuneri. Prin urmare, efectul combinat al adoptării și punerii în aplicare a propunerilor va avea un impact semnificativ asupra protecției drepturilor fundamentale la viață privată și la protecția datelor cu caracter personal, consacrate la articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene („Carta UE”) și la articolul 16 din Tratatul privind funcționarea Uniunii Europene („TFUE”).

CEPD și AEPD au emis deja avize comune privind DGA<sup>2</sup> și AIR, iar AEPD a emis avize cu privire la Strategia europeană privind datele, la DMA și la DSA<sup>3</sup>. Aceste avize evidențiază o serie de preocupări și formulează recomandări pentru o mai bună aliniere a propunerilor la legislația în vigoare a Uniunii

<sup>1</sup> Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, O strategie europeană privind datele, COM(2020) 66 final.

<sup>2</sup> CEPD a emis, de asemenea, Declarația nr. 05/2021 referitoare la Legea privind guvernarea datelor în lumina evoluțiilor legislative.

<sup>3</sup> AEPD a emis, de asemenea, un aviz preliminar referitor la spațiul european al datelor privind sănătatea. O prezentare generală a tuturor avizelor și declarațiilor emise de CEPD și AEPD este furnizată ca anexă la prezenta declarație.

privind protecția datelor. CEPD regretă faptul că, până în prezent, o serie de recomandări nu au fost pe deplin abordate de colegiuitor<sup>4</sup>.

**Prin această declarație, CEPD atrage atenția asupra mai multor preocupări majore și îndeamnă colegiuitorul să ia măsuri ferme. Preocupările noastre se împart în trei categorii: (1) lipsa de protecție a drepturilor și libertăților fundamentale ale persoanelor; (2) supravegherea fragmentată; și (3) riscurile de neconcordanțe.**

**CEPD consideră că, dacă nu sunt modificate, propunerile vor avea un impact negativ asupra drepturilor și libertăților fundamentale ale persoanelor și vor conduce la un nivel semnificativ de incertitudine juridică, ce ar submina atât cadrul juridic existent, cât și pe cel viitor. Ca atare, este posibil ca propunerile să nu creeze condițiile pentru inovare și creștere economică pe care chiar ele le au în vedere.**

## 1. LIPSA DE PROTECȚIE A DREPTURILOR ȘI LIBERTĂȚILOR FUNDAMENTALE ALE PERSOANELOR

În cadrul propunerilor s-au făcut anumite alegeri care pot avea un impact de lungă durată asupra drepturilor și libertăților fundamentale ale persoanelor și ale societății în ansamblu. Deși propunerile vizează, în general, reducerea unor riscuri diverse, CEPD își exprimă profunda îngrijorare cu privire la o serie de opțiuni selectate și consideră că drepturile și libertățile fundamentale ale persoanelor necesită o protecție suplimentară. Printre exemplele concrete se numără:

- Propunerea de regulament AIR ar permite utilizarea **sistemelor de IA care clasifică persoanele** pe baza datelor biometrice (cum ar fi recunoașterea facială) pe criterii de **etnie, gen, orientare politică sau sexuală** sau alte motive interzise de discriminare sau a sistemelor de IA a căror valabilitate științifică nu este dovedită sau care contravin în mod direct valorilor fundamentale ale UE<sup>5</sup>. CEPD consideră că astfel de sisteme ar trebui interzise în UE și invită colegiuitorii să includă o astfel de interdicție în cadrul AIR. În plus, CEPD consideră că utilizarea IA pentru a **indica emoțiile unei persoane fizice** este extrem de nedorită și ar trebui interzisă, cu excepția anumitor cazuri de utilizare bine specificate, și anume în scopuri medicale sau de cercetare, sub rezerva unor garanții, condiții și limite adecvate<sup>6</sup>.
- În aceeași ordine de idei, având în vedere efectul negativ semnificativ asupra drepturilor și libertăților fundamentale ale persoanelor fizice, CEPD reiterează faptul că AIR **ar trebui să includă o interdicție privind utilizarea IA pentru recunoașterea automată a caracteristicilor umane în spații publice** – cum ar fi a fețelor, dar și a mersului, a amprentelor digitale, a ADN-ului, a vocii, a modului de apăsare a tastelor și a altor semnale biometrice sau

---

<sup>4</sup> Preocupările evidențiate în prezenta declarație privesc textul inițial al propunerilor formulate de Comisie și nu se referă la nicio poziție ulterioară a Parlamentului European sau a Consiliului Uniunii Europene, cu excepția cazului în care se indică altfel în mod explicit.

<sup>5</sup> De exemplu, poligraf, anexa III, punctul 6 litera (b) și punctul 7 litera (a) din AIR. Avizul comun al CEPD-AEPD privind AIR, punctul 32.

<sup>6</sup> Avizul comun al CEPD-AEPD privind AIR, punctul 35.

comportamentale – în orice context<sup>7</sup>. Propunerea de regulament AIR permite în prezent utilizarea sistemelor de identificare biometrică la distanță în timp real în spații publice în scopul aplicării legii în anumite cazuri<sup>8</sup>. CEPD salută rezoluția PE recent adoptată, în care sunt evidențiate riscurile semnificative<sup>9</sup>.

- CEPD consideră, de asemenea, că **publicitatea specifică online ar trebui reglementată mai strict** în cadrul DSA în favoarea unor forme mai puțin intruzive de publicitate care nu necesită urmărirea interacțiunii utilizatorilor cu conținuturile și îndeamnă colegiitorul să ia în considerare o eliminare treptată care să conducă la **interzicerea publicității specifice pe baza urmării generale**<sup>10</sup>, în timp ce crearea de profiluri ale copiilor ar trebui, per ansamblu, să fie interzisă.
- CEPD recomandă introducerea unor **obligații privind interoperabilitatea** atât în Actul legislativ privind serviciile digitale, cât și în Actul legislativ privind piețele digitale, pentru a promova un mediu digital mai deschis concurenței, facilitând alegerea de către cetățeni a serviciilor care oferă o mai bună protecție a vieții private și a datelor<sup>11</sup>.

## 2. SUPRAVEGHERE FRAGMENTATĂ

Toate propunerile prevăd instituirea unor autorități de supraveghere și a unor noi structuri europene de cooperare între aceste autorități („comitete europene”)<sup>12</sup>. Deși prelucrarea datelor cu caracter personal este esențială pentru activitățile reglementate de propuneri, autoritățile de supraveghere în domeniul protecției datelor nu sunt desemnate ca fiind principalele autorități competente. CEPD reamintește că, în ceea ce privește protecția și libera circulație a datelor cu caracter personal, articolul 16 alineatul (2) din TFUE și articolul 8 alineatul (3) din Carta UE impun ca supravegherea prelucrării datelor cu caracter personal să fie încredințată unor autorități independente de protecție a datelor<sup>13</sup>.

În plus, CEPD este foarte preocupat de faptul că propunerile nu stabilesc cu precizie modul în care noile organisme de supraveghere (și comitetele europene care le însoțesc) ar trebui să coopereze cu autoritățile de supraveghere în domeniul protecției datelor (și cu CEPD). În special, propunerile nu abordează în mod adecvat situațiile de suprapunere potențială a competențelor și nici nu se consultă

---

<sup>7</sup> Avizul comun al CEPD-AEPD privind AIR, punctul 32.

<sup>8</sup> Prevăzute la articolul 5 alineatul (1) litera (d) punctele (i)-(iii) din AIR.

<sup>9</sup> Rezoluția Parlamentului European din 6 octombrie 2021 privind inteligența artificială în dreptul penal și utilizarea sa de către autoritățile polițienești și judiciare în procedurile penale [2020/2016(INI)].

<sup>10</sup> A se vedea, de asemenea, Avizul AEPD privind DSA, punctele 69-70, precum și Rezoluția Parlamentului European din 20 octombrie 2020 conținând recomandări adresate Comisiei referitoare la un act legislativ privind serviciile digitale: adaptarea normelor de drept comercial și civil pentru entitățile comerciale care își desfășoară activitatea online [2020/2019(INL)], punctul 15.

<sup>11</sup> A se vedea, de asemenea, Avizul AEPD privind DSA, punctele 84-85 și Avizul AEPD privind DMA, punctele 37-38.

<sup>12</sup> Comitetul consultativ pentru piețele digitale (DMAC) în temeiul DMA; Comitetul european pentru servicii digitale (EBDS) în temeiul DSA; Comitetul european pentru inteligența artificială (EAIB) în temeiul AIR; Comitetul european pentru inovare în domeniul datelor (EDIB) în temeiul DGA.

<sup>13</sup> A se vedea Declarația CEPD nr. 05/2021 referitoare la Legea privind guvernarea datelor în lumina evoluțiilor legislative, pagina 3; avizul comun al CEPD-AEPD privind AIR, pagina 16.

în chestiuni de interes reciproc. Apare astfel **riscul existenței unor structuri de supraveghere paralele**, în care autorități competente diferite supraveghează aceleași entități în legătură cu aceleași activități (de prelucrare), **fără a exista o cooperare structurată** între ele.

### Printre exemplele concrete se numără:

- Propunerea de act legislativ privind serviciile digitale impune autorităților competente să supravegheze **sistemele de recomandare**<sup>14</sup> ale platformelor online foarte mari (care implică adesea crearea de profiluri ale persoanelor vizate în sensul RGPD); precum și măsurile instituite pentru **evaluarea și atenuarea riscurilor sistemice, inclusiv a riscului la adresa dreptului la viață privată**<sup>15</sup>. Aceeași propunere conține, de asemenea, dispoziții privind **codurile de conduită** care pot viza prelucrarea datelor cu caracter personal<sup>16</sup>. Cu toate acestea, nu impune autorităților competente să se consulte în mod oficial sau să coopereze cu CEPD sau cu membrii săi. Acest aspect prezintă riscul unor orientări contradictorii sau chiar al unor rezultate diferite în ceea ce privește acțiunile de asigurare a respectării legislației întreprinse de autoritățile de supraveghere.
- Propunerea de DGA definește **noi tipuri de furnizori de servicii și organizații** care ar prelucra volume mari de date potențial sensibile, în special serviciile de intermediere de date și organizațiile de promovare a altruismului în materie de date. Cu toate acestea, **regimul de „verificare” pentru aceste entități are aproape un caracter declarativ și, ca atare, nu oferă o protecție suficientă persoanelor vizate**<sup>17</sup>, deoarece se limitează la verificarea de către autoritatea competentă a cerințelor (în principal formale)<sup>18</sup>, care trebuie să aibă loc într-un termen foarte scurt<sup>19</sup>.
- Propunerea de AIR prevede un **sistem de certificare și coduri de conduită** pentru sistemele de IA cu grad ridicat de risc, dar nu este clar dacă și în ce mod aceste certificate și coduri pot interacționa cu cerințele RGPD<sup>20</sup>. Acest fapt ar putea determina situații în care sistemele de IA, în pofida faptului că sunt certificate (marcajul CE) în temeiul AIR pentru a fi introduse pe piață sau puse în funcțiune, nu ar fi conforme cu normele și principiile privind protecția datelor (în special, DPbDD – protecția datelor începând cu momentul conceperii și în mod implicit)<sup>21</sup>. În plus, propunerea de AIR nu conține nicio trimitere la mecanismele (obligatorii) de

---

<sup>14</sup> Articolul 29 din DSA.

<sup>15</sup> În special în contextul articolului 27 (identificarea și evaluarea celor mai importante și recurente riscuri sistemice, precum și cele mai bune practici pentru atenuarea acestor riscuri), care face trimitere la articolul 26, inclusiv la articolul 26 alineatul (1) litera (b), precum și al articolelor 35 și 36 din Actul legislativ privind serviciile digitale (coduri de conduită).

<sup>16</sup> A se vedea articolele 35 și 36 din DSA.

<sup>17</sup> A se vedea avizul comun al CEPD-AEPD privind DGA, punctele 136, 140, 151, 155, 175, 180 și 191.

<sup>18</sup> Prevăzute la articolul 11 din DGA pentru furnizorii de servicii de partajare de date și, respectiv, la articolele 16-19 pentru organizațiile de promovare a altruismului în materie de date.

<sup>19</sup> O săptămână de la data notificării, pentru furnizorii de servicii de partajare de date [articolul 10 alineatul (7) din DGA]; douăsprezece săptămâni de la data cererii, pentru organizațiile de promovare a altruismului în materie de date [articolul 17 alineatul (5) din DGA].

<sup>20</sup> A se vedea avizul comun al CEPD-AEPD privind AIR, punctul 74.

<sup>21</sup> A se vedea avizul comun al CEPD-AEPD privind AIR, punctul 76.

monitorizare a codurilor de conduită menite să verifice dacă furnizorii de sisteme de IA care nu prezintă un grad ridicat de risc respectă dispozițiile acestora<sup>22</sup>.

- Propunerea de act legislativ privind piețele digitale impune gatekeeperilor să faciliteze exercitarea **portabilității datelor** în conformitate cu RGPD și să ofere, în anumite condiții, **acces la date**, inclusiv la date cu caracter personal, în temeiul articolului 6 alineatul (1) literele (h) și (i), și la date anonimizate, în temeiul articolului 6 alineatul (1) litera (j), fără să prevadă un temei juridic clar pentru prelucrarea datelor cu caracter personal sau o obligație de consultare și cooperare între orice autoritate competentă desemnată în temeiul DMA și autoritatea competentă în domeniul protecției datelor în contextul supravegherii respectării acestor dispoziții ale DMA.

Pentru a asigura complementaritatea în materie de supraveghere și pentru a spori securitatea juridică, CEPD recomandă în mod ferm ca fiecare propunere să menționeze în mod clar autoritățile de supraveghere în domeniul protecției datelor din rândul autorităților competente relevante cu care va avea loc cooperarea. În plus, fiecare propunere ar trebui să **prevadă un temei juridic explicit pentru schimbul de informații necesar unei cooperări eficiente și să identifice circumstanțele în care ar trebui să aibă loc cooperarea**. În plus, propunerile ar trebui să permită autorităților de supraveghere competente din cadrul fiecărei propuneri să **facă schimb de informații** obținute în contextul oricăror audituri și investigații legate de prelucrarea datelor cu caracter personal cu autoritățile competente în domeniul protecției datelor, fie la cerere, fie din proprie inițiativă<sup>23</sup>. CEPD ar dori să sublinieze necesitatea asigurării faptului că autoritățile de supraveghere în domeniul protecției datelor dispun de **resurse suficiente** pentru a îndeplini aceste sarcini suplimentare.

### 3. RISCURI DE NECONCORDANȚE

Toate propunerile vizează reglementarea tehnologiilor sau a activităților care implică prelucrarea datelor cu caracter personal. Ca atare, cadrul existent în materie de protecție a datelor este pe deplin aplicabil. Cu toate acestea, textul din partea dispozitivă a propunerilor poate **crea ambiguitate** în ceea ce privește aplicabilitatea cadrului de protecție a datelor în anumite cazuri. Colegiitorul ar trebui să soluționeze orice ambiguități **pentru a asigura** securitatea juridică și pentru a spori coerența cu cadrul existent în materie de protecție a datelor, în scopul asigurării punerii sale efective în aplicare. În orice caz, propunerile ar trebui să **precizeze în mod clar că acestea nu afectează ori subminează aplicarea normelor existente în materie de protecție a datelor, precum și să asigure faptul că normele privind protecția datelor prevalează** ori de câte ori sunt prelucrate date cu caracter personal<sup>24</sup>.

În plus, unele dispoziții utilizează aceeași terminologie ca RGPD sau Directiva privind viața privată și comunicațiile electronice, fără o trimitere explicită la legislația menționată anterior. Acest aspect riscă să afecteze interpretarea conceptelor de bază ale RGPD (cum ar fi noțiunile esențiale de „consimțământ” sau „persoană vizată”)<sup>25</sup>. De asemenea, implică riscul ca anumite dispoziții să fie interpretate ca fiind o abatere de la RGPD sau de la Directiva privind viața privată și comunicațiile

<sup>22</sup> A se vedea avizul comun al CEPD-AEPD privind AIR, punctul 79.

<sup>23</sup> A se vedea, de asemenea, Avizul AEPD privind DSA, punctele 87-89 și Avizul AEPD privind DMA, punctele 39-41.

<sup>24</sup> În conformitate cu drepturile fundamentale la viața privată și la protecția datelor cu caracter personal, consacrate la articolele 7 și 8 din Carta UE și la articolul 16 din TFUE.

<sup>25</sup> CEPD salută faptul că, în mandatul Consiliului privind DGA, astfel cum a fost adoptat la 24 septembrie 2021, noțiunile de consimțământ și de persoană vizată au fost aliniate la cerințele privind consimțământul din RGPD.

electronice. În consecință, anumite dispoziții ar putea fi interpretate cu ușurință într-un mod care nu este în concordanță cu cadrul juridic existent, conducând ulterior la insecuritate juridică.

### Printre exemplele concrete se numără:

- Propunerea de act legislativ privind serviciile digitale impune furnizorilor de servicii să ofere utilizatorilor cel puțin o opțiune pentru a primi recomandări de conținut care nu implică utilizarea creării de profiluri<sup>26</sup>. Cu toate acestea, principiul protecției datelor începând cu momentul conceperii și al protecției datelor în mod implicit impune ca sistemele care oferă astfel de recomandări să nu se bazeze pe crearea de profiluri *în mod implicit*<sup>27</sup>.
- În multe cazuri, **temeiul juridic** pentru prelucrarea datelor cu caracter personal nu reiese clar din textul juridic al propunerilor. Un exemplu din propunerea de DGA este lipsa de claritate în ceea ce privește reutilizarea datelor cu caracter personal deținute de organismele din sectorul public<sup>28</sup>. Propunerea de AIR indică faptul că nu oferă un temei juridic general pentru prelucrarea datelor cu caracter personal, precizând în același timp că furnizorii de sisteme de IA cu grad ridicat de risc „pot prelucra categorii speciale de date cu caracter personal” pentru a asigura monitorizarea, detectarea și corectarea erorilor sistematice și prevede garanții suplimentare pentru prelucrarea respectivă<sup>29</sup>.
- **Suprapunerea terminologiei** (parțial) cu sensuri clar diferite, cum ar fi „servicii de intermediere online” în propunerea de DMA și „servicii de intermediere de date” în propunerea de DGA creează confuzii și afectează claritatea propunerilor.
- Unul dintre principalele motive de îngrijorare cu privire la propunerea de DGA este faptul că dispozițiile nu specifică într-o măsură suficientă **dacă se referă la date fără caracter personal, la date cu caracter personal sau la ambele tipuri de date** și nici nu precizează fără echivoc faptul că, în cazul „seturilor de date mixte”, se aplică RGPD. Ca atare, nu reiese în mod clar că respectivul cadru de protecție a datelor ar rămâne aplicabil ori de câte ori are loc prelucrarea datelor cu caracter personal și în cazurile în care trebuie luate în considerare riscuri specifice pentru reidentificarea datelor cu caracter personal anonimizate<sup>30</sup>. Această lipsă a distincției poate crea confuzie, de exemplu, în ceea ce privește necesitatea unui temei juridic în contextul RGPD (situație valabilă în cazul tuturor prelucrărilor de date cu caracter personal care intră în domeniul său de aplicare)<sup>31</sup>.

---

<sup>26</sup> Articolul 29 din DSA.

<sup>27</sup> A se vedea Avizul AEPD privind DSA, punctul 73.

<sup>28</sup> Articolul 5 alineatul (6) din DGA.

<sup>29</sup> Articolul 10 alineatul (5) din AIR.

<sup>30</sup> A se vedea avizul comun al CEPD-AEPD privind DGA, pagina 16.

<sup>31</sup> A se vedea în continuare punctele 47-56 din avizul comun al CEPD-AEPD privind DGA, în care se subliniază insecuritatea juridică în ceea ce privește temeiul juridic pentru prelucrarea datelor cu caracter personal.

## În perspectivă:

CEPD este conștient de faptul că una dintre inițiativele-cheie ale Strategiei europene privind datele este de a crea **spații europene comune ale datelor** în sectoarele strategice și domeniile de interes public, inclusiv în domeniul sănătății („spațiul european al datelor privind sănătatea”). În avizul comun privind DGA, CEPD și AEPD au subliniat deja că orice inițiativă viitoare, cum ar fi **Legea privind datele**, care ar putea avea un impact asupra prelucrării datelor cu caracter personal trebuie să asigure și să susțină respectarea și aplicarea acquis-ului UE în domeniul protecției datelor cu caracter personal<sup>32</sup>.

La momentul redactării prezentei declarații, scopul și conținutul propunerilor pentru o lege privind datele sau pentru spațiul european al datelor privind sănătatea nu sunt încă disponibile. Cu toate acestea, este clar că ambele inițiativă vor viza sporirea accesului la date (cu caracter personal) și a reutilizării acestora în scopul efectuării schimbului de date între părțile private și publice.

În mod similar, CEPD invită, prin urmare, Comisia să evite ambiguitățile în noile propuneri, pentru a asigura securitatea juridică și coerența cu cadrul existent în materie de protecție a datelor, în scopul asigurării punerii sale efective în aplicare. În orice caz, propunerile ar trebui să precizeze în mod clar că **acestea nu afectează ori subminează aplicarea normelor existente în materie de protecție a datelor, precum și să asigure faptul că normele privind protecția datelor prevalează ori de câte ori sunt prelucrate date cu caracter personal**<sup>33</sup>.

În plus, ținând seama de provocările specifice generate de intensificarea schimbului de date, CEPD solicită ca viitoarele propuneri legislative privind spațiile europene ale datelor și Legea privind datele să definească de la bun început garanții **specifice de protecție a datelor**, asigurând un nivel ridicat de protecție a datelor, ținând seama, după caz, de prelucrarea categoriilor speciale de date, cum ar fi datele privind sănătatea. Prin definirea explicită a acestor garanții încă de la început, putem asigura un nivel adecvat de protecție a datelor cu caracter personal și putem evita o posibilă incertitudine juridică.

## Pe lângă preocupările generale identificate mai sus, CEPD dorește să sublinieze:

(i) **caracterul inalienabil** al dreptului la protecția datelor cu caracter personal ca drept ce revine **fiecărei persoane**, instituit în temeiul articolului 16 alineatul (1) din TFUE și al articolului 8 din Carta UE, la care nu se poate renunța<sup>34</sup>.

(ii) necesitatea de a include garanții **specifice pentru a asigura respectarea tuturor principiilor privind protecția datelor**, în special **reducerea la minimum a datelor, limitarea scopului și transparența**. Printre garanțiile relevante se numără, fără a se limita la acestea, precizarea tipurilor de date care pot fi prelucrate, a scopurilor în care datele pot fi prelucrate, a persoanelor vizate, a părților cu care se poate face schimb de date cu caracter personal, precum și a perioadelor de stocare. Ar trebui să se acorde o atenție deosebită garanțiilor privind prelucrarea în **scopul cercetării științifice**, asigurând

---

<sup>32</sup> Avizul comun al CEPD-AEPD privind DGA, punctul 19.

<sup>33</sup> În conformitate cu drepturile fundamentale la viață privată și la protecția datelor cu caracter personal, consacrate la articolele 7 și 8 din Carta UE și la articolul 16 din TFUE.

<sup>34</sup> Declarația CEPD referitoare la Legea privind guvernarea datelor în lumina evoluțiilor legislative, pagina 4.

**gestionarea legală, responsabilă și etică a datelor**, cum ar fi **cerințele de verificare** pentru cercetătorii care vor avea acces la volume mari de date potențial sensibile cu caracter personal<sup>35</sup>.

(iii) importanța obligației de **protecție a datelor începând cu momentul conceperii și în mod implicit**, care este deosebit de relevantă în contextul „**obiectelor conectate**” (de exemplu, internetul obiectelor și internetul corpurilor<sup>36</sup>), având în vedere riscurile semnificative la adresa drepturilor și libertăților fundamentale ale persoanelor în cauză<sup>37</sup>.

Pentru Comitetul european pentru protecția datelor,

Președinte

(Andrea Jelinek)

---

<sup>35</sup> A se vedea, de exemplu, condițiile prevăzute la articolul 31 alineatul (4) și la articolul 31 alineatul (5) din DSA.

<sup>36</sup> A se vedea Evaluarea inițială a impactului Legii privind datele, pagina 6, care face trimitere la „aparate electrocasnice inteligente, dispozitive portabile și asistenți casnici”, disponibilă la adresa:

[https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Legea-privind-datele-si-modificarea-normelor-referitoare-la-protectia-juridica-a-bazelor-de-date\\_ro](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Legea-privind-datele-si-modificarea-normelor-referitoare-la-protectia-juridica-a-bazelor-de-date_ro).

<sup>37</sup> A se vedea Avizul 8/2014 privind evoluțiile recente din sfera internetului obiectelor al Grupului de lucru „Articolul 29” pentru protecția datelor, p. 7-11, disponibil la adresa:

[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223\\_ro.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_ro.pdf).



ANEXĂ: Lista avizelor și declarațiilor anterioare adoptate de CEPD și AEPD

- ) Avizul comun nr. 3/2021 al CEPD-AEPD privind Propunerea de regulament al Parlamentului European și al Consiliului privind guvernarea datelor la nivel european (Legea privind guvernarea datelor), adoptat la 11 martie 2021, disponibil la adresa: [https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal\\_ro](https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_ro)
- ) Declarația CEPD nr. 05/2021 referitoare la Legea privind guvernarea datelor în lumina evoluțiilor legislative, adoptată la 19 mai 2021, disponibilă la adresa: [https://edpb.europa.eu/system/files/2021-08/edpb\\_statementondga\\_19052021\\_ro.pdf](https://edpb.europa.eu/system/files/2021-08/edpb_statementondga_19052021_ro.pdf)
- ) Avizul comun 5/2021 al CEPD-AEPD privind propunerea de regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială (Legea privind inteligența artificială), adoptat la 18 iunie 2021, disponibil la adresa: [https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal\\_ro](https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_ro)
- ) Avizul nr. 1/2021 al AEPD referitor la propunerea de act legislativ privind serviciile digitale, adoptat la 10 februarie 2021, disponibil la adresa: [https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act\\_en](https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act_en)
- ) Avizul nr. 2/2021 al AEPD referitor la propunerea de act legislativ privind piețele digitale, adoptat la 10 februarie 2021, disponibil la adresa: [https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act\\_en](https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act_en)
- ) Avizul nr. 3/2020 al AEPD referitor la Strategia europeană privind datele, adoptat la 16 iunie 2020, disponibil la adresa: [https://edps.europa.eu/sites/default/files/publication/20-06-16\\_opinion\\_data\\_strategy\\_en.pdf](https://edps.europa.eu/sites/default/files/publication/20-06-16_opinion_data_strategy_en.pdf)
- ) Avizul preliminar nr. 8/2020 al AEPD referitor la spațiul european al datelor privind sănătatea, adoptat la 17 noiembrie 2020, disponibil la adresa: [https://edps.europa.eu/sites/default/files/publication/20-11-17\\_preliminary\\_opinion\\_european\\_health\\_data\\_space\\_en.pdf](https://edps.europa.eu/sites/default/files/publication/20-11-17_preliminary_opinion_european_health_data_space_en.pdf).