# Avizul comun nr. 3/2022 al CEPD-AEPD privind Propunerea de regulament referitor la spațiul european al datelor privind sănătatea

**Adoptat la 12 iulie 2022**

# CUPRINS

## Rezumat

Prin prezentul aviz comun, CEPD și AEPD urmăresc să atragă atenția asupra unei serii de preocupări generale cu privire la Propunerea referitoare la spațiul european al datelor privind sănătatea și să îndemne co-legiuitorul să ia măsuri decisive.

CEPD și AEPD iau act de faptul că Propunerea urmărește să sprijine persoanele fizice să preia controlul asupra propriilor date privind sănătatea, să sprijine utilizarea datelor privind sănătatea pentru o mai bună furnizare a asistenței medicale, o mai bună cercetare, inovare și elaborare de politici și să permită UE să utilizeze pe deplin potențialul oferit de schimbul, utilizarea și reutilizarea în condiții de siguranță și securitate a datelor privind sănătatea. Într-adevăr, „facilitarea utilizării datelor electronice privind sănătatea", atât pentru utilizare primară, cât și pentru utilizare secundară, ar putea contribui în mod semnificativ atât la interesele publice, cât și la interesul persoanelor vizate/pacienților individuali.

Deși efortul de a consolida controlul și drepturile persoanelor vizate asupra datelor lor cu caracter personal privind sănătatea este binevenit, ar trebui subliniat faptul că această Propunere aduce în principal câteva „completări" la unele dintre drepturile persoanelor vizate prevăzute deja în RGPD. De fapt, Propunerea ar putea chiar să slăbească protecția drepturilor la viață privată și la protecția datelor, în special având în vedere categoriile de date cu caracter personal și scopurile care sunt legate de utilizarea secundară a datelor.

CEPD și AEPD iau act de faptul că dispozițiile din această Propunere vor adăuga încă un nivel la colecția deja complexă (pe mai multe niveluri) de dispoziții (care se regăsesc atât în dreptul Uniunii, cât și în dreptul intern al statelor membre) referitoare la prelucrarea datelor privind sănătatea (în sectorul asistenței medicale). Interacțiunea dintre aceste diferite acte legislative trebuie să fie (extrem de) clară.

În special, CEPD și AEPD consideră că este important să se clarifice relația dintre dispozițiile din Propunerea în cauză și cele din RGPD și din legislația statelor membre. CEPD și AEPD recunosc intenția și eforturile de a rămâne în limitele RGPD în propunerea privind EHDS (European Health Data Space, „spațiul european al datelor privind sănătatea"). Acest lucru poate fi recunoscut, de exemplu, atunci când creează, prin intermediul dreptului Uniunii, temeiuri juridice și/sau excepții pentru prelucrarea datelor privind sănătatea care se încadrează în structura RGPD prevăzută la articolele 6 și 9 din RGPD. Cu toate acestea, în ceea ce privește nivelul dorit de claritate a acestor dispoziții, rămân încă multe de făcut (prin îmbunătățirea dispozițiilor și clarificări suplimentare), în special în ceea ce privește interacțiunea dispozițiilor cu legislația statelor membre în temeiul articolului 9 alineatul (4) din RGPD. Aceste preocupări sunt reflectate în observațiile referitoare atât la capitolul II, cât și la capitolul IV din Propunere.

În ceea ce privește domeniul de aplicare al Propunerii, CEPD și AEPD recomandă excluderea de la articolul 33 alineatul (1) litera (f) din Propunere a aplicațiilor de wellness și a altor aplicații digitale, precum și a datelor privind bunăstarea și comportamentul, relevante pentru sănătate. În cazul în care aceste date sunt păstrate, prelucrarea pentru utilizarea secundară a datelor cu caracter personal care provin din aplicații de wellness și din alte aplicații digitale ar trebui să facă obiectul consimțământului prealabil în sensul RGPD. În plus, CEPD și AEPD reamintesc că o astfel de prelucrare poate intra în domeniul de aplicare al Directivei 2002/58/CE („Directiva privind viața privată și comunicațiile electronice").

De asemenea, CEPD și AEPD recomandă insistent să nu se extindă domeniul de aplicare al excepțiilor din RGPD în ceea ce privește drepturile persoanei vizate la propunere și, în special, la articolul 38 alineatul (2) din Propunere. O astfel de derogare mai degrabă subminează posibilitatea persoanelor vizate de a exercita un control efectiv asupra datelor lor cu caracter personal decât să o consolideze și, prin urmare, pare a fi în contradicție cu obiectivul prevăzut la articolul 1 alineatul (2) litera (a) din Propunere.

CEPD și AEPD salută faptul că Propunerea face trimitere la drepturile prevăzute de RGPD (de exemplu, dreptul de acces gratuit și dreptul de a obține o copie a datelor). Cu toate acestea, CEPD și AEPD iau act de faptul că descrierea drepturilor, astfel cum este prevăzută în Propunere, nu este în concordanță cu cea din RGPD. După cum s-a menționat mai sus, acest lucru poate genera insecuritate juridică pentru persoanele vizate, care ar putea să nu fie în măsură să facă distincția între cele două tipuri de drepturi. În acest scop și pentru a evita complexitatea implementării lor practice, CEPD și AEPD îndeamnă co-legiuitorul să asigure claritatea juridică în ceea ce privește interacțiunea dintre drepturile persoanei vizate introduse de Propunere și dispozițiile generale cuprinse în RGPD privind drepturile persoanelor vizate.

CEPD și AEPD recunosc dispozițiile din capitolul III care vizează îmbunătățirea interoperabilității dosarelor electronice de sănătate și facilitarea conectivității aplicațiilor de wellness cu astfel de dosare electronice de sănătate. Totuși, CEPD și AEPD sunt de părere că acestea din urmă nu ar trebui să fie incluse în utilizarea secundară a datelor privind sănătatea prevăzută la capitolul IV din Propunere. În primul rând, deoarece pentru datele privind sănătatea generate de aplicațiile de wellness și de alte aplicații digitale în domeniul sănătății nu se aplică aceleași cerințe de calitate a datelor și aceleași caracteristici ca în cazul datelor generate de dispozitivele medicale. În plus, aceste aplicații generează un volum enorm de date și pot fi extrem de invazive, deoarece se referă la fiecare pas făcut de persoane în viața lor de zi cu zi. Chiar dacă datele privind sănătatea ar putea fi într-adevăr separate de alte tipuri de date, s-ar putea face cu ușurință deducții legate de practicile alimentare și de alte obiceiuri, care dezvăluie informații deosebit de sensibile, cum ar fi orientarea religioasă.

În ceea ce privește scopurile utilizării secundare a datelor privind sănătatea enumerate la articolul 34 alineatul (1) din Propunere, CEPD și AEPD înțeleg că articolul 34 alineatul (1) literele (f) și (g) din Propunere poate include orice formă de „activități de dezvoltare și inovare pentru produse sau servicii care contribuie la sănătatea publică sau la securitatea socială” sau „formarea, testarea și evaluarea algoritmilor, inclusiv a dispozitivelor medicale, a sistemelor de IA și a aplicațiilor de sănătate digitală, care contribuie la sănătatea publică sau la securitatea socială”. CEPD și AEPD sunt de părere că Propunerea ar trebui să delimiteze și mai mult aceste scopuri și să definească cazurile în care există o legătură suficientă cu sănătatea publică și/sau securitatea socială. Acest lucru va fi esențial pentru realizarea unui echilibru, ținând seama în mod adecvat de obiectivele urmărite de Propunere și de protecția datelor cu caracter personal ale persoanelor vizate afectate de prelucrare.

În plus, articolul 34 alineatul (1) din Propunere conține mai multe tipuri de utilizare secundară, care s-ar încadra în diferite categorii de motive de excepție prevăzute la articolul 9 alineatul (2) din RGPD. Cu toate acestea, CEPD și AEPD consideră că acest lucru nu se reflectă în criteriile pe baza cărora organismele de acces la datele privind sănătatea ar trebui să evalueze și să decidă cu privire la cererile de acces la date (articolul 45 din Propunere) pentru a emite o autorizație de acces la date (articolul 46 din Propunere). În acest scop, CEPD și AEPD subliniază că criteriile prevăzute în acest sens la articolul 46 din Propunere se limitează la dispozițiile și principiile acestei Propunerii și nu este clar modul în care aceste dispoziții se referă la principiile și dispozițiile RGPD, în special la articolul 9 alineatul (2) din RGPD.

În ceea ce privește capitolul V, CEPD și AEPD recunosc că infrastructura pentru schimbul de date electronice privind sănătatea prevăzută în această Propunere privind EHSD nu vizează (sau nu ar putea avea ca rezultat) în niciun caz crearea unei baze de date centrale a UE cu date privind sănătatea, ci va facilita doar schimbul de astfel de date privind sănătatea din bazele de date descentralizate. Cu toate acestea, din cauza volumului mare de date care ar fi prelucrate, a naturii lor extrem de sensibile, a riscului de acces ilegal și a necesității de a asigura pe deplin supravegherea eficace a acestor date, CEPD și AEPD solicită adăugarea la Propunere a unei dispoziții care să prevadă stocarea datelor electronice cu caracter personal privind sănătatea în UE/SEE, fără a aduce atingere transferurilor ulterioare în conformitate cu capitolul V din RGPD.

În cele din urmă, în ceea ce privește modelul de guvernanță creat de Propunere, sarcinile și competențele noilor organisme publice trebuie să fie atent adaptate, în special ținând seama de sarcinile și competențele autorităților naționale de supraveghere, ale CEPD și ale AEPD în domeniul prelucrării datelor cu caracter personal (privind sănătatea). Ar trebui evitată suprapunerea competențelor și ar trebui specificate domeniile și cerințele în materie de cooperare.

**Comitetul European pentru Protecția Datelor și Autoritatea Europeană pentru Protecția Datelor,**

având în vedere articolul 42 alineatul (2) din Regulamentul (UE) 2018/1725 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,

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum a fost modificat prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018,

**A ADOPTAT PREZENTUL AVIZ COMUN**

# 1 CONTEXT

1. Propunerea de Regulament al Parlamentului European și al Consiliului referitor la spațiul european al datelor privind sănătatea („propunerea”) va contribui la realizarea viziunii Comisiei privind transformarea digitală a UE până în 2030[1].

2. Comitetul European pentru Protecția Datelor („CEPD”) și Autoritatea Europeană pentru Protecția Datelor („AEPD”) remarcă faptul că, potrivit Comisiei, Propunerea „îi ajută pe cetățeni să preia controlul asupra datelor lor medicale, sprijină utilizarea datelor privind sănătatea pentru a îmbunătăți asistența medicală, cercetarea, inovarea și elaborarea politicilor și îi permite UE să valorifice pe deplin potențialul oferit de schimbul, utilizarea și reutilizarea în condiții de siguranță și securitate a datelor medicale”[2].

3. Astfel cum se explică în expunerea de motive, Propunerea este în conformitate cu obiectivele generale ale UE. Printre acestea se numără construirea unei Uniuni Europene a sănătății mai puternice, punerea în aplicare a Pilonului european al drepturilor sociale, îmbunătățirea funcționării pieței interne, promovarea sinergiilor cu agenda privind piața internă digitală a UE și realizarea unei agende ambițioase în materie de cercetare și inovare. În plus, Propunerea va oferi un set important de elemente care vor contribui la crearea Uniunii Europene a sănătății, prin încurajarea inovării și cercetării și printr-o mai bună abordare a viitoarelor crize sanitare.

# 2 DOMENIUL DE APLICARE AL AVIZULUI

[1] Expunerea de motive, p. 2.
[2] https://ec.europa.eu/health/ehealth-digital-health-and-care/european-health-data-space_ro.

4. La 3 mai 2022, Comisia a publicat Propunerea de Regulament al Parlamentului European și al Consiliului referitor la spațiul european al datelor privind sănătatea („Propunerea”).

5. La 4 mai 2022, Comisia a solicitat un aviz comun din partea CEPD și AEPD („avizul”) în temeiul articolului 42 alineatul (2) din Regulamentul (UE) 2018/1725[3] („RPDUE”) cu privire la Propunere.

6. Propunerea are o importanță deosebită pentru protecția drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ale acestora. Domeniul de aplicare al avizului se limitează la aspectele Propunerii legate de datele cu caracter personal și care implică aceste date, care constituie unul dintre pilonii principali ai Propunerii.

7. CEPD și AEPD salută expunerea de motive a Propunerii, în care se afirmă că „[a]vând în vedere că un volum substanțial de date electronice care urmează să fie accesate în spațiul european al datelor privind sănătatea sunt date cu caracter personal privind sănătatea referitoare la persoane fizice din UE, propunerea este concepută în deplină conformitate nu numai cu RGPD, ci și cu Regulamentul (UE) 2018/1725 (Regulamentul UE privind protecția datelor)”.

8. În același sens, CEPD și AEPD subliniază că este necesar să se asigure și să se susțină respectarea și aplicarea acquis-ului UE în domeniul protecției datelor. Atunci când datele cu caracter personal sunt implicate în contextul Propunerii, este esențial să se evite în mod clar în textul juridic al Propunerii orice inconsecvență și posibil conflict cu Regulamentul General privind Protecția Datelor[4] („RGPD”), cu Directiva privind viața privată și comunicațiile electronice[5] și cu RPDUE. Acest lucru trebuie asigurat nu doar din motive de securitate juridică, ci și pentru a evita ca Propunerea să aibă ca efect periclitarea directă sau indirectă a drepturilor fundamentale la viață privată și la protecția datelor cu caracter personal, astfel cum sunt prevăzute la articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene („Carta”) și la articolul 16 din Tratatul privind Funcționarea Uniunii Europene („TFUE”).

9. Întrucât Propunerea, astfel cum se explică mai în detaliu în aviz, ridică o serie de preocupări cu privire la protecția drepturilor fundamentale la viață privată și la protecția datelor cu caracter personal, scopul prezentului aviz nu este să furnizeze o listă exhaustivă a tuturor aspectelor și nici să ofere întotdeauna propuneri alternative de sugestii de formulare. În schimb, prezentul aviz vizează abordarea principalelor aspecte critice ale Propunerii în ceea ce privește viața privată și protecția datelor.

# 3 EVALUARE

[3] 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.
[4] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE, JO L 119, 4.5.2016, p. 1.
[5] 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, JO L 201, 31.7.2002, p. 37.

## 3.1 Observații generale

10. CEPD și AEPD recunosc obiectivul Propunerii de a extinde utilizarea datelor electronice privind sănătatea pentru furnizarea de asistență medicală persoanei de la care au fost colectate datele respective („utilizare primară") și de a aduce îmbunătățiri în sectoare precum cercetarea, inovarea, elaborarea politicilor, siguranța pacienților, medicina personalizată, statisticile oficiale sau activitățile de reglementare („utilizare secundară"). CEPD și AEPD recunosc, de asemenea, obiectivul Propunerii de a îmbunătăți funcționarea pieței interne prin stabilirea unui cadru juridic uniform pentru dezvoltarea, comercializarea și utilizarea sistemelor de dosare electronice de sănătate („sistemele DES").

11. Cu toate acestea, CEPD și AEPD subliniază că protecția datelor cu caracter personal este un element integrant al încrederii pe care persoanele și organizațiile ar trebui să o aibă în dezvoltarea economiei digitale[6] și în accesul la asistență medicală echitabilă, în special în contextul prelucrării datelor privind sănătatea în cadrul EHDS.

12. În acest sens, CEPD și AEPD subliniază că succesul EHDS va depinde de un temei juridic solid pentru prelucrare în conformitate cu legislația UE privind protecția datelor, de instituirea unui mecanism solid de guvernanță a datelor și de garanții eficace pentru drepturile și interesele persoanelor fizice care respectă pe deplin RGPD. Ar trebui oferite asigurări suficiente cu privire la o gestionare legală, responsabilă și etică, ancorată în valorile UE, inclusiv cu privire la respectarea drepturilor fundamentale. În acest sens, CEPD și AEPD consideră că spațiul european al datelor privind sănătatea ar trebui să servească drept exemplu de transparență, de responsabilitate efectivă și de echilibru adecvat între interesele persoanelor vizate și interesul comun al societății în ansamblu.

13. În capitolele următoare ale avizului, CEPD și AEPD oferă recomandări cu privire la modul în care se poate asigura conformitatea dispozițiilor relevante ale Propunerii nu numai cu cadrul juridic al UE privind protecția datelor, ci și cu interpretarea actuală a jurisprudenței aplicabile a Curții de Justiție a Uniunii Europene („CJUE"). Având în vedere domeniul de aplicare larg al drepturilor și obligațiilor prevăzute în Propunere în ceea ce privește accesul, utilizarea și partajarea categoriilor speciale de date cu caracter personal, cum este cazul datelor privind sănătatea, este posibil ca trimiterile generale la RGPD și la RPDUE să nu fie suficiente. În acest sens, CEPD și AEPD consideră că ar putea exista un risc de interpretare eronată a dispozițiilor-cheie legate de protecția datelor, ceea ce, la rândul său, poate duce la o scădere a nivelului de protecție acordat în prezent persoanelor vizate în temeiul cadrului juridic existent al UE privind protecția datelor (RGPD, RPDUE și Directiva privind viața privată și comunicațiile electronice). Prin urmare, CEPD și AEPD consideră că sunt necesare specificații suplimentare, astfel cum vor fi detaliate în continuare în prezentul aviz.

14. CEPD și AEPD iau act cu satisfacție de faptul că Propunerea urmărește, de asemenea, să contribuie la atenuarea fragmentării actuale a normelor aplicabile prelucrării datelor privind sănătatea și cercetării științifice. În același timp, CEPD și AEPD ridică anumite semne de întrebare cu privire la compatibilitatea deplină a unora dintre dispozițiile capitolelor II și IV din Propunere (în special accesul cadrelor medicale la date electronice restricționate privind sănătatea, înregistrarea sistematică a datelor relevante privind sănătatea de către cadrele medicale sau gestionarea constatărilor neașteptate de către organismele de acces la datele privind sănătatea față de persoanele fizice) cu legislația statului membru în sectorul e-sănătății, în absența unei competențe legislative generale a

[6] Avizul comun privind DGA (Legea privind guvernanța datelor).

UE de armonizare în acest domeniu. În această privință, ar trebui reamintit faptul că, în temeiul articolului 168 din TFUE, acțiunea Uniunii încurajează cooperarea dintre statele membre în domeniul sănătății publice și, dacă este necesar, sprijină acțiunea acestora prin completarea politicii naționale, respectând în același timp responsabilitățile statelor membre în ceea ce privește definirea politicii lor de sănătate, precum și organizarea și prestarea de servicii de sănătate și de asistență medicală.

## 3.2 Interacțiunea Propunerii cu legislația UE privind protecția datelor

15. CEPD și AEPD salută considerentul 4 din Propunere, conform căruia „[p]relucrarea datelor electronice cu caracter personal privind sănătatea face obiectul dispozițiilor Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului și, pentru instituțiile și organele Uniunii, ale Regulamentului (UE) 2018/1725 al Parlamentului European și al Consiliului. Trimiterile la dispozițiile Regulamentului (UE) 2016/679 ar trebui înțelese, de asemenea, ca trimiteri la dispozițiile corespunzătoare din Regulamentul (UE) 2018/1725 pentru instituțiile și organele Uniunii, după caz”.

16. În plus, în conformitate cu expunerea de motive, Propunerea se bazează pe articolele 114 și 16 din Tratatul privind Funcționarea Uniunii Europene („TFUE”). În lumina Propunerii, în timp ce articolul 114 din TFUE vizează îmbunătățirea funcționării pieței interne prin măsuri de apropiere a normelor naționale, Propunerea vizează extinderea utilizării datelor electronice privind sănătatea, consolidând în același timp drepturile care decurg din articolul 16 din TFUE.

17. În acest sens, în conformitate cu jurisprudența CJUE, CEPD și AEPD subliniază că articolul 16 din TFUE prevede un temei juridic adecvat în cazurile în care protecția datelor cu caracter personal este unul dintre obiectivele sau componentele esențiale ale normelor adoptate de legiuitorul UE[7]. În plus, CEPD și AEPD reamintesc că aplicarea articolului 16 din TFUE implică, de asemenea, necesitatea de a se asigura supravegherea independentă a respectării cerințelor privind prelucrarea datelor cu caracter personal, astfel cum se prevede, de asemenea, la articolul 8 din Cartă[8].

18. Într-adevăr, în ceea ce privește aspectul referitor la supravegherea independentă, CEPD și AEPD subliniază că, în conformitate cu considerentul 43 din Propunere, autoritățile de supraveghere ar trebui să aibă sarcina de a asigura respectarea dispozițiilor relevante din RGPD și din RPDUE, în special în ceea ce privește prelucrarea datelor cu caracter personal pentru utilizări secundare în contextul capitolului IV din Propunere. În acest sens, CEPD și AEPD recomandă includerea unei dispoziții corespunzătoare în partea dispozitivă a textului.

19. În ceea ce privește recurgerea la articolul 16 din TFUE ca (unul dintre cele două[9]) temei (temeiuri) juridic (juridice) al (ale) Propunerii, CEPD și AEPD recunosc că **scopul** Propunerii este de a specifica „dispoziții și garanții suplimentare obligatorii din punct de vedere juridic[10]” în ceea ce privește protecția datelor privind sănătatea. Astfel de dispoziții sunt „suplimentare” celor din RGPD. Propunerea prevede „cerințe și standarde specifice”[11] care sunt adaptate pentru prelucrarea

[7] Avizul din 26 iulie 2017, PNR Canada, procedura de aviz 1/15, ECLI:EU:C:2017:592, punctul 96.
[8] OJ, Legea privind IA.
[9] AEPD și CEPD, în conformitate cu mandatele lor, nu vor aborda în prezentul aviz chestiunea justificării recurgerii la un temei juridic dublu și se vor limita la considerații legate de recurgerea la articolul 16 din TFUE.
[10] Expunerea de motive a Propunerii, p. 6.
[11] Idem.

electronică a datelor privind sănătatea și care „concretizează posibilitatea oferită de RGPD privind o legislație a UE în mai multe scopuri”[12].

20. În ceea ce privește **conținutul** Propunerii**,** CEPD și AEPD doresc să prezinte două observații generale.

21. În primul rând, Propunerea conține în principal norme privind prelucrarea datelor cu caracter personal (privind sănătatea), fie pentru utilizare primară, fie pentru utilizare secundară. Având în vedere impactul acestor dispoziții asupra „centrului de greutate” general al Propunerii, CEPD și AEPD sunt de acord că conținutul Propunerii conferă articolului 16 din TFUE statutul de temei juridic necesar. Acest lucru nu aduce atingere observațiilor din prezentul aviz cu privire la interacțiunea mai multor dispoziții ale Propunerii cu cele din RGPD, interacțiune care necesită în mod ferm clarificări suplimentare și, uneori, o reflecție și o revizuire suplimentare, astfel cum au fost dezvoltate în continuare în prezentul aviz.

22. CEPD și AEPD iau act, de asemenea, de faptul că, în conformitate cu considerentul 37, Propunerea are ca scop includerea în dreptul Uniunii a posibilității de a utiliza excepțiile de la articolul 9 alineatul (2) literele (g), (i) și (j) din RGPD. CEPD și AEPD remarcă, de asemenea, că, pentru utilizarea secundară a datelor privind sănătatea, Propunerea creează o obligație pentru deținătorii de date în sensul articolului 6 alineatul (1) litera (c) din RGPD de a divulga date cu caracter personal organismelor de acces la datele privind sănătatea. În același timp, CEPD și AEPD înțeleg că Propunerea nu urmărește să creeze un temei juridic pentru solicitanții de date în raport cu articolul 6 din RGPD, nici să modifice cerințele de informare în temeiul RGPD sau al Directivei privind viața privată și comunicațiile electronice, nici să modifice vreun drept prevăzut în acestea.

23. În al doilea rând, CEPD și AEPD iau act de faptul că Propunerea conține cel puțin o derogare explicită de la o dispoziție a RGPD: într-adevăr, articolul 38 alineatul (2) din Propunere scutește anumite entități (organismele de acces la datele privind sănătatea) de la aplicarea dispozițiilor articolului 14 din RGPD privind informațiile care trebuie furnizate persoanelor vizate. CEPD și AEPD consideră că o astfel de derogare mai degrabă subminează posibilitatea persoanelor vizate de a exercita un control efectiv asupra datelor lor cu caracter personal decât să o consolideze și, prin urmare, pare a fi în contradicție cu obiectivul prevăzut la articolul 1 alineatul (2) litera (a) din Propunere. În plus, CEPD și AEPD se întreabă dacă este necesar și justificat să se introducă o restricție privind dreptul la informare, astfel cum se explică în detaliu la punctele 26, 34, 96 și 97 din prezentul aviz, inclusiv în lumina articolului 23 din RGPD.

24. La un nivel mai general, CEPD și AEPD avertizează cu privire la legislația care prevede derogări de la sarcinile și competențele autorităților de supraveghere a protecției datelor și de la normele general aplicabile ale RGPD, în conformitate cu articolul 8 din Cartă. O astfel de legislație afectează în mod inevitabil și, în cele din urmă, are potențialul de a submina, în timp, caracterul central al normelor orizontale adoptate în temeiul articolului 16 din TFUE. Autoritățile independente de supraveghere ar trebui să fie însărcinate cu supravegherea Propunerii, în ceea ce privește prelucrarea datelor cu caracter personal.

25. În orice caz, CEPD și AEPD se întreabă dacă este necesară și justificată o restricție a dreptului la informare în acest context. Într-adevăr, atât articolul 14 alineatul (5) litera (b), cât și articolul 14 alineatul (5) litera (c) din RGPD îi scutesc pe operatori de la respectarea articolului 14 din RGPD în anumite cazuri, și anume în cazul în care (1) furnizarea acestor informații se dovedește a fi imposibilă

[12] Idem.

sau ar implica eforturi disproporționate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva condițiilor și a garanțiilor prevăzute la articolul 89 alineatul (1) sau în măsura în care obligația menționată la alineatul (1) de la prezentul articol este susceptibilă să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective[13]; și (2) obținerea sau divulgarea datelor cu caracter personal este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern sub incidența căruia intră operatorul și care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate. În măsura în care Propunerea privind spațiul european al datelor privind sănătatea prevede în mod expres obținerea sau divulgarea de date cu caracter personal, ar trebui să se evalueze mai degrabă dacă aceasta conține garanții adecvate pentru protejarea intereselor legitime ale persoanelor vizate.

26. În cele din urmă, CEPD și AEPD remarcă faptul că, deși Propunerea acoperă și aplicațiile de wellness și alte aplicații digitale de sănătate, Directiva privind viața privată și comunicațiile electronice nu este inclusă la articolul 1 alineatul (4). Deși pun sub semnul întrebării includerea unor astfel de aplicații în domeniul de aplicare al capitolului IV din Propunere, astfel cum se va explica în următorul capitol, CEPD și AEPD recomandă includerea unei trimiteri la Directiva privind viața privată și comunicațiile electronice, în cazul în care aceste aplicații sunt încă menționate în Propunere.

27. În plus, articolul 1 alineatul (4) din Propunere ar trebui, de asemenea, să facă trimitere la RPDUE, iar dispozițiile relevante din RPDUE ar trebui, de asemenea, să fie identificate în mod explicit în întreaga Propunere[14]. Trimiterile explicite la articolele relevante din RPDUE în partea dispozitivă a Propunerii par a fi mai mult decât justificate, în primul rând, deoarece Comisia va acționa în calitate de persoană împuternicită de operator pentru datele electronice privind sănătatea comunicate prin „MyHealth@EU” [articolul 12 alineatul (7) din Propunere], în al doilea rând, deoarece instituțiile, organele, oficiile și agențiile Uniunii pot avea acces regulat la datele electronice privind sănătatea (considerentul 41 din Propunere) și, în al treilea rând, deoarece datele deținute de instituțiile UE pot fi, de asemenea, puse la dispoziție pentru utilizare secundară (considerentul 46 din Propunere).

### 3.3 Interacțiunea dintre Propunere și DGA, Legea privind datele și Legea privind IA

28. CEPD și AEPD iau act de faptul că, în conformitate cu articolul 1 alineatul (4) din Propunere, Regulamentul „nu aduce atingere altor acte juridice ale Uniunii privind accesul la datele electronice privind sănătatea, partajarea sau utilizarea secundară a acestora sau cerințelor legate de prelucrarea datelor în legătură cu datele electronice privind sănătatea, în special Regulamentelor (UE) 2016/679, (UE) 2018/1725, [...] [Legea privind guvernanța datelor – COM/2020/767 final] și [...] [Legea privind datele – COM/2022/68 final].” În plus, în conformitate cu articolul 1 alineatul (5) din Propunere, Regulamentul „nu aduce atingere Regulamentelor (UE) 2017/745 și [...] [Legea privind inteligența artificială – COM/2021/206 final] în ceea ce privește securitatea dispozitivelor medicale și a sistemelor de IA care interacționează cu sistemele DES”.

[13] În astfel de cazuri, operatorul ia măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate, inclusiv punerea informațiilor la dispoziția publicului.

[14] În conformitate cu considerentul 4 din Propunere, trimiterile la dispozițiile RGPD ar trebui înțelese și ca trimiteri la dispozițiile corespunzătoare din RPDUE. Deși scopul considerentului 4 este clar, CEPD și AEPD recomandă ferm ca dispozițiile relevante din RPDUE să fie identificate în mod explicit în partea dispozitivă a Propunerii ca atare.

29. Deși salută trimiterea explicită la Propunere, care nu aduce atingere Legii privind guvernanța datelor („DGA”), Legii privind datele și Legii privind inteligența artificială („IA”), CEPD și AEPD consideră că interacțiunea specifică a Propunerii cu inițiativele menționate mai sus, care fac parte din pachetul digital, precum și cu Regulamentul privind dispozitivele medicale (MDR)[15], ar trebui abordată mai bine. Pentru a ilustra acest punct și doar cu titlu de exemplu, Propunerea introduce o definiție a noțiunii de „deținător de date” în temeiul articolului 2 alineatul (2) litera (y), care ar putea să nu fie în concordanță cu definiția noțiunii de „deținător de date” din DGA și din Legea privind datele. Acest lucru ar putea duce la insecuritate juridică în ceea ce privește entitățile care ar intra sub incidența unei astfel de definiții, în pofida faptului că ar constitui un aspect central al Propunerii, având în vedere că aceasta ar determina – în mod esențial – entitățile care vor fi supuse obligației de a pune la dispoziție date electronice privind sănătatea pentru o utilizare secundară.

30. CEPD și AEPD iau act, de asemenea, de faptul că obiectivul general al Propunerii este de a se asigura un control sporit al persoanelor fizice din UE asupra datelor lor electronice privind sănătatea, ceea ce nu se poate realiza dacă interacțiunea dintre reglementările relevante nu este identificată în mod clar. Securitatea juridică este esențială nu numai pentru a garanta că diferitele părți interesate se simt în siguranță să acționeze în noul cadru, ci și pentru a garanta drepturile persoanelor fizice. Prin urmare, CEPD și AEPD recomandă clarificarea suplimentară a interacțiunii dintre Propunere și inițiativele și instrumentele juridice menționate mai sus.

# 4 DISPOZIȚII GENERALE (CAPITOLUL I)

## 4.1 Articolul 1: Obiectul și domeniul de aplicare al Propunerii

31. CEPD și AEPD salută faptul că Propunerea vizează, printre altele, consolidarea drepturilor persoanelor fizice în ceea ce privește disponibilitatea și controlul datelor lor electronice privind sănătatea.

32. CEPD și AEPD cunosc faptul că pandemia de COVID-19 a accelerat considerabil gradul de utilizare a dispozitivelor medicale, a aplicațiilor de wellness sau a dispozitivelor purtabile în rândul populației generale. Cu toate acestea, o astfel de tehnologie generează un volum enorm de date, adesea categorii speciale de date cu caracter personal, și poate fi extrem de invazivă. Mai mult decât urmărirea acțiunilor și a deciziilor oamenilor, în prezent este posibil să se urmărească corpul, mintea și emoțiile oamenilor la un nivel pe care oamenii înșiși nu l-ar putea atinge. Aceste date pot fi apoi utilizate pentru a anticipa acțiunile oamenilor și pentru a le manipula comportamentul, chiar și la nivel de grup.

33. CEPD și AEPD iau act de faptul că, astfel cum se prevede la articolul 1 alineatul (2) litera (a) din Propunere, primul obiectiv al Propunerii este de a consolida drepturile persoanelor fizice în ceea ce privește disponibilitatea și controlul datelor lor electronice privind sănătatea. În același timp, CEPD și AEPD observă, de asemenea, că, spre deosebire de utilizarea primară, pentru care Propunerea permite persoanelor fizice să restricționeze accesul la datele lor cu caracter personal, în cazul utilizării secundare a datelor, nu există această opțiune. În plus, în conformitate cu articolul 38 alineatul (2) din Propunere, „[o]rganismele de acces la datele privind sănătatea nu sunt obligate să furnizeze fiecărei persoane fizice informațiile specifice în temeiul articolului 14 din Regulamentul (UE) 2016/679 cu

[15] Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului, 5.5.2017, L 117/1.

privire la utilizarea datelor lor pentru proiecte care fac obiectul unei autorizații privind datele [...]". CEPD și AEPD subliniază că dreptul la informare și dreptul la opoziție sunt legate în mod indisolubil. Prin restricționarea dreptului la informare în temeiul RGPD, CEPD și AEPD sunt de părere că Propunerea nu poate atinge obiectivele prevăzute la articolul 1 alineatul (2) litera (a) din Propunere. De fapt, abordarea avută în vedere pare să submineze drepturile persoanelor fizice la viață privată și la protecția datelor cu caracter personal, în special ținând seama de definiția foarte largă a noțiunii de „utilizare secundară" și de categoriile minime de date electronice pentru utilizare secundară introduse de propunere, care nu se limitează doar la cercetarea științifică, ci include și alte scopuri, cum ar fi inovarea.

34. În plus, CEPD și AEPD iau act de faptul că articolul 1 alineatul (3) litera (a) din Propunere prevede că Propunerea se aplică „(...) producătorilor și furnizorilor de **sisteme DES** și de **aplicații de wellness** introduse pe piață și puse în funcțiune în Uniune și utilizatorilor acestor produse", în timp ce articolul 33 alineatul (1) literele (f) și (n) din Propunere enumeră printre categoriile minime de date electronice pentru uz secundar datele electronice privind sănătatea generate de persoane, inclusiv **datele generate de dispozitive medicale, aplicații de wellness sau alte aplicații de sănătate digitală, precum și datele privind bunăstarea și comportamentul, relevante pentru sănătate** (subliniere adăugată). În primul rând, există o neconcordanță între domeniul de aplicare al Propunerii și categoriile de date enumerate la articolul 33 alineatul (1) litera (f) din Propunere: cel dintâi se referă numai la producătorii și furnizorii de sisteme DES și aplicații de wellness, în timp ce cele din urmă includ și dispozitivele medicale pe lângă aplicațiile de wellness și alte aplicații de sănătate digitală. CEPD și AEPD înțeleg că dispozitivele medicale intră, de asemenea, în domeniul de aplicare al Propunerii. Astfel, din motive de claritate juridică, CEPD și AEPD recomandă adăugarea producătorilor și furnizorilor de dispozitive medicale la articolul 1 alineatul (3) litera (a) din Propunere.

35. În plus, CEPD și AEPD subliniază că, pentru datele privind sănătatea generate de aplicațiile de wellness și de alte aplicații de sănătate digitală, nu există aceleași cerințe de calitate a datelor și aceleași caracteristici ca în cazul datelor generate de dispozitivele medicale (acestea din urmă făcând obiectul standardelor și legislației specifice existente). În plus, ar trebui remarcat faptul că aplicațiile de sănătate digitală pot colecta date cu caracter personal care depășesc datele privind sănătatea: de exemplu, prin colectarea de informații cu caracter personal privind practicile alimentare și alte obiceiuri, se pot dezvălui indirect informații deosebit de sensibile, cum ar fi orientarea religioasă.

36. În acest context, deși înțeleg posibila necesitate de a include dispozitivele medicale în domeniul de aplicare al Propunerii, **CEPD și AEPD recomandă excluderea de la articolul 33 alineatul (1) litera (f) și, respectiv, litera (n) din Propunere a aplicațiilor de wellness și a altor aplicații digitale, precum și a datelor privind bunăstarea și comportamentul, relevante pentru sănătate**. În cazul în care aceste date sunt păstrate, prelucrarea pentru utilizarea secundară a datelor cu caracter personal care provin din aplicații de wellness și din alte aplicații digitale ar trebui să facă obiectul consimțământului prealabil în sensul RGPD. În plus, CEPD și AEPD reamintesc că o astfel de prelucrare poate intra în domeniul de aplicare al Directivei 2002/58/CE („Directiva privind viața privată și comunicațiile electronice").

37. CEPD și AEPD iau act de faptul că, în conformitate cu articolul 2 alineatul (2) din Propunere, definiția noțiunii de „deținător de date" include în mod explicit instituțiile Uniunii Europene („IUE"). Cu toate acestea, **IUE poate însemna atât un operator de date cu caracter personal și date privind sănătatea (și, prin urmare, un deținător de date), cât și un utilizator de date cu caracter personal și privind**

**sănătatea**[16]. Acest lucru este explicat în considerentul 41 și la articolele 34, 45 și 48 din Propunere. Prin urmare, din motive de securitate juridică, CEPD și AEPD **recomandă să se clarifice dacă IUE sunt incluse și în definiția noțiunii de „utilizator de date”**. În cele din urmă, CEPD și AEPD reamintesc că, întrucât instituțiile, organele, oficiile și agențiile Uniunii nu fac obiectul jurisdicțiilor naționale, ar trebui aduse clarificări specifice în ceea ce privește sancțiunile care pot fi impuse de organismele de acces la datele privind sănătatea, astfel cum se prevede la articolul 43 din Propunere.

## 4.2 Articolul 2: Definiții

38. CEPD și AEPD iau act de faptul că articolul 2 din Propunere prevede definiții relevante pentru înțelegerea Regulamentului în ansamblu. Cu toate acestea, CEPD și AEPD consideră că mai multe dintre acestea sunt foarte largi și deschise interpretării, la rândul lor putând genera insecuritate juridică.

39. În primul rând, articolul 2 alineatul (1) litera (a) din Propunere prevede că se aplică **definițiile din Regulamentul (UE) 2016/679**. În același timp, Propunerea introduce noi definiții și face trimitere la concepte specifice din alte regulamente, cum ar fi Legea privind datele. De exemplu, Propunerea introduce o definiție a noțiunii de „destinatar al datelor”, deși o astfel de definiție este deja prevăzută la articolul 4 alineatul (9) din RGPD. Întrucât Propunerea urmărește să completeze anumite dispoziții din RGPD, din motive de securitate juridică, CEPD și AEPD recomandă să se explice motivele pentru care sunt necesare definiții suplimentare sau, în cazul cel mai extrem, cu titlu de excepție, să se identifice definițiile din RGPD care nu se aplică.

40. Articolul 2 alineatul (2) litera (a) din Propunere definește noțiunea de **„date electronice cu caracter personal privind sănătatea”** ca fiind date privind sănătatea și date genetice, astfel cum sunt definite în RGPD, precum și date referitoare la factorii determinanți ai sănătății sau date prelucrate în legătură cu furnizarea de servicii de asistență medicală, prelucrate în format electronic. În acest sens, trebuie subliniat faptul că considerentul 35 din RGPD include deja „informații [...] colectate [...] în cadrul acordării serviciilor [de asistență medicală]”. În plus, considerentul 54 din Propunere se referă, de asemenea, la „factorii determinanți care au efect asupra stării de sănătate”, în special în contextul prelucrării unor astfel de date privind sănătatea din motive de interes public. Pentru a asigura o aliniere cât mai mare cu RGPD, CEPD și AEPD recomandă modificarea definiției de la articolul 2 alineatul (2) litera (a) din Propunere pentru a se referi pur și simplu la „date privind sănătatea și date genetice, astfel cum sunt definite în Regulamentul (UE) 2016/679 [...] prelucrate în format electronic”.

---

[16] Instituțiile, organele și agențiile UE prelucrează date privind sănătatea în principal în următoarele contexte:
1. recrutarea (examinare medicală de angajare);
2. sănătatea în muncă (vizită medicală anuală)/securitatea și sănătatea în muncă;
3. rambursarea cheltuielilor medicale (Sistemul comun de asigurări de sănătate);
4. concediile medicale (certificate medicale) și proceduri de invaliditate și
5. îndeplinirea unei sarcini încredințate misiunii IUE (de exemplu, Centrul European de Prevenire și Control al Bolilor și Agenția Europeană pentru Medicamente).

Operațiunile de prelucrare care implică date privind sănătatea pot prezenta riscuri specifice și mai mari pentru drepturile și libertățile persoanelor vizate, care sunt membri ai personalului, agenți temporari, agenți contractuali, experți naționali, stagiari ai acestor organisme, candidați pentru posturile menționate anterior și vizitatori ai IUE. Aceste riscuri sunt similare celor cu care se confruntă persoanele vizate atunci când datele lor privind sănătatea sunt prelucrate de operatori care nu sunt IUE.

41. Pe de altă parte, articolul 2 alineatul (2) litera (b) din Propunere definește noțiunea de „**date electronice fără caracter personal privind sănătatea**” ca fiind date privind sănătatea și date genetice în format electronic care nu se încadrează în definiția datelor cu caracter personal prevăzută la articolul 4 punctul 1 din RGPD. În acest sens, CEPD și AEPD subliniază din nou[17] că distincția dintre categoria datelor cu caracter personal și cea a datelor fără caracter personal este dificil de aplicat în practică. Într-adevăr, dintr-o combinație de date fără caracter personal este posibil să se deducă sau să se genereze date cu caracter personal, adică date referitoare la o persoană identificată sau identificabilă, în special atunci când datele fără caracter personal sunt rezultatul anonimizării datelor cu caracter personal și chiar mai mult în contextul prelucrării datelor privind sănătatea. În acest context, CEPD și AEPD iau act de riscul de reidentificare prevăzut în considerentul 64 din Propunere și recomandă să se clarifice faptul că, în cazul seturilor de date mixte (în care datele cu caracter personal și datele fără caracter personal sunt „legate în mod indisolubil”), se aplică protecția prevăzută de RGPD și de Propunerea referitoare la datele electronice cu caracter personal privind sănătatea.

42. Articolul 2 alineatul (2) litera (d) și articolul 2 alineatul (2) litera (e) din Propunere definesc noțiunile de „**utilizare primară a datelor electronice privind sănătatea**”, respectiv de „**utilizare secundară a datelor electronice privind sănătatea**”. CEPD și AEPD consideră că aceste definiții pot genera insecuritate juridică și incoerență cu RGPD, în special în ceea ce privește definiția utilizării secundare a datelor electronice privind sănătatea. În special, a doua parte a articolului 2 alineatul (2) litera (e) din Propunere prevede că „[d]atele utilizate pot include date electronice cu caracter personal privind sănătatea colectate inițial în contextul utilizării primare, dar și date electronice privind sănătatea colectate în scopul utilizării secundare.” CEPD și AEPD consideră că, întrucât conceptul de „utilizare secundară a datelor cu caracter personal” nu apare în RGPD, a doua parte a definiției „utilizării secundare a datelor electronice privind sănătatea” se abate de la conceptul RGPD de „prelucrare ulterioară a datelor cu caracter personal”. De fapt, acesta din urmă trebuie înțeles în raport cu scopul pentru care un anumit operator a colectat inițial datele, indiferent de aspectele lor calitative. Prin urmare, CEPD și AEPD recomandă corectarea acestor definiții în lumina RGPD și, în special, clarificarea legăturii dintre definiția utilizării secundare a datelor electronice privind sănătatea în sensul Propunerii și conceptul de „utilizare ulterioară a datelor cu caracter personal” în sensul RGPD, în special ținând seama de regimul special deja prevăzut de RGPD pentru cercetarea științifică.

43. Articolul 2 alineatul (2) litera (f) din Propunere definește noțiunea de **„interoperabilitate”** ca fiind „capacitatea organizațiilor, precum și a aplicațiilor software sau a dispozitivelor aceluiași producător sau ale unor producători diferiți de a interacționa în vederea atingerii unor obiective reciproc avantajoase, care implică schimbul de informații și cunoștințe între aceste organizații, aplicații software sau dispozitive, fără a modifica conținutul datelor, prin intermediul proceselor pe care le sprijină”. În acest sens, CEPD și AEPD consideră că o astfel de definiție ar putea necesita clarificări suplimentare în ceea ce privește interacțiunea sa cu definițiile noțiunii de „interoperabilitate” deja existente în alte acte legislative, cum ar fi DGA și Regulamentul eIDAS.

44. Articolul 2 alineatul (2) litera (y) din Propunere definește un **„deținător de date”** ca fiind „orice persoană fizică sau juridică care este o entitate sau un organism din sectorul sănătății sau al îngrijirii sau care desfășoară activități de cercetare în legătură cu aceste sectoare, incluzând instituțiile, organele, oficiile și agențiile Uniunii, care are dreptul sau obligația, în conformitate cu prezentul Regulament, cu legislația aplicabilă a Uniunii sau cu legislația națională de punere în aplicare a dreptului Uniunii sau, în cazul datelor fără caracter personal, prin controlul proiectării tehnice a unui

[17] Avizul comun al CEPD-AEPD referitor la Legea privind DGA, punctul 58.

produs și a serviciilor conexe, care are capacitatea de a pune la dispoziție anumite date, inclusiv de a înregistra, a furniza, a restricționa accesul sau a face schimb de anumite date". După cum s-a subliniat deja mai sus la punctul 29, aceasta este o definiție centrală, care, totuși, este atât de amplă încât nu permite să se identifice în mod clar cine s-ar califica drept deținător de date[1] și să se înțeleagă care este interacțiunea cu definiția deținătorului de date prevăzută în Legea privind datele și DGA. În cazul în care această dispoziție nu definește în mod clar cine intră sub incidența acestei definiții, ea poate genera insecuritate juridică în ceea ce privește persoana care are obligația de a pune datele la dispoziție pentru o utilizare secundară în temeiul articolului 33 alineatul (1) și al articolului 44 din Propunere, ceea ce, la rândul său, ar putea submina dreptul persoanelor vizate la viață privată și la protecția datelor. În plus, definiția este incompatibilă cu articolul 3 alineatul (8) din Propunere, care se referă, de asemenea, la sectorul securității sociale, care nu este inclus în prezent în aceeași definiție prevăzută la articolul 2 alineatul (2) litera (y) din Propunere. Prin urmare, CEPD și AEPD sunt de părere că, din motive de securitate juridică, este important să se clarifice acest concept.

45. Articolul 2 alineatul (2) litera (z) din Propunere definește noțiunea de **„utilizator de date"** ca fiind „o persoană fizică sau juridică care are acces legal la date electronice privind sănătatea cu sau fără caracter personal, pentru utilizare secundară". În această privință, CEPD și AEPD consideră că relația sa cu definiția noțiunii de „destinatar al datelor" de la articolul 2 alineatul (2) litera (k) din propunere, precum și cu definiția noțiunii de „destinatar" din RGPD este neclară. Această lipsă de claritate se aplică, de asemenea, interacțiunii acestei definiții cu noțiunea de „utilizator de date" din cadrul DGA. În plus, CEPD și AEPD fac trimitere la recomandarea formulată la punctul 37 din prezentul aviz cu privire la includerea IUE în această definiție. În cele din urmă, AEPD și CEPD consideră că, în loc să se prevadă că o persoană juridică are acces legal la date electronice cu caracter personal privind sănătatea, ar fi mai adecvat să se menționeze dacă și în ce condiții acest acces poate fi acordat sau nu.

# 5 UTILIZAREA PRIMARĂ A DATELOR ELECTRONICE PRIVIND SĂNĂTATEA (CAPITOLUL II)

46. CEPD și AEPD iau act de faptul că, în ceea ce privește utilizarea primară a datelor electronice privind sănătatea, astfel cum se prevede în Propunere, trebuie să se ajungă la un echilibru între facilitarea disponibilității evidențelor electronice, atât la nivel național, cât și la nivelul UE sau internațional, și impactul asupra drepturilor și libertăților persoanelor în general, precum și asupra drepturilor conferite de RGPD. CEPD și AEPD consideră că, pentru a atinge acest obiectiv, co-legiuitorul ar trebui să țină seama de următoarele aspecte ale Propunerii.

47. În primul rând, CEPD și AEPD iau act de faptul că articolul 3 din Propunere se referă la drepturile persoanelor fizice în ceea ce privește utilizarea primară a datelor lor personale electronice privind sănătatea[18]. CEPD și AEPD au motive serioase de îngrijorare cu privire la interacțiunea acestor drepturi nou introduse cu cele prevăzute la articolele 15-22 din RGPD. În special, CEPD și AEPD sunt preocupate de suprapunerea drepturilor prevăzute în Propunere cu cele prevăzute în RGPD și de riscul de insecuritate juridică pe care acest lucru l-ar putea genera față de persoanele vizate. Prin urmare, din

[18] De exemplu, în ceea ce privește noul drept al persoanei vizate de a restricționa accesul cadrelor medicale la toate sau la o parte din datele sale electronice privind sănătatea, stabilit la articolul 3 alineatul (9) din Propunere, nu este clar dacă normele și garanțiile specifice care urmează să fie stabilite de legislația statelor membre în conformitate cu aceleași dispoziții respectă normele prevăzute la articolul 18 alineatele (2) și (3) din RGPD privind dreptul la restricționarea prelucrării datelor.

motive de securitate juridică, CEPD și AEPD îndeamnă co-legiuitorul să clarifice relația dintre aceste drepturi și să se asigure că acestea nu limitează (direct sau indirect) domeniul de aplicare al drepturilor persoanelor fizice în temeiul legislației UE privind protecția datelor.

48. Articolul 3 din Propunere introduce dreptul de acces imediat și dreptul de a acorda acces la date sau de a solicita transmiterea acestora destinatarilor la alegerea lor, precum și dreptul de a restricționa accesul cadrelor medicale la toate datele lor electronice privind sănătatea sau la o parte a acestora și de a obține informații cu privire la furnizorii de asistență medicală și cadrele medicale care au accesat datele lor electronice privind sănătatea în contextul asistenței medicale. Astfel cum se menționează în considerentul 1 din Propunere, „[s]copul prezentului Regulament este de a institui spațiul european al datelor privind sănătatea (European Health Data Space - „EHDS") pentru a îmbunătăți accesul persoanelor fizice la datele lor electronice cu caracter personal privind sănătatea și controlul acestora asupra datelor respective în contextul asistenței medicale (utilizarea primară a datelor electronice privind sănătatea) [...]". Considerentul 6 din Propunere explică faptul că spațiul european al datelor privind sănătatea se bazează pe drepturile prevăzute în RGPD ale persoanelor vizate și le dezvoltă suplimentar, sprijinind în același timp o aplicare coerentă a acestor drepturi, astfel cum sunt aplicate datelor electronice privind sănătatea.

49. În acest context, CEPD și AEPD subliniază că, la momentul redactării prezentului aviz, nu a fost efectuată nicio evaluare a impactului asupra protecției datelor [19] cu privire la Propunere. Drept urmare, nu a avut loc o evaluare a modului în care modificările avute în vedere ar putea afecta drepturile și libertățile persoanei vizate, și nici a riscurilor aferente.

50. În plus, CEPD și AEPD salută faptul că Propunerea face trimitere la drepturile prevăzute de RGPD (de exemplu, dreptul de acces gratuit și dreptul de a obține o copie a datelor)[20]. Cu toate acestea, CEPD și AEPD iau act de faptul că descrierea drepturilor, astfel cum este prevăzută în Propunere, nu este în concordanță cu cea din RGPD. După cum s-a menționat mai sus, acest lucru poate genera insecuritate juridică pentru persoanele vizate, care ar putea să nu fie în măsură să facă distincția între cele două tipuri de drepturi. În acest scop și pentru a evita complexitatea implementării lor practice, CEPD și AEPD îndeamnă co-legiuitorul să asigure claritatea juridică în ceea ce privește interacțiunea dintre drepturile persoanei vizate introduse de propunere și dispozițiile generale cuprinse în RGPD privind drepturile persoanelor vizate.

51. Acest lucru este cu atât mai relevant pentru a se asigura faptul că persoanele vizate cu capacitate limitată de a accesa și de a utiliza servicii digitale nu sunt obligate să se bazeze pe terți pentru a-și exercita drepturile fundamentale și, prin urmare, nu sunt obligate să își expună viața privată și datele cu caracter personal în fața altor persoane fizice pentru a putea solicita accesul la datele lor, în conformitate cu articolul 3 alineatul (5) litera (b) din Propunere.

---

[19] Propunerea este însoțită de un document de lucru al serviciilor Comisiei privind Raportul de Evaluare a Impactului (doc. 8751/22 ADD 3 din 6 mai 2022), care oferă doar o imagine de ansamblu asupra a trei opțiuni de politică privind impactul asupra drepturilor fundamentale. Aceasta nu constituie o evaluare a impactului asupra protecției datelor în sensul RGPD, care ar fi indispensabilă pentru o analiză aprofundată a evaluării riscurilor pe care le-ar implica o prelucrare la scară foarte largă a unor categorii speciale de date și care ar oferi măsurile de atenuare și garanțiile necesare.

[20] A se vedea, de exemplu, articolul 15 alineatele (1) și (3) din RGPD, în ceea ce privește existența dreptului de acces și a dreptului de a obține o copie a datelor, precum și articolul 12 alineatul (5) din RGPD, care prevede exercitarea drepturilor în mod gratuit.

52. CEPD și AEPD iau act de faptul că reprezentarea unei persoane vizate atunci când își exercită drepturile în materie de protecție a datelor trebuie să îndeplinească anumite cerințe de securitate juridică. Conceptul de autorizare introdus prin articolul 3 alineatul (5) din Propunere cu privire la serviciile generale de împuternicire în vederea accesului ar putea să nu fie suficient pentru a asigura că persoanele vizate nu au fost obligate în niciun fel să ofere acces la datele lor, în numele lor, altor persoane fizice la alegerea lor[21].

53. În plus, CEPD și AEPD subliniază că un astfel de concept larg de autorizare fără nicio garanție deschide calea unei posibile utilizări abuzive a dreptului de acces la datele electronice privind sănătatea. Astfel, cerința ca un reprezentant să fie doar o persoană fizică nu împiedică în mod necesar accesul la date al societăților private. Prin urmare, pentru a preveni un astfel de posibil abuz, CEPD și AEPD recomandă instituirea unor garanții suplimentare care să însoțească un astfel de mecanism de autorizare.

54. În ceea ce privește dreptul la rectificare prevăzut la articolul 3 alineatul (7) din Propunere, CEPD și AEPD remarcă faptul că nu reiese clar din Propunere cine va fi responsabil de asigurarea rectificării datelor. Acest lucru este problematic, având în vedere că, în acest context, există mai multe surse și destinatari ai datelor cu caracter personal, la nivel național, dar și la nivelul UE și chiar la nivel internațional. CEPD și AEPD subliniază că, în conformitate cu RGPD, o astfel de obligație revine operatorului de date. Cu toate acestea, întrucât, în acest context, există mai mulți operatori care contribuie la punerea la dispoziție a datelor electronice privind sănătatea, CEPD și AEPD solicită co-legiuitorilor să clarifice în Propunere modul în care va fi asigurată în practică respectarea dreptului la rectificare.

55. CEPD și AEPD iau act de faptul că articolul 3 alineatul (8) din Propunere prevede că persoanele fizice au dreptul de a acorda acces unui deținător de date din sectorul sănătății sau al securității sociale sau de a solicita unui deținător de date din sectorul sănătății sau al securității sociale să își transmită datele electronice privind sănătatea unui destinatar al datelor, la alegere, din sectorul sănătății sau al securității sociale, imediat, gratuit și fără impedimente din partea deținătorului datelor sau a producătorilor sistemelor utilizate de titularul respectiv. În acest sens, CEPD și AEPD subliniază că destinatarul datelor trebuie să fie identificat în mod corespunzător de sistem, inclusiv să demonstreze că entitatea care primește datele aparține sectorului sănătății sau sectorului securității sociale.

56. În plus, CEPD și AEPD consideră că, în conformitate cu cele stabilite de însăși persoana vizată, atunci când decide cărui destinatar al datelor îi vor fi puse la dispoziție datele sale electronice privind sănătatea în conformitate cu articolul 3 alineatul (8) din Propunere, acesta din urmă ar trebui să se asigure că persoana vizată ar putea, de asemenea, să decidă ce date urmează să fie transmise, în același sens cu ceea ce prevede propunerea la articolul 3 alineatul (9). Mai precis, CEPD și AEPD subliniază că propunerea ar trebui să prevadă posibilitatea ca numai datele necesare în scopul în cauză să fie transmise, impunând adoptarea unor măsuri tehnice de protejare a vieții private din faza de proiectare, pentru a respecta principiul reducerii la minimum a datelor.

57. În cele din urmă, CEPD și AEPD iau act de faptul că, deși articolul 3 alineatul (8) din Propunere introduce un nou drept al persoanei vizate de a-și transmite datele electronice privind sănătatea unui

[21] Ar trebui să se țină seama de faptul că, în unele state membre, acest lucru ar putea fi realizat în mod legal numai prin intermediul notarului, indiferent dacă persoana care obține accesul este sau nu tutore legal. Este important să se amintească faptul că intervenția notarului are legătură cu necesitatea de a asigura o manifestare liberă a voinței persoanelor vizate.

destinatar ales, acesta nu stabilește o obligație explicită corespunzătoare pentru deținătorul datelor de a proceda astfel. Întrucât articolul 9 alineatul (1) din RGPD nu permite, în principiu, prelucrarea datelor cu caracter personal privind sănătatea și nici a datelor genetice, cu excepția cazului în care se aplică una dintre derogările prevăzute la articolul 9 alineatul (2) din RGPD, CEPD și AEPD recomandă co-legiuitorului să alinieze articolul 3 alineatul (8) din Propunere la articolul 6 din RGPD și la articolul 9 alineatul (2) din RGPD, precum și să clarifice interacțiunea acestei dispoziții cu eventualele condiții suplimentare, inclusiv limitări, în ceea ce privește prelucrarea datelor privind sănătatea sau genetice pe care statele membre ar fi putut să le mențină sau să le fi introdus în temeiul articolului 9 alineatul (4) din RGPD.

58. CEPD și AEPD salută dispoziția de la articolul 3 alineatul (10) din Propunere, deoarece aceasta garantează că persoanele vizate au un control efectiv asupra datelor lor cu caracter personal, permițându-le să identifice accesul potențial ilegal la datele lor privind sănătatea. Cu toate acestea, CEPD și AEPD consideră că nu este clar dacă dreptul de a obține informații se realizează prin intermediul unei proceduri de notificare automată ori de câte ori există acces la date sau dacă este posibil numai la cerere. CEPD și AEPD consideră că prima opțiune este cea mai adecvată soluție pentru capacitarea persoanei vizate. Prin urmare, CEPD și AEPD recomandă ca acest aspect să fie luat în considerare de co-legiuitori și, prin urmare, să fie clarificat în consecință.

59. În ceea ce privește articolul 4 alineatul (1) din Propunere, astfel cum constată CEPD și AEPD, cadrele medicale: (a) au acces la datele electronice privind sănătatea ale persoanelor fizice pe care le tratează, indiferent de statul membru de afiliere și de statul membru de tratament și (b) se asigură că datele electronice cu caracter personal privind sănătatea ale persoanelor fizice tratate sunt actualizate cu informații referitoare la serviciile de sănătate furnizate. În acest sens, întrucât CEPD și AEPD remarcă faptul că este posibil ca accesul la datele electronice cu caracter personal privind sănătatea să fi fost deja abordat și reglementat la nivel național, recomandă co-legiuitorilor să clarifice relația dintre această dispoziție și legislația națională care reglementează deja această chestiune.

60. În primul rând, în ceea ce privește articolul 4 alineatul (1) din Propunere, CEPD și AEPD subliniază că articolul 9 alineatul (1) din RGPD nu permite, în principiu, prelucrarea datelor cu caracter personal privind sănătatea și nici a datelor genetice, cu excepția cazului în care se aplică una dintre derogările prevăzute la articolul 9 alineatul (2) din RGPD. Prin urmare, CEPD și AEPD recomandă ca articolul 4 alineatul (1) din Propunere să fie aliniat cu articolul 9 alineatul (2) litera (h) din RGPD.

61. În al doilea rând, CEPD și AEPD consideră că această dispoziție nu este în conformitate cu principiile RGPD privind reducerea la minimum a datelor și limitarea scopului, întrucât accesul nu se acordă numai când este necesar și pe baza principiului necesității de a cunoaște. Prin urmare, și pentru a oferi garanții adecvate persoanelor vizate, CEPD și AEPD recomandă să se specifice că acest acces trebuie să aibă loc numai pe baza principiului necesității de a cunoaște.

62. În al treilea rând, CEPD și AEPD subliniază că noțiunea de „cadru medical” cuprinde o mare varietate de profesii cu caracter distinct și care necesită diferite tipuri de implicare, de luare a deciziilor și de responsabilități (de exemplu, medici, asistenți medicali, tehnicieni de laborator și imagistică, nutriționiști, fizioterapeuți, psihologi, farmaciști). Prin urmare, CEPD și AEPD recomandă să nu se pună toate datele privind sănătatea la dispoziția tuturor cadrelor medicale, fără discriminare, ci numai la dispoziția celor pentru care accesul este considerat necesar pentru a îndeplini o sarcină specifică. Prin urmare, CEPD și AEPD subliniază importanța principiilor necesității și proporționalității în acest context. CEPD și AEPD iau act de faptul că, în conformitate cu articolul 4 alineatul (2) din Propunere, statele membre, potrivit principiului reducerii la minimum a datelor, stabilesc norme care prevăd

categoriile de date electronice cu caracter personal privind sănătatea solicitate de diferite profesii din domeniul sănătății. CEPD și AEPD iau act de faptul că Propunerea atribuie în mod explicit această responsabilitate statelor membre, conferindu-i caracter obligatoriu. În acest scop, CEPD și AEPD recomandă înlocuirea expresiei „pot stabili" cu „stabilesc", astfel încât să se asigure că astfel de norme vor fi stabilite de statele membre.

63. CEPD și AEPD iau act de faptul că articolul 4 alineatul (3) din Propunere prevede că se permite accesul cadrelor medicale cel puțin la categoriile prioritare de date electronice menționate la articolul 5 din Propunere, fără a stabili dacă toate categoriile prioritare sunt accesate de către toate cadrele medicale. Astfel cum s-a indicat mai sus, CEPD și AEPD consideră că accesul ar trebui acordat numai ținând seama de ceea ce este necesar în scopul tratamentului medical. CEPD și AEPD consideră că relația dintre articolul 4 alineatul (2) și articolul 4 alineatul (3) din Propunere ar trebui clarificată mai detaliat în Propunere.

64. Articolul 4 alineatul (4) din Propunere prevede posibilitatea de a se face derogare de la restricțiile privind accesul selectate de persoana vizată, prevăzute la articolul 3 alineatul (9) din Propunere, în cazul în care accesul este necesar pentru a proteja interesul vital al persoanei vizate sau al unei alte persoane fizice. În acest sens, CEPD și AEPD recomandă co-legiuitorilor să precizeze că dreptul persoanelor fizice de a obține informații privind accesul cadrelor medicale la datele lor electronice privind sănătatea, prevăzut la articolul 3 alineatul (10), include accesul la informațiile restricționate prevăzute la articolul 3 alineatul (9) din Propunere.

65. Articolul 7 din Propunere prevede obligația statelor membre de a asigura înregistrarea „în mod sistematic" de către cadrele medicale a datelor relevante privind sănătatea în legătură cu serviciile de sănătate pe care le furnizează persoanelor fizice, în format electronic, într-un sistem DES. CEPD și AEPD sunt preocupate de trimiterea la o astfel de înregistrare sistematică, deoarece aceasta pare să nu fie în conformitate cu principiul RGPD privind reducerea la minimum a datelor. Prin urmare, CEPD și AEPD sugerează modificarea textului Propunerii prin eliminarea expresiei „în mod sistematic" pentru a alinia dispoziția la principiul reducerii la minimum a datelor.

66. CEPD și AEPD salută dispozițiile privind gestionarea identității electronice prevăzute la articolul 9 din Propunere, întrucât consideră că identificarea și autentificarea securizată a persoanelor fizice și a cadrelor medicale care utilizează servicii electronice de asistență medicală sau care accesează date cu caracter personal privind sănătatea este unul dintre elementele esențiale pentru protejarea drepturilor persoanelor vizate în cauză. În acest sens, CEPD și AEPD subliniază că ar putea fi necesar să se aibă în vedere mecanisme diferite de identificare și autentificare pentru cadrele medicale, în funcție de calitatea în care aceștia accesează datele, și anume ca profesioniști sau în nume personal.

67. În ceea ce privește instituirea Autorității privind sănătatea digitală, prevăzută la articolul 10 din Propunere, CEPD și AEPD sunt preocupate de faptul că unele dintre sarcinile lor se pot suprapune cu cele ale autorităților de supraveghere a protecției datelor în temeiul RGPD, în special în ceea ce privește drepturile persoanei vizate și securitatea prelucrării datelor. Din motive de securitate juridică și pentru a îmbunătăți claritatea textului juridic, CEPD și AEPD sugerează mutarea dispoziției de la articolul 3 alineatul (11) ultima teză din Propunere la articolul 10 din Propunere.

68. În ceea ce privește articolul 11 din Propunere, care stabilește dreptul persoanelor fizice și juridice de a depune o plângere la autoritatea privind sănătatea digitală, CEPD și AEPD consideră că simpla furnizare de informații cu privire la existența unei plângeri către autoritățile de protecție a datelor nu este suficientă pentru a le permite să investigheze și să evalueze orice aspecte ale plângerii legate de protecția datelor. Prin urmare, CEPD și AEPD recomandă să se clarifice faptul că, în cazul în care

plângerea are oarecum o legătură cu protecția datelor, chiar dacă subiectul este legat de noile drepturi ale persoanelor fizice introduse prin articolul 3 din Propunere, autoritatea privind sănătatea digitală transmite o copie a plângerii autorității relevante de supraveghere a protecției datelor.

69. La un nivel mai general, CEPD și AEPD sugerează introducerea unei consultări obligatorii și a unei obligații de cooperare cu autoritățile pentru protecția datelor în ceea ce privește evaluarea plângerilor, precum și punerea în aplicare a Propunerii ori de câte ori sunt implicate aspecte legate de protecția datelor. În plus, CEPD și AEPD subliniază că autoritățile de protecție a datelor sunt singurele autorități competente responsabile cu aspectele legate de protecția datelor și, prin urmare, ar trebui să rămână singurul punct de contact pentru persoana vizată în ceea ce privește aceste aspecte, inclusiv pentru a evita orice confuzie pentru persoanele vizate cu privire la modalitățile în care acestea își pot exercita drepturile în materie de protecție a datelor.

70. Articolul 13 din Propunere prevede posibilitatea ca serviciile de sănătate digitală transfrontaliere suplimentare să fie furnizate prin intermediul MyHealth@EU și ca aceasta din urmă să faciliteze schimbul de date cu alte infrastructuri sau cu alte servicii din domeniul sănătății, al asistenței medicale sau al securității sociale. Aceeași dispoziție prevede obligația statelor membre și a Comisiei de a depune eforturi pentru a asigura interoperabilitatea MyHealth@EU cu sistemele tehnologice instituite la nivel internațional pentru schimbul de date electronice privind sănătatea.

71. CEPD și AEPD remarcă faptul că astfel de posibilități sunt prezentate în termeni generali și este destul de neclar în ce circumstanțe și în ce condiții pot fi partajate cu participanții din țări terțe datele electronice privind sănătatea. Având în vedere garanțiile prevăzute în capitolul V din RGPD pentru transferurile internaționale de date, CEPD și AEPD recomandă co-legiuitorilor să clarifice faptul că verificarea conformității care urmează să fie efectuată de Comisie cu privire la punctul național de contact al țării terțe sau la sistemul instituit la nivel internațional acoperă, de asemenea, îndeplinirea cerințelor prevăzute în capitolul V din RGPD, înainte de a stabili, printr-un act de punere în aplicare, că un astfel de punct sau sistem național de contact respectă cerințele MyHealth@EU în scopul schimbului electronic de date privind sănătatea.

# 6 SISTEMELE DES ȘI APLICAȚIILE DE WELLNESS (CAPITOLUL III)

72. Capitolul III din Propunere se axează pe punerea în aplicare a unui sistem obligatoriu de autocertificare pentru sistemele DES, în cazul în care aceste sisteme trebuie să respecte cerințele esențiale legate de interoperabilitate și securitate prevăzute în anexa II la Propunere. După cum s-a subliniat în expunerea de motive, „[a]ceastă abordare este necesară pentru a se asigura că dosarele electronice de sănătate sunt compatibile între diferitele sisteme și permit transmiterea cu ușurință a datelor electronice privind sănătatea între ele”. CEPD și AEPD salută faptul că, în conformitate cu articolele 15 și 17 din Propunere, sistemele DES trebuie să facă obiectul unei proceduri prealabile de evaluare a conformității înainte ca acestea să poată fi introduse pe piață sau puse în funcțiune în alt mod în UE.

73. Cu toate acestea, CEPD și AEPD iau act de faptul că unele dintre cerințele esențiale prevăzute în anexa II la Propunere se referă la aspecte legate de protecția datelor cu caracter personal, cum ar fi cele care abordează punerea în aplicare a drepturilor persoanelor fizice, astfel cum sunt prevăzute în

capitolul II din Propunere, sau prelucrarea securizată a datelor electronice privind sănătatea[22]. În plus, specificațiile comune care urmează să fie adoptate de Comisie, prin intermediul unor acte de punere în aplicare, în ceea ce privește cerințele esențiale prevăzute în anexa II, în temeiul articolului 23 alineatul (3) din Propunere, pot acoperi elemente referitoare la protecția datelor, cum ar fi cerințele legate de calitatea datelor, inclusiv caracterul complet și acuratețea datelor electronice privind sănătatea, precum și cerințele și principiile legate de securitate, confidențialitate, integritate, siguranța pacienților și protecția datelor electronice privind sănătatea[23].

74. În primul rând, CEPD și AEPD subliniază că existența conformității sistemelor DES cu cerințele esențiale legate de interoperabilitate și securitate prevăzute în anexa II la Propunere nu înseamnă neapărat că operațiunile de prelucrare care stau la baza funcționării lor sunt legale în sine, deoarece ar putea să existe cerințe suplimentare care decurg din legislația UE privind protecția datelor care trebuie să fie respectate de către operator. Cu toate acestea, deși CEPD și AEPD înțeleg că cerințele esențiale și specificațiile comune menționate anterior nu sunt direct legate de legislația UE privind protecția datelor, unele dintre acestea pot avea un impact semnificativ asupra aspectelor relevante pentru protecția datelor cu caracter personal ale persoanelor vizate în cauză. În acest sens, CEPD și AEPD iau act de faptul că cerințele menționate anterior nu par să țină seama în mod corespunzător de principiile reducerii la minimum a datelor și protecției datelor începând cu momentul conceperii ca aspecte esențiale care trebuie luate în considerare la proiectarea unui sistem DES pentru a proteja în mod adecvat interesele și drepturile persoanelor vizate în ceea ce privește protecția datelor și a vieții private. În plus, cerințele referitoare la perioadele de păstrare și la drepturile de acces de la punctul 3.8 din anexa II la Propunere nu iau în considerare scopul specific al operațiunilor de prelucrare a datelor, ca element-cheie de luat în considerare pentru proiectarea caracteristicilor de stocare ale unui sistem DES, alături de „originile și categoriile de date electronice privind sănătatea”.

75. Având în vedere riscurile pe care le prezintă dispozițiile privind disponibilitatea obligatorie, partajarea transfrontalieră, accesul și alte utilizări ale datelor electronice privind sănătatea conținute în sistemele DES și impactul asupra persoanelor în cauză, CEPD și AEPD sunt de părere că, pentru a consolida protecția persoanelor și încrederea acestora în aceste sisteme, ar fi cel mai adecvat să se introducă o procedură de evaluare a conformității de către o parte terță pentru sistemele DES[24], prin implicarea unor organisme notificate în evaluarea măsurilor, inclusiv a soluțiilor tehnice, luate de producător pentru a respecta cerințele de interoperabilitate și de securitate prevăzute în anexa II la Propunere. În acest sens, CEPD și AEPD remarcă pozitiv faptul că această chestiune va face obiectul unei evaluări specifice în contextul evaluării și revizuirii propunerii efectuate de Comisie după 5 ani de la intrarea sa în vigoare.

---

[22] A se vedea, de exemplu, punctul 1.3 și cerințele de securitate enumerate la punctul 3 din anexa II, cum ar fi punctul 3.1 privind prevenirea accesului neautorizat; punctul 3.2. privind mecanismele de identificare și autentificare; punctul 3.3. privind mecanismele de control al accesului; punctul 3.4. privind mecanismele de înregistrare pentru accesarea datelor și punctul 3.5. privind mecanismele de restricționare a accesului cadrelor medicale.

[23] A se vedea articolul 23 alineatul (3) literele (c) și (e) din Propunere, precum și articolul 10 alineatul (2) litera (h) din Propunere.

[24] A se vedea, de exemplu, procedura de evaluare a conformității ca parte terță prevăzută în Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului.

76. În plus, CEPD și AEPD recomandă modificarea Propunerii pentru a clarifica relația dintre sistemul obligatoriu de autocertificare pentru sistemele DES și cerințele privind protecția datelor. În plus, trebuie subliniat faptul că, ori de câte ori specificațiile comune menționate la articolul 23 din Propunere au un impact asupra cerințelor de protecție a datelor ale sistemelor DES, actele de punere în aplicare care urmează să fie adoptate de Comisie în temeiul articolului 23 din Propunere ar trebui să facă obiectul unei consultări atât a AEPD, cât și a CEPD, în conformitate cu articolul 42 alineatul (2) din RPDUE. Aceleași considerații se aplică etichetării voluntare a aplicației de wellness, care se bazează, de asemenea, pe cerințele esențiale prevăzute în anexa II la Propunere și pe specificațiile comune menționate la articolul 23 din Propunere.

77. În ceea ce privește gestionarea riscurilor prezentate de sistemele DES și a incidentelor grave, precum și punerea în aplicare a acțiunilor corective, în temeiul articolului 29 din Propunere, CEPD și AEPD recomandă stabilirea unei obligații de informare și cooperare cu autoritățile pentru protecția datelor, după caz. Într-adevăr, nu este clar dacă referirea la riscul pentru „alte aspecte legate de protecția interesului public" printre riscurile care pot fi prezentate de un sistem DES, implicând astfel intervenția autorității de supraveghere a pieței, poate include protecția datelor cu caracter personal. În plus, nu se poate exclude situația în care un incident grav care implică un sistem DES[25] să fie generat de disfuncționalități sau deteriorări ale caracteristicilor sau ale performanței unui sistem DES, care afectează, de asemenea, protecția datelor cu caracter personal.

78. CEPD și AEPD salută, în principiu, articolul 31 din Propunere privind etichetarea voluntară a aplicațiilor de wellness, deoarece acest lucru poate asigura transparența pentru utilizatorii aplicațiilor de wellness în ceea ce privește principalele lor caracteristici, sprijinind astfel utilizatorii în alegerea aplicațiilor de wellness fiabile. Cu toate acestea, articolele 31 și 32 din Propunere se referă numai la interoperabilitatea aplicațiilor de wellness cu sistemele DES și instituie un mecanism de conformitate voluntară limitat la cerințele de interoperabilitate și securitate prevăzute în anexa II la Propunere, în vederea asigurării posibilității ca aplicațiile de wellness să transmită date electronice privind sănătatea către sistemele DES.

79. În acest sens, CEPD și AEPD subliniază că eticheta care însoțește aplicațiile de wellness în temeiul articolului 31 din Propunere nu înseamnă neapărat că operațiunile de prelucrare care stau la baza funcționării aplicației respective sunt legale în sine și pot fi utilizate ca atare de către utilizator. Operatorul va trebui să respecte și alte cerințe care decurg din legislația UE privind protecția datelor. CEPD și AEPD recomandă clarificarea acestui aspect în Propunere, chiar și într-un considerent. Considerentul 35 din Propunere prevede că „[u]tilizatorii de aplicații de wellness, cum ar fi aplicațiile mobile, ar trebui să fie informați cu privire la capacitatea unor astfel de aplicații de a fi conectate și de a furniza date sistemelor DES sau soluțiilor electronice naționale de sănătate, în cazurile în care datele produse de aplicațiile de wellness sunt utile în scopuri de asistență medicală". Cu toate acestea, condițiile în care astfel de aplicații de wellness pot fi conectate în mod legal și pot furniza date cu caracter personal sistemelor DES (sau soluțiilor naționale electronice de sănătate) în temeiul legislației privind protecția datelor nu sunt specificate în Propunere. Ceea ce pare clar din lista categoriilor minime de date electronice pentru utilizare secundară, prevăzută la articolul 33 din Propunere, este că, în mod indirect – odată încărcate într-un sistem DES[26] – sau direct – în măsura în care acestea sunt colectate și/sau prelucrate de entități care se încadrează în definiția noțiunii de „deținător de date" în

[25] A se vedea definiția prevăzută la articolul 2 alineatul (2) litera (q) din Propunere.
[26] A se vedea articolul 3 alineatul (6) și articolul 33 alineatul (1) litera (a) din Propunere.

temeiul articolului 2 alineatul (2) litera (y) din Propunere[27] –, datele cu caracter personal produse de aplicațiile de wellness se încadrează în aceste categorii și, ulterior, fac obiectul obligației deținătorilor de date de a le pune la dispoziție pentru utilizare secundară, în conformitate cu dispozițiile capitolului IV din Propunere.

80. Disponibilitatea obligatorie a datelor electronice privind sănătatea generate de dispozitivele medicale, de aplicațiile de wellness sau de alte aplicații digitale din domeniul sănătății pentru utilizare secundară trebuie să fie evaluată în raport cu evoluțiile tehnologice rapide din domeniul tehnologiei mobile și purtabile și cu popularitatea tot mai mare a așa-numitelor aplicații și dispozitive „quantified self" (monitorizare personală), care permit persoanelor să înregistreze toate tipurile de aspecte legate de personalitatea, mentalitatea, corpul lor, tiparele lor comportamentale și locul în care se află. În mod evident, acest tip de prelucrare a datelor merită o atenție deosebită, deoarece nu este ușor de recunoscut drept prelucrare a datelor privind sănătatea de către persoanele vizate. Totuși, în același timp, acest lucru implică riscuri reale la adresa vieții private, în special în cazul în care astfel de date sunt prelucrate în scopuri suplimentare și/sau în combinație cu alte date sau sunt transferate către terți. Aceste tipuri de prelucrare a datelor pot crea riscuri specifice, inclusiv riscul de tratament inechitabil sau nedrept pe baza datelor privind starea de sănătate presupusă sau reală a unei persoane obținute, de exemplu, prin crearea de profiluri, din detalii foarte intime privind viața sa privată, indiferent dacă aceste concluzii privind starea sa de sănătate sunt sau nu exacte. De fapt, aceste riscuri pot fi legate și de fiabilitatea și exactitatea datelor generate de dispozitivele medicale, de aplicațiile de wellness sau de alte aplicații digitale în domeniul sănătății. În acest context, CEPD și AEPD recunosc că articolul 33 alineatul (3) încearcă să delimiteze datele generate de dispozitivele medicale, aplicațiile de wellness sau alte aplicații digitale în domeniul sănătății care trebuie puse la dispoziție pentru utilizări secundare. Cu toate acestea, CEPD și AEPD subliniază că este încă neclar fie ce tip de date se încadrează în această categorie, fie cine ar evalua valabilitatea și calitatea acestora odată introduse de persoane fizice în propriul lor DES în temeiul articolului 3 alineatul (6) și al articolului 33 alineatul (1) litera (a) din Propunere sau puse la dispoziție direct de către deținătorii de date în temeiul articolului 33 alineatul (1) literele (f) și (n) din Propunere.

81. În acest sens, CEPD și AEPD recomandă excluderea din domeniul de aplicare al capitolului IV din Propunere a aplicațiilor de wellness și a altor aplicații digitale. În cazul în care aceste date sunt menținute în domeniul de aplicare al capitolului IV, CEPD și AEPD subliniază că utilizatorii trebuie să dispună în continuare de libertatea de a decide dacă și care dintre datele lor cu caracter personal generate de aplicația de wellness și de alte aplicații digitale – în pofida faptului că au fost încărcate în propriile lor DES – vor fi partajate cu alți destinatari și prelucrate ulterior pentru utilizări secundare. Prin urmare, CEPD și AEPD recomandă modificarea propunerii pentru a se asigura că persoanele vizate sunt informate în mod corespunzător cu privire la opțiunile lor posibile în ceea ce privește potențialele utilizări ulterioare ale datelor lor electronice privind sănătatea, inclusiv ale celor generate de aplicațiile de wellness și de alte aplicații digitale. În al doilea rând, condițiile specifice pentru prelucrarea ulterioară a acestor date cu caracter personal trebuie să fie stabilite în mod clar în conformitate cu legislația privind protecția datelor și trebuie instituite mecanisme adecvate pentru a asigura respectarea voinței persoanelor vizate cu privire la prelucrarea ulterioară a datelor lor cu caracter personal privind sănătatea generate de aplicațiile de wellness și de alte aplicații digitale.

[27] A se vedea articolul 33 alineatul (1) literele (f) și (n) din Propunere.

# 7 UTILIZAREA SECUNDARĂ A DATELOR ELECTRONICE PRIVIND SĂNĂTATEA (CAPITOLUL IV)

82. După cum recunosc CEPD și AEPD, capitolul IV din Propunere urmărește să faciliteze utilizarea secundară a datelor electronice privind sănătatea și salută faptul că o astfel de utilizare secundară a datelor electronice privind sănătatea poate genera beneficii considerabile pentru binele public. Cu toate acestea, CEPD și AEPD consideră că astfel de activități de prelucrare ulterioară nu sunt lipsite de riscuri pentru drepturile și libertățile persoanelor vizate.

83. CEPD și AEPD iau act de faptul că, în conformitate cu considerentul 37 din Propunere, „[...] [Regulamentul] oferă temeiul juridic în conformitate cu articolul 9 alineatul (2) literele (g), (h) [...] și (j) din Regulamentul (UE) 2016/679 pentru utilizarea secundară a datelor privind sănătatea, stabilind garanțiile pentru prelucrare, în scopuri legale, guvernanța de încredere pentru furnizarea accesului la datele privind sănătatea (prin intermediul organismelor de acces la datele privind sănătatea) și pentru prelucrarea într-un mediu securizat, precum și modalitățile de prelucrare a datelor prevăzute în autorizația privind datele". În acest context, același considerent prevede că solicitantul de date trebuie să facă dovada unui temei juridic în conformitate cu articolul 6 din RGPD, în baza căruia ar putea fi făcută o cerere de acces la date în lumina Propunerii, fără ca acest aspect să fie neapărat reflectat în partea dispozitivă a Propunerii. Pe de altă parte, CEPD și AEPD iau act de faptul că articolul 34 alineatul (1) din Propunere prevede o listă a scopurilor în care datele electronice privind sănătatea pot fi prelucrate pentru utilizare secundară, care includ, dar nu se limitează la scopul cercetării științifice legate de sectorul sănătății sau al îngrijirii.

84. În acest sens, CEPD și AEPD au prezentat trei preocupări principale.

85. **În primul rând**, CEPD și AEPD constată lipsa unei delimitări adecvate a scopurilor enumerate la articolul 34 alineatul (1) din Propunere în care datele electronice privind sănătatea pot fi prelucrate ulterior și, în special, își exprimă îngrijorarea cu privire la articolul 34 alineatul (1) literele (f) și (g) din Propunere, care ar putea include orice formă de „activități de dezvoltare și inovare pentru produse sau servicii care contribuie la sănătatea publică sau la securitatea socială" sau „formarea, testarea și evaluarea algoritmilor, inclusiv a dispozitivelor medicale, a sistemelor de IA și a aplicațiilor de sănătate digitală, care contribuie la sănătatea publică sau la securitatea socială". CEPD și AEPD recomandă ferm ca Propunerea să delimiteze în continuare aceste scopuri și să circumscrie cazurile în care există o legătură suficientă cu sănătatea publică și/sau securitatea socială, pentru a obține un echilibru care să țină seama în mod adecvat de obiectivele urmărite de propunere și de protecția datelor cu caracter personal ale persoanelor vizate afectate de prelucrare.

86. **În al doilea rând**, având în vedere observațiile de mai sus și în pofida formulării de la considerentul 37 din Propunere, CEPD și AEPD consideră că Propunerea necesită îmbunătățiri suplimentare pentru a asigura conformitatea cu articolul 9 din RGPD.

87. Într-adevăr, scopurile în care datele electronice privind sănătatea pot fi prelucrate pentru utilizare secundară în temeiul articolului 34 alineatul (1) din Propunere includ mai multe tipuri de utilizare secundară, care s-ar încadra în diferite categorii de motive de excepție prevăzute la articolul 9 alineatul (2) din RGPD. Cu toate acestea, CEPD și AEPD consideră că acest lucru nu se reflectă în criteriile pe baza cărora organismele de acces la datele privind sănătatea ar trebui să evalueze și să decidă cu privire la cererile de acces la date (articolul 45 din Propunere) pentru a emite o autorizație de acces la date (articolul 46 din Propunere). În acest scop, CEPD și AEPD subliniază că criteriile

prevăzute în acest sens la articolul 46 din Propunere se limitează la dispozițiile și principiile prezentei Propuneri și sunt lipsite de claritate în ceea ce privește modul în care aceste dispoziții se referă la principiile și dispozițiile RGPD, în special la articolul 9 alineatul (2) din RGPD.

88. În plus față de cele menționate mai sus, CEPD și AEPD solicită clarificări specifice cu privire la modul și situațiile în care articolul 9 alineatul (2) litera (j) din RGPD ar fi aplicabil în cazul prelucrării datelor privind sănătatea „în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice" (pe baza dreptului Uniunii sau a legislației statelor membre) și al „garanțiilor adecvate", astfel cum se prevede la articolul 89 alineatul (1) din RGPD.

89. **În al treilea rând**, CEPD și AEPD analizează modul în care această excepție, interpretată în lumina dreptului Uniunii, de la articolul 9 alineatul (2) din RGPD, poate fi reconciliată cu articolul 9 alineatul (4) din RGPD și cu posibilitatea ca legislația statelor membre să introducă condiții suplimentare, inclusiv limitări în ceea ce privește prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea. În acest sens, CEPD și AEPD consideră că Propunerea ar putea clarifica modul în care excepția de la articolul 9 alineatul (1) din RGPD, care decurge din Propunere, dar care nu este încă specificată în mod explicit în niciuna dintre dispozițiile acesteia, s-ar putea armoniza cu legislația națională diferită a statelor membre.

90. Drept urmare**, CEPD și AEPD solicită ca Propunerea să asigure compatibilitatea deplină cu articolul 9 alineatul (2) din RGPD și, în special, în ceea ce privește aplicarea sa în scopurile enumerate la articolul 34 alineatul (1) literele (f) și (g) din Propunere**. În plus, CEPD și AEPD recomandă, de asemenea, modificarea în consecință a articolului 46 din Propunere, pentru a integra și a reflecta în mod corespunzător diferențele în ceea ce privește obiectivele și cerințele pentru utilizarea secundară a datelor electronice privind sănătatea.

91. În ceea ce privește **categoriile minime de date electronice privind sănătatea pentru utilizare secundară**, CEPD și AEPD iau act de faptul că, în temeiul articolului 33 alineatul (1) din Propunere, apare o obligație legală, potrivit căreia deținătorii de date, servindu-se de dreptul Uniunii, trebuie să pună la dispoziție categorii specifice de date electronice privind sănătatea pentru utilizare secundară. CEPD și AEPD constată că articolul 41 alineatul (1) din Propunere indică faptul că această (nouă) obligație juridică completează orice altă obligație juridică (deja) prevăzută în alte acte legislative ale Uniunii sau în legislația națională de punere în aplicare a dreptului Uniunii. Astfel cum se indică în considerentul 37 din Propunere, CEPD și AEPD remarcă faptul că articolul 33 alineatul (1) din Propunere ar servi drept bază juridică în temeiul articolului 6 alineatul (1) litera (c) din RGPD și ar prevedea, de asemenea, o excepție de la interdicția prevăzută la articolul 9 alineatul (1) din RGPD pentru deținătorul de date de a prelucra (și, prin urmare, de a pune la dispoziție și de a furniza) date electronice cu caracter personal privind sănătatea. În această privință, deși CEPD și AEPD recunosc că o astfel de obligație juridică pentru deținătorii de date se încadrează – în principiu – în sistemul RGPD, ea poate genera insecuritate juridică.

92. În acest sens, articolul 33 alineatul (5) din Propunere prevede că „[î]n cazul în care dreptul intern impune consimțământul persoanei fizice, organismele de acces la datele privind sănătatea se bazează pe obligațiile prevăzute în prezentul capitol pentru a oferi acces la datele electronice privind sănătatea". CEPD și AEPD consideră, în primul rând, că tipul de „cerințe privind consimțământul" din dreptul intern la care se referă dispoziția este neclar. Mai precis, **CEPD și AEPD subliniază lipsa de claritate cu privire la etapa din procedura prevăzută în propunere în ceea ce privește utilizarea secundară a datelor electronice privind sănătatea în care organismele de acces la datele privind sănătatea pot să nu țină seama de astfel de cerințe prevăzute în dreptul intern**, în special atunci când

intră sub incidența articolului 9 alineatul (4) din RGPD. În plus, CEPD și AEPD recomandă clarificări și precizări suplimentare în legătură cu articolul 46 alineatul (6) litera (f) din Propunere, care prevede posibilitatea ca organismul de acces la datele privind sănătatea să introducă „condiții specifice din autorizația privind datele acordată".

93. Articolul 36 din Propunere prevede **instituirea unor organisme de acces la datele privind sănătatea**. În acest sens, CEPD și AEPD subliniază că responsabilitatea organismului de acces la datele privind sănătatea de a evalua temeiul juridic propus de utilizatorul de date va necesita disponibilitatea unei expertize juridice adecvate în cadrul organismului de acces la datele privind sănătatea. CEPD și AEPD iau act de faptul că, până în prezent, acest lucru nu este menționat în mod explicit la articolul 36 din Propunere. Cu toate acestea, CEPD și AEPD subliniază că evaluarea temeiului juridic de către organismul de acces la datele privind sănătatea poate fi – întotdeauna – verificată și – atunci când este necesar – invalidată de APD relevantă. În acest scop, CEPD și AEPD solicită o claritate specifică în ceea ce privește interacțiunea dintre rolul organismului de acces la datele privind sănătatea și cel al APD respective în contextul oricărei chestiuni legate de protecția datelor.

94. Necesitatea de a clarifica relația dintre Propunere și legislația statelor membre este exemplificată suplimentar în contextul **cererilor de autorizații privind datele în contextul accesului transfrontalier la date electronice cu caracter personal privind sănătatea pentru utilizare secundară** (secțiunea 4, articolele 52-54 din Propunere). CEPD și AEPD iau act de faptul că, deși Propunerea urmărește să faciliteze utilizarea secundară transfrontalieră, prin instituirea unor „puncte naționale de contact" și a unei infrastructuri transfrontaliere (HealthData@EU), utilizatorii de date vor trebui, eventual, să se adreseze organismelor respective de acces la datele privind sănătatea din fiecare stat membru. Într-adevăr, CEPD și AEPD înțeleg că articolul 45 alineatul (3) din Propunere prevede doar o coordonare limitată între organismele de acces la datele medicale implicate, în vederea obținerii unei autorizații privind datele. Cu toate acestea, CEPD și AEPD consideră că Propunerea nu oferă clarificări adecvate cu privire la legislația națională specifică ce va fi aplicată în contextul autorizațiilor privind datele transfrontaliere (cea a organismului de acces la datele privind sănătatea respectiv sau cea a solicitantului de date), inclusiv cu privire la temeiul juridic care va trebui să fie identificat (de către solicitantul datelor) și evaluat (de către organismul de acces la datele privind sănătatea). În sfârșit, în această privință, ar trebui remarcat de asemenea că, atât de partea organismului de acces la datele privind sănătatea, cât și de partea utilizatorului de date, pot exista lacune (semnificative) în materie de expertiză pentru a depăși problemele legate de identificarea și aprecierea diferențelor în ceea ce privește (cerințele care trebuie îndeplinite, astfel cum sunt prevăzute în) legislația statului membru referitoare la un astfel de temei juridic.

95. CEPD și AEPD iau act de faptul că articolul 38 alineatul (2) din Propunere prevede că organismele care au acces la datele privind sănătatea nu sunt obligate să furnizeze informațiile specifice în temeiul articolului 14 din RGPD fiecărei persoane fizice cu privire la utilizarea datelor sale pentru proiecte care fac obiectul unei autorizații privind datele. În acest sens, CEPD și AEPD consideră că derogarea introdusă poate avea consecințe nedorite asupra drepturilor și libertăților fundamentale ale persoanelor vizate, din cauza lipsei unor condiții concrete în care s-ar aplica o astfel de derogare.

96. În plus, CEPD și AEPD reamintesc importanța obligațiilor de transparență față de persoanele vizate și îndeamnă co-legiuitorul să identifice situațiile specifice pentru a se asigura că o astfel de dispoziție nu poate fi invocată în mod sistematic de către organismele de acces la datele medicale. Prin urmare, CEPD și AEPD recomandă modificarea în consecință a dispoziției, ținând seama de faptul că cerințele prevăzute la articolul 14 din RGPD nu pot fi respinse în mod sistematic fără o evaluare și o justificare

adecvate și relevante cu privire la necesitatea de a se baza pe o astfel de derogare[28]. În cazul în care se menține restricționarea dreptului la informare, CEPD și AEPD semnalează co-legiuitorilor necesitatea de a lua în considerare condițiile prevăzute la articolul 23 din RGPD.

97. Articolul 40 din Propunere definește altruismul în materie de date și prevede promovarea acestuia în contextul sănătății. În acest sens, CEPD și AEPD consideră că dispoziția este neclară, în special în ceea ce privește interacțiunea cu dispoziția respectivă introdusă de DGA. În acest scop, CEPD și AEPD recomandă clarificarea dispoziției în consecință.

98. CEPD și AEPD remarcă pozitiv dispoziția de la articolul 44 alineatul (3) din Propunere, care prevede că, în cazul în care organismele care au acces la datele privind sănătatea trebuie să ofere acces la date în format pseudonimizat, utilizatorii de date nu trebuie să reidentifice datele electronice privind sănătatea furnizate în acest format (informațiile pentru inversarea pseudonimizării sunt disponibile numai pentru organismele de acces la datele privind sănătatea). În plus, CEPD și AEPD salută faptul că aceeași dispoziție din Propunere prevede că nerespectarea de către utilizatorul de date a măsurilor organismului de acces la datele privind sănătatea care asigură pseudonimizarea face obiectul unor garanții adecvate pentru cel dintâi.

99. În cele din urmă, articolul 48 din Propunere prevede că, prin derogare de la articolul 46 din Propunere, nu este necesară o autorizație privind datele pentru ca organismele din sectorul public și instituțiile, organele, oficiile și agențiile Uniunii să acceseze datele electronice privind sănătatea în temeiul aceluiași articol. CEPD și AEPD consideră că ar trebui să se solicite, de asemenea, o autorizație pentru a permite verificarea respectării tuturor cerințelor relevante, inclusiv a celor privind legalitatea și necesitatea. În plus, CEPD și AEPD consideră că o astfel de cerință este importantă pentru promovarea transparenței, întrucât Propunerea prevede ca organismele de acces la datele privind sănătatea să furnizeze publicului larg informații cu privire la toate autorizațiile privind datele emise în temeiul articolului 46.

# 8 ACȚIUNI SUPLIMENTARE (CAPITOLUL V)

## 8.1 Stocarea datelor electronice cu caracter personal privind sănătatea în UE și conformitatea transferurilor internaționale de date cu capitolul V din RGPD

100. Capitolul V din Propunere urmărește să propună alte măsuri de promovare a consolidării capacităților de către statele membre pentru a însoți dezvoltarea spațiului european al datelor privind sănătatea. În plus, acest capitol reglementează accesul internațional și transferul de date electronice *fără caracter personal* (privind sănătatea), precum și accesul internațional și transferul de date electronice *cu caracter personal* privind sănătatea.

101. În ceea ce privește accesul internațional la date electronice *cu caracter personal* privind sănătatea și transferul internațional al acestora, articolul 63 din Propunere specifică faptul că statele membre „pot menține sau introduce condiții suplimentare, inclusiv limitări, în conformitate cu și în condițiile prevăzute la articolul 9 alineatul (4) din Regulamentul (UE) 2016/679”.

102. **În primul rând**, CEPD și AEPD ar dori să reamintească faptul că, în hotărârea sa în cauza Digital Rights Ireland, CJUE a considerat că absența unei cerințe de păstrare a datelor în UE înseamnă că „[...] nu se

[28] A se vedea, de asemenea, punctul 25 de mai sus.

poate considera că controlul exercitat de o autoritate independentă, impus în mod expres la articolul 8 alineatul (3) din Cartă, al respectării cerințelor de protecție și de securitate [...] este garantat în totalitate. Or, un astfel de control efectuat în temeiul dreptului Uniunii constituie un element esențial al respectării protecției persoanelor în ceea ce privește prelucrarea datelor cu caracter personal”[29]. Cu alte cuvinte, CJUE a statuat în mod explicit, în cazul de față, că nu poate fi asigurat pe deplin controlul respectării cerințelor de protecție și securitate de către o autoritate independentă de supraveghere în absența unei cerințe de păstrare a datelor în cauză pe teritoriul UE. Neimpunerea obligației de păstrare a datelor în Uniune s-a numărat printre considerațiile care au determinat CJUE să concluzioneze că legiuitorul Uniunii a depășit limitele impuse de respectarea principiului proporționalității în lumina articolului 7, a articolului 8 și a articolului 52 alineatul (1) din Cartă[30].

103. Necesitatea de a impune o cerință de stocare a datelor cu caracter personal în UE în anumite cazuri specifice a fost ulterior confirmată și completată în hotărârea Tele 2, în care CJUE a considerat că „[ț]inând seama de cantitatea datelor păstrate, de caracterul sensibil al respectivelor date, precum și de riscul de acces ilicit la acestea, furnizorii de servicii de comunicații electronice trebuie, în scopul de a asigura deplina integritate și confidențialitate a datelor menționate, să garanteze un nivel deosebit de ridicat de protecție și de securitate prin măsuri tehnice și organizatorice adecvate. În special, reglementarea națională trebuie să prevadă păstrarea pe teritoriul Uniunii, precum și distrugerea iremediabilă a datelor la finalul duratei de păstrare a acestora” (sublinierea noastră)[31]. Din nou, CJUE a evidențiat că, pentru a garanta nivelul necesar de securitate și protecție a datelor în cauză, legislația relevantă **trebuie** să impună păstrarea datelor în UE.

104. Potrivit CEPD și AEPD, constatările făcute de Curte în aceste două hotărâri de referință sunt, de asemenea, relevante în contextul Propunerii, întrucât aceasta se va aplica (i) prelucrării unui volum mare de date cu caracter personal, (ii) care au un caracter extrem de sensibil și (iii) pentru care nu există niciun element obiectiv pentru a concluziona că riscul de acces ilegal este inferior celui identificat în contextul hotărârilor menționate mai sus[32]. În special, CEPD și AEPD subliniază că probabilitatea de aplicare a constatării Curții datelor în cauză este cu atât mai mare, având în vedere că datele privind sănătatea ar putea să fie considerate chiar mai sensibile decât datele din telecomunicații (și anume datele în cauză din cele două hotărâri menționate mai sus).

---

[29] Hotărârea Curții (Marea Cameră) din 8 aprilie 2014, Digital Rights Ireland Ltd, cauzele conexate C-293/12 și C-594/12; punctul 68. A se vedea de asemenea Concluziile avocatului general Cruz Villalón prezentate la 12 decembrie 2013 în aceeași cauză, la punctele 78 și 79, în care se arată că lipsa dispoziției care prevede cerința de „a stoca [...] datele care trebuie păstrate pe teritoriul unui stat membru, care ține de competența unui stat membru”, „agravează [...] riscul unei exploatări care nu respectă cerințele care decurg din dreptul la respectarea vieții private” și „agravează considerabil riscul ca acestea să poată fi accesibile sau divulgate cu nerespectarea acestei reglementări”.

[30] Hotărârea Curții (Marea Cameră) din 8 aprilie 2014, Digital Rights Ireland Ltd, cauzele conexate C-293/12 și C-594/12; punctul 69.

[31] Hotărârea Curții (Marea Cameră) din 21 decembrie 2016, Tele2 Sverige AB/Post- och telestyrelsen și Secretary of State for the Home Department/Tom Watson și alții, cauzele conexate C-203/15 și C-698/15, punctul 122. A se vedea, de asemenea, Concluziile avocatului general Saugmandsgaard Øe prezentate la 19 iulie 2016, Tele2 Sverige AB/Post- och telestyrelsen și Secretary of State for the Home Department/Tom Watson și alții, cauzele conexate C-203/15 și C-698/15, punctele 239-241.

[32] CEPD și AEPD iau act de faptul că acest risc de acces ilegal este de așa natură încât a determinat efectiv Comisia să dedice o dispoziție specifică în acest sens în ceea ce privește datele fără caracter personal (articolul 62 din Propunere).

105. În acest context, CEPD și AEPD împărtășesc preocupările Curții cu privire la necesitatea de a atenua riscurile de acces ilegal și de supraveghere ineficace în ceea ce privește anumite tipuri de date și anumite tipuri de operațiuni de prelucrare. În special, CEPD și AEPD remarcă faptul că, în cazul în care infrastructura de prelucrare este situată în state care nu sunt membre ale UE/SEE, controlul autorității de supraveghere a protecției datelor din UE asupra conformității cu normele UE de protecție a datelor ar putea să nu fie întotdeauna pe deplin asigurat.

106. În plus, după cum constată CEPD și AEPD, Comisia a propus recent anumite cerințe de stocare a datelor într-un alt context: articolul 17 alineatul (1) litera (c) din recenta Propunere de Regulament al Parlamentului European și al Consiliului privind securitatea informațiilor în instituțiile, organele, oficiile și agențiile Uniunii prevede într-adevăr că „informațiile sensibile neclasificate [ar trebui] stocate și prelucrate în UE”[33]. La un nivel mai general, CEPD și AEPD remarcă faptul că dreptul Uniunii oferă deja mai multe exemple de acte legislative existente care impun stocarea datelor cu caracter personal în UE și care, de obicei, merg și mai departe prin restricționarea transferurilor[34]. Prin urmare, CEPD și AEPD concluzionează că dreptul Uniunii impune, în anumite situații specifice, ca datele să fie stocate în UE pentru a atenua riscul de acces ilegal și pentru a asigura o supraveghere eficace.

107. **În al doilea rând**, CEPD și AEPD iau act de faptul că articolul 62 din Propunere, referitor la accesul internațional și transferurile de date electronice fără caracter personal privind sănătatea, se referă în mai multe cazuri la date electronice fără caracter personal privind sănătatea „deținute în Uniune”, ceea ce ar părea să indice o ipoteză generală potrivit căreia această categorie de date ar trebui să fie stocate în Uniune. AEPD și CEPD consideră că aceeași abordare ar trebui adoptată și pentru datele cu caracter personal care intră în domeniul de aplicare al Propunerii, deoarece ar fi dificil să se justifice cerința de a stoca date electronice fără caracter personal privind sănătatea în UE și să nu existe aceeași cerință pentru datele electronice cu caracter personal privind sănătatea.

108. **În al treilea rând**, CEPD și AEPD doresc să clarifice în acest context că obligația de a stoca date cu caracter personal în UE nu împiedică transferurile de date electronice cu caracter personal privind sănătatea către țări terțe sau organizații internaționale. Într-adevăr, este posibil să se reconcilieze o cerință generală de stocare a datelor cu caracter personal în UE cu transferurile specifice permise în conformitate cu capitolul V din RGPD (de exemplu, în contextul cercetării științifice, al plății asistenței

---

[33] Propunere de regulament al Parlamentului European și al Consiliului privind securitatea informațiilor în instituțiile, organele, oficiile și agențiile Uniunii,
COM/2022/119 final; https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX:52022PC0119.

[34] A se vedea, de exemplu, articolul 6 alineatul (8) din Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, cercetarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave: „[s]tocarea, prelucrarea și analiza datelor din PNR de către UIP se realizează exclusiv într-un loc sigur sau în locuri sigure de pe teritoriul statelor membre”; Articolul 3 din Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS); Articolul 41 din Regulamentul (UE) 2017/2226 al Parlamentului European și al Consiliului din 30 noiembrie 2017 de instituire a Sistemului de intrare/ieșire (EES) pentru înregistrarea datelor de intrare și de ieșire și a datelor referitoare la refuzul intrării ale resortisanților țărilor terțe care trec frontierele externe ale statelor membre, de stabilire a condițiilor de acces la EES în scopul aplicării legii și de modificare a Convenției de punere în aplicare a Acordului Schengen și a Regulamentelor (CE) nr. 767/2008 și (UE) nr. 1077/2011; Articolul 39 din Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen din a doua generație (SIS II).

medicale, al cooperării internaționale). În consecință, CEPD și AEPD consideră că obligația de a stoca datele în UE ar fi proporțională și nu ar depăși ceea ce este necesar pentru atingerea obiectivului urmărit, și anume acela de a stabili o garanție suplimentară în vederea atenuării riscului de acces ilegal și de supraveghere ineficace a datelor în cauză, având în vedere caracterul extrem de sensibil al acestora.

109. **În al patrulea rând**, CEPD și AEPD iau act, de asemenea, de faptul că articolul 63 din Propunere prevede că statele membre pot menține sau introduce condiții suplimentare, inclusiv limitări, în conformitate cu și în condițiile prevăzute la articolul 9 alineatul (4) din RGPD. Astfel de limitări impuse la nivel național pot include obligația de a stoca date în UE. CEPD și AEPD atrag atenția asupra faptului că o astfel de obligație se aplică deja în mai multe state membre și consideră că este probabil ca mai multe state membre să impună sau să continue să impună obligații similare în cazul în care problema nu este armonizată la nivelul UE.

110. Având în vedere cele de mai sus, CEPD și AEPD consideră, prin urmare, că este esențial să se evite o abordare inconsecventă și fragmentată în întreaga UE, care ar conduce la grade diferite de protecție a persoanelor vizate, ceea ce ar fi în contradicție cu unul dintre obiectivele-cheie ale RGPD[35]. Prin urmare, CEPD și AEPD consideră că obligațiile suplimentare, inclusiv stocarea datelor medicale electronice cu caracter personal în UE, ar trebui să fie abordate, în măsura posibilului, la nivelul UE, și anume în Propunere, pentru a asigura un nivel ridicat uniform de protecție a persoanelor vizate în întreaga UE, precum și pentru a menține buna funcționare a pieței interne, în conformitate cu articolul 114 din TFUE pe care se bazează propunerea.

111. Din toate motivele de mai sus și ținând seama în mod corespunzător de caracterul extrem de sensibil al datelor cu caracter personal în cauză, **CEPD și AEPD consideră că articolul 63** din **Propunere ar trebui să impună operatorilor și persoanelor împuternicite de operatori stabiliți în UE care prelucrează date electronice cu caracter personal privind sănătatea în domeniul de aplicare al propunerii obligația de a stoca aceste date în UE.** Astfel cum s-a explicat mai sus, o astfel de cerință de stocare în UE a datelor electronice cu caracter personal privind sănătatea **nu ar trebui să aducă atingere posibilității de a transfera date electronice cu caracter personal privind sănătatea în conformitate cu capitolul V din RGPD**[36]. CEPD și AEPD recomandă, de asemenea, să se reamintească în preambul faptul că operatorii și persoanele împuternicite de operatori care prelucrează date electronice cu caracter personal privind sănătatea fac în continuare obiectul articolului 48 din RGPD privind transferurile sau divulgările neautorizate de dreptul Uniunii și ar trebui să respecte această dispoziție în cazul unei cereri de acces care provine dintr-o țară terță[37].

---

[35] A se vedea considerentul 53 din RGPD referitor la articolul 9 alineatul (4) din RGPD: „[t]otuși, acest lucru nu ar trebui să împiedice libera circulație a datelor cu caracter personal în cadrul Uniunii atunci când aceste condiții se aplică prelucrării transfrontaliere a unor astfel de date".

[36] Și cu condiția respectării celorlalte condiții din RGPD, în special a articolului 6 din RGPD privind obligația ca prelucrarea să fie legală.

[37] Articolul 48 din RGPD: „[o]rice hotărâre a unei instanțe sau a unui tribunal și orice decizie a unei autorități administrative a unei țări terțe care impun unui operator sau persoanei împuternicite de operator să transfere sau să divulge date cu caracter personal poate fi recunoscută sau executată în orice fel numai dacă se bazează pe un acord internațional, cum ar fi un tratat de asistență judiciară reciprocă în vigoare între țara terță solicitantă și Uniune sau un stat membru, fără a se aduce atingere altor motive de transfer în temeiul prezentului capitol."

## 8.2 Achizițiile publice și finanțarea din partea Uniunii

112. CEPD și AEPD iau act de faptul că articolul 60 din Propunere abordează chestiunea cerințelor suplimentare pentru achizițiile publice și finanțarea din partea Uniunii. CEPD și AEPD consideră că recomandările de mai sus (privind stocarea datelor în UE și conformitatea cu capitolul 5 și, în special, cu articolul 48 din RGPD) ar fi cel mai bine operaționalizate dacă ar fi integrate într-un stadiu incipient atunci când se achiziționează[38] sau se finanțează servicii furnizate de operatori și de persoanele împuternicite de operatori stabiliți în UE care prelucrează date electronice cu caracter personal privind sănătatea.

113. Prin urmare, **CEPD și AEPD recomandă ca articolul 60 din Propunere să se refere, de asemenea, ca o condiție pentru achiziționarea sau finanțarea serviciilor furnizate de operatorii și de persoanele împuternicite de operatori stabiliți în UE care prelucrează date electronice cu caracter personal privind sănătatea, la faptul că astfel de operatori și persoane împuternicite de operatori (i) vor stoca aceste date în UE și (ii) au demonstrat în mod corespunzător că nu fac obiectul legislației unor țări terțe care să contravină normelor UE privind protecția datelor.**

## 8.3 Puncte naționale de contact ale unei țări terțe sau sisteme instituite la nivel internațional

114. CEPD și AEPD iau act de faptul că articolul 13 alineatul (3) și articolul 52 alineatul (5) din Propunere prevăd posibilitatea ca punctele naționale de contact ale unei țări terțe sau sistemele instituite la nivel internațional să fie recunoscute ca fiind conforme cu cerințele MyHealth@EU și, respectiv, HealthData@EU. CEPD și AEPD reamintesc că transferurile care rezultă din conectarea la MyHealth@EU și HealthData@EU și din utilizarea acestora ar trebui să respecte capitolul V din RGPD.

115. CEPD și AEPD iau act de faptul că articolul 13 alineatul (3) și articolul 52 alineatul (5) din Propunere prevăd posibilitatea ca punctele naționale de contact ale unei țări terțe sau sistemele instituite la nivel internațional să fie recunoscute ca fiind conforme cu cerințele MyHealth@EU și, respectiv, HealthData@EU. CEPD și AEPD reamintesc că transferurile care rezultă din conectarea la MyHealth@EU și HealthData@EU și din utilizarea acestora ar trebui să respecte capitolul V din RGPD.

116. În special, CEPD și AEPD iau act de faptul că atât articolul 13 alineatul (3), cât și articolul 52 alineatul (5) din Propunere se referă la verificările de conformitate care trebuie efectuate de Comisie înainte de emiterea actului de punere în aplicare prin care se stabilește că un punct național de contact al unei țări terțe sau un sistem instituit la nivel internațional respectă cerințele MyHealth@EU sau HealthData@EU. CEPD și AEPD iau act, de asemenea, de faptul că considerentul 26 din Propunere, referitor la MyHealth@EU, se referă la necesitatea ca aceste verificări să asigure „conformitatea punctului național de contact cu specificațiile tehnice, normele de protecție a datelor și alte cerințe [...]". **În acest sens, CEPD și AEPD recomandă clarificarea directă, atât la articolul 13 alineatul (3), cât și la articolul 52 alineatul (5) din Propunere, a faptului că verificările conformității ar trebui să**

[38] În acest sens, considerentul 78 din RGPD prevede că „[principiile] protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor ar trebui să fie luate în considerare și în contextul licitațiilor publice". În plus, considerentul 77 din Directiva 2014/24/UE privind achizițiile publice prevede că „[l]a elaborarea specificațiilor tehnice, autoritățile contractante ar trebui să ia în considerare cerințele care derivă din dreptul Uniunii în domeniul legislației în materie de protecția datelor, în special în legătură cu conceperea prelucrării datelor cu caracter personal (protecția datelor din momentul conceperii)".

**asigure respectarea capitolului V din RGPD de îndată ce punctul național de contact al unei țări terțe sau un sistem instituit la nivel internațional este conectat la MyHealth@EU sau HealthData@EU.**

# 9 GUVERNANȚA ȘI COORDONAREA LA NIVEL EUROPEAN (CAPITOLUL VI)

117. CEPD și AEPD iau act de faptul că articolul 64 din Propunere instituie comitetul EHDS, un organism de coordonare care urmărește să faciliteze cooperarea și schimbul de informații între statele membre. După cum iau act CEPD și AEPD, comitetul EHDS va fi compus din reprezentanți ai autorităților digitale din domeniul sănătății și ai organismelor de acces la datele privind sănătatea din toate statele membre și **va fi prezidat de Comisie.** CEPD și AEPD iau act de faptul că, în conformitate cu Propunerea, reprezentanții CEPD și AEPD pot fi invitați la reuniuni atunci când sunt discutate aspecte legate de protecția datelor. **CEPD și AEPD consideră că reprezentanții lor ar trebui să fie membri permanenți ai comitetului EHDS (prin urmare, nu numai potențiali invitați) și ar trebui să participe la toate discuțiile privind aspecte legate de protecția datelor cu caracter personal**, pentru a asigura o interpretare și o aplicare coerente a dispozițiilor introduse de propunere în ceea ce privește dispozițiile RGPD.

118. În plus, articolul 65 alineatul (1) din Propunere definește sarcinile comitetului EHDS în ceea ce privește utilizarea primară a datelor electronice privind sănătatea. Potrivit observațiilor CEPD și AEPD, Comisia va fi în măsură să emită contribuții scrise și să facă schimb de bune practici cu privire la aspecte legate de punerea în aplicare a Propunerii, în special cu privire la dispozițiile prevăzute în capitolele II și III din Propunere [articolul 65 alineatul (1) litera (b) punctul (i)] și cu privire la orice aspect al utilizării primare a datelor electronice privind sănătatea [articolul 65 alineatul (1) litera (b) punctul (iii)]. Întrucât capitolul II din Propunere prevede drepturi de protecție a datelor similare cu cele prevăzute de RGPD (a se vedea punctul 28), potrivit CEPD și AEPD, Comitetul EHDS nu ar trebui să fie în măsură să emită contribuții scrise referitoare la aspecte legate de drepturile în materie de protecție a datelor. În caz contrar, **CEPD și AEPD subliniază că există riscul ca Propunerea să introducă o divergență în interpretarea sau aplicarea drepturilor de protecție a datelor** stabilite de CEPD și AEPD. În plus, CEPD și AEPD iau act de faptul că această dispoziție va crea incertitudine juridică, ceea ce va fi, de asemenea, în contradicție cu obiectivele Propunerii de îmbunătățire a funcționării pieței interne prin stabilirea unui **cadru juridic uniform** (considerentul 1 din Propunere). În plus, articolul 65 alineatul (2) din Propunere specifică sarcinile comitetului EHDS referitoare la utilizarea secundară a datelor electronice privind sănătatea. CEPD și AEPD își reiterează avertismentul referitor la competențele Comitetului EHDS de a publica contribuții scrise cu privire la aspecte legate de drepturile în materie de protecție a datelor în ceea ce privește utilizarea secundară a datelor electronice privind sănătatea.

119. În plus, în conformitate cu articolul 65 alineatul (1) litera (d) și cu articolul 65 alineatul (2) litera (d) din Propunere, CEPD și AEPD iau act de posibilitatea comitetului EHDS de a face schimb de informații privind riscurile și incidentele de protecție a datelor legate de utilizarea primară și secundară a datelor electronice privind sănătatea, împreună cu informații privind gestionarea acestora. **Încă o dată, CEPD și AEPD subliniază că există riscul ca Propunerea să introducă o divergență între CEPD, AEPD și Comitetul EHDS în ceea ce privește identificarea sau gestionarea încălcărilor securității datelor**, întrucât comitetul EDHS va fi în măsură să facă schimb de informații cu privire la modul în care ar putea fi gestionate incidentele de protecție a datelor. În plus, nu există claritate în ceea ce privește

destinatarii informațiilor pe care Comitetul EHDS le va partaja. La un nivel mai general, CEPD și AEPD recomandă co-legiuitorului să specifice interacțiunea dintre CEPD, AEPD și Comitetul EHDS în ceea ce privește aspectele legate de protecția datelor, care ar trebui să rămână competența exclusivă a autorităților de protecție a datelor.

120. În privința aceluiași capitol, CEPD și AEPD iau act de faptul că articolul 66 din Propunere prevede instituirea de către Comisie a două subgrupuri de exercitare în comun a competenței de operator pentru infrastructurile transfrontaliere MyHealth@EU și HealthData@EU (articolele 12 și 52 din propunere). **CEPD și AEPD iau act de faptul că domeniul de aplicare al sarcinilor grupurilor de exercitare în comun a competenței de operator nu este definit în mod clar și că acestea se pot suprapune cu sarcinile comitetului EHDS** în temeiul articolului 65 din propunere. La un nivel mai general, CEPD și AEPD recomandă ca interacțiunea dintre diferitele organisme, grupuri și organizații menționate în propunere să fie clar definită.

121. În plus, CEPD și AEPD constată unele neconcordanțe între sarcinile subgrupurilor și competența Comisiei de a adopta acte delegate sau puse în aplicare cu privire la aceleași subiecte. De exemplu, în conformitate cu articolul 52 alineatul (13) din Propunere, Comisia poate stabili cerințele, specificațiile tehnice și arhitectura informatică a HealthData@EU prin acte de punere în aplicare, în timp ce unul dintre cele două subgrupuri va lua, de asemenea, decizii privind dezvoltarea și exploatarea aceleiași infrastructuri. **Prin urmare, CEPD și AEPD recomandă clarificarea interacțiunii dintre Comisie și aceste subgrupuri.**

# 10 DELEGAREA ȘI COMITETUL (CAPITOLUL VII)

122. Capitolul VII din Propunere permite Comisiei să adopte acte delegate cu privire la mai multe aspecte concrete reglementate de Propunere. În acest sens, CEPD și AEPD iau act de faptul că, indiferent de implicarea statelor membre în procesul decizional, competența de a decide să modifice sau să extindă unele dintre aspectele esențiale abordate de Propunere lasă în continuare Comisiei o marjă considerabilă de manevră pentru a modifica sau a extinde domeniul de aplicare al aceleiași Propuneri într-un mod care ar putea afecta drepturile în materie de protecție a datelor și competența exclusivă a statelor membre de a-și defini politicile naționale în domeniul sănătății.

123. În special, CEPD și AEPD consideră că articolul 5 alineatul (2) și articolul 33 alineatul (7) din Propunere ridică semne de întrebare, întrucât Comisia este împuternicită să modifice lista categoriilor prioritare de date electronice privind sănătatea care urmează să fie accesate și schimbate între statele membre pentru utilizarea primară, precum și lista datelor electronice privind sănătatea, sub rezerva disponibilității obligatorii și a accesului terților pentru utilizare secundară. Întrucât orice modificare a unor astfel de categorii de date cu caracter personal, în special a categoriilor speciale de date, ar putea necesita o reevaluare a riscurilor la adresa drepturilor fundamentale și a intereselor persoanelor vizate, aceste aspecte constituie chestiuni de fond care ar trebui considerate elemente esențiale, în temeiul articolului 290 din TFUE.

124. Prin urmare, CEPD și AEPD consideră că astfel de aspecte nu ar trebui excluse de la nivelul legislativ, unde ar trebui să se prevadă în mod clar orice restricționare a drepturilor fundamentale pentru a se obține previzibilitatea indispensabilă a instrumentului juridic, în timp ce, prin adoptarea de acte delegate, ar trebui adăugate doar câmpuri de date mai detaliate (subcategorii de date) care se încadrează în categoriile de date deja definite prevăzute la articolul 5 alineatul (1) și la articolul 33 alineatul (1) din Propunere.

125. În plus, CEPD și AEPD iau act de faptul că criteriile prevăzute la articolul 5 alineatul (2) litera (b) din Propunere pentru a ghida Comisia în ceea ce privește stabilirea categoriilor prioritare de date electronice privind sănătatea care urmează să fie adăugate pe lista stabilită la articolul 5 alineatul (1) din Propunere par vagi și ar trebui să fie delimitate suplimentar[39].

126. În cele din urmă, chiar dacă articolul 67 alineatul (4) din Propunere prevede consultarea de către Comisie a experților desemnați de fiecare stat membru, ceea ce poate implica o anumită expertiză în chestiuni legate de protecția datelor, CEPD și AEPD recomandă introducerea unei trimiteri clare la articolul 42 din RPDUE pentru a clarifica faptul că AEPD și CEPD trebuie consultate, după caz, atunci când sunt propuse astfel de acte delegate.

## 11 DIVERSE (CAPITOLUL VIII)

127. CEPD și AEPD iau act de faptul că, potrivit capitolului VIII din Propunere, responsabilitatea pentru stabilirea sancțiunilor aplicabile în cazul încălcării Regulamentului le revine statelor membre ale UE. CEPD și AEPD consideră că acest lucru ar putea genera incertitudini juridice semnificative în ceea ce privește aplicarea corespunzătoare a normelor stabilite în Propunere în diferite state membre, din cauza stabilirii în mod diferit a cuantumului sancțiunilor, care ar putea fi aplicate în valori minime și maxime semnificativ diferite de la un stat membru la altul. În acest sens, CEPD și AEPD iau act de faptul că ar trebui stabilite norme armonizate privind sancțiunile pentru a asigura o aplicare echitabilă și sigură, în special în contextul cazurilor transfrontaliere.

128. În cele din urmă, CEPD și AEPD iau act de faptul că, în conformitate cu observațiile anterioare privind autocertificarea sistemelor DES, perioadele de evaluare și revizuire stabilite în temeiul articolului 70 din Propunere sunt prea lungi pentru a asigura punerea în aplicare corespunzătoare în timp util.

| | |
|---|---|
| Pentru Autoritatea Europeană pentru Protecția Datelor, | Pentru Comitetul European pentru Protecția Datelor, |
| Autoritatea Europeană pentru Protecția Datelor | Președinta |
| (Wojciech Wiewiorowski) | (Andrea Jelinek) |

[1] De exemplu, nu este clar dacă producătorii s-ar încadra în această categorie.

[39] Criteriile se referă la „categoria utilizată într-un număr semnificativ de sisteme DES utilizate în statele membre”, conform celor mai recente informații.