EUROPEAN DATA PROTECTION SUPERVISOR

Avizul 3/2015

Marea oportunitate a Europei

Recomandările AEPD cu privire la opțiunile Uniunii Europene privind reforma în materie de protecție a datelor

28 iulie 2015

La 24 iunie 2015, cele trei instituții principale ale UE, Parlamentul European, Consiliul și Comisia Europeană au demarat negocierile din cadrul procedurii de codecizie cu privire la propunerea de regulament general privind protecția datelor (RGPD), o procedură cunoscută ca „trilog" informal.[1] Temeiul trilogului îl constituie propunerea Comisiei din ianuarie 2012, Rezoluția legislativă a Parlamentului European din 12 martie 2014 și abordarea generală a Consiliului adoptată la 15 iunie 2015.[2] Cele trei instituții se angajează să trateze RGPD ca parte a pachetului mai amplu de reforme privind protecția datelor, care cuprinde directiva propusă pentru activitățile polițienești și judiciare. Procesul ar trebui să se încheie la sfârșitul anului 2015 și va permite, probabil, adoptarea oficială a ambelor instrumente la începutul anului 2016, care va fi urmată de o perioadă de tranziție de doi ani.[3]

Autoritatea Europeană pentru Protecția Datelor (AEPD) este o instituție independentă a UE. Autoritatea nu ia parte la trilog, dar răspunde, în conformitate cu articolul 41 alineatul (2) din Regulamentul (CE) nr. 45/2001, „în ceea ce privește prelucrarea datelor cu caracter personal [...] de respectarea de către instituțiile și organele comunitare a drepturilor și libertăților fundamentale ale persoanelor fizice, în special a vieții private a acestora", și „[...] de consilierea instituțiilor și organelor comunitare și a persoanelor vizate asupra tuturor aspectelor privind prelucrarea de date cu caracter personal". *Directorul Autorității și adjunctul acestuia au fost numiți în decembrie 2014, cu misiunea specifică de a fi mai constructivi și proactivi; în martie 2015, aceștia au publicat o strategie pe cinci ani care stabilește modul în care intenționează să pună în aplicare acest mandat și să răspundă pentru ceea ce întreprind.[4]*

Prezentul aviz reprezintă prima etapă în cadrul strategiei AEPD. Bazându-se pe discuțiile cu instituțiile UE, statele membre, societatea civilă, reprezentanții industriei și alte părți interesate, recomandările noastre au drept scop să ajute participanții la trilog să ajungă la consens în timp util. Avizul abordează RGPD în două părți:

- *viziunea AEPD asupra unor norme de protecție a datelor orientate către viitor, cu exemple ilustrative ale recomandărilor noastre; și*
- *o anexă („Anexa la Avizul 3/2015: Tabel comparativ al textelor RGPD cu recomandarea AEPD") care conține un tabel cu patru coloane pentru compararea, articol cu articol, a textului RGPD, astfel cum a fost adoptat de Comisie, Parlament și, respectiv, Consiliu, cu recomandarea AEPD.*

Avizul este publicat pe site-ul nostru și prin intermediul unei aplicații pentru comunicații mobile. Acesta va fi completat în toamna anului 2015 cu recomandări privind atât considerentele RGPD, cât și protecția datelor în domeniul activităților polițienești și judiciare, după ce Consiliul adoptă o poziție generală cu privire la directivă.

Avizul cuprinzător al AEPD cu privire la pachetul de reforme propus de Comisie în martie 2012 rămâne valabil. După trei ani a trebuit totuși să ne actualizăm recomandarea de implicare mai directă privind pozițiile colegiuitorilor și să formulăm recomandări precise.[5] Ca avizul din 2012, prezentul aviz este în conformitate cu avizele și declarațiile Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, inclusiv „Anexa" privind „Temele principale în vederea trilogului" adoptată la 18 iunie, la care AEPD a contribuit ca membru titular al grupului de lucru.[6]

O oportunitate rară: De ce este această reformă atât de importantă

UE este pe ultima sută de metri a unui maraton de reformare a normelor privind informaţiile cu caracter personal. Este posibil ca Regulamentul general privind protecţia datelor să afecteze, în următoarele decenii, toate persoanele fizice din UE, toate organizaţiile din UE care prelucrează date cu caracter personal şi organizaţiile din afara UE care prelucrează date cu caracter personal referitoare la persoanele fizice din UE.[7] Acum este momentul să protejăm drepturile şi libertăţile fundamentale ale persoanelor într-o societate a viitorului bazată pe date.

O protecţie eficientă a datelor conferă încredere persoanelor şi stimulează întreprinderile şi autorităţile publice responsabile. Legile din acest domeniu sunt complexe şi tehnice, necesitând consultanţă de specialitate, în special din partea autorităţilor independente de protecţie a datelor, care înţeleg provocările pe care la presupune respectarea acestora. RGPD ar putea fi unul dintre cele mai lungi din repertoriul legislativ al Uniunii; prin urmare, UE trebuie să urmărească acum să fie selectivă, să se axeze pe dispoziţiile care sunt cu adevărat necesare şi să evite detaliile care, ca o consecinţă neintenţionată, ar putea interfera în mod nejustificat cu tehnologiile viitoare. Textele fiecărei instituţii promovează claritatea şi caracterul inteligibil al prelucrării datelor cu caracter personal: prin urmare, RGPD trebuie să respecte aceeaşi cerinţă, fiind cât mai concis şi uşor de înţeles.

Parlamentul şi Consiliul, în calitate de colegiuitori, trebuie să stabilească textul juridic final, cu ajutorul Comisiei ca iniţiator al legislaţiei şi gardian al tratatelor. AEPD nu ia parte la negocierile „trilogului", dar avem competenţa legală de a oferi consiliere şi de a face acest lucru în mod proactiv, în conformitate cu mandatul primit de directorul Autorităţii şi de adjunctul acestuia la numire, precum şi cu strategia recentă a AEPD. Prezentul aviz valorifică mai mult de un deceniu de experienţă în materie de supraveghere a respectării protecţiei datelor şi consiliere cu privire la politici pentru a orienta instituţiile spre un rezultat care va servi intereselor persoanei.

Legiferarea este arta posibilului. Opţiunile disponibile, sub forma respectivelor texte preferate de Comisie, Parlament şi Consiliu, conţin fiecare numeroase prevederi demne de luat în seamă, dar toate pot fi îmbunătăţite. În opinia noastră, rezultatul nu va fi perfect, dar ne propunem să sprijinim instituţiile în obţinerea celui mai bun rezultat posibil. Acesta este motivul pentru care recomandările noastre nu depăşesc limitele celor trei texte. Avem trei preocupări constante:

- o situaţie mai avantajoasă pentru cetăţeni,
- norme care să funcţioneze în practică,
- norme care să dureze o generaţie întreagă.

Prezentul aviz reprezintă un exerciţiu de transparenţă şi responsabilitate, principii duale care sunt probabil inovaţia cea mai remarcabilă a RGPD. Procedura de trilog este supusă unui control mai serios decât oricând. Recomandările noastre sunt publice şi dorim să îndemnăm toate instituţiile UE să ia iniţiativa şi să conducă prin puterea exemplului, astfel încât această reformă legislativă să fie rezultatul unei proceduri transparente şi nu al unui compromis ascuns.

UE are nevoie de noi prevederi în materie de protecţie a datelor, de un nou capitol. Restul lumii ne urmărește îndeaproape. Calitatea noii legi și modul în care interacţionează cu sistemele juridice și tendinţele globale sunt extrem de importante. Prin prezentul aviz, AEPD îşi face cunoscute dorinţa și disponibilitatea de a se asigura că UE valorifică în cea mai mare măsură această oportunitate istorică.

I. CUPRINS

1 O situaţie mai avantajoasă pentru cetăţeni

Normele UE au urmărit întotdeauna să faciliteze fluxurile de date, atât în cadrul UE, precum şi cu partenerii săi comerciali, demonstrând în acelaşi timp o preocupare esenţială pentru drepturile şi libertăţile persoanelor fizice. Internetul permite un grad fără precedent de conectivitate, exprimare individuală şi câmp de manevră pentru a furniza valoare întreprinderilor şi consumatorilor. Cu toate acestea, confidenţialitatea este mai importantă ca niciodată pentru europeni. Conform sondajului Eurobarometru privind protecţia datelor din iunie 2015,[8] mai mult de şase din zece cetăţeni nu au încredere în întreprinderile online, iar două treimi din ei sunt îngrijoraţi de faptul că nu deţin controlul complet asupra informaţiilor pe care le furnizează online.

Cadrul reformat trebuie să menţină şi, dacă este posibil, să îmbunătăţească standardele aplicabile persoanelor fizice. Pachetul de reformă privind protecţia datelor a fost propus în primul rând ca vehicul pentru „consolidarea drepturilor la confidenţialitate pe internet", asigurându-se că oamenii sunt „mai bine informaţi cu privire la drepturile lor şi au mai mult control asupra informaţiilor care îi privesc".[9] Reprezentanţii organizaţiilor societăţii civile s-au adresat în scris Comisiei Europene în aprilie 2015 pentru a solicita instituţiilor să rămână fidele acestor intenţii.[10]

Principiile existente stipulate în Cartă, dreptul primar al UE, trebuie să fie aplicate în mod consecvent, dinamic şi inovator, astfel încât să fie eficiente în practică pentru cetăţeni. Reforma trebuie să fie cuprinzătoare şi, de aceea, este necesar să existe un angajamentul faţă de un pachet, dar, deoarece este probabil ca prevederile privind prelucrarea datelor să fie cuprinse în instrumente juridice separate, este nevoie de claritate cu privire la domeniul de aplicare concret şi modul în care acestea conlucrează, fără portiţe pentru compromisuri cu privire la garanţii.[11]

Pentru AEPD, punctul de plecare este demnitatea persoanei, care transcende chestiunile privind simpla respectare a legislaţiei.[12] Recomandările noastre se bazează pe o evaluare a fiecărui articol din RGPD, în mod individual şi cumulat, în funcţie de posibilitatea sa de a consolida poziţia persoanei fizice în raport cu cadrul actual. Punctul de referinţă îl constituie principiile care stau la baza protecţiei datelor, adică articolul 8 din Carta drepturilor fundamentale.[13]

1. Definiţii: să clarificăm ce înseamnă informaţii cu caracter personal

- Persoanele fizice ar trebui să îşi poată exercita mai eficient drepturile cu privire la orice informaţie care le poate identifica sau individualiza, chiar dacă informaţia este considerată „devenită pseudonim".[14]

2. Toate prelucrările de date trebuie să fie atât legale, cât şi justificate

- Cerinţele ca prelucrarea tuturor datelor să se limiteze la scopuri specifice şi să aibă un temei juridic sunt cumulative, nu alternative. Recomandăm evitarea oricărei contopiri – care ar însemna şi o atenuare – a acestor principii. În schimb, UE ar trebui să păstreze, să simplifice şi să operaţionalizeze teza instituită potrivit căreia datele cu caracter personal ar trebui să fie folosite numai în moduri compatibile cu scopurile iniţiale ale colectării.[15]

- Consimţământul reprezintă un posibil temei juridic pentru prelucrare, dar nu trebuie să fie permise casetele care impun bifarea atunci când nu există nicio alegere semnificativă pentru persoana respectivă şi atunci când nu este deloc necesar ca datele să fie prelucrate. Recomandăm să se permită oamenilor să îşi acorde consimţământul limitat sau amplu pentru cercetarea clinică, de exemplu, care să fie respectat şi să poată fi retras.[16]

- AEPD susţine soluţii judicioase şi inovatoare pentru transferurile internaţionale de informaţii cu caracter personal care să faciliteze schimburile de date şi să respecte principiile privind protecţia şi supravegherea datelor. Recomandăm insistent să se evite permiterea transferurilor pe baza intereselor legitime ale operatorului, din cauza protecţiei insuficiente oferite persoanei, iar UE nu ar trebui să permită accesul direct al autorităţilor din ţări terţe la datele din UE. Orice solicitare de transfer emisă de autorităţile dintr-o ţară terţă ar trebui să fie recunoscută numai dacă respectă normele prevăzute în tratatele de asistenţă judiciară reciprocă, acordurile internaţionale sau alte canale legale de cooperare internaţională.[17]

3. O supraveghere mai independentă, mai autoritară

- Autorităţile pentru protecţia datelor din UE ar trebui să fie pregătite să îşi exercite rolurile în momentul în care intră în vigoare RGPD, iar Comitetul european pentru protecţia datelor ar trebui să fie pe deplin operaţional imediat ce Regulamentul devine aplicabil.[18]

- Autorităţile ar trebui să poată primi şi examina plângerile şi cererile înaintate de persoanele vizate sau organisme, organizaţii şi asociaţii.

- Protejarea drepturilor persoanelor fizice necesită un sistem eficient de răspundere şi acordare de despăgubiri pentru prejudiciile cauzate prin prelucrarea ilegală a datelor. Având în vedere obstacolele evidente existente în calea obţinerii de reparaţii în practică, persoanele ar trebui să poată fi reprezentate de organisme, organizaţii şi asociaţii în cadrul procedurilor judiciare.[19]

2 Norme care vor funcţiona în practică

Garanţiile nu ar trebui să fie confundate cu formalităţile. Detaliile excesive sau tentativele de microgestiune a proceselor de afaceri riscă să devină depăşite în viitor. Putem deschide o filă din manualul UE în materie de concurenţă în care un corpus relativ limitat de legislaţie secundară este aplicat riguros şi încurajează o cultură a responsabilităţii şi a sensibilizării în rândul întreprinderilor.[20]

Fiecare dintre cele trei texte necesită o mai mare claritate şi simplitate din partea celor responsabili de prelucrarea informaţiilor cu caracter personal.[21] De asemenea, obligaţiile tehnice trebuie să fie, la rândul lor, concise şi uşor de înţeles pentru a putea fi puse în aplicare în mod corespunzător de către operatori.[22]

Procedurile existente nu sunt bătute în cuie: recomandările noastre au scopul de a identifica modalităţi de debirocratizare, reducând la minim solicitările de documente şi formalităţile irelevante. Recomandăm legiferarea numai în cazul în care acest lucru este

cu adevărat necesar. Aceasta oferă un câmp de manevră pentru companii, autorităţi publice sau autorităţi de protecţie a datelor: este nevoie de o răspundere mai mare şi de consiliere din partea autorităţilor pentru protecţia datelor. În ansamblu, recomandările noastre ar avea drept rezultat un text al RGPD cu aproape 30% mai scurt decât dimensiunea medie a textelor celor trei instituţii.[23]

1. Garanţii eficace, nu proceduri

- Documentele ar trebui să fie un mijloc de realizare a conformităţii, nu un obiectiv al acesteia; reforma trebuie să se concentreze pe rezultate. Recomandăm o abordare ajustabilă care să reducă obligaţiile operatorilor cu privire la documente la o politică unică referitoare la modul în care va fi respectat regulamentul, ţinând seama de riscuri, conformitatea fiind demonstrată transparent, indiferent dacă este vorba despre transferuri, contracte cu persoanele împuternicite de către operatori sau notificări privind încălcările.[24]

- Pe baza unor criterii explicite de evaluare a riscurilor şi bazându-ne pe experienţa noastră de supraveghere a instituţiilor UE, recomandăm impunerea transmiterii de notificări privind încălcarea securităţii datelor la autoritatea de supraveghere şi a evaluărilor impactului asupra protecţiei datelor numai în cazul în care drepturile şi libertăţile persoanelor vizate sunt în pericol.[25]

- Ar trebui încurajate în mod activ iniţiativele din partea mediului de afaceri, fie prin reguli corporatiste obligatorii, fie prin mărci de protecţie a vieţii private.[26]

2. Un echilibru mai bun între interesul public şi protecţia datelor cu caracter personal

- Normele în materie de protecţie a datelor nu ar trebui să împiedice cercetarea istorică, statistică şi ştiinţifică de interes public real. Cei responsabili trebuie să ia măsurile necesare pentru a împiedica utilizarea informaţiilor cu caracter personal contrar intereselor persoanei, acordând o atenţie deosebită normelor care reglementează informaţiile sensibile cu privire la sănătate, de exemplu.[27]

- Cercetătorii şi arhiviştii ar trebui să poată stoca datele cât timp este necesar, cu respectarea acestor garanţii.[28]

3. Încrederea în autorităţile de supraveghere şi împuternicirea acestora

- Recomandăm să se permită autorităţilor de supraveghere să emită orientări pentru operatorii de date şi să elaboreze propriile reguli de procedură în spiritul unei aplicări simplificate şi mai uşoare a RGPD de către o autoritate de supraveghere unică (conceptul ghişeului unic) aproape de cetăţeni („proximitate”). [29]

- Autorităţile ar trebui să poată stabili sancţiuni corective şi administrative eficiente, proporţionale şi cu efect de descurajare, pe baza tuturor circumstanţelor relevante.[30]

3 Norme care să dureze o generație întreagă

Principalul pilon al cadrului actual, Directiva 95/46/CE, a servit drept model pentru legislația ulterioară privind prelucrarea datelor în UE și în întreaga lume și chiar a constituit baza pentru formularea dreptului la protecția datelor cu caracter personal din articolul 8 din Carta drepturilor fundamentale. Această reformă va reglementa prelucrarea datelor pentru o generație care nu știe cum ar fi viața fără internet. Prin urmare, UE trebuie să înțeleagă pe deplin implicațiile acestui act pentru persoanele fizice și durabilitatea acestuia în raport cu dezvoltarea tehnologică.

În ultimii ani s-a înregistrat o creștere exponențială în ceea ce privește generarea, culegerea, analiza și schimbul de informații cu caracter personal, rezultatul inovațiilor tehnologice, cum ar fi internetul obiectelor, cloud computing, volumele mari de date și datele deschise, a căror exploatare Uniunea Europeană o consideră esențială pentru competitivitatea sa.[31] Având în vedere longevitatea Directivei 95/46/CE, este rezonabil să ne așteptăm la un interval de timp asemănător până la următoarea revizuire majoră a normelor privind protecția datelor, poate nu mai devreme de sfârșitul anilor 2030. Cu mult înainte de acest moment, este de așteptat ca tehnologiile bazate pe date să se îndrepte spre sistemele de inteligență artificială, de procesare a limbajului natural și sistemele biometrice, permițând crearea unor aplicații cu o capacitate de învățare automatizată pentru inteligență avansată.

Aceste tehnologii pun sub semnul întrebării principiile în materie de protecție a datelor. Prin urmare, o reformă orientată spre viitor trebuie să fie bazată pe demnitatea persoanei și fundamentată pe etică. Aceasta trebuie să corecteze dezechilibrul dintre inovarea în domeniul protecției datelor cu caracter personal și exploatarea acestora, astfel încât garanțiile să aibă efect în societatea noastră digitală.

1. Practici comerciale responsabile și inovații tehnice

- Reforma ar trebui să inverseze tendința recentă de urmărire secretă și luare a deciziilor pe baza unor profiluri ascunse persoanei. Problema nu o constituie mesajele publicitare orientate sau practica elaborării profilurilor, ci mai degrabă lipsa de informații semnificative privind logica algoritmică care elaborează aceste profiluri și are un efect asupra persoanei vizate.[32] Recomandăm o mai mare transparență din partea operatorilor.

- Susținem insistent introducerea principiilor de protecție a datelor începând cu momentul conceperii și protecția implicită a datelor ca mijloc de impulsionare a soluțiilor orientate spre piață în economia digitală. Recomandăm o formulare mai simplă a cerinței ca drepturile și interesele persoanei să fie integrate în dezvoltarea de produse și în setările implicite.[33]

2. Mai multe drepturi pentru persoanele fizice

- În mediul digital, portabilitatea datelor este poarta de acces spre controlul utilizatorului; acum, persoanele fizice își dau seama că le lipsește acest lucru. Recomandăm să se permită persoanelor vizate, la cerere, transferul direct de date de la un operator la altul și să li se acorde dreptul de a primi o copie a datelor pe care le pot transfera la un alt operator.[34]

3. Norme rezistente în timp

- Recomandăm evitarea unui limbaj şi a unor practici care sunt susceptibile de a deveni depăşite sau discutabile.[35]

4 Aspecte nerezolvate

Adoptarea de către UE a unui pachet de reforme orientate spre viitor privind protecţia datelor va fi o realizare impresionantă şi totuşi incompletă.

Toate instituţiile sunt de acord că principiile RGPD ar trebui să se aplice în mod consecvent instituţiilor UE. Am susţinut securitatea juridică şi uniformitatea cadrului juridic, acceptând în acelaşi timp unicitatea sectorului public al UE şi necesitatea de a evita orice diminuare a nivelului actual al obligaţiilor (precum şi necesitatea de a asigura baza legală şi organizaţională pentru AEPD). Prin urmare, Comisia ar trebui să formuleze o propunere în conformitate cu RGPD pentru revizuirea Regulamentului (CE) nr. 45/2001, cât mai curând posibil după finalizarea discuţiilor privind RGPD, astfel încât ambele texte să poată deveni aplicabile în acelaşi timp.[36]

În al doilea rând, este clar că Directiva 2002/58/CE („Directiva privind confidenţialitatea în mediul electronic") va trebui modificată. Mult mai important este însă faptul că UE are nevoie de un cadru clar privind confidenţialitatea comunicaţiilor, un element integrant al dreptului la viaţă privată, care să reglementeze toate serviciile care permit comunicaţii, nu numai pe cele oferite de furnizorii de comunicaţii electronice accesibile publicului. Acest lucru trebuie realizat prin intermediul unui regulament armonizator şi sigur din punct de vedere juridic care să prevadă cel puţin aceleaşi standarde de protecţie ca Directiva privind confidenţialitatea în mediul electronic în condiţii echitabile.

Prin urmare, prezentul aviz recomandă asumarea unui angajament faţă de adoptarea rapidă a propunerilor în aceste două domenii cât mai curând posibil.

5 Un moment definitoriu pentru drepturile digitale în Europa și în afara ei

Pentru prima dată în decurs de o generaţie, UE are ocazia de a moderniza şi de a armoniza normele privind modul în care sunt tratate informaţiile personale. Confidenţialitatea şi protecţia datelor nu sunt în concurenţă cu creşterea economică şi comerţul internaţional, nici cu serviciile şi produsele de calitate; acestea fac parte din propunerea privind calitatea şi valoarea. Aşa cum recunoaşte Consiliul European, încrederea este o condiţie necesară pentru produsele şi serviciile inovatoare care se bazează pe prelucrarea datelor cu caracter personal.

În 1995, UE era o deschizătoare de drumuri în domeniul protecţiei datelor. Acum, peste 100 de ţări din întreaga lume au legi privind protecţia datelor şi mai puţin de jumătate dintre acestea sunt ţări europene.[37] Cu toate acestea, UE continuă să solicite o atenţie deosebită din partea ţărilor care au în vedere constituirea sau revizuirea cadrelor lor juridice. Într-o perioadă în care încrederea oamenilor în companii şi guverne a fost zguduită de dezvăluirile privind supravegherea în masă şi încălcările securităţii datelor, legiuitorilor UE le revine o responsabilitate considerabilă, pentru că se estimează că deciziile luate de ei în acest an vor avea un impact care va depăşi graniţele Europei.

În opinia AEPD, textele RGPD sunt pe drumul cel bun, dar încă mai există motive de îngrijorare, unele chiar foarte grave. Există întotdeauna un risc în cadrul procesului de codecizie: anumite dispoziţii pot fi slăbite de către negociatori bine intenţionaţi de dragul compromisului politic. Cu toate acestea, în domeniul reformei protecţiei datelor lucrurile stau altfel, pentru că avem de-a face cu drepturi fundamentale şi modul în care acestea vor fi protejate timp de o întreagă generaţie.

În acest context, prezentul aviz încearcă să sprijine principalele instituţii ale UE în rezolvarea problemelor. Vrem nu doar drepturi mai solide pentru persoana vizată şi o mai mare responsabilitate din partea operatorului; vrem să facilităm inovarea printr-un cadru legal neutru faţă de tehnologie, dar pozitiv faţă de beneficiile pe care tehnologia le poate aduce societăţii.

Negocierile aflându-se pe ultima sută de metri, sperăm că recomandările noastre vor ajuta UE să reuşească promovarea unei reforme care să rămână fidelă scopului său de-a lungul anilor şi deceniilor care vor urma: un nou capitol pentru protecţia datelor dintr-o perspectivă globală, în care UE va conduce prin puterea exemplului.

Bruxelles, 28 iulie 2015

Giovanni BUTTARELLI

Autoritatea Europeană pentru Protecţia Datelor

Note

[1] Declaraţii comune. Declaraţie comună a Parlamentului European, a Consiliului şi a Comisiei Europene privind aspectele practice în cadrul procedurii de codecizie (articolul 251 din Tratatul CE) (2007/C 145/02), JO C 145, 30.6.2007.

[2] COM(2012) 11 final; Rezoluţia legislativă a Parlamentului European din 12 martie 2014 referitoare la propunerea de regulament al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (Regulament general privind protecţia datelor), P7_TA (2014)0212; Propunerea de regulament al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (Regulament general privind protecţia datelor) – Pregătirea abordării generale, documentul Consiliului 9565/15, 11 iunie 2015.

[3] Titlul complet este Propunere de directivă privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi la libera circulaţie a acestor date, COM(2012) 10 final; Rezoluţia legislativă a Parlamentului European din 12 martie 2014 referitoare la propunerea de directivă a Parlamentului European şi a Consiliului privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi la libera circulaţie a acestor date, P7_TA(2014) 0219. În ceea ce priveşte calendarul şi sfera de aplicare a trilogului, a se vedea Concluziile Consiliului European din 25-26 iunie 2015, EUCO 22/15; o „foaie de parcurs" pentru trilog a fost indicată într-o conferinţă de presă comună a Parlamentului, Consiliului şi Comisiei http://audiovisual.europarl.europa.eu/AssetDetail.aspx?id=690e8d8d-682d-4755-bfb6-a4c100eda4ed [ultima accesare la 20 iulie 2015], dar nu a fost publicată oficial. RGPD va intra în vigoare la 20 de zile de la data publicării în Jurnalul Oficial şi se preconizează că va fi pe deplin aplicabil la doi ani de la intrarea sa în vigoare (articolul 91).

[4] Anunţul privind postul vacant de director al Autorităţii Europene pentru Protecţia Datelor COM/2014/10354 (2014/C 163 A/02), JO C 163 A/6 28.5.2014. Strategia AEPD pentru perioada 2015-2019 a promis să „caute soluţii viabile care să evite birocraţia, să rămână flexibile la inovaţia tehnologică şi fluxurile transfrontaliere de date şi să permită persoanelor fizice să îşi exercite drepturile mai eficient atât în mediul online, cât şi în afara acestuia"; Conducerea prin puterea exemplului: Strategia AEPD pentru perioada 2015-2019, martie 2015.

[5] Avizul AEPD referitor la pachetul de reformă privind protecţia datelor, 7 martie 2015.

[6] A se vedea anexa la Scrisoarea Grupului de lucru pentru protecţia persoanelor în ceea ce priveşte prelucrarea datelor cu caracter personal către Věra Jourová, comisarul pentru justiţie, protecţia consumatorilor şi egalitatea de gen, 17 iunie 2015.

[7] Domeniul de aplicare material şi teritorial al RGPD este greu de sintetizat. Instituţiile par să fie de acord cel puţin cu faptul că domeniul de aplicare vizează organizaţiile constituite în UE care sunt responsabile pentru prelucrarea datelor cu caracter personal fie în UE, fie în afara acesteia, organizaţiile cu sediul în afara UE care prelucrează date cu caracter personal ale persoanelor fizice din UE în cadrul furnizării de produse sau servicii sau al monitorizării persoanelor din UE. (A se vedea articolul 2 cu privire la domeniul de aplicare material şi articolul 3 cu privire la domeniul de aplicare teritorial.)

[8] Printre alte rezultate se numără: şapte din zece persoane sunt îngrijorate că informaţiile lor sunt folosite în alt scop decât cel pentru care au fost colectate, una din şapte persoane consideră că în orice situaţie ar trebui să se solicite explicit consimţământul înainte ca datele să fie colectate şi prelucrate, iar două treimi cred că este important să îşi poată transfera informaţiile

cu caracter personal de la un furnizor vechi de servicii la unul nou; Eurobarometrul special 431 privind protecţia datelor, iunie 2015. Rezultate comparabile au fost furnizate în 2014 de centrul Pew Research, care a constatat că 91% dintre americani consideră că au pierdut controlul asupra modului în care companiile le colectează şi utilizează informaţiile cu caracter personal, 80% dintre utilizatorii reţelelor sociale sunt preocupaţi în legătură cu terţii precum agenţiile de publicitate sau companiile care le obţin datele, iar 64% spun că guvernul ar trebui să facă mai mult pentru a reglementa activitatea celor care publică reclame; Sondajul de tip panel al centrului Pew Research privind confidenţialitatea, ianuarie 2014.

[9] Comisia propune o reformă cuprinzătoare a normelor în materie de protecţie a datelor pentru a spori controlul utilizatorilor asupra datelor lor şi a reduce costurile pentru întreprinderi.

[10] Scrisoarea din partea unor ONG-uri către domnul preşedinte Juncker, 21 aprilie 2015 https://edri.org/files/DP_letter_Juncker_20150421.pdf şi răspunsul transmis de Şeful de Cabinet al vicepreşedintelui Timmermans, 17 iulie 2015 https://edri.org/files/eudatap/Re_EC_EDRi-GDPR.pdf [accesat la 23 iulie 2015]. În mai 2015, AEPD s-a întâlnit cu reprezentanţii câtorva dintre aceste ONG-uri pentru a discuta despre preocupările exprimate; COMUNICAT DE PRESĂ AEPD/2015/04, 1 iunie 2015, Reforma UE în domeniul protecţiei datelor: AEPD se întâlneşte cu grupurile internaţionale pentru libertăţi civile; înregistrarea completă a discuţiei este disponibilă pe site-ul AEPD (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Pressnews/Videos/GDPR_civil_soc).

[11] Articolul 2 alineatul (2) litera (e).

[12] Articolul 1.

[13] Articolul 8 din Cartă prevede următoarele [sublinierea noastră]:

> *1. Orice persoană are dreptul la protecţia datelor cu caracter personal care o privesc.*
>
> *2. Asemenea date trebuie* ***tratate în mod corect****, în* ***scopurile precizate*** *şi* ***pe baza consimţământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege****. Orice persoană are dreptul de acces la datele colectate care o privesc, precum şi* ***dreptul de a obţine rectificarea acestora****.*
>
> *3. Respectarea acestor norme se supune* ***controlului unei autorităţi independente****.*

[14] Articolul 10. Cu excepţia cazului şi până în momentul în care există o definiţie clară şi obligatorie din punct de vedere juridic pentru „datele devenite pseudonim" – diferite de „datele cu caracter personal", acest tip de date trebuie să rămână în sfera de aplicare a normelor de protecţie a datelor.

[15] Articolul 6 alineatele (2) şi (4). Având în vedere că au existat unele incertitudini cu privire la sensul termenului „compatibilitate", recomandăm, în urma Avizului Grupului de lucru pentru protecţia persoanelor în ceea ce priveşte prelucrarea datelor cu caracter personal cu privire la limitarea scopului, criteriile generale pentru a verifica dacă prelucrarea este compatibilă [a se vedea articolul 5 alineatul (2)].

[16] Separarea funcţională eficientă constituie un mijloc de asigurare a prelucrării legale în lipsa consimţământului, dar interesul legitim nu ar trebui să fie interpretat excesiv. Un drept necondiţionat de a renunţa poate fi, de asemenea, o alternativă adecvată în unele situaţii. Stabilirea acordării în mod liber a consimţământului depinde în parte de (a) existenţa unui dezechilibru semnificativ între persoana vizată şi operator şi (b) în cazurile de prelucrare în conformitate cu articolul 6 alineatul (1) litera (b), condiţionarea sau nu a executării unui contract sau a prestării unui serviciu de consimţământul privind prelucrarea unor date care nu sunt necesare în aceste scopuri. [A se vedea articolul 7 alineatul (4).] Acest lucru reflectă dispoziţia din legislaţia UE privind consumatorii: în conformitate cu articolul 3 alineatul (1) din Directiva 93/13/CEE a Consiliului din 5 aprilie 1993 privind clauzele abuzive în contractele încheiate cu consumatorii, „o clauză contractuală care nu s-a negociat individual se consideră ca

fiind abuzivă în cazul în care, în contradicţie cu cerinţa de bună credinţă, provoacă un dezechilibru semnificativ între drepturile şi obligaţiile părţilor care decurg din contract, în detrimentul consumatorului".

[17] Exemple de astfel de norme sunt deciziile privind gradul de adecvare pentru sectoarele şi teritoriile menţionate, revizuirile periodice ale deciziilor privind gradul de adecvare şi regulile corporatiste obligatorii. A se vedea articolele 40-45.

[18] Articolul 73.

[19] Articolul 76. Cu privire la dificultatea obţinerii de reparaţii pentru încălcarea normelor în materie de protecţie a datelor, a se vedea raportul Agenţiei pentru Drepturi Fundamentale, Accesul la căile de atac în domeniul protecţiei datelor cu caracter personal în statele membre ale UE, 2013.

[20] Normele UE pun accentul pe autoevaluarea companiilor referitor la respectarea articolului 101 din TFUE cu privire la interzicerea acordurilor anticoncurenţiale, în timp ce firmele dominante pe o piaţă au o „responsabilitate specială" de a evita orice acţiune care ar putea afecta concurenţa efectivă (articolul 9 din Orientările Comisiei 2009/C 45/02); a se vedea Avizul preliminar al AEPD privind protecţia vieţii private şi competitivitatea în epoca bazelor de date de dimensiuni foarte mari, 14 martie 2014.

[21] Cele trei texte se referă în diverse feluri la „un mod şi o formă inteligibile, utilizând un limbaj clar şi simplu" (considerentul 57, PE, articolul 19, COM şi Consiliul), calitatea de a fi „clar şi neechivoc" [considerentul 99, PE, articolul 10 litera (a) PE] şi furnizarea de „informaţii clare şi uşor de înţeles" (articolul 10 PE, articolul 11 PE) şi informaţii care sunt „concise, transparente, clare şi uşor accesibile" (considerentul 25, PE, COM şi Consiliul, articolul 11 PE).

[22] Prevederile privind actele delegate au fost eliminate în mare măsură în versiunile Parlamentului şi Consiliului. Considerăm că UE ar putea merge mai departe şi ar putea supune aceste chestiuni tehnice evaluării unor autorităţi independente.

[23] Recomandările noastre ar avea drept rezultat un text de aproximativ 20 000 de cuvinte; dimensiunea medie a textelor celor trei instituţii este de aproximativ 28 000 de cuvinte.

[24] Articolul 22.

[25] Articolele 31 şi 33.

[26] Articolul 39.

[27] Articolul 83. Cercetarea şi arhivarea în sine nu constituie un temei juridic pentru prelucrare, motiv pentru care recomandăm eliminarea articolului 6 alineatul (2).

[28] Articolul 83a.

[29] Grupul de lucru pentru protecţia persoanelor în ceea ce priveşte prelucrarea datelor cu caracter personal a prezentat o viziune asupra guvernării, mecanismului coerenţei şi ghişeului unic bazată pe încrederea în autorităţile independente de prelucrare a datelor (APD) şi formulată pe trei niveluri:

- APD individuală, care este puternică şi are resurse complete pentru a se ocupa de cazurile din sfera sa de competenţă;
- cooperarea eficientă între APD cu un avantaj clar în cazurile transfrontaliere;
- Comitetul european pentru protecţia datelor, care trebuie să fie autonom, cu personalitate juridică proprie, prevăzut cu mijloace suficiente, alcătuit din autorităţi de prelucrare a datelor care sunt egale şi care lucrează într-un spirit de solidaritate, cu puterea de a lua decizii cu caracter obligatoriu şi având sprijinul unui secretariat care serveşte comitetul prin preşedinte.

[30] De asemenea, recomandăm clarificarea competenței autorităților de supraveghere și desemnarea unei autorități principale în cazurile de prelucrare transnațională, păstrând în același timp capacitatea autorităților de supraveghere de a se ocupa de cazurile pur locale. Recomandăm o versiune simplificată a mecanismului coerenței, care să ofere mai multă claritate cu privire la modul de identificare a cazurilor în care autoritățile de supraveghere trebuie să consulte Comitetul european pentru protecția datelor și în care Comitetul trebuie să emită o decizie cu caracter obligatoriu pentru a asigura aplicarea consecventă a regulamentului.

[31] Comunicarea Comisiei referitoare la O strategie privind piața unică digitală pentru Europa, COM(2015) 192 final; Concluziile Consiliului European din iunie 2015, EUCO 22/15; Concluziile Consiliului privind transformarea digitală a industriei europene, 8993/15.

[32] Articolul 14 litera (h).

[33] Articolul 23.

[34] Articolul 18. Mai recomandăm ca, pentru a avea efect, dreptul la portabilitatea datelor să aibă o sferă largă de aplicare și să nu fie aplicat doar în cazul operațiunilor de prelucrare care utilizează datele furnizate de persoana vizată.

[35] Recomandăm, de exemplu, omiterea termenilor cum ar fi „online", „în scris" și „societatea informațională".

[36] O opțiune pe care am prefera-o este ca acest lucru să se facă prin intermediul unei prevederi în RGPD.

[37] Greenleaf, Graham, „Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority" (30 ianuarie 2015); (2015) 133 Privacy Laws & Business International Report, februarie 2015; UNSW Law Research Paper Nr. 2015-21.