



COMISIA EUROPEANĂ

Bruxelles, 25.1.2012
SEC(2012) 73 final

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMAT AL EVALUĂRII IMPACTULUI

care însoțește documentul

Regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor)

și

Directivă a Parlamentului European și a Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, precum și libera circulație a acestor date

{COM(2012) 11 final}
{SEC(2012) 72 final}

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMAT AL EVALUĂRII IMPACTULUI

care însoțește documentul

Regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor)

și

Directivă a Parlamentului European și a Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, precum și libera circulație a acestor date

1. INTRODUCERE

De la adoptarea, în 1995, a cadrului juridic actual al UE cu privire la protecția datelor, evoluțiile rapide tehnologice și ale mediului de afaceri au adus noi provocări în ceea ce privește protecția datelor cu caracter personal. Amploarea schimbului de date și a colectării acestora a crescut în mod semnificativ. Tehnologia permite atât societăților private, cât și autorităților publice să utilizeze datele cu caracter personal la o scară fără precedent pentru a-și continua activitățile. Din ce în ce mai mult, cetățenii își fac publice la nivel mondial informațiile personale, fără a fi pe deplin conștienți de riscurile implicate.

Consolidarea încrederii în mediul online este esențială pentru dezvoltarea economică. Din cauza lipsei de încredere, consumatori ezită să facă cumpărături online și să adopte noi servicii, inclusiv servicii publice de e-guvernare. Dacă nu se răspunde acestei lipse de încredere, ea va continua să încetinească dezvoltarea de utilizări inovatoare ale noilor tehnologii, să acționeze ca un obstacol în calea creșterii economice și să împiedice sectorul public să se bucure de beneficiile potențiale ale digitizării serviciilor sale.

În plus, prin articolul 16 din TFUE, Tratatul de la Lisabona a creat o bază juridică nouă pentru o abordare modernizată și globală a protecției datelor și a liberei circulații a datelor cu caracter personal, care acoperă, de asemenea, cooperarea polițienească și judiciară în materie penală.

2. DEFINIREA PROBLEMEI

Evaluarea impactului prezintă și analizează trei domenii problematice principale:

2.1. Problema 1: Obstacole pentru întreprinderi și autorități publice ca urmare a fragmentării, incertitudinii juridice și aplicării inconsecvente a legii

În pofida obiectivului directivei de a asigura un nivel echivalent de protecție a datelor în cadrul UE, există încă diferențe considerabile între normele în vigoare în statele membre. Prin urmare, operatorii de date s-ar putea să se găsească în situația în care să se confrunte cu 27 de legislații naționale și cerințe diferite la nivelul UE. Rezultatul este un mediu juridic fragmentat care a generat un context de incertitudine juridică și de protecție inegală a persoanelor. Acest lucru a cauzat costuri și **sarcini administrative** inutile (reprezentând **aproximativ 3 miliarde de euro pe an** în scenariul de bază) pentru întreprinderi și constituie un factor de descurajare pentru întreprinderile, inclusiv IMM-uri, care își desfășoară activitatea pe piața unică și care doresc să își extindă activitățile și la nivel transfrontalier.

În plus, resursele și competențele autorităților naționale responsabile cu protecția datelor variază considerabil între statele membre. Aceasta înseamnă că, în unele cazuri, autoritățile respective nu sunt în măsură să își îndeplinească sarcinile de aplicare a legii în mod satisfăcător. Cooperarea dintre aceste autorități la nivel european – prin intermediul grupului consultativ existent (Grupul de lucru articolul 29) – nu conduce întotdeauna la respectarea consecventă a legii și, prin urmare, trebuie, de asemenea, să fie îmbunătățită.

2.2. Problema 2: Dificultăți pentru persoanele fizice în ceea ce privește păstrarea controlului asupra datelor lor cu caracter personal

Având în vedere lipsa de armonizare în legislațiile naționale în ceea ce privește protecția datelor și competențele divergente ale autorităților naționale de protecție a datelor, este mai dificil pentru persoanele fizice să își exercite drepturile în unele state membre decât în altele, în special în contextul online.

Persoanele fizice au pierdut, de asemenea, controlul asupra propriilor date, ca urmare a volumului considerabil de date care sunt transmise în fiecare zi și din cauza faptului că utilizatorii nu sunt întotdeauna pe deplin conștienți că propriile lor date sunt colectate. Deși numeroși europeni consideră că divulgarea de date cu caracter personal face din ce în ce mai mult parte din viața modernă¹, 72 % dintre utilizatorii de internet din Europa încă se tem că li se cer prea multe date cu caracter personal online și adesea aceștia nu știu cum să își exercite drepturile în acest context.

2.3. Problema 3: Lacune și inconsecvențe în ceea ce privește protecția datelor cu caracter personal în domeniul cooperării polițienești și judiciare în materie penală

Domeniul de aplicare al directivei, care se baza pe un temei juridic din domeniul pieței interne, a exclus în mod explicit cooperarea polițienească și judiciară în materie penală. Decizia-cadru adoptată în 2008 pentru a reglementa prelucrarea datelor în domeniul cooperării polițienești și al cooperării judiciare în materie penală reflectă caracteristicile specifice ale structurii UE bazate pe „piloni”, anterioare Tratatului de la Lisabona, și este caracterizată de **un domeniu de aplicare limitat și de diverse alte lacune**, conducând adesea la incertitudine juridică pentru persoane și pentru autoritățile de aplicare a legii, precum și la dificultăți practice legate de punerea în aplicare a legislației. Mai mult, decizia-cadru oferă

¹ A se vedea Eurobarometrul special 359 – *Atitudini privind protecția datelor și identitatea electronică în Uniunea Europeană*, iunie 2011, p. 23.

posibilități largi de derogare de la principiile generale de protecție a datelor la nivel național, acestea rămânând astfel nearmonizate. Aceasta riscă nu numai să contracareze însuși obiectivul acestor principii și, prin urmare, să afecteze dreptul fundamental al persoanelor fizice la protecția datelor lor cu caracter personal în acest domeniu, ci și să împiedice buna desfășurare a schimbului de date cu caracter personal între autoritățile naționale relevante.

3. ANALIZA SUBSIDIARITĂȚII ȘI PROPORȚIONALITĂȚII

În lumina problemelor subliniate mai sus, analiza subsidiarității indică necesitatea unor măsuri la nivelul UE, pe baza următoarelor motive:

- dreptul la protecția datelor cu caracter personal este consacrat la articolul 8 din Carta drepturilor fundamentale. Articolul 16 din TFUE reprezintă temeiul juridic pentru adoptarea normelor UE privind protecția datelor;
- datele cu caracter personal pot fi transferate din ce în ce mai rapid peste granițele naționale, atât în cadrul UE, cât și către țări terțe. În plus, există dificultăți practice în ceea ce privește controlul aplicării legislației privind protecția datelor, fiind necesară o cooperare între statele membre și autoritățile acestora, care să fie organizată la nivelul UE, pentru a asigura coerența necesară și un nivel ridicat de protecție în cadrul Uniunii;
- un stat membru nu poate reduce în mod individual problemele în situația actuală. Acesta este în special cazul acelor probleme care provin din fragmentarea legislației naționale de punere în aplicare a cadrului de reglementare al UE privind protecția datelor;
- deși ar fi posibil ca statele membre să adopte politici care să garanteze că acest drept nu este încălcat, acest obiectiv nu ar putea fi atins în mod uniform în absența unor norme UE comune și ar crea restricții privind fluxurile transfrontaliere de date cu caracter personal.

Acțiunile avute în vedere sunt proporționale, dat fiind că intră sub incidența competențelor Uniunii, astfel cum sunt definite în tratate, și sunt necesare pentru a asigura uniformitatea aplicării legislației UE, asigurând o protecție egală și eficace a drepturilor fundamentale ale persoanelor. Este esențial ca măsurile să fie luate la nivelul UE, pentru a se garanta în continuare credibilitatea și un nivel ridicat de protecție a datelor în contextul globalizării, menținându-se, în același timp, libera circulație a datelor. Pentru buna funcționare a pieței interne, este necesar ca dispozițiile să asigure condiții de concurență echitabile pentru operatorii economici.

4. OBIECTIVE

Principalele **obiective de politică** sunt următoarele:

- **consolidarea dimensiunii pieței interne de protecție a datelor**, prin reducerea fragmentării, creșterea coerenței și **simplificarea** cadrului de reglementare, ceea ce duce la eliminarea unor costuri inutile și la **reducerea sarcinii administrative**;
- **creșterea gradului de eficacitate al exercitării dreptului fundamental la protecția datelor și abilitarea persoanelor pentru ca acestea să își poată controla propriile date**;

- **sporirea coerenței cadrului UE de protecție a datelor**, inclusiv în domeniul cooperării polițienești și al cooperării judiciare în materie penală, ținând seama pe deplin de intrarea în vigoare a Tratatului de la Lisabona.

5. OPȚIUNI DE POLITICĂ

5.1. Opțiunea 1: Măsuri de mică amploare

Această opțiune ar consta în principal în elaborarea de **comunicări interpretative de către Comisie**, crearea de **instrumente de asistență tehnică și** furnizarea de **fonduri**, precum și **încurajarea standardizării și autoreglementării**, pentru a consolida punerea în practică a normelor existente de către operatorii de date și pentru a crește nivelul de informare a cetățenilor. Comisia ar propune **doar modificări legislative foarte limitate** pentru a clarifica conceptele actuale din directivă și ar viza anumite aspecte care nu pot fi abordate eficient în niciun alt mod. Această opțiune de politică ar fi relevantă doar pentru problemele 1 și 2.

Modificările legislative limitate ar introduce în mod explicit principiile de transparență și de minimizare a datelor, precum și un temei juridic pentru „regulile corporatiste obligatorii” privind transferurile internaționale.

5.2. Opțiunea 2: Un cadru legislativ modernizat

Comisia ar prezenta **propuneri legislative pentru a armoniza mai mult normele materiale**, a clarifica dispozițiile specifice și a trata inconsecvențele cauzate de abordările diferite din statele membre. Aceste propuneri ar aborda problemele 1 și 2, dat fiind că, pe de o parte, ar **facilita fluxurile de date în cadrul UE și dinspre UE spre țări terțe** și, pe de altă parte, ar **clarifica și ar consolida drepturile persoanelor fizice** (de exemplu, dreptul de acces, „dreptul de a fi uitat”, elaborarea de modalități mai clare de exprimare a consimțământului și de notificare a cazurilor de încălcare a securității datelor cu caracter personal) și ar **consolida responsabilitatea și „gradul de răspundere” al operatorilor de date și al persoanelor împuternicite de către aceștia** [de exemplu, prin introducerea, dacă este cazul, a obligației de a numi responsabili cu protecția datelor (RPD) sau de a efectua evaluări ale impactului asupra protecției datelor]. Această opțiune ar institui, în special, un „**ghiseu unic**” pentru operatorii de date (adică o legislație unică și o singură autoritate de protecție a datelor, APD). Cerințele generale privind notificarea ar fi simplificate (printr-o „înregistrare de bază”). De asemenea, această opțiune ar **consolida independența APD și ar armoniza competențele acestora**. Cooperarea și asistența reciprocă între APD ar fi consolidate, inclusiv prin intermediul unui nou „**mecanism pentru asigurarea coerenței**”, la care ar participa atât Comitetul european pentru protecția datelor (care ar urma să fie înființat), cât și Comisia.

În ceea ce privește protecția datelor în domeniul cooperării polițienești și judiciare în materie penală (problema 3), Comisia ar prezenta propuneri pentru a înlocui decizia-cadru cu un **nou instrument cu un domeniu de aplicare extins** și ar aborda **cele mai importante lacune și deficiențe**, atât pentru a consolida drepturile persoanelor fizice, cât și pentru a facilita cooperarea între autoritățile de aplicare a legii, luând în același timp în considerare caracteristicile specifice ale sectorului aplicării legii.

5.3. Opțiunea 3: Norme juridice detaliate la nivelul UE

Această opțiune ar include majoritatea elementelor din opțiunea 2, precum și o **legislație UE mult mai detaliată**, inclusiv la nivel sectorial (de exemplu, în sectorul sănătății și în sectorul medical) și o **structură de aplicare a legii centralizată la nivelul UE** (de exemplu, prin înființarea unei autorități UE de protecție a datelor). De asemenea, ea ar presupune eliminarea cerințelor de notificare generală (cu excepția verificării prealabile a operațiunilor riscante de prelucrare a datelor), înființarea unui sistem de certificare la nivelul UE pentru procesele și produsele care se conformează normelor de protecție a datelor și definirea unor sancțiuni penale armonizate la nivelul UE pentru încălcări ale normelor de protecție a datelor. Consimțământul ar fi definit drept „condiția prealabilă” pentru prelucrarea datelor.

În ceea ce privește cooperarea polițienească și judiciară în materie penală, pe lângă măsurile substanțiale din cadrul opțiunii 2, aceasta ar include elaborarea unor norme detaliate pentru dreptul de acces al persoanelor fizice (întotdeauna direct). De asemenea, ea ar implica **modificarea dispozițiilor relevante ale tuturor instrumentelor existente pentru foștii piloni**, pentru a le alinia complet cu noile norme armonizate extinse.

6. EVALUAREA IMPACTULUI

6.1. Opțiunea de politică 1: Măsuri de mică amploare

Comunicările Comisiei privind interpretarea dispozițiilor directivei nu ar fi obligatorii și, prin urmare, ar avea doar un **impact limitat asupra reducerii incertitudinii juridice și a costurilor**. Un grad mai ridicat de autoreglementare la nivelul UE ar putea contribui la creșterea clarității juridice pentru operatorii de date în anumite sectoare, însă **nu ar fi suficient** pentru a garanta aplicarea eficientă și consecventă a normelor în absența unui cadru juridic de bază clar și armonizat al UE.

Campaniile de sensibilizare ar ajuta persoanele fizice să își cunoască mai bine drepturile în materie de protecția datelor și să înțeleagă mai bine modalitățile practice de a le exercita. Acest lucru **nu** ar fi totuși **suficient** pentru ca persoanele fizice să își cunoască drepturile, în cazul în care aceste drepturi nu sunt clar definite în lege. **Clarificările legislative** ale principiilor legate de transparență, minimizarea datelor, caracterul adecvat și regulile corporatiste obligatorii ar contribui la creșterea gradului de armonizare și de securitate juridică pentru persoane fizice și întreprinderi.

În ceea ce privește controlul aplicării legislației, comunicările Comisiei nu ar elimina reticența statelor membre de a modifica normele naționale, pentru a oferi o mai mare independență și competențe armonizate autorităților de protecție a datelor. O coordonare consolidată prin Grupul de lucru articolul 29 și schimburile dintre APD ar avea un impact pozitiv asupra creșterii gradului de coerență a aplicării normelor; cu toate acestea, **divergențele persistente între legislațiile naționale și între interpretările acestora ar limita efectul ameliorării cooperării dintre APD**.

Impactul financiar și economic preconizat al acestei opțiuni de politică este limitat, iar problemele identificate ar rămâne, în mare măsură, nerezolvate.

6.2. Opțiunea de politică 2: Un cadru legislativ modernizat

Incertitudinea juridică pentru societățile private și autoritățile publice **se va reduce semnificativ**. Dispozițiile problematice vor fi clarificate, iar gradul de coerență va crește, grație reducerii marjei de interpretare, precum și măsurilor de punere în aplicare și/sau actelor delegate adoptate de către Comisie.

Înlocuirea notificării generale a activităților de prelucrare a datelor cu un **sistem de „înregistrare”** simplificat și **armonizat** și păstrarea, în același timp, a verificărilor prealabile pentru datele sensibile și operațiunile riscante de prelucrare a datelor va scuti operatorii de date de o obligație care este în prezent pusă în aplicare în mod divergent. Consolidarea responsabilității operatorilor de date și a persoanelor împuternicite de aceștia, prin introducerea, în anumite cazuri și cu praguri bine definite și specifice, de responsabili cu protecția datelor sau de evaluări ale impactului asupra protecției datelor și prin introducerea principiului de protecție a datelor începând cu momentul conceperii, va oferi modalități mai simple de a asigura și de a demonstra respectarea normelor.

Clarificarea și simplificarea normelor, prin definirea unei legislații unice aplicabile pe întreg teritoriul UE și înființarea unui „ghișeu unic” pentru supravegherea procesului de protecție a datelor va consolida piața internă, inclusiv prin înlăturarea diferențelor dintre formalitățile administrative ale APD. Aceasta va duce la **economii globale de 2,3 miliarde EUR** pe an, numai la nivelul sarcinii administrative.

Aplicarea legislației va deveni, de asemenea, mai coerentă, prin consolidarea și armonizarea competențelor APD și prin crearea unui mecanism solid de cooperare și asistență reciprocă pentru cazurile care au o dimensiune europeană, precum și prin armonizarea infracțiunilor care fac obiectul unor sancțiuni administrative.

Instituirea unei **obligații armonizate la nivelul UE de notificare a cazurilor de încălcare a securității datelor** va proteja mai bine persoanele fizice, va asigura coerența între sectoare și va evita dezavantajele concurențiale.

Drepturile persoanelor vizate și capacitatea de control a persoanelor fizice în ceea ce privește propriile date ar fi consolidate considerabil prin introducerea de noi drepturi, precum și prin îmbunătățirea și clarificarea celor existente. Minorii vor beneficia de măsuri care să țină seama în mod specific de vulnerabilitatea acestora. Asociațiile vor avea mai multe posibilități de a sprijini persoanele vizate în exercitarea drepturilor lor, inclusiv prin acțiuni în fața instanțelor.

Aplicarea principiilor generale privind protecția datelor în domeniul cooperării polițienești și al cooperării judiciare în materie penală ar consolida coerența globală a cadrului UE de protecție a datelor, respectând în același timp elementele specifice inerente aplicării legii. Drepturile persoanelor fizice ar fi consolidate în special prin extinderea sferei de aplicare a normelor de protecție a datelor în acest domeniu pentru a cuprinde și prelucrarea „internă”, stabilindu-se condițiile necesare pentru a garanta dreptul de acces și elaborându-se norme mai stricte privind limitarea scopului.

În ceea ce privește **impactul financiar și economic**, obligația societăților economice mai mari (peste 250 de angajați) de a desemna responsabili cu protecția datelor nu va **crea costuri disproporționate**, dat fiind că, în general, în aceste societăți există deja astfel de responsabili. Costurile de conformitate s-ar ridica la 320 de milioane EUR pe an. Obligația ar acoperi un

sector minim necesar de operatori de date, întrucât IMM-urile ar fi în general scutite de această obligație, cu excepția cazului în care activităților lor de prelucrare a datelor implică riscuri semnificative legate de protecția datelor. Autoritățile și organismele publice ar avea dreptul să numească un singur RPD pentru mai multe entități (de exemplu, un responsabil pentru mai multe filiale, departamente, birouri), în funcție de structura organizatorică a acestora.

Simplificarea normelor pentru transferurile internaționale (de pildă, prin extinderea domeniului de aplicare al „regulilor corporatiste obligatorii”) ar avea, de asemenea, un impact pozitiv asupra competitivității pe plan internațional a întreprinderilor din UE.

Consolidarea independenței și a competențelor APD, corelată cu obligația statelor membre de a le pune acestora la dispoziție suficiente resurse, ar genera costuri suplimentare pentru autoritățile publice care nu dispun în prezent de competențe și resurse adecvate.

Noul mecanism de cooperare și asistență reciprocă între APD ar presupune, de asemenea, costuri suplimentare pentru autoritățile naționale de protecție a datelor și pentru AEPD. De pildă, sarcinile suplimentare care ar reveni AEPD în ceea ce privește dotarea secretariatului Comitetului european pentru protecția datelor, care înlocuiește Grupul de lucru articolul 29, și, în special, participarea la mecanismul pentru asigurarea coerenței ar putea necesita o creștere a resurselor actuale ale AEPD cu o sumă suplimentară de 3 milioane EUR pe an în medie pentru primii șase ani, inclusiv credite pentru 10 resurse umane suplimentare.

6.3. Opțiunea de politică 3: Norme juridice detaliate la nivelul UE

Adăugarea unor alte dispoziții juridice detaliate, inclusiv a celor sectoriale, dincolo de măsurile prevăzute în cadrul opțiunii 2, ar duce la o **reducere maximă a diferențelor dintre statele membre**. Cu toate acestea, s-ar putea să nu existe suficientă flexibilitate pentru ca statele membre să poată ține seama de specificul național.

Eliminarea totală a notificărilor, cu excepția cazului verificărilor prealabile, ar simplifica foarte mult cadrul de reglementare și ar reduce sarcina administrativă.

Înființarea unei Agenții de protecție a datelor la nivelul UE ar îmbunătăți considerabil **coerența aplicării legislației** și ar soluționa consecvențele pentru cazurile cu o dimensiune europeană clară, dar competențele unei astfel de agenții europene ar putea fi mult prea extinse în cadrul legislației UE. Această opțiune ar fi însă foarte costisitoare pentru bugetul UE. Armonizarea sancțiunilor penale ar consolida, de asemenea, aplicarea consecventă a legislației, însă s-ar confrunta, la rândul lor, cu o opoziție puternică din partea statelor membre.

Drepturile persoanelor vizate, inclusiv drepturile copiilor, ar fi consolidate, de exemplu prin extinderea definiției datelor sensibile pentru ca aceasta să cuprindă și datele minorilor, datele biometrice și cele financiare. Prin introducerea unui drept la „acțiunile colective” s-ar putea permite exercitarea deplină a drepturilor pe cale judiciară. Din armonizarea nivelului sancțiunilor, inclusiv al celor penale, ar trebui să rezulte o mai mare consolidare a drepturilor individuale la nivelul UE.

Modificările explicite ale tuturor instrumentelor care extind normele generale de protecție a datelor către domeniul cooperării polițienești și judiciare în materie penală ar avea un impact pozitiv în ceea ce privește consecvența și coerența normelor din acest domeniu și consolidarea

drepturilor persoanelor fizice. Cu toate acestea, o astfel de abordare radicală ar întâmpina rezistență din partea statelor membre și ar fi dificil de realizat din punct de vedere politic.

7. COMPARAREA OPȚIUNILOR

Opțiunea de politică 1 ar duce la niveluri scăzute de conformitate și ar presupune costuri administrative reduse, în special pentru operatorii de date din sectorul privat, deoarece majoritatea costurilor suplimentare ar fi suportate de autoritățile publice naționale și europene. În același timp, **impactul pozitiv al acesteia în ceea ce privește problemele identificate și realizarea obiectivelor de politică ar fi limitat.**

În ceea ce privește fezabilitatea politică, deși propunerile nu sunt susceptibile de a stârni controverse, această opțiune de politică riscă să se confrunte cu rezistența părților interesate, ca urmare a domeniului de aplicare și a impactului său limitat în ceea ce privește problemele identificate, și nu ar fi considerată suficient de ambițioasă.

Opțiunea de politică 2 va duce la o **reducere semnificativă a fragmentării și a incertitudinii juridice.** Se preconizează că aceasta va avea un impact mult mai mare în abordarea problemelor identificate și în atingerea obiectivelor de politică. Se preconizează că echilibrul dintre realizarea conformității și **costurile administrative aferente acestei opțiuni de politică va fi rezonabil, având în vedere beneficiile și economiile în valoare de 2,3 miliarde EUR pe an în ceea ce privește sarcinile administrative, un aspect foarte important pentru întreprinderi.** Această opțiune va asigura o aplicare mai bună și mai coerentă a normelor, la nivel global. Eliminarea notificărilor în favoarea unui sistem mult mai simplu de „înregistrare de bază” ar permite, de asemenea, simplificarea cadrului de reglementare și ar reduce sarcina administrativă.

În ceea ce privește acceptul părților interesate, această opțiune s-ar bucura în general de o primire pozitivă din partea operatorilor economici și a autorităților publice, deoarece le-ar permite acestora să își reducă la nivel global cheltuielile de conformitate, în special cele generate de fragmentarea actualului regim. Structurile responsabile de protecția datelor și, în special, APD ar saluta consolidarea drepturilor în materie de protecția datelor. În ceea ce privește al treilea obiectiv general, această opțiune ar contribui la atingerea obiectivelor privind garantarea **unei mai mari coerențe și consecvențe a normelor de protecție a datelor în domeniul cooperării polițienești și al cooperării judiciare în materie penală,** prin abrogarea deciziei-cadru și adaptarea conținutului acesteia în funcție de Tratatul de la Lisabona, eliminând astfel lacunele acesteia, în special prin extinderea domeniului său de aplicare pentru a cuprinde și prelucrarea „internă”.

Opțiunea de politică 3 include majoritatea măsurilor prevăzute în opțiunea de politică 2, fiind în același timp mai ambițioasă în ceea ce privește mai multe aspecte. Prin urmare, ea ar avea un **impact pozitiv puternic în ceea ce privește atât reducerea costurilor legate de fragmentare, cât și consolidarea drepturilor persoanelor fizice.** În plus, această opțiune ar spori la maximum consecvența și coerența normelor de protecție a datelor în cadrul celui de-al treilea pilon și ar ridica nivelul standardelor de protecție a datelor în acest context. Cu toate acestea, unele dintre măsurile incluse în cadrul acestei opțiuni au un **cost de conformitate excesiv de ridicat sau riscă să se confrunte cu o opoziție puternică din partea părților interesate.** În plus, modificarea simultană a tuturor instrumentelor anterioare din cel de-al treilea pilon ar fi foarte complexă și ar putea crea controverse la nivel politic.

Opțiunea preferată:

Opțiunea preferată este opțiunea 2, combinată cu:

- eliminarea obligațiilor de notificare, prevăzută de opțiunea 3 și
- unele „măsuri de mică amploare” din opțiunea 1: încurajarea tehnologiilor menite să sporească protecția vieții private și a sistemelor de certificare, precum și campaniile de sensibilizare.

Opțiunea preferată este cea care are cele mai multe șanse de a atinge obiectivele de politică fără a impune costuri de conformitate excesive și reducând considerabil sarcina administrativă.

Se preconizează că normele consolidate de protecție a datelor vor genera unele costuri de conformitate suplimentare, în special în ceea ce privește operatorii care realizează activități riscante de prelucrare a datelor. Cu toate acestea, un regim solid de protecție a datelor poate oferi un avantaj concurențial pentru economia UE, în sensul că un nivel mai ridicat de protecție și un număr redus, conform estimărilor, de incidente și încălcări legate de protecția datelor pot spori încrederea consumatorilor. Crearea obligației pentru întreprinderi de a adopta standarde înalte de protecție a datelor poate duce, de asemenea, la îmbunătățirea pe termen lung a activității întreprinderilor europene, care ar putea deveni lideri mondiali în domeniul tehnologiilor menite să sporească protecția vieții private sau în ceea ce privește soluțiile de protecție a datelor începând cu momentul conceperii, atrăgând astfel întreprinderi, locuri de muncă și capital spre Uniunea Europeană.

În plus, pentru întreprinderile care își desfășoară activitatea în cadrul pieței interne a UE, creșterea armonizării va simplifica procesul de prelucrare transfrontalieră a datelor cu caracter personal și îl va face mai puțin costisitor. Acest aspect ar trebui să ofere un stimulent considerabil acestui tip de întreprinderi, pentru ca ele să se extindă la nivel transfrontalier și să exploateze pe deplin avantajele pieței interne, ceea ce ar avea efecte benefice atât pentru consumatori, cât și pentru economia europeană în ansamblul său.

Opțiunea preferată include o soluție echilibrată și în ceea ce privește problema 3, deoarece consolidează drepturile cetățeanului, elimină lacunele și reduce consecvențele în ceea ce privește protecția datelor în domeniul cooperării polițienești și judiciare în materie penală, facilitând în același timp cooperarea în materie de aplicare a legii și respectând elementele specifice sectorului și necesitățile sale operaționale.

8. MONITORIZARE ȘI EVALUARE

Monitorizarea și evaluarea impactului opțiunii preferate se va concentra asupra unor elemente cum ar fi utilizarea instrumentelor noi introduse de reformă, competențele și resursele autorităților naționale de protecție a datelor, sancțiunile aplicate pentru încălcarea legislației privind protecția datelor, timpul petrecut de operatorii de date în vederea asigurării conformității și costurile aferente acestui proces, precum și cultivarea încrederii cetățenilor în ceea ce privește protecția propriilor date cu caracter personal în mediul online.