GRUPUL DE LUCRU PENTRU PROTECȚIA DATELOR INSTITUIT ÎN TEMEIUL ARTICOLULUI 29

00062/10/RO
WP 173

Avizul 3/2010 privind principiul responsabilității

Adoptat la 13 iulie 2010

Acest grup de lucru a fost constituit în conformitate cu articolul 29 din Directiva 95/46/CE. Este un organism consultativ european independent în domeniul protecției datelor şi respectării vieții private. Sarcinile acestuia sunt definite la articolul 30 din Directiva 95/46/CE şi la articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de către Direcția C (Drepturi fundamentale şi cetățenia Uniunii Europene) a Comisiei Europene, Direcția Generală Justiție, B-1049 Bruxelles, Belgia, Biroul nr. LX-46 01/190.

Site web: http://ec.europa.eu/justice/policies/privacy/index_en.htm

REZUMAT

Principiile si obligațiile UE privind protecția datelor sunt adeseori insuficient reflectate în măsuri și practici interne concrete. Până în momentul în care protecția datelor nu va deveni parte a valorilor și practicilor comune ale unei organizații și responsabilitățile nu vor fi repartizate în mod explicit, respectarea efectivă a acestor principii și obligații va fi supusă unui risc considerabil, iar incidentele nefericite privind protecția datelor pot continua să apară.

Pentru a încuraja protecția efectivă a datelor, cadrul de reglementare al UE are nevoie de instrumente suplimentare. Prezentul aviz are ca obiectiv consilierea Comisiei asupra modului de modificare a Directivei privind protecția datelor în acest sens. În special, prezentul aviz înaintează o propunere concretă în vederea instituirii unui principiu al responsabilității, care impune operatorilor de date obligația de a adopta măsuri adecvate și eficace pentru a garanta că principiile și obligațiile prevăzute de directivă sunt respectate și pentru a demonstra acest lucru, la cerere, autorităților de supraveghere. Acest lucru ar contribui la trecerea protecției datelor „din teorie în practică", precum și la sprijinirea autorităților de protecție a datelor în îndeplinirea atribuțiilor lor de supraveghere și de punere în aplicare.

Avizul conține sugestii pentru a garanta faptul că principiul responsabilității oferă securitate juridică, permițând în același timp scalabilitatea (adică, permite stabilirea măsurilor concrete care să fie aplicate în funcție de riscul prelucrării și de tipurile de date prelucrate). Avizul analizează apoi impactul pe care acest principiu l-ar putea avea asupra altor domenii, inclusiv asupra transferurilor internaționale de date, asupra cerințelor de notificare, a sancțiunilor și eventual, și asupra elaborării programelor sau sigiliilor de certificare.

Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal

înființat prin Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995,

având în vedere articolul 29 și articolul 30 alineatul (1) litera (a) și alineatul (3) din această directivă, precum și articolul 15 alineatul (3) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002,

având în vedere Regulamentul său de procedură,

adoptă prezentul aviz:

1. INTRODUCERE

1. Protecția datelor trebuie să treacă „din teorie în practică". Prevederile legale în materie trebuie să fie traduse în măsuri concrete de protecție a datelor. Pentru a încuraja protecția efectivă a datelor, cadrul de reglementare al UE are nevoie de instrumente suplimentare. În cadrul discuțiilor privind viitorul cadrului european și mondial de protecție a datelor, s-a sugerat recurgerea la mecanisme bazate pe responsabilitate, ca modalitate de încurajare a operatorilor de date să utilizeze instrumente practice pentru o protecție efectivă a datelor.

2. În documentul său din decembrie 2009 privind viitorul protecției vieții private (WP 168), grupul de lucru instituit în temeiul articolului 29 și-a exprimat punctul de vedere potrivit căruia cadrul juridic actual nu a asigurat cu succes traducerea cerințelor de protecție a datelor în mecanisme eficiente care oferă o protecție reală. În vederea îmbunătățirii acestei situații, grupul de lucru a propus Comisiei să aibă în vedere instituirea unor mecanisme bazate pe responsabilitate, cu accent special pe posibilitatea de a introduce „principiul responsabilității" în Directiva revizuită privind protecția datelor[1]. Acest principiu ar consolida rolul operatorului de date și ar spori responsabilitatea acestuia.

3. Pe scurt, un principiu legal al responsabilității ar obliga explicit operatorii de date să aplice măsuri adecvate și eficace în vederea garantării principiilor și obligațiilor prevăzute în directivă și să dovedească acest lucru la cerere. Acest lucru ar trebui

---

[1] „Pentru a soluționa această problemă, ar trebui introdus în cadrul global un principiu al responsabilității. În temeiul acestui principiu, operatorii de date avea obligația să ia măsurile necesare pentru a se asigura că principiile și obligațiile esențiale ale directivei actuale sunt respectate în prelucrarea datelor cu caracter personal. O astfel de dispoziție ar consolida necesitatea de a crea politici și mecanisme care să transpună în realitate principiile și obligațiile conținute de actuala directivă. Ar consolida necesitatea de a lua măsuri eficiente, având ca rezultat o punere în aplicare efectivă pe plan intern a principiilor și obligațiilor conținute în directivă. În plus, principiul responsabilității ar obliga operatorii de date să dispună de mecanismele interne necesare pentru a-și demonstra (părților externe interesate, inclusiv autorităților naționale însărcinate cu protecția datelor) conformitatea. Necesitatea de a furniza dovezi privind măsurile adecvate luate în vederea asigurării conformității vor facilita în mare măsură punerea în practică a normelor aplicabile" (WP168, punctul 79] Pentru mai multe informații, a se vedea, de asemenea, punctele 74-78.

să se traducă în practică prin programe scalabile, care să urmărească aplicarea principiilor de protecție a datelor existente (denumite uneori „programe de asigurare a conformității"). Ca o completare a acestui principiu, ar putea fi definite cerințe specifice suplimentare care urmăresc aplicarea garanțiilor de protecție a datelor sau asigurarea eficacității acestora. Un exemplu în acest sens ar fi o dispoziție care să solicite realizarea unei evaluări a impactului asupra protecției vieții private a operațiunilor de prelucrare a datelor cu risc ridicat.

4. Prezentul aviz se întemeiază pe contribuțiile anterioare pe acest subiect ale grupului de lucru instituit în temeiul articolului 29, formulate în avizul privind viitorul protecției vieții private, în vederea consilierii Comisiei în cadrul procesului de revizuire în curs a Directivei 95/46/CE. În acest scop, avizul este structurat în patru secțiuni. Prima secțiune analizează necesitatea, pentru operatorii de date, de a-și consolida practicile interne (politici și proceduri) pentru a se asigura că fiecare prelucrare se realizează în conformitate cu normele aplicabile, și de a vedea cum pot contribui la realizarea acestui obiectiv sistemele bazate pe responsabilitate. Se analizează în continuare felul în care ar trebui să arate arhitectura juridică a unui sistem bazat pe responsabilitate, precum și precedentele existente în domeniul protecției datelor și în alte domenii. Cea de a doua secțiune înaintează o propunere concretă de principiu al responsabilității și descrie motivația din spatele fiecărui aspect al propunerii. A treia secțiune analizează diferite elemente referitoare la un sistem juridic, care integrează un sistem general bazat pe responsabilitate. Această secțiune include o analiză a necesității ca o astfel de propunere să furnizeze securitate juridică, fiind în același timp formulată în termeni suficient de generali încât să permită scalabilitatea (să permită stabilirea măsurilor concrete și a metodelor de verificare care să fie aplicate în funcție de riscul prelucrării și de tipurile de date prelucrate). Sunt analizate apoi aspecte conexe, cum ar fi raportul cu transferurile internaționale; este furnizată o descriere a avantajului pe care l-ar oferi autorităților de protecție un mecanism bazat pe responsabilitate și este avut în vedere rolul pe care l-ar putea avea certificarea în acest context.

II. RESPONSABILITATE: SCOPURI, ARHITECTURĂ JURIDICĂ, PRECEDENTE ȘI TERMINOLOGIE

II.1 Responsabilitatea ca motor al punerii în aplicare eficace a principiilor privind protecția datelor

5. În ziua de astăzi, există o necesitate și un interes crescând al operatorilor de date de a garanta adoptarea unor măsuri eficace care să asigure o protecție reală a datelor. Există mai multe motive pentru aceasta, care sunt analizate mai jos.

6. În primul rând, asistăm la un așa-numit efect de „afluență a datelor", caracterizat de o creștere continuă a numărului de date cu caracter personal care există, sunt generate, prelucrate și transferate mai departe. Acest fenomen este favorizat atât de progresele tehnologice și anume, de dezvoltarea sistemelor de informații și de comunicații, cât și de creșterea capacității persoanelor de a utiliza și de a interacționa cu tehnologia. Cu cât crește volumul de date disponibile care circulă în lume, cu atât cresc și riscurile de încălcări ale securității datelor. Acest lucru

subliniază încă o dată necesitatea ca operatorii de date să pună în aplicare, atât în sectorul privat, cât și în cel public, mecanisme interne reale și eficace pentru a garanta protecția datelor cu caracter personal.

7. În al doilea rând, volumul în continuă creștere de date cu caracter personal este însoțit de o creștere a valorii acestora, pe plan social, politic și economic. În anumite sectoare, în special în mediul online, datele cu caracter personal au devenit *de facto* moneda de schimb pentru conținutul online. În același timp, din punctul de vedere al societății, există o recunoaștere din ce în ce mai mare a valorii sociale a protecției datelor. În concluzie, cu cât datele cu caracter personal devin mai valoroase pentru operatorii de date din diverse sectoare, cu atât cetățenii, consumatorii și societatea în ansamblul său devin din ce în ce mai conștienți de valoarea acestora, ceea ce la rândul său, susține necesitatea de a aplica măsuri stricte pentru protecția acestora.

8. În fine, din cele de mai sus rezultă că situațiile de încălcare a securității datelor cu caracter personal pot avea efecte negative semnificative pentru operatorii de date din sectorul public și din sectorul privat. Potențiale probleme în funcționarea aplicațiilor eGuvernare, eSănătate ar avea consecințe dezastruoase în plan economic și mai ales, ar genera prejudicii de imagine. Astfel, minimizarea riscurilor, construirea și menținerea unei bune reputații și atragerea încrederii cetățenilor și consumatorilor devin esențiale pentru operatorii de date din toate sectoarele.

9. În concluzie, aspectele menționate mai sus demonstrează că este absolut necesar ca operatorii de date să aplice măsuri reale și efective de protecție a datelor care să asigure o bună guvernanță în materie, reducând în același timp la minimum riscurile de natură juridică, economică și de imagine care pot decurge dintr-o practică deficitară în materie de protecție a datelor. Astfel cum se arată în cele ce urmează, mecanismele bazate pe responsabilitate urmăresc atingerea acestor obiective.

II.2 O posibilă arhitectură juridică globală pentru mecanismele bazate pe responsabilitate

10. Un aspect interesant de analizat în acest context este modul în care cadrul juridic ar putea încuraja operatorii de date să adopte măsuri care să asigure o protecție reală în practică. Cu alte cuvinte, cum ar trebui să arate arhitectura juridică a sistemelor bazate pe responsabilitate.

11. Cu titlu de remarcă preliminară, înainte de a analiza acest subiect, ar trebui subliniat de la început faptul că aceste sisteme nu schimbă și nu afectează în niciun fel principiile de fond ale protecției datelor, dimpotrivă, sunt destinate să le îmbunătățească aplicarea în practică.

12. Un mod de a incita operatorii de date să adopte astfel de măsuri ar fi acela de a insera un principiu al responsabilității în versiunea revizuită a directivei. Efectele preconizate ale unei astfel de dispoziții ar include punerea în aplicare a măsurilor și a procedurilor cu caracter intern în vederea aplicării principiilor existente de protecție a datelor și a garantării eficacității acestora, precum și obligația de a

dovedi acest lucru, la cererea autorităților de protecție a datelor. Astfel cum se va vedea mai jos, tipul de proceduri și mecanisme variază în funcție de riscurile reprezentate de prelucrarea și de natura datelor.

13. În plus față de cele menționate mai sus, ar putea fi avute în vedere, de asemenea, cerințe specifice precum obligația de evalua impactul asupra vieții private în anumite cazuri, sau numirea de responsabili cu protecția datelor. Aceste cerințe specifice ar putea completa principiul general al responsabilității.

14. Grupul de lucru instituit în temeiul articolului 29 recunoaște că operatorii de date ar putea dori să pună în aplicare politici și proceduri care nu sunt prevăzute *stricto sensu* în legislația privind protecția datelor. De exemplu, un operator de date ar putea dori să se angajeze să răspundă într-o perioadă de timp foarte scurtă cererilor de consultare a datelor, chiar dacă legea prevede o anumită flexibilitate, sau ar putea dori să se angajeze să răspundă cererilor de consultare simultan online și offline, pentru a garanta o recepționare promptă și eficientă a acestor informații. Se poate de asemenea imagina o situație în care operatorul de date dorește să depășească cerințele minimale prevăzute de cadrul juridic general. De exemplu, un operator de date ar putea să decidă numirea unui responsabil cu protecția datelor, chiar dacă acest lucru nu este obligatoriu conform legislației existente, sau ar putea să dorească să comande unei terțe părți efectuarea unui audit cu privire la *toate* operațiunile de prelucrare a datelor în vederea evaluării conformității acestora cu cadrul juridic în vigoare. Grupul de lucru instituit în temeiul articolului 29 salută aceste inițiative și ar dori ca noul cadru juridic privind protecția datelor să încurajeze operatorii de date să adopte astfel de măsuri.

15. Potrivit celor menționate mai sus, „arhitectura juridică" a mecanismelor de responsabilitate ar putea să prevadă două niveluri: primul nivel ar consta în cerințele juridice minimale obligatorii pentru *toți* operatorii de date. Acesta ar cuprinde două elemente: punerea în aplicare a măsurilor/procedurilor și păstrarea unei evidențe a acestora. Acest prim nivel ar putea fi completat cu cerințe suplimentare. Al doilea nivel ar cuprinde sisteme voluntare de responsabilitate care merg dincolo de aceste cerințe juridice minimale, în ceea ce privește principiile subsecvente protecției datelor (care prevăd standarde mai ridicate decât cele necesare conform normelor în vigoare) și/sau în ceea ce privește modalitățile de punere în aplicare sau de garantare a eficacității măsurilor (punerea în aplicare a cerințelor care depășesc nivelul minim). Deși recunoaște importanța și avantajele acestor sisteme, prezentul aviz tratează în principal cerințele referitoare la primul nivel, în special la principiul general al responsabilității.

II.3 Principiul responsabilității în domeniul protecției datelor și în alte domenii, și terminologia

Precedente

16. Grupul de lucru instituit în temeiul articolului 29 observă faptul că principiul responsabilității nu este nou în sine. Recunoașterea sa expresă figura deja în orientările Organizației pentru Cooperare și Dezvoltare Economică (OCDE) privind protecția vieții private, adoptate în 1980. La capitolul „principiul

responsabilității", acestea prevăd: „*Un operator de date ar trebui să răspundă pentru respectarea măsurilor care pun în aplicare principiile [materiale] sus-menționate*."

17. Acest principiu a fost inclus recent în mod explicit în „standardele internaționale de la Madrid", elaborate în cadrul Conferinței internaționale a comisarilor pentru protecția datelor și a vieții private"[2]. De asemenea, a fost încorporat în cea mai recentă versiune a proiectului de norme ISO 29100 care instituie cadrul pentru respectarea vieții private[3] și reprezintă unul din principalele concepte ale cadrului APEC pentru protecția vieții private și ale normelor transnaționale ale acestuia în materie.

18. Din punct de vedere reglementar, grupul de lucru instituit în temeiul articolului 29 constată că principiile privind informarea obiectivă, cuprinse în legea canadiană privind protecția informațiilor cu caracter personal și a documentelor electronice, fac referire la responsabilitate. Primul principiu prevede, între altele, elaborarea și punerea în aplicare de politici și practici care să vizeze respectarea celor 10 principii privind informarea obiectivă, și în special, crearea de proceduri pentru primirea plângerilor și a cererilor de informații și soluționarea acestora.

19. În plus față de cele menționate anterior, grupul de lucru privind articolul 29 constată că regulile corporatiste obligatorii („BCR") utilizate în contextul transferurilor internaționale de date reflectă principiul responsabilității. Aceste reguli constituie de fapt coduri de bune practici elaborate și aplicate de organizațiile multinaționale, care conțin măsuri interne având ca obiectiv punerea în aplicare a principiilor privind protecția datelor (precum auditul, programele de formare, rețeaua responsabililor cu protecția vieții private, sistemul de gestionare a plângerilor). Odată revizuite de autoritățile naționale însărcinate cu protecția datelor, se presupune că regulile corporatiste obligatorii oferă garanțiile adecvate pentru transferurile sau categoriile de transferuri de date cu caracter personal între întreprinderi care aparțin aceluiași grup și care au obligația să respecte aceste reguli în temeiul articolului 25 și al articolului 26 alineatul (2) din Directiva 95/46/CE.

20. Există exemple de aplicare a principiului responsabilității în afara domeniului protecției datelor, cum ar fi un program care precizează politicile și procedurile operatorilor de date în vederea garantării conformității cu legislația și reglementările în vigoare. De exemplu, programele de asigurare a conformității sunt obligatorii în temeiul reglementărilor în domeniul serviciilor financiare. În alte situații, aceste programe nu sunt obligatorii, dar sunt încurajate, de exemplu, în domeniul dreptului concurenței. Astfel, în Canada, Comisarul pentru concurență a elaborat politici foarte detaliate în materie de programe corporatiste

---

[2] Persoana responsabilă: „ a. ia toate măsurile necesare pentru respectarea principiilor și obligațiilor prevăzute în acest document și în legislația națională aplicabilă, și b. dispune de mecanismele interne în vigoare pentru a demonstra respectarea acestor principii persoanelor vizate și autorităților de control în exercitarea atribuțiilor lor, conform articolului 23."

[3] În plus față de cele sus-menționate, „Centre for Information Policy Leadership" participă în prezent la o inițiativă care vizează analizarea efectelor principiului responsabilității în materie de protecție a datelor și a vieții private. A se vedea: www.informationpolicycentre.com

de garantare a conformității, programe la care companiile pot decide în mod voluntar dacă aderă sau nu. Comisarul canadian pentru concurență subliniază totuși importanța conformității ca instrument de atenuare a riscurilor și accentuează avantajele juridice, economice și de imagine[4] ale acestei conformități.

Terminologie

21. Termenul „accountability" este un termen uzual din limba engleză, existând un consens larg cu privire la înțelesul său – chiar dacă este dificil de definit în practică. În general, se poate spune totuși că se pune accentul pe modul în care este asumată responsabilitatea și cum poate fi verificat acest lucru. În engleză, „responsability" și „accountability" sunt două fețe ale aceleiași monede și ambele, elemente esențiale ale bunei guvernanțe. Încrederea poate apărea numai atunci când se poate demonstra asumarea eficace a responsabilităților în practică.

22. În cea mai mare parte a limbilor europene, în principal din cauza diversității sistemelor juridice, termenul „accountability" este dificil de tradus. În consecință, există un risc semnificativ de a întâlni interpretări diferite ale termenului și de a ajunge la o lipsă de armonizare. Au fost sugerate alte cuvinte care să redea sensul termenului „accountability".Printre acestea se numără „reinforced responsability" (responsabilitate consolidată), „assurance" (asigurare), „reliability" (fiabilitate), „trustworthiness" (încredere) și, în franceză, „obligation de rendre des comptes"(obligația de a de a răspunde pentru acțiunile întreprinse) etc. S-ar putea, de asemenea, considera că „accountability" face trimitere la „punerea în aplicare a principiilor de protecție a datelor".

23. Prin urmare, în prezentul document, ne concentrăm asupra măsurilor care ar trebui luate sau care ar trebui preconizate pentru a garanta conformitatea în materia protecției datelor. În acest sens trebuie înțeles termenul de „responsabilitate", utilizat în prezentul aviz pentru a face trimitere la „accountability", fără a aduce atingere oricărei alte formule care ar reflecta cu mai multă precizie conceptul vizat aici. Iată de ce prezentul document nu se concentrează asupra termenilor ci, în mod pragmatic, asupra măsurilor care trebuie luate, mai degrabă decât asupra conceptului în sine.

III. SPRE O PROPUNERE DE DISPOZIȚIE GENERALĂ ÎN MATERIE DE RESPONSABILITATE

III.1 O dispoziție generală care vizează reafirmarea și consolidarea responsabilității operatorilor de date

24. Grupul de lucru instituit în temeiul articolului 29 a analizat mai departe posibilitatea de a introduce, în lumina considerentelor evocate în secțiunea I, soluții întemeiate pe responsabilitate în noul cadrul juridic global în materie de protecție a datelor.

---

4 www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02732.html.

25. Această analiză a confirmat punctul de vedere al grupului, formulat deja în avizul privind viitorul protecției vieții private, conform căruia un principiu general al responsabilității ar trebui să fie inclus într-un cadru legislativ complet. Obiectivul unei astfel de dispoziții ar fi acela de a reafirma și de a consolida responsabilitatea operatorilor de date în cadrul misiunii lor de prelucrare a datelor cu caracter personal, și aceasta fără a aduce atingere măsurilor concrete care ar putea completa acest principiu.

26. Această nouă dispoziție ar fi conformă cu dispozițiile specifice existente deja în cadrul legislativ actual. Poate fi citat, în acest sens, articolul 6 din Directiva 95/46/CE, care, în primul alineat, face referire la principiile privind calitatea datelor iar în alineatul al doilea menționează că „operatorul de date trebuie să asigure respectarea primului alineat". Sau, de asemenea, articolul 17 alineatul (1) care solicită operatorilor de date să aplice măsuri de natură tehnică și organizațională. Într-adevăr, o clauză generală de responsabilitate ar consolida efectiv obligația operatorilor de date de a respecta cerințele articolului 17 în materie de securitate, în plus față de alte cerințe prevăzute în alte dispoziții.

III.2 Spre o propunere concretă privind un principiu general de responsabilitate

27. Noua dispoziție ar avea ca obiectiv favorizarea adoptării de măsuri concrete și practice, în vederea transformării principiilor generale de protecție a datelor în politici și proceduri concrete, definite la nivelul operatorului de date, în conformitate cu legile și reglementările aplicabile. Operatorul de date ar trebui să asigure, de asemenea, eficacitatea măsurilor luate și să demonstreze, la cerere, ca a aplicat aceste măsuri.

28. În mod schematic, o astfel de dispoziție generală s-ar concentra pe două elemente importante:

    (i) necesitatea ca operatorul de date să ia măsuri adecvate și eficiente în vederea aplicării principiilor privind protecția datelor;
    (ii) necesitatea de a demonstra la cerere că au fost aplicate măsuri adecvate și eficiente. În consecință, operatorul de date furnizează dovezi privind îndeplinirea cerinței de la punctul (i) de mai sus.

29. Obligația ar trebui să se aplice tuturor operatorilor de date, în toate situațiile.

30. Primul element al obligației solicită operatorilor de date aplicarea de măsuri adecvate. Tipurile de măsuri vizate nu vor fi precizate în textul dispoziției generale privind responsabilitatea. Orientări ulterioare furnizate de autoritățile naționale însărcinate cu protecția datelor, de Grupul de lucru instituit în temeiul articolului 29 și de Comisie (prin procedurile de comitologie) ar putea preciza, pentru anumite cazuri, un set minim de măsuri specifice, considerate ca fiind adecvate. Un exemplu de astfel de măsuri ar fi adoptarea, în anumite situații, de politici și procese interne necesare pentru punerea în aplicare a principiilor de protecție a datelor, care ar reflecta legislația și reglementările aplicabile.

31. Punerea în aplicare a acestor măsuri şi procese ar putea fi realizată, de asemenea, într-un mod eficace, prin atribuirea responsabilităţilor şi formarea membrilor personalului care participă la operaţiunile de prelucrare. În special, conform articolului 18 din directivă, operatorii de date ar trebui încurajaţi să numească funcţionari responsabili cu protecţia datelor cu caracter personal. În orice caz, ar trebui încurajată atribuirea responsabilităţii la diferite niveluri ale organizaţiei pentru a garanta asumarea acestor responsabilităţi.

32. În ceea ce priveşte transferurile de date cu caracter personal în afara Uniunii Europene, operatorii de date ar trebui să adopte şi să pună în aplicare măsuri adecvate pentru a se conforma cerinţei, prevăzute la articolul 26 din directivă, de a furniza „garanţii suficiente", cum ar fi regulile corporatiste obligatorii.

33. De asemenea, operatorii de date ar trebui să garanteze că măsurile practice puse în aplicare pentru a respecta principiile de protecţie a datelor sunt eficace. În cazul prelucrărilor de date de o mai mare amploare, mai complexe sau care prezintă un risc ridicat, eficacitatea măsurilor adoptate ar trebui verificată periodic. Există diferite modalităţi de a evalua eficacitatea (sau ineficacitatea) măsurilor: controale, audit intern şi extern etc.

34. În baza celor enunţate mai sus, grupul de lucru instituit în temeiul articolului 29 a analizat conţinutul unei propuneri de dispoziţie concretă care ar putea fi introdusă într-un cadru legislativ global şi care ar putea fi formulată după cum urmează:

„Articolul X – Punerea în aplicare a principiilor privind protecţia datelor

1. Operatorul de date aplică măsuri adecvate şi eficace în vederea garantării respectării principiilor şi a obligaţiilor prevăzute în directivă.
2 Operatorul de date demonstrează autorităţii de supraveghere, la cerere, respectarea alineatului (1).

IV. ANALIZAREA DIFERITELOR ELEMENTE LEGATE DE PRINCIPIUL GENERAL AL RESPONSABILITĂŢII

IV.1 Consolidarea obligaţiilor existente

35. Grupul de lucru instituit în temeiul articolului 29 constată că anumiţi operatori de date ar putea percepe principiul general al responsabilităţii ca o sursă de noi cerinţe juridice împovărătoare pentru ei, dată fiind, în special, situaţia economică dificilă actuală existentă la nivelul Uniunii Europene. Aceasta ar fi o greşeală.

36. Grupul de lucru instituit în temeiul articolului 29 doreşte să sublinieze faptul că majoritatea cerinţelor prevăzute în această nouă dispoziţie există de fapt la ora actuală, deşi sunt mai puţin explicite în legislaţia existentă. În temeiul cadrului juridic existent, operatorii de date au deja obligaţia de a respecta principiile şi obligaţiile stabilite de directivă. Pentru a realiza acest lucru, în mod implicit este necesară instituirea şi eventual, verificarea procedurilor referitoare la protecţia datelor. Din această perspectivă, o dispoziţie privind responsabilitatea nu reprezintă o mare noutate şi în general, nu impune cerinţe care să nu existe deja în

mod implicit în legislația în vigoare. În concluzie, noua dispoziție nu urmărește să supună operatorii de date unor noi principii ci, mai degrabă, să asigure respectarea eficace, *de facto*, a celor existente.

37. De fapt, o evoluție legislativă oarecum similară a avut loc în 2009, cu ocazia modificării Directivei 2002/58[5]. În acest caz, legea impunea o obligație de punere în aplicare a unei politici de securitate, și anume, să se „*asigure punerea în aplicare a unei politici de securitate în ceea ce privește prelucrarea datelor cu caracter personal*." Astfel, în ceea ce privește dispozițiile referitoare la securitate conținute de această directivă, legiuitorul a decis că era necesar să se introducă o cerință explicită de elaborare și de punere în aplicare a unei politici de securitate. În plus, articolul 18 din Directiva 95/46 referitor la desemnarea funcționarilor responsabili cu protecția datelor, precum și sistemul de reguli corporatiste obligatorii sus-menționat, oferă deja exemple de măsuri practice care pot fi adoptate de operatorii de date.

38. Consecințele respectării (sau nerespectării) principiului responsabilității reprezintă o altă chestiune legată de punctul de mai sus. Grupul de lucru instituit în temeiul articolului 29 subliniază faptul că principiul responsabilității nu presupune în mod necesar că operatorul de date respectă principiile de fond prevăzute în directivă; cu alte cuvinte, principiul responsabilității nu oferă o prezumție legală de conformitate și nu înlocuiește niciunul din aceste principii. Este posibil ca un operator de date să pună în aplicare și să verifice măsurile pe care le-a aplicat și cu toate acestea, să comită o neregulă. În consecință, adoptarea de către un operator de date de măsuri care respectă principiile nu trebuie în nici un caz să îl protejeze de măsurile coercitive care ar putea fi luate împotriva sa de autoritățile de protecție a datelor. În practică, operatorii de date din sectorul public și din sectorul privat care au adoptat măsuri în cadrul unor programe solide de asigurare a conformității sunt mai susceptibili de a respecta legea. Într-adevăr, întrucât au aplicat măsuri eficace destinate respectării principiilor de fond privind protecția datelor, este mai puțin probabil ca aceștia să încalce legea. Prin urmare, în evaluarea sancțiunilor referitoare la încălcarea principiilor privind protecția datelor, autoritățile de protecție a datelor ar putea să țină cont de punerea în aplicare (sau de absența punerii în aplicare) a măsurilor și de verificarea acestora.

IV.2 Măsuri adecvate în vederea punerii în aplicare a dispozițiilor directivei

39. O dispoziție privind responsabilitatea ar obliga operatorii de date să definească și să pună în aplicare măsurile necesare pentru a garanta respectarea principiilor și obligațiilor cuprinse în directivă și pentru a verifica periodic eficacitatea acestora.

40. Principiul general de responsabilitate propus evită în mod intenționat detalierea tipului de măsuri care trebuie să fie puse în aplicare. Acest lucru ridică următoarele două probleme esențiale și conexe: *(i)* ce măsuri comune ar permite

---

[5] Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului

aplicarea principiului responsabilității? *(ii)* cum pot fi adaptate măsurile unor circumstanțe specifice?

Măsuri: exemplificare

41. Grupul de lucru instituit în temeiul articolului 29 consideră că măsurile comune de responsabilitate ar putea include lista neexhaustivă următoare:

    - instituirea unor proceduri interne *anterior* inițierii unor noi operațiuni de prelucrare a datelor cu caracter personal (control intern, evaluare etc.)[6];
    - introducerea unor politici scrise și obligatorii de protecție a datelor de care să se țină seama și care să fie aplicate noilor operațiuni de prelucrare a datelor (de exemplu, respectarea criteriilor de calitate a datelor, preavizul, principiile de securitate, consultarea etc.), care ar trebui să fie puse la dispoziția persoanelor vizate;
    - trecerea în revistă a procedurilor în vederea asigurării identificării adecvate a tuturor operațiunilor de prelucrare a datelor și păstrarea unei evidențe cu privire la acestea;
    - numirea unui responsabil cu protecția datelor și a altor persoane cu responsabilități în domeniul protecției datelor;
    - furnizarea unei protecții adecvate a datelor, formarea și pregătirea membrilor personalului. Dintre aceștia ar trebui să facă parte acele persoane cu atribuții în prelucrarea (sau responsabile de prelucrarea) datelor cu caracter personal (cum ar fi directorii de resurse umane) dar și directorii IT, dezvoltatorii și directorii de entități operaționale. Ar trebui puse la dispoziție resurse suficiente pentru gestionarea protecției vieții private etc.
    - instituirea de proceduri pentru gestionarea cererilor de consultare, de corectare și de ștergere a datelor, care ar trebui să fie transparente pentru persoanele vizate;
    - crearea unui mecanism intern de gestionare a plângerilor;
    - instituirea unor proceduri interne pentru gestionarea și semnalarea eficace a situațiilor de încălcare a securității datelor;
    - efectuarea unor evaluări ale impactului asupra vieții private în circumstanțe specifice;
    - punerea în aplicare și supravegherea procedurilor de verificare pentru a garanta faptul că toate măsurile există nu doar pe hârtie ci sunt aplicate și funcționează în practică (audit intern sau extern etc.).

42. Ar putea fi avută în vedere și o strategie complementară principiului general al responsabilității. În această ipoteză, cadrul juridic ar putea să includă nu doar un principiu general al responsabilității, ci și o listă orientativă de măsuri care ar putea fi încurajate la nivel național[7]. Această dispoziție ar putea conține o listă

---

[6] Operațiunile existente de prelucrare a datelor ar avea nevoie de o perioadă de tranziție pentru a se asigura conformitatea acestora cu legea.

[7] De exemplu, standardele internaționale adoptate la Madrid de către autoritățile de protecție a datelor prevăd, la articolul 22, o dispoziție privind măsuri proactive, cu următorul text: „*Statele, prin intermediul legislației lor naționale, ar trebui să încurajeze punerea în aplicare, de către persoanele implicate în oricare din etapele prelucrării, a măsurilor vizând promovarea unei mai bune respectări a legislației aplicabile privind protecția dreptului la viață privată, cu privire la prelucrarea datelor cu caracter personal. Aceste măsuri ar putea include, printre altele:*

orientativă și neexhaustivă de măsuri care ar putea constitui un „set de instrumente utile" pentru operatorii de date. Aceasta ar furniza, de asemenea, orientări operatorilor cu privire la ce ar putea constitui, după caz, măsuri adecvate de adoptat de către aceștia. Această listă exemplificativă nu ar face, bineînțeles, decât să însoțească obligația legală generală de a adopta măsuri adecvate.

Scalabilitatea măsurilor

43. Lista de mai sus cuprinde cu titlu exemplificativ măsurile pe care operatorii de date ar putea să le aplice pentru a se conforma primei părți a principiului responsabilității (*Operatorul aplică măsuri adecvate și eficace în vederea garantării respectării principiilor și obligațiilor prevăzute în directivă.).*

44. Câteva din aceste măsuri reprezintă „măsuri fundamentale", care vor trebui puse în aplicare în majoritatea operațiunilor de prelucrare a datelor. Elaborarea de politici și proceduri interne vizând aplicarea principiilor (proceduri privind gestionarea cererilor de consultare, gestionarea plângerilor) ar putea constitui exemple de măsuri adecvate în cazul anumitor prelucrări de date. Pertinența măsurilor va trebui să fie decisă de la caz la caz. Revine operatorilor de date obligația de a lua aceste decizii, pe baza orientărilor emise de autoritățile naționale însărcinate cu protecția datelor și de grupul de lucru instituit în temeiul articolului 29, acolo unde este cazul (a se vedea mai jos).

45. Din cele de mai sus rezultă că, pentru stabilirea tipurilor de măsuri care să fie aplicate, nu există alte opțiuni în afara celor „pe măsură". Într-adevăr, măsurile specifice care trebuie aplicate trebuie stabilite în funcție de faptele și circumstanțele fiecărui caz în parte, acordându-se o atenție specială riscului

---

a) punerea în aplicare a unor proceduri de prevenire și detectare a încălcărilor, care s-ar putea baza pe modele standardizate de guvernanță și/sau gestionare a securității informațiilor;

b) numirea unuia sau mai multor responsabili cu protecția datelor, cu calificare corespunzătoare, care dispun de resurse și au competențe suficiente pentru exercitarea în mod corespunzător a atribuțiilor lor de supraveghere;

c) implementarea periodică a unor programe de formare, de pregătire și de sensibilizare a membrilor organizației care au ca scop o mai bună înțelegere a legislației aplicabile privind protecția dreptului la viață privată în raport cu prelucrarea datelor cu caracter personal, precum și a procedurilor instituite de organizație în acest scop;

d) realizarea periodică a unor audituri transparente, de către părți calificate și, de preferință, independente, care să verifice respectarea legislației aplicabile privind protecția dreptului la viață privată în raport cu prelucrarea datelor cu caracter personal, precum și a procedurilor instituite de organizație în acest scop;

e) adaptarea sistemelor informatice și/sau a tehnologiilor informației pentru prelucrarea datelor cu caracter personal la legislația aplicabilă privind protecția dreptului la viață privată în raport cu prelucrarea datelor cu caracter personal, în special în momentul în care se decide cu privire la specificațiile tehnice ale acestora și cu privire la dezvoltarea și punerea lor în aplicare;

f) aplicarea evaluărilor impactului asupra protecției vieții private anterior punerii în aplicare a unor noi sisteme informatice și/sau tehnologii ale informației pentru prelucrarea datelor cu caracter personal, precum și anterior introducerii unor noi metode de prelucrare a datelor sau a unor modificări substanțiale ale prelucrării în curs.

g) adoptarea de coduri de bune practici obligatori,i care cuprind elemente ce permit măsurarea eficienței acestora în materie de respectare și de nivel de protecție a datelor cu caracter personal și care prevăd măsuri eficace în caz de nerespectare;

h) punerea în aplicare a unui plan de intervenție care stabilește orientările pentru acțiunile de întreprins în ipoteza unei încălcări a legislației aplicabile privind protecția dreptului la viață privată în raport cu prelucrarea datelor cu caracter personal, incluzând cel puțin obligația de a stabili cauza și gravitatea încălcării, de a descrie efectele sale prejudiciabile și de a lua măsurile adecvate în vederea evitării încălcărilor viitoare."

prelucrării și tipurilor de date. O abordare unitară ar obliga operatorii de date să adopte structuri care nu ar fi potrivite și care, în final, s-ar solda cu un eșec.

46. În temeiul acestei abordări, operatorii ar trebui să poată adapta măsurile la specificitățile situației lor particulare și la operațiunile de prelucrare vizate. În acest context, grupul de lucru instituit în temeiul articolului 29 reamintește criteriile utilizate la articolul 17 din directivă[8] în vigoare în vederea stabilirii tipului de măsuri de securitate care să fie aplicate, și anume, riscurile reprezentate de prelucrarea datelor și de natura datelor. Acești doi factori pot fi utilizați în mod analog pentru a stabili tipurile generale de măsuri care trebuie aplicate. Mai concret, aspecte precum amploarea operațiunii/operațiunilor de prelucrare a datelor, scopurile urmărite și numărul de transferuri de date avute în vedere pot determina gradul de risc. Tipul de date, inclusiv eventualul lor caracter sensibil, ar trebui de asemenea avut în vedere. O analiză a nevoii de a impune anumite obligații operatorului de date sau designerilor și/sau producătorilor de ICT (tehnologii ale informațiilor și ale comunicațiilor) ar putea fi, de asemenea, realizată din perspectiva principiului responsabilității.

47. Chiar dacă respectă aceste criterii, operatorii de date de talie mare ar trebui, în principiu, să aplice măsuri stricte. În anumite cazuri, dacă, de exemplu, efectuează operațiuni riscante de prelucrare a datelor precum cele privind datele din dosarele medicale online, operatorii de talie mică sau mijlocie pot fi obligați să introducă măsuri stricte de protecție. Spre exemplu, o administrație locală (o primărie), o întreprindere multinațională, o întreprindere mică online, o organizație pentru care prelucrarea datelor reprezintă activitatea de bază sau o organizație cu antecedente privind încălcarea legii ar avea nevoie de măsuri specifice proprii în vederea asigurării unei guvernanțe credibile și eficace a informației. În cazuri simple, cum ar fi prelucrarea datelor cu caracter personal referitoare la resursele umane în vederea creării unei baze de date pentru o întreprindere, „obligația de a dovedi" prevăzută la alineatul (2) din dispoziția privind responsabilitatea ar putea fi îndeplinită ușor (de exemplu, prin note de informare, prin descrierea măsurilor elementare de securitate etc.). În schimb, în alte situații mai complexe, care implică, de exemplu, utilizarea unor instrumente biometrice inovatoare, îndeplinirea „obligației de a dovedi" ar putea necesita măsuri suplimentare. Astfel, s-ar putea ca operatorul să trebuiască să dovedească faptul că a efectuat o evaluare a impactului asupra vieții private, că membrii personalului care realizează prelucrarea au fost formați și sunt informați periodic etc.

48. Transparența face parte din numeroase măsuri de responsabilitate. Transparența față de subiecții datelor și față de public în general contribuie la responsabilizarea operatorilor de date. Un grad mai mare de responsabilitate se obține, de exemplu, prin publicarea pe Internet a politicilor privind viața privată, prin asigurarea transparenței în ceea ce privește procedurile interne de gestionare a plângerilor și prin publicarea de rapoarte anuale.

---

8 *„Având în vedere cele mai noi tehnici din sector și costurile punerii lor în aplicare, aceste măsuri trebuie să asigure un nivel de securitate adecvat riscurilor prezentate de prelucrare și de natura datelor de protejat".*

Orientări și securitate juridică

49. Deși nevoia de scalabilitate și deci de flexibilitate militează în favoarea unui limbaj deschis, grupul de lucru instituit în temeiul articolului 29 este conștient de faptul că o dispoziție foarte generală, care lasă loc flexibilității și scalabilității poate genera și incertitudine. Operatorii pot considera astfel că dispoziția nu este suficient de detaliată pentru a oferi securitate juridică. Aceștia pot fi nesiguri în privința nivelului de detaliu cerut în cadrul politicilor și procedurilor privind protecția vieții private, în privința momentului și a modului de desemnare a unui responsabil cu protecția datelor, în privința momentului optim pentru organizarea sesiunilor de formare etc. Această incertitudine se poate manifesta și cu privire la tipul de control necesar extern, sau intern. Mai mult, operatorii de date se pot teme că li se impun interpretări naționale divergente și arbitrare în ceea ce privește obiectul și natura obligațiilor lor.

50. Grupul de lucru instituit în temeiul articolului 29 înțelege această îngrijorare. Cu toate acestea, pentru motivele menționate mai sus privind nevoia de flexibilitate și scalabilitate, soluția pentru a obține securitate juridică nu poate fi prevăzută în directivă. Pentru a atinge securitatea juridică necesară, grupul de lucru consideră că ar putea fi utilă armonizarea orientărilor emise de Comisie (prin intermediul măsurilor tehnice de punere în aplicare, de exemplu) și/sau de grupul de lucru, pentru a oferi o mai mare securitate și pentru a elimina eventualele divergențe în aplicare[9]. Grupul de lucru instituit în temeiul articolului 29 ar putea, de asemenea, să elaboreze orientări generale care să schițeze elementele necesare pentru un operator de date standard. Această bază de plecare ar putea fi adaptată nevoilor specifice ale fiecărui operator de date.

51. Ar putea fi, de asemenea, utilă elaborarea *unui model de program de conformitate a datelor, care ar servi ca bază pentru operatorii de date de talie mijlocie și mare* în elaborarea propriilor programe, așa cum s-a procedat și în cazul BCR, pe baza orientărilor elaborate de grupul de lucru instituit în temeiul articolului 29[10]. Aceste modele ar trebui create în urma unei analize atente a practicilor și a modelelor disponibile în vigoare și cu consultarea tuturor părților interesate. Acesta este un domeniu în care va fi necesară implicarea serioasă a tuturor părților interesate.

Eficacitatea măsurilor

52. Aceleași problemele analizate mai sus privind măsurile aplicabile apar și în contextul garantării eficacității acestor măsuri. Mijloacele de garantare a eficacității măsurilor diferă în funcție de tipul prelucrării de date.

---

9 Un exemplu de o astfel de orientare este instrumentul de autoevaluare PIPEDA publicat de Biroul Comisarului pentru viața privată din Canada pentru a sprijini operatorii de talie medie și mare să elaboreze și să pună în aplicare o bună guvernanță și gestionare a vieții private. Instrumentul de autoevaluare este disponibil la adresa: http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.pdf .

10 Documentul 153 al grupului de lucru instituit în temeiul articolului 29 care cuprinde un tabel cu elementele și principiile care se regăsesc în regulile corporatiste obligatorii și documentul 154 care cuprinde un cadru pentru structura regulilor corporatiste obligatorii.

53. Pot exista diferite modalități de a evalua eficacitatea (sau ineficacitatea) măsurilor de către operatorii de date. În cazul prelucrărilor de date de o mai mare amploare, mai complexe, sau care prezintă un risc ridicat, auditurile interne sau externe sunt metoda obișnuită de verificare. Modul în care sunt realizate auditurile poate, de asemenea, să varieze, de la auditul complet și până la auditul negativ (care, la rândul lor, pot îmbrăca diferite forme). Pentru a hotărî modalitățile de garantare a eficacității măsurilor, grupul de lucru instituit în temeiul articolului 29 sugerează utilizarea acelorași criterii ca și cele folosite pentru măsuri, care rezultă din articolul 17 al Directivei 95/46/CE, și anume, riscurile reprezentate de prelucrarea datelor și de natura acestora. Prin urmare, modul în care un operator va garanta eficacitatea măsurilor va depinde de caracterul sensibil al datelor, de volumul de date prelucrate și de riscurile particulare asociate operațiunilor de prelucrare a datelor. Orientările grupului de lucru instituit în temeiul articolului 29 cu privire la măsuri pot să includă și orientări cu privire la acest aspect.

IV.3 Corelarea cu alte cerințe

Notificări prealabile

54. Ar putea fi realizată o analiză cu privire la impactul posibil asupra notificărilor prealabile al definirii garanțiilor adecvate la nivelul operatorului de date. S-ar putea considera că anumite mecanisme de responsabilitate ar putea înlocui sau ar putea diminua cerințele administrative din legislația actuală privind protecția datelor, cum a fost sugerat deja în avizul privind viitorul protecției vieții private emis de grupul de lucru instituit în temeiul articolului 29.

Transferuri internaționale de date

55. Regulile corporatiste obligatorii sunt un exemplu privind modul în care principiile privind protecția datelor ar putea fi puse în aplicare pe baza principiului responsabilității. Acestea constituie o modalitate recunoscută și acceptată de grupul de lucru, de furnizare a garanțiilor adecvate pentru transferurile în afara Uniunii Europene.

56. Este vorba despre un domeniu în care ar fi utilă o analiză aprofundată în lumina revizuirii Directivei 95/46/CE. Ar fi important să se analizeze în special dacă articolul 26 alineatul (2) din directivă („*un stat membru poate autoriza un transfer [...] în cazul în care operatorul oferă garanții suficiente[...]*; *aceste garanții pot rezulta în special din clauze contractuale adecvate*”) acoperă în întregime regulile corporatiste obligatorii și, eventual, alte mecanisme similare de responsabilitate, ca instrumente care permit oferirea de garanții adecvate.

57. În acest context, ar fi interesantă evaluarea, între altele, a mecanismelor utilizate intern de către operatorii de date pentru punerea în aplicare a principiilor și a obligațiilor de protecție a datelor, precum și a sistemelor de verificare. De asemenea, ar fi relevantă analizarea mecanismelor care ar permite raționalizarea sistemului actual bazat pe autorizarea transferurilor de date de către autoritățile naționale însărcinate cu protecția datelor.

IV.4 Rolul autorităților însărcinate cu protecția datelor

58. Se pune totuși o întrebare: principiul responsabilității propus în prezentul aviz va afecta atribuțiile autorităților însărcinate cu protecția datelor, în special, în ceea ce privește domeniul de punere în aplicare? Cum se va arăta mai jos, principiul nu va priva autoritățile însărcinate cu protecția datelor de nici o prerogativă. Din contră, va fi benefic pentru acestea.

59. În ceea ce privește aplicarea, principiul, astfel cum este propus, recunoaște competența autorităților însărcinate cu protecția datelor de a solicita operatorului de date să dovedească respectarea principiului responsabilității, contribuind astfel la consolidarea activităților acestor autorități. Acest lucru garantează că autoritățile rămân competente pentru a lua măsuri coercitive în orice moment. Trebuie subliniat faptul că, în orice caz, autoritățile însărcinate cu protecția datelor rămân competente să supravegheze nu numai măsurile adoptate de operatorii de date, ci, mai ales, respectarea principiilor și a obligațiilor subiacente.

60. Mai mult, punerea în aplicare a principiului responsabilității va furniza informații utile autorităților însărcinate cu protecția datelor, care le vor putea utiliza pentru a supraveghea gradul de conformitate a măsurilor. Într-adevăr, întrucât operatorii de date vor trebui să fie capabili să dovedească autorităților dacă și în ce măsură au aplicat măsurile, informații foarte pertinente în materie de conformitate vor fi puse astfel la dispoziția autorităților. Acestea vor putea astfel să folosească aceste informații în contextul acțiunilor lor de punere în aplicare. În plus, în cazul în care aceste informații nu sunt furnizate la cerere, autoritățile însărcinate cu protecția datelor vor avea un motiv întemeiat de a acționa împotriva operatorilor de date, independent de pretinsa încălcare a altor principii subiacente de protecție a datelor.

61. Acest principiu ar trebui, de asemenea, să fie determinant pentru autoritățile însărcinate cu protecția datelor, deoarece le-ar ajuta să devină mai selective și mai strategice, permițându-le să își investească resursele pentru a genera un grad cât mai mare de conformitate.

62. Grupul de lucru instituit în temeiul articolului 29 constată că principiul responsabilității ar putea contribui la acumularea unei experiențe juridice și tehnice în domeniul punerii în aplicare a cerințelor privind protecția datelor. Persoanele care posedă cunoștințe solide, precum și o bună înțelegere a aspectelor de natură tehnică și juridică privind protecția datelor, dar care au și abilități de comunicare și de formare a personalului, de elaborare și punere în aplicare a politicilor și a auditurilor, vor fi indispensabile în acest domeniu. O astfel de experiență va fi necesară atât în intern, cât și sub forma unui serviciu extern la care vor putea apela întreprinderile. Această evoluție se va dovedi capitală, prin aceea că va permite operatorilor de date să își îndeplinească obligațiile, inclusiv, dacă este necesar, prin realizarea de audituri interne sau externe. În același timp, această evoluție va fi benefică pentru autoritățile însărcinate cu protecția datelor, pentru că, în măsura în care sistemul va contribui la conformitatea globală, autoritățile vor avea la dispoziție mai multe informații solide privind practicile interne ale întreprinderilor, iar formarea de profesioniști cu înaltă calificare în

domeniul protecției datelor va facilita, fără îndoială, interacțiunea acestora cu operatorii de date.

63. Se poate concluziona că activitatea autorităților însărcinate cu protecția datelor se concentrează mai mult pe un rol „ex post" decât pe un rol „ex ante". Întrucât responsabilitatea pune accent pe anumite rezultate care trebuie obținute în materie de bună guvernanță în domeniul protecției datelor, se consideră că aceasta este orientată spre rezultate, cu un accent „ex post" (cu alte cuvinte, responsabilitatea intervine după începerea prelucrării datelor).

IV. 5 Sancțiuni

64. Sistemul propus poate funcționa doar dacă autorităților însărcinate cu protecția datelor li se încredințează competențe importante în materie de sancțiuni. Astfel, în momentul și în cazul în care operatorii de date nu respectă principiul responsabilității, trebuie să poată fi aplicate sancțiuni importante. De exemplu, un operator de date care nu își onorează angajamentele luate în temeiul politicilor interne ar trebui să poată fi pedepsit. Bineînțeles, acest lucru se adaugă încălcării propriu-zise a principiilor de fond de protecție a datelor.

65. În plus față de cele de mai sus, grupul de lucru instituit în temeiul articolului 29 consideră că atribuțiile autorităților însărcinate cu protecția datelor ar trebui să includă posibilitatea de a impune operatorilor de date instrucțiuni precise cu privire la sistemul lor de conformitate.

IV.6 Dezvoltarea de programe de certificare

66. Pe termen lung, dispoziția privind responsabilitatea poate încuraja dezvoltarea de programe și sigilii de certificare. Astfel de programe ar contribui la dovedirea faptului că un operator de date a respectat dispozițiile, și anume, că a definit și a aplicat măsuri adecvate care au fost auditate periodic. Această dezvoltare poate fi favorizată de diverși factori.

67. În general, este de așteptat ca, pentru a se diferenția de concurență, serviciile de evaluare a impactului asupra vieții private/de audit/de protecție a datelor să propună din ce în ce mai multe certificate și sigilii. Operatorii de date vor putea astfel decide să recurgă la servicii demne de încredere care furnizează certificate. Atunci când anumite sigilii vor fi recunoscute pentru testele riguroase, operatorii de date vor putea să le prefere pe acestea pentru a beneficia de un „confort" sporit în materie de conformitate și pentru a avea un atu în fața concurenței.

68. Recurgerea la regulile corporatiste obligatorii ca temei juridic pentru transferurile internaționale de date obligă operatorii de date să dovedească faptul că au instituit garanții adecvate, caz în care autoritățile însărcinate cu protecția datelor pot să autorizeze transferurile. Acesta este un domeniu în care serviciile de certificare ar putea fi utile. Aceste servicii ar analiza garanțiile furnizate de operatorul de date și, după caz, le-ar certifica. O autoritate însărcinată cu protecția datelor ar putea utiliza în acest caz certificarea furnizată de un anumit program de certificare în analiza pe care o efectuează cu privire la regulile corporatiste obligatorii pentru a afla dacă un operator de date a furnizat garanții suficiente pentru transferurile

internaționale de date. Acest lucru ar contribui la simplificarea procesului de autorizare a acestor tipuri de transferuri.

IV.7 Reglementarea programelor de certificare

69. Aceleași motive care favorizează dezvoltarea de servicii de certificare stau și la baza necesității de reglementare a acestor servicii. Într-adevăr, dacă aceste servicii au ca scop furnizarea de probe fiabile de conformitate în materie de protecție a datelor (autorităților, operatorilor de date și consumatorilor în general) și dacă acestea se integrează fără probleme pe piața internă, apare necesară definirea regulilor pentru furnizarea acestor servicii. Autoritățile însărcinate cu protecția datelor ar trebui să aibă un rol cheie în elaborarea acestor reguli (de exemplu, modele de referință etc.) și ar trebui să fie în măsură să definească regulile pentru punerea în aplicare a acestora, ceea ce presupune că dispun de resurse suficiente în acest sens. Mai mult, autoritățile însărcinate cu protecția datelor ar trebui să joace un rol în certificarea organismelor de certificare, mai ales în domeniul transferurilor internaționale de date. Întrucât calitatea serviciilor și necesitatea respectării regulilor pieței interne sunt criterii cheie, legislația ar trebui să stabilească condițiile care permit atingerea acestei calități. Acest lucru nu poate fi lăsat la latitudinea pieței, experiența în alte domenii și în special în domeniul certificării mărfurilor, demonstrând o tendință scădere a calității. Concurența între prestatorii de servicii ar putea conduce la o scădere a prețurilor și chiar la o anumită flexibilitate a procedurilor. În concluzie, fie că sunt adoptate sau nu la nivel transfrontalier, regulile par a fi necesare pentru garantarea unei bune calități a serviciilor și a unor condiții echitabile de piață.

70. Grupul de lucru instituit în temeiul articolului 29 constată că legislația existentă în materie de acreditare[11] poate fi aplicabilă serviciilor de certificare în domeniul protecției datelor. Această legislație furnizează deja structura necesară pentru stabilirea regulilor în materia organizării și funcționării organismelor de acreditare. Aceste reguli se aplică acreditării voluntare și cazurilor specifice în care acreditarea este obligatorie.

71. În mod evident, acest tip de serviciu ar favoriza, de asemenea, armonizarea normelor subiacente pe baza cărora se va realiza evaluarea entităților. Orientările menționate (provenind de la grupul de lucru instituit în temeiul articolului 29 sau de la Comisie), care definesc modelele de programe de conformitate a datelor vor juca un rol primordial în acest sens.

V. CONCLUZII

72. Dezvoltarea de noi tehnologii și globalizarea din ce în ce mai accentuată au condus la o proliferare a informațiilor cu caracter personal care sunt colectate, triate, transferate sau păstrate în alte scopuri. Riscurile asociate acestor date au cunoscut și ele o creștere exponențială.

---

[11] Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93

73. Grupul de lucru instituit în temeiul articolului 29 este convins de faptul că această creștere, atât a riscurilor cât și a valorii datelor cu caracter personal, justifică în sine consolidarea rolului și a responsabilității operatorilor de date. Un cadru de reglementare care să țină cont de această nouă realitate trebuie să prevadă instrumentele necesare în vederea încurajării operatorilor de date să pună în practică măsuri adecvate și eficace care să garanteze că principiile de protecție a datelor vor da rezultate. Proceduri având ca obiectiv identificarea tuturor operațiunilor de prelucrare a datelor, răspunsul la cererile de consultare și alocarea judicioasă a resurselor, inclusiv desemnarea persoanelor responsabile de organizarea conformității în materie de protecție a datelor, reprezintă exemple de astfel de măsuri.

74. În vederea încurajării protecției datelor în practică, grupul de lucru instituit în temeiul articolului 29 sugerează în primul rând includerea în propunerile de modificare a directivei privind protecția datelor a unei noi dispoziții prin care se solicită operatorilor de date să aplice măsuri adecvate și eficace pentru a garanta respectarea principiilor și a obligațiilor în materie și să dovedească această conformitate autorităților, la cererea acestora. Aceste măsuri ar trebui să încurajeze respectarea principiilor și a obligațiilor în materie de protecție a datelor, limitând în același timp riscurile de acces neautorizat, de abuz, de pierderi etc. Obligația de a dovedi, la cerere, aplicarea măsurilor necesare ar trebui să se dovedească un instrument util pentru autoritățile însărcinate cu protecția datelor, în îndeplinirea misiunilor lor de executare.

75. Obligația de a aplica aceste măsuri ar trebui să incumbe operatorilor de date din toate sectoarele (public și privat) și ar trebui să fie scalabilă astfel încât tipul de măsuri să poată fi proporționale cu riscurile asociate prelucrării datelor și cu natura datelor.

Adoptat la Bruxelles, la 13 iulie 2010

Pentru grupul de lucru
Președintele
Jacob KOHNSTAMM