GRUPUL DE LUCRU PENTRU PROTECŢIA DATELOR INSTITUIT ÎN TEMEIUL ARTICOLULUI 29

01037/12/RO
WG196

Avizul nr. 05/2012 privind „cloud computing”

Adoptat la 1 iulie 2012

Acest grup de lucru a fost instituit în temeiul articolului 29 din Directiva 95/46/CE. Acesta este un organ consultativ european independent pentru protecţia datelor şi a vieţii private. Atribuţiile acestuia sunt descrise la articolul 30 din Directiva 95/46/CE şi articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de Direcţia C (Drepturi fundamentale şi cetăţenie) a Comisiei Europene, Direcţia Generală Justiţie, B-1049 Bruxelles, Belgia, biroul nr. MO-59 02/013.

Site web: http://ec.europa.eu/justice/data-protection/index_ro.htm

Rezumat

În cadrul prezentului aviz, Grupul de lucru instituit în temeiul articolului 29 analizează toate aspectele relevante pentru furnizorii de servicii de cloud computing care operează în interiorul Spațiului Economic European (SEE) și pentru clienții acestora, specificând toate principiile aplicabile prevăzute în Directiva UE privind protecția datelor (95/46/CE) și în Directiva 2002/58/CE asupra confidențialității și comunicațiilor electronice (astfel cum a fost revizuită prin Directiva 2009/136/CE), după caz.

În ciuda beneficiilor recunoscute ale cloud computing din punct de vedere atât economic, cât și societal, prezentul aviz subliniază modul în care introducerea la scară largă a serviciilor de cloud computing poate genera o serie de riscuri asociate protecției datelor, în special lipsa controlului asupra datelor cu caracter personal, precum și informații insuficiente cu privire la modalitatea, locul și entitatea de prelucrare/sub-prelucrare a datelor. Aceste riscuri trebuie evaluate cu atenție de către organismele publice și întreprinderile private atunci când intenționează să contracteze serviciile unui furnizor de servicii de cloud computing. Prezentul aviz examinează aspectele asociate partajării resurselor cu alte părți, lipsa transparenței unui lanț de externalizare format din mai multe persoane împuternicite de către operator și subcontractanți, lipsa unui cadru global comun al portabilității datelor și incertitudinea cu privire la admisibilitatea transferului de date cu caracter personal către furnizorii de servicii de cloud computing stabiliți în afara SEE. În mod similar, lipsa transparenței în ceea ce privește informațiile pe care le poate furniza un operator persoanei de la care sunt colectate date cu privire la modul în care sunt prelucrate datele cu caracter personal ale acesteia este subliniată în prezentul aviz ca un motiv serios de preocupare. Persoanele de la care sunt colectate date trebuie[1] să fie informate cu privire la organismul care le prelucrează datele și la scopurile prelucrării, precum și pentru a-și putea exercita drepturile de care beneficiază în acest sens.

O concluzie cheie a prezentului aviz este aceea că întreprinderile și administrațiile care doresc să utilizeze cloud computing ar trebui să efectueze, într-o primă etapă, o analiză cuprinzătoare și detaliată a riscurilor. Toți furnizorii de servicii de cloud computing care operează în interiorul SEE ar trebui să furnizeze clienților care solicită astfel de servicii toate informațiile necesare în vederea evaluării corecte a avantajelor și dezavantajelor adoptării unui astfel de serviciu. Securitatea, transparența și siguranța juridică pentru clienți ar trebui să constituie vectorii cheie care stau la baza ofertelor de servicii de cloud computing.

În ceea ce privește recomandările cuprinse în prezentul aviz, sunt subliniate responsabilitățile clientului serviciilor de cloud computing în calitate de operator și se recomandă așadar ca acesta să opteze pentru un furnizor de servicii de cloud computing care garantează conformitatea cu legislația UE privind protecția datelor. În cadrul avizului este abordată chestiunea garanțiilor contractuale adecvate, cu cerința ca orice contract

[1] Cuvintele-cheie „TREBUIE” (din engleză MUST sau SHALL), „NU TREBUIE” (din engleză MUST NOT sau SHALL NOT), „OBLIGATORIU” (din engleză REQUIRED), „AR TREBUI” (din engleză SHOULD), „NU AR TREBUI” (din engleză SHOULD NOT), „SE RECOMANDĂ” (din engleză RECOMMENDED), „ESTE POSIBIL” sau „POATE” (din engleză MAY) și „OPȚIONAL” (din engleză OPTIONAL) trebuie interpretate în conformitate cu descrierea acestora din RFC 2119. Documentul este disponibil la http://www.ietf.org/rfc/rfc2119.txt. Cu toate acestea, pentru facilitarea lecturii, aceste cuvinte nu apar scrise cu majuscule în prezenta specificație.

încheiat între un client care beneficiază de servicii de cloud computing și furnizorul serviciilor respective să prevadă suficiente garanții în termeni de măsuri tehnice și organizaționale. Semnificativă este, de asemenea, recomandarea privitoare la faptul că un client care beneficiază de servicii de cloud computing ar trebui să verifice dacă furnizorul acestora poate garanta legalitatea tuturor transferurilor internaționale de date.

Ca oricare alt proces evolutiv, dezvoltarea cloud computing ca paradigmă tehnologică globală reprezintă o provocare. Prezentul aviz, în forma în care a fost adoptat, poate fi considerat o etapă importantă în definirea atribuțiilor care urmează să fie asumate în acest sens de către comunitatea de protecție a datelor în anii următori.

Cuprins

1. Introducere

Pentru unii, cloud computing reprezintă una dintre cele mai importante revoluții tehnologice care a apărut în ultimii ani. Pentru alții, aceasta reprezintă evoluția naturală a unui set de tehnologii destinate realizării visului mult așteptat al unei informatici utilitare. În orice caz, un pentru un număr mare de părți interesate cloud computing ocupă un loc primordial în dezvoltarea strategiilor lor tehnologice.

Cloud computing constă într-un set de tehnologii și modele de servicii care se axează pe utilizarea și furnizarea de aplicații informatice, capacitate de prelucrare, stocare și spațiu pentru memorie, toate bazate pe internet. Cloud computing poate genera importante beneficii economice, deoarece resurse la cerere pot fi configurate, extinse și accesate pe internet cu destul de multă ușurință. Pe lângă beneficiile economice, cloud computing poate aduce beneficii în materie de securitate; întreprinderile, în special cele mici și mijlocii, pot achiziționa, la un cost marginal, tehnologii de nivel înalt care, în mod normal, nu s-ar încadra în limitele lor bugetare.

Există o varietate de servicii oferite de furnizorii de cloud computing, de la sisteme virtuale de prelucrare a datelor (care înlocuiesc și/sau funcționează în paralel cu serverele convenționale, sub controlul direct al operatorului), la servicii de asistență pentru dezvoltarea de aplicații și găzduire web avansată, până la soluții informatice online care pot înlocui aplicațiile instalate în mod convențional pe computerele personale ale utilizatorilor finali. Printre acestea se numără aplicațiile de prelucrare de text, agendele și calendarele, sistemele de evidență pentru stocarea online a documentelor și soluții externalizate de corespondență electronică. Câteva dintre definițiile utilizate cel mai frecvent pentru diversele tipuri de servicii sunt cuprinse în anexa la prezentul aviz.

În prezentul aviz, Grupul de lucru instituit în temeiul articolului 29 (denumit în continuare „WG29") analizează legislația aplicabilă și obligațiile operatorilor din interiorul Spațiului Economic European (denumit în continuare „SEE") și ale furnizorilor de servicii de cloud computing care au clienți în interiorul SEE. Avizul se axează pe situația în care relația se presupune a fi o relație operator – persoană împuternicită de operator, unde clientul este considerat a fi operator, iar furnizorul de servicii de cloud computing este considerat a fi persoana împuternicită de operator. În cazul în care furnizorul acționează, de asemenea, ca operator, acesta trebuie să îndeplinească cerințe suplimentare. Prin urmare, o condiție prealabilă pentru utilizarea acordurilor de servicii de cloud computing este aceea ca operatorul să efectueze un exercițiu adecvat de evaluare a riscurilor, incluzând locațiile serverelor unde sunt prelucrate datele și luarea în calcul a riscurilor și beneficiilor din perspectiva protecției datelor, în conformitate cu criteriile subliniate în cele ce urmează.

Prezentul aviz precizează principiile aplicabile atât în cazul operatorilor, cât și în cazul persoanelor împuternicite de operator prevăzute în Directiva generală privind protecția datelor (95/46/CE), cum ar fi specificarea și limitarea scopului, ștergerea datelor și măsurile tehnice și organizaționale. Avizul oferă orientări privind cerințele legate de securitate ca garanție atât structurală, cât și procedurală. O atenție deosibită este acordată angajamentelor contractuale care ar trebui să reglementeze, în acest context, relația dintre un operator și o persoană împuternicită. Obiectivele clasice de securitate a datelor sunt disponibilitatea, integritatea și confidențialitatea. Cu toate acestea, protecția datelor nu se limitează numai la securitatea datelor, prin urmare, aceste obiective sunt completate cu obiectivele specifice ale protecției datelor referitoare la transparență, izolare, posibilitatea de intervenție și portabilitate pentru a

respecta dreptul persoanelor la protecția datelor, consacrat prin articolul 8 din Carta drepturilor fundamentale a Uniunii Europene.

În ceea ce privește transferurile de date cu caracter personal în afara SEE, sunt analizate instrumente precum clauzele contractuale standard adoptate de către Comisia Europeană, mecanismele privind nivelul adecvat de protecție a datelor și eventualele viitoare regulile corporatiste obligatorii (BCR) care să se aplice persoanelor împuternicite, precum și riscurile în ceea ce privește protecția datelor care decurg din solicitările internaționale de aplicare a legii.

Prezentul aviz se încheie cu recomandări adresate clienților serviciilor de cloud computing în calitate de operatori, furnizorilor de servicii de cloud computing în calitate de persoane împuternicite de operator, precum și Comisiei Europene cu privire la modificările viitoare ale cadrului european de protecție a datelor.

Grupul internațional de lucru de la Berlin privind protecția datelor în domeniul telecomunicațiilor a adoptat *Memorandumul de la Sopot*[2] în aprilie 2012. Memorandumul examinează aspecte legate de viața privată și protecția datelor asociate cloud computing și subliniază faptul că cloud computing nu trebuie să conducă la o diminuare a standardelor în ceea ce privește protecția datelor comparativ cu prelucrarea convențională a datelor.

2. Riscurile în ceea ce privește protecția datelor asociate cloud computing

Întrucât prezentul aviz se axează pe operațiunile de prelucrare a datelor cu caracter personal care utilizează servicii de cloud computing, sunt avute în vedere numai riscurile specifice asociate acestui context[3]. Majoritatea acestor riscuri se încadrează în două mari categorii, și anume lipsa controlului asupra datelor și informații insuficiente cu privire la operațiunea de prelucrare în sine (absența transparenței). Printre riscurile specifice asociate cloud computing avute în vedere în prezentul aviz se numără:

Lipsa controlului

Prin încredințarea datelor cu caracter personal sistemelor gestionate de un furnizor de servicii de cloud computing, este posibil ca clienții acestuia să nu mai poată deține controlul exclusiv asupra datelor și să nu mai poată implementa măsurile tehnice și organizaționale necesare asigurării disponibilității, integrității, confidențialității, transparenței, izolării[4], posibilității de intervenție și portabilității datelor. Lipsa controlului se poate manifesta astfel:

- Lipsa disponibilității cauzată de lipsa interoperabilității (blocajul de către furnizor): dacă furnizorul de cloud computing se bazează pe proprietatea asupra tehnologiei sale, este posibil ca un client să întâmpine dificultăți pentru a transfera date și documente între diferite sisteme bazate pe cloud computing (portabilitatea datelor) sau pentru a

---

2 http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf

3 Pe lângă riscurile asociate datelor cu caracter personal prelucrate prin intermediul cloud computing menționate explicit în prezentul aviz, trebuie avute în vedere, de asemenea, toate riscurile asociate externalizării prelucrării datelor cu caracter personal.

4 În Germania s-a introdus conceptul mai extins de „imposibilitate de stabilire a unei legături” („*unlinkability*”). Cf. nota de subsol 24 de mai jos.

face schimb de informații cu entități care utilizează servicii de cloud computing gestionate de diferiți furnizori (interoperabilitate).

- Lipsa integrității cauzată de partajarea resurselor: Un mediu de cloud computing este format din sisteme și infrastructuri partajate. Furnizorii de astfel de servicii prelucrează datele cu caracter personal care provin dintr-o gamă largă de surse în termeni de persoane și organizații de la care se colectează date și există posibilitatea apariției unor interese conflictuale și/sau a unor obiective diferite.
- Lipsa confidențialității privind cererile de aplicare a legii adresate direct unui furnizor de servicii de cloud computing: Datele cu caracter personal prelucrate într-un mediu de cloud computing pot face obiectul unor solicitări cereri de aplicare a legii din partea autorităților de aplicare a legii din statele membre ale UE și din țări terțe. Există riscul ca datele cu caracter personal să poată fi dezvăluite autorităților (străine) de aplicare a legii fără un temei juridic valid la nivelul UE, survenind astfel o încălcare a legislației UE privind protecția datelor.
- Lipsa posibilității de intervenție cauzată de complexitatea și dinamica lanțului de externalizare: Serviciul de cloud computing oferit de un furnizor ar putea fi produs prin combinarea mai multor servicii oferite de o serie de alți furnizori, care pot fi adăugate sau înlăturate în mod dinamic pe durata contractului cu un client.
- Lipsa posibilității de intervenție (drepturile persoanelor vizate): Este posibil ca un furnizor de servicii de cloud computing să nu ofere măsurile și instrumentele necesare pentru a asista operatorul în activitatea de gestionare a datelor referitoare la, de exemplu, accesarea, ștergerea sau corectarea datelor.
- Lipsa izolării: Un furnizor de servicii de cloud computing poate utiliza controlul său fizic asupra datelor provenite de la clienți diferiți pentru a conecta datele cu caracter personal. În cazul în care administratorilor li se oferă drepturi de acces cu un grad suficient de privilegiere (funcții cu risc ridicat), aceștia ar putea conecta informații provenite de la diferiți clienți.

Lipsa informațiilor privind prelucrarea (transparență)

Informațiile insuficiente cu privire la operațiunile de prelucrare ale unui furnizor de cloud computing prezintă un risc atât pentru operatori, cât și pentru persoanele vizate deoarece este posibil ca aceștia să nu fie conștienți de potențialele amenințări și riscuri și, prin urmare, să nu poată adopta măsurile pe care le consideră adecvate.

O serie de potențiale amenințări ar putea rezulta din faptul că operatorul nu știe că

- lanțul de prelucrare are loc prin implicarea mai multor persoane împuternicite și subcontractanți.
- datele cu caracter personal sunt prelucrate în diferite locații geografice din cadrul SEE. Aceasta are un impact direct asupra legislației aplicabile în cazul unor litigii privind protecția datelor care ar putea apărea între utilizator și furnizor.
- datele cu caracter personal sunt transferate către țări terțe din afara SEE. Țările terțe ar putea să nu ofere un nivel adecvat de protecție a datelor, iar transferurile ar putea să nu fie protejate prin măsuri adecvate (de exemplu, clauze contractuale standard sau reguli corporatiste obligatorii) fiind, astfel, ilegale.

Există o cerință conform căreia persoanele de la care sunt colectate date cu caracter personal în vederea prelucrării într-un mediu de cloud computing trebuie să fie informate cu privire la identitatea operatorului de date și la scopul prelucrării (cerință existentă pentru toți operatorii în conformitate cu Directiva 95/46/CE privind protecția datelor).

Având în vedere potențiala complexitate a lanțurilor de prelucrare într-un mediu de cloud computing, în vederea asigurării prelucrării corecte a datelor cu privire la persoana vizată (articolul 10 din Directiva 95/46/CE), operatorii ar trebui, ca bună practică, să ofere, de asemenea, informații suplimentare cu privire la subcontractanții care furnizează servicii de cloud computing.

3. Cadrul juridic

3.1 Cadrul de protecție a datelor

Cadrul juridic relevant este reprezentat de Directiva 95/46/CE privind protecția datelor. Directiva se aplică în orice caz care implică prelucrare de date cu caracter personal ca urmare a utilizării serviciilor de cloud computing. Directiva 2002/58/CE asupra confidențialității și comunicațiilor electronice (astfel cum a fost revizuită prin Directiva 2009/136/CE) se aplică în cazul prelucrării datelor cu caracter personal asociate furnizării de servicii de comunicații electronice accesibile publicului în rețele de comunicații publice (operatori de telecomunicații), fiind, prin urmare, relevantă dacă astfel de servicii sunt furnizate prin intermediul unei soluții de cloud computing[5].

3.2 Legislația aplicabilă

Criteriile de stabilire a aplicabilității unei legi sunt prevăzute în articolul 4 din Directiva 95/46/CE, referitor la legislația care se aplică în cazul operatorilor[6] cu unul sau mai multe sedii în interiorul SEE, precum și la legislația care se aplică în cazul operatorilor stabiliți în afara SEE, dar care utilizează echipamente localizate pe teritoriul SEE în scopul prelucrării datelor cu caracter personal. Grupul de lucru instituit în temeiul articolului 29 a analizat acest aspect în Avizul său nr. 8/2010 privind legislația aplicabilă[7].

În primul caz, factorul care determină aplicarea legislației UE în cazul operatorului este reprezentat de locația sediului acestuia și de activitățile pe care le desfășoară, în conformitate cu articolul 4 alineatul (1) litera (a) din directivă, tipul de model de serviciu de cloud computing fiind irelevant. Legislația aplicabilă este cea din țara în care este stabilit operatorul care contractează servicii de cloud computing mai curând decât locul în care sunt stabiliți furnizorii de cloud computing.

În cazul în care operatorul este stabilit în mai multe state membre, prelucrând date ca parte a activităților sale în țările respective, legislația aplicabilă va fi cea a fiecărui stat membru în care are loc prelucrarea de date.

---

5 Directiva 2002/58/CE asupra confidențialității și comunicațiilor electronice (astfel cum a fost modificată prin Directiva 2009/136/CE): Directiva 2002/58/CE privind confidențialitatea în domeniul telecomunicațiilor se aplică în cazul furnizorilor de servicii de comunicații electronice puse la dispoziția publicului și solicită acestora să asigure conformitatea cu obligațiile referitoare la secretul comunicațiilor și la protecția datelor cu caracter personal, precum și cu drepturile și obligațiile privind rețelele și serviciile de comunicații electronice. În cazurile în care furnizorii de cloud computing acționează ca furnizori de servicii de comunicații electronice puse la dispoziția publicului, aceștia intră sub incidența acestei directive.

6 Conceptul de operator este definit în articolul 2 litera (h) din directivă și a fost analizat de către WG29 în Avizul său nr. 1/2010 privind conceptele de „operator” și „persoană împuternicită de către operator”.

7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_ro.pdf

Articolul 4 alineatul (1) litera (c)[8] se referă la modul în care se aplică legislația referitoare la protecția datelor în cazul operatorilor care nu sunt stabiliți în interiorul SEE, dar care recurg la mijloace automate sau neautomate situate pe teritoriul unui stat membru, cu excepția cazului în care aceste mijloace sunt folosite numai în vederea tranzitului. Aceasta înseamnă că, în situația în care un client al unor servicii de cloud computing stabilit în afara SEE contractează un furnizor localizat pe teritoriul SEE, furnizorul exportă legislația privind protecția datelor către client.

3.3 Sarcinile și responsabilitățile diferiților actori

Astfel cum s-a specificat anterior, cloud computing implică o serie de actori diferiți. Este importantă evaluarea și clarificarea rolului fiecăruia dintre acești actori pentru a putea stabili obligațiile specifice ale acestora în raport cu legislația actuală referitoare la protecția datelor.

Trebuie reamintit faptul că WG29 a subliniat în Avizul său nr. 1/2010 privind conceptele de „operator" și „persoană împuternicită de către operator" că „*primul și cel mai important rol al conceptului de operator este acela de a stabili cine va fi responsabil de respectarea normelor de protecție a datelor și modul în care persoanele vizate își pot exercita drepturile în practică. Cu alte cuvinte: alocarea responsabilității.*" Aceste două criterii generale responsabile pentru conformitate și alocarea responsabilității ar trebui reținute de către părțile implicate în cadrul analizei în cauză.

3.3.1 Client al serviciilor de cloud computing și furnizor de servicii de cloud computing

Clientul serviciilor de cloud computing determină scopul final al prelucrării și decide cu privire la externalizarea operațiunii de prelucrare și la delegarea parțială sau totală a activităților de prelucrare către o organizație externă. Prin urmare, clientul serviciilor de cloud computing acționează ca un operator de date. Directiva definește operatorul ca fiind „*persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal*". Clientul serviciilor de cloud computing, în calitate de operator, trebuie să accepte responsabilitatea respectării legislației privind protecția datelor și este responsabil și supus îndeplinirii tuturor obligațiilor legale prevăzute în Directiva 95/46/CE. Clientul serviciilor de cloud computing poate însărcina furnizorul să aleagă metodele și măsurile tehnice și organizaționale care urmează a fi utilizate în vederea atingerii scopurilor formulate de către operator.

Furnizorul de servicii de cloud computing reprezintă entitatea care furnizează servicii de cloud computing sub diferitele forme discutate mai sus. Atunci când furnizorul de servicii furnizează mijloacele și platforma, acționând în numele clientului serviciilor, acesta este considerat persoană împuternicită de către operator, și anume, în conformitate cu Directiva 95/46/CE „*persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care prelucrează datele cu caracter personal pe seama operatorului"*.[9][10]

---

[8] Articolul 4 alineatul (1) litera (c) prevede că legislația unui stat membru este aplicabilă atunci când „operatorul nu este stabilit pe teritoriul Comunității, dar în scopul prelucrării datelor cu caracter personal recurge la mijloace automate sau neautomate, situate pe teritoriul statului membru respectiv, cu excepția cazului în care aceste mijloace sunt folosite numai în vederea tranzitului pe teritoriul Comunității".

[9] Prezentul aviz se axează numai pe relația standard operator – persoană împuternicită de operator.

[10] Mediul de cloud computing poate fi utilizat, de asemenea, de către persoanele fizice (utilizatori) exclusiv pentru a derula activități personale sau casnice. În acest caz, trebuie analizat cu atenție dacă se aplică așa-

Astfel cum se specifică în Avizul nr. 1/2010, pot fi utilizate o serie de criterii[11] pentru evaluarea controlului prelucrării. În fapt, ar putea exista situații în care un furnizor de servicii de cloud computing ar putea fi considerat fie un operator comun, fie un operator distinct, în funcție de circumstanțele concrete. De exemplu, acest lucru ar putea fi valabil în cazul în care furnizorul prelucrează date în scopuri proprii.

Trebuie subliniat faptul că inclusiv în cazul mediilor complexe de prelucrare a datelor, în care diferiți operatori au un anumit rol în prelucrarea datelor cu caracter personal, respectarea normelor de protecție a datelor și răspunderea determinată de posibila încălcare a normelor respective sunt repartizate în mod clar, pentru a evita diminuarea protecției datelor cu caracter personal sau apariția unui „conflict negativ de competență" și a unor lacune din cauza cărora unele obligații sau drepturi care decurg din directivă nu ar fi asigurate de niciuna dintre părți.

În cadrul scenariului actual privind cloud computing, este posibil ca clienții serviciilor de cloud computing să nu aibă loc de manevră în negocierea termenilor contractuali de utilizare a serviciilor respective deoarece ofertele standardizate reprezintă o trăsătură a multor servicii de cloud computing. Cu toate acestea, în , clientul este cel care decide cu privire la alocarea unei părți sau a totalității operațiunilor de prelucrare unor servicii de cloud computing în scopuri precise; rolul furnizorului de astfel de servicii va fi cel al unui contractor în raport cu clientul, ceea ce constituie punctul cheie în acest caz. Astfel cum se menționează în Avizul nr. 1/2010[12] privind conceptele de „operator" și „persoană împuternicită de către operator" al Grupului de lucru instituit în temeiul articolului 29, „*diferența dintre puterea contractuală a unui mic operator de date în raport cu marii furnizori de servicii nu ar trebui să justifice acceptarea de către operator a unor clauze și condiții contractuale neconforme cu legislația privind protecția datelor"*. Din acest motiv, operatorul trebuie să opteze pentru un furnizor de servicii de cloud computing care garantează conformitatea cu legislația privind protecția datelor. O atenție deosebită trebuie acordată caracteristicilor contractelor aplicabile – acestea trebuie să includă un set de garanții standardizate privind protecția datelor, inclusiv cele subliniate de către grupul de lucru la punctul 3.4.3 (Măsuri tehnice și organizaționale) și la punctul 3.5 (fluxuri transfrontaliere de date) – precum și tuturor mecanismelor suplimentare care se pot dovedi adecvate pentru facilitarea precauției necesare și a responsabilității (precum audituri și certificări independente de către terți ale serviciilor unui furnizor – a se vedea punctul 4.2).

Furnizorii de servicii de cloud computing (în calitate de persoane împuternicite) au obligația asigurării confidențialității. Directiva 95/46/CE prevede că: „*Orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de către operator, inclusiv persoana împuternicită, care are acces la datele cu caracter personal nu trebuie să le prelucreze decât la instrucțiunile operatorului, cu excepția cazului în care este obligat prin lege.*" Accesul furnizorului de servicii de cloud computing la date în cursul furnizării serviciilor este, de asemenea, în mod fundamental reglementat de cerința respectării dispozițiilor articolului 17 din directivă – a se vedea secțiunea 3.4.2.

---

numita excepție privind gospodăriile care scutește utilizatorii de calificarea drept operatori. Acest aspect nu face însă obiectul prezentului aviz.

[11] De exemplu, nivelul instrucțiunilor, monitorizarea de către clientul serviciilor de cloud computing, expertiza părților.

[12] Avizul nr. 1/2010 privind conceptele de „operator" și „persoană împuternicită de către operator" - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_ro.pdf

Persoanele împuternicite trebuie să aibă în vedere tipul de mediu de cloud computing în cauză (public, privat, comunitar sau hibrid / IaaS, SaaS sau PaaS [a se vedea anexa a) Modele de implementare – b) Modele de furnizare a serviciului]), precum și tipul serviciului contractat de către client. Persoanele împuternicite sunt responsabile pentru adoptarea de măsuri de securitate în linie cu cele prevăzute de legislația UE astfel cum se aplică aceasta în jurisdicția operatorului și cea a persoanei împuternicite. Persoanele împuternicite trebuie, de asemenea, să sprijine și să asiste operatorul în respectarea drepturilor (exercitate) ale persoanelor vizate.

3.3.2 Subcontractanți

Serviciile de cloud computing pot presupune implicarea unui număr de părți contractate care acționează ca persoane împuternicite de către operator. Este, de asemenea, o practică obișnuită ca persoanele împuternicite de operator să contracteze subcontractanți adiționali care obțin ulterior acces la datele cu caracter personal. În cazul în care persoanele împuternicite subcontractează servicii către subcontractanți, acestea sunt obligate să pună aceste informații la dispoziția clientului, detaliind tipul serviciului contractat, caracteristicile subcontractanților actuali sau potențiali și garanții potrivit cărora entitățile respective oferă furnizorului de cloud computing servicii care respectă dispozițiile Directivei 95/46/CE.

Prin urmare, toate obligațiile relevante trebuie să se aplice, de asemenea, în cazul subcontractanților în temeiul contractelor încheiate între furnizorul de servicii de cloud computing și subcontractant care reflectă prevederile contractuale dintre client și furnizorul de servicii. În Avizul său nr. 1/2010 privind conceptele de „operator” și „persoană împuternicită de către operator”, Grupul de lucru instituit în temeiul articolului 29 a făcut referire la numărul mare de persoanele împuternicite în cazurile în care persoanele împuternicite pot avea o relație directă cu operatorul sau în care operează ca subcontractanți în situația în care persoanele împuternicite externalizează o parte a activității de prelucrare cu care au fost însărcinați. „*Directiva nu prevede ca, din motive organizaționale, să nu poată fi desemnate mai multe entități în calitate de persoane împuternicite sau de subcontractanți, prin subdivizarea sarcinilor relevante. Totuși, în cadrul prelucrării datelor, toate aceste persoane trebuie să respecte instrucțiunile operatorului de date*.”[13]

În astfel de scenarii, obligațiile și responsabilitățile care derivă din legislația privind protecția datelor ar trebui stabilite clar și nu dispersate de-a lungul lanțului de externalizare sau de subcontractare, pentru a asigura controlul efectiv asupra activităților de prelucrare și pentru alocarea responsabilității clare pentru acestea.

Un posibil model de asigurări care poate fi folosit pentru a clarifica sarcinile și obligațiile persoanelor împuternicite atunci când subcontractează activități de prelucrare a datelor a fost introdus pentru prima dată prin Decizia din 5 februarie 2010 a Comisiei privind clauzele contractuale standard pentru transferul de date cu caracter personal către persoanele împuternicite de către operator stabilite în țări terțe[14]. Conform modelului, subcontractarea este permisă numai cu consimțământul scris prealabil al operatorului și cu un acord scris care impune subcontractantului aceleași obligații precum cele impuse persoanei împuternicite. În cazul în care subcontractantul nu își îndeplinește obligațiile privind protecția datelor în temeiul unui astfel de acord scris, persoana împuternicită este pe deplin responsabilă față de operator pentru respectarea, de către subcontractant, a obligațiilor în temeiul acordului respectiv. O astfel de prevedere ar putea fi utilizată în cadrul oricăror clauze contractuale

[13] Cf. WP169, p. 29, Avizul nr. 1/2010 privind conceptele de „operator” și „persoană împuternicită de către operator” (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_ro.pdf)

[14] A se vedea FAQ II.5 din WP176.

convenite între un operator și un furnizor de servicii de cloud computing, în care acesta din urmă intenționează să furnizeze servicii prin subcontractare, pentru a asigura garanțiile necesare pentru subcontractarea serviciilor de prelucrare a datelor.

O soluție similară privind asigurările în cursul subcontractării serviciilor de prelucrare a fost propusă recent de către Comisie în propunerea de Regulament general privind protecția datelor[15]. Acțiunile unei persoane împuternicite de operator trebuie să fie reglementate de un contract sau alt document juridic care obligă persoana împuternicită în raport cu operatorul și care stipulează în special că, printre alte cerințe, persoana împuternicită recrutează o altă persoană împuternicită de către operator numai cu autorizarea prealabilă a operatorului [articolul 26 alineatul (2) din propunere].

În opinia WG29, persoana împuternicită își poate subcontracta activitățile numai pe baza acordului operatorului, care ar putea fi acordat de manieră generală la începutul furnizării serviciului[16] cu obligația clară ca persoana împuternicită să informeze operatorul cu privire la toate modificările pe care intenționează să le aducă în ceea ce privește adăugarea sau înlocuirea subcontractanților, operatorul având posibilitatea în orice moment de a se opune unor astfel de modificări sau de a înceta contractul. Ar trebui să existe obligația clară ca furnizorul de servicii de cloud computing să numească toți subcontractanții contractați. În plus, ar trebui încheiat un contract între furnizorul de servicii de cloud computing și subcontractant care să reflecte prevederile contractuale dintre client și furnizorul de servicii de cloud computing. Operatorul ar trebui să poată face uz de posibilități contractuale de remediere în cazul încălcării contractului de către subcontractanți. Acest lucru ar putea fi stabilit prin garantarea faptului că persoana împuternicită este direct responsabilă față de operator pentru oricare încălcare cauzată de subcontractanții pe care i-a recrutat sau prin crearea unui drept de beneficiu în favoarea operatorului, ca parte terță, în cadrul contractelor semnate între persoana împuternicită de operator și subcontractanți sau prin faptul că respectivele contracte vor fi semnate în numele operatorului de date, acesta devenind parte la contract.

3.4 Cerințe privind protecția datelor în relația client-furnizor

3.4.1 Conformitatea cu principiile fundamentale

Legalitatea prelucrării datelor cu caracter personal în mediul de cloud computing depinde de aderarea la principiile fundamentale ale legislației UE privind protecția datelor. Și anume, trebuie garantată transparența în raport cu persoana de la care se colectează date, principiul specificării scopului și limitării la acesta trebuie respectat, iar datele cu caracter personal trebuie șterse imediat ce păstrarea acestora nu mai este necesară. Mai mult, trebuie implementate măsuri tehnice și organizaționale adecvate pentru a asigura un nivel adecvat de protecție și de securitate a datelor.

3.4.1.1 Transparența

Transparența este de o importanță cheie pentru o activitate corectă și legitimă de prelucrare a datelor cu caracter personal. Directiva 95/46/CE obligă clientul serviciilor de cloud computing să furnizeze persoanei de la care colectează date care o privesc informații privind identitatea acestuia și scopul prelucrării datelor. Clientul serviciilor de cloud computing ar

[15] Propunere de Regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, 25.1.2012.

[16] A se vedea FAQ II, 1) din WP176, adoptat la 12 iulie 2010.

trebui, de asemenea, să furnizeze oricare alte informații suplimentare precum cele referitoare la destinatarii sau categoriile de destinatari ai datelor, care ar putea include, de asemenea, persoane împuternicite sau subcontractanți, în măsura în care astfel de informații suplimentare sunt necesare pentru a asigura prelucrarea corectă a datelor cu privire la persoana vizată (cf. articolul 10 din directivă)[17].

Transparența trebuie, de asemenea, garantată în relația (relațiile) dintre clientul serviciilor de cloud computing, furnizorul de astfel de servicii și subcontractanți (dacă există). Clientul este singurul în măsură să evalueze legalitatea prelucrării datelor cu caracter personal în mediul de cloud computing dacă furnizorul informează clientul cu privire la toate aspectele relevante. Un operator care intenționează să angajeze un furnizor de servicii de cloud computing ar trebui să verifice cu atenție termenii și condițiile acestuia și să le evalueze din perspectiva protecției datelor.

Transparența în mediul de cloud computing înseamnă că este necesar ca fiecare client al unor astfel de servicii să cunoască toți subcontractanții care contribuie la furnizarea respectivului serviciu de cloud computing, precum și locația tuturor centrelor de date în care ar putea fi prelucrate datele cu caracter personal[18].

Dacă furnizarea serviciului presupune instalarea de programe informatice în sistemele clientului serviciilor de cloud computing (de exemplu, browser plug-in), furnizorul de astfel de servicii ar trebui, ca bună practică, să informeze clientul cu privire la acest fapt și, în special, cu privire la implicațiile acestuia din perspectiva protecției și securității datelor. Invers, clientul ar trebui să ridice această problemă *ex ante*, în cazul în care aceasta nu este abordată în mod suficient de către furnizorul de servicii de cloud computing.

3.4.1.2 Specificarea și limitarea scopului

Principiul specificării scopului și limitării la acesta prevede ca datele cu caracter personal să fie colectate în scopuri determinate, explicite și legitime și să nu mai fie prelucrate ulterior într-un mod incompatibil cu aceste scopuri [cf. articolul 6 alineatul (1) litera (b) din Directiva 95/46/CE]. Clientul serviciilor de cloud computing trebuie să determine scopul (scopurile) prelucrării datelor anterior colectării datelor cu caracter personal și să informeze persoanele vizate cu privire la acesta (acestea). Clientul nu trebuie să prelucreze datele cu caracter personal în alte scopuri incompatibile cu cele inițiale.

Mai mult, trebuie să se garanteze faptul că datele cu caracter personal nu sunt prelucrate (în mod ilegal) în alte scopuri de către furnizorul de servicii de cloud computing sau de către unul dintre subcontractanții acestuia. Deoarece un scenariu tipic de servicii de cloud computing ar putea cu ușurință implica un număr mare de subcontractanți, riscul prelucrării datelor cu caracter personal în alte scopuri incompatibile trebuie, prin urmare, să fie evaluat ca fiind destul de ridicat. Pentru a minimiza riscul, contractul încheiat între furnizorul de servicii de cloud computing și client ar trebui să includă măsuri tehnice și organizaționale de atenuare a riscului și să ofere asigurări privind arhivarea și auditul operațiunilor relevante de prelucrare a datelor cu caracter personal efectuate de către angajații furnizorului de servicii de cloud computing sau de către subcontractanți[19]. Ar trebui impuse sancțiuni prin contract împotriva furnizorului sau subcontractantului în caz de încălcare a legislației privind protecția datelor.

---

[17] Există o obligație corespunzătoare de informare a persoanei vizate atunci când sunt înregistrate sau comunicate către terți date care nu au fost colectate de la persoana vizată ci din diferite surse (cf. articolul 11).

[18] Doar atunci acesta va putea evalua dacă datele cu caracter personal pot fi transferate către o țară terță din afara Spațiului Economic European (SEE) care nu asigură un nivel adecvat de protecție a datelor în sensul Directivei 95/46/CE. Cf., de asemenea, secțiunea 3.4.6 de mai jos.

[19] Cf. secțiunea 3.4.3 de mai jos.

3.4.1.3 Ștergerea datelor

În conformitate cu articolul 6 alineatul (1) litera (e) din Directiva 95/46/CE, datele cu caracter personal trebuie păstrate într-o formă care permite identificarea persoanelor vizate o perioadă nu mai lungă decât este necesar în vederea atingerii scopurilor pentru care au fost colectate sau pentru care vor fi prelucrate ulterior. Datele cu caracter personal care nu mai sunt necesare trebuie șterse sau anonimizate în mod real. Dacă datele nu pot fi șterse ca urmare a unor norme legale de păstrare (de exemplu, reglementări fiscale), accesul la datele cu caracter personal ar trebui blocat. Este responsabilitatea clientului serviciilor de cloud computing să garanteze faptul că datele cu caracter personal sunt șterse imediat ce acestea nu mai sunt necesare în sensul menționat mai sus[20].

Principiul ștergerii datelor se aplică în cazul datelor cu caracter personal indiferent dacă acestea sunt stocate pe unități de hard disk sau pe alte suporturi de stocare (de exemplu, casete de siguranță). Deoarece datele cu caracter personal pot fi păstrate în mod redundant pe servere diferite, în locații diferite, trebuie să se garanteze faptul că fiecare apariție a acestora este ștearsă definitiv (și anume, versiunile anterioare, fișierele temporare și chiar fragmente de fișiere trebuie, de asemenea, șterse).

Clienții serviciilor de cloud computing trebuie să fie conștienți de faptul că datele arhivate[21] care facilitează posibilitatea auditării, de exemplu, a stocării, modificărilor sau ștergerii de date pot fi considerate, de asemenea, date cu caracter personal referitoare la persoana care a inițiat respectiva operațiune de prelucrare[22].

Ștergerea sigură a datelor cu caracter personal presupune fie distrugerea sau demagnetizarea suportului de stocare, fie ștergerea efectivă a datelor cu caracter personal stocate prin suprascriere. Pentru suprascrierea datelor cu caracter personal, ar trebui utilizate instrumente informatice speciale care suprascriu date de mai multe ori în conformitate cu o specificație recunoscută.

Clientul serviciilor de cloud computing ar trebui să se asigure că furnizorul de servicii garantează ștergerea sigură în sensul menționat mai sus și că în dintre furnizor și client este cuprinsă prevederea clară a ștergerii datelor cu caracter personal[23]. Același lucru este valabil, de asemenea, pentru contractele încheiate între furnizorii de servicii de cloud computing și subcontractanți.

3.4.2 Garanții contractuale ale relației (relațiilor) „operator” – „persoană împuternicită de operator”

În cazul în care operatorii decid să contracteze servicii de cloud computing, aceștia trebuie să împuternicească o persoană care să prezinte suficiente garanții referitoare la măsurile de securitate tehnică și de organizare privind prelucrarea care urmează să fie efectuată și să asigure respectarea acestor măsuri [articolul 17 alineatul (2) din Directiva 95/46/CE]. Mai mult, aceștia sunt obligați prin lege să semneze un contract oficial cu furnizorul de servicii de cloud computing, în conformitate cu articolul 17 alineatul (3) din Directiva 95/46/CE.

---

[20] Ștergerea datelor constituie o problemă atât pe durata contractului de servicii de cloud computing, cât și după încetarea acestuia. Aceasta este, de asemenea, relevantă în cazul înlocuirii sau retragerii unui subcontractant.

[21] Observații privind cerințele de arhivare sunt prezentate mai jos, în cadrul secțiunii 4.3.4.2.

[22] Aceasta înseamnă că trebuie să se definească perioade rezonabile de păstrare a fișierelor arhivate și că trebuie să existe procese care să mențină ștergerea sau anonimizarea acestor date la momentul oportun.

[23] Cf. secțiunea 3.4.3 de mai jos.

Articolul menționat stabilește cerința existenței unui contract sau a altul act juridic obligatoriu care să reglementeze relația dintre operator și persoana împuternicită. În scopul păstrării probelor, elementele contractului sau actului juridic care se referă la protecția datelor și la cerințele referitoare la măsurile tehnice și organizatorice se consemnează în scris sau în altă formă echivalentă.

Ca cerințe minime, contractul trebuie să prevadă în special că persoana împuternicită trebuie să respecte instrucțiunile operatorului și că persoana împuternicită trebuie să pună în aplicare măsuri tehnice și organizaționale pentru a proteja în mod corespunzător datele cu caracter personal.

Pentru a garanta siguranța juridică, contractul ar trebui, de asemenea, să cuprindă următoarele aspecte:

1. Detalii privind instrucțiunile clientului (extindere și modalitățile) care urmează să fie furnizate furnizorului, acordând o atenție deosebită acordurilor aplicabile privind nivelul serviciilor (care ar trebui să fie obiective și măsurabile) și sancțiunile relevante (financiare sau de altă natură, inclusiv posibilitatea de a acționa în instanță furnizorul în caz de neconformitate).
2. Specificarea măsurilor de securitate pe care trebuie să le respecte furnizorul de servicii de cloud computing, în funcție de riscurile prezentate de prelucrare și de natura datelor care trebuie protejate. Este foarte important să fie specificate măsuri tehnice și organizaționale concrete precum cele subliniate la punctul 3.4.3 de mai jos. Aceasta nu aduce atingere aplicării de măsuri mai stricte, dacă există, care ar putea fi prevăzute în conformitate cu legislația națională a clientului.
3. Obiectul și perioada furnizării serviciului de cloud computing de către furnizorul de servicii, extinderea, modul și scopul prelucrării de date cu caracter personal de către furnizor, precum și tipurile de date cu caracter personal prelucrate.
4. Specificarea condițiilor pentru transmiterea datelor (cu caracter personal) sau distrugerea datelor odată cu încetarea serviciului. Mai mult, trebuie să se garanteze faptul că datele cu caracter personal sunt șterse în siguranță la cererea clientului serviciilor de cloud computing.
5. Includerea clauzei de confidențialitate, obligatorie atât pentru furnizorul de cloud computing, cât și pentru oricare dintre angajații acestuia care ar putea avea acces la date. Numai persoanele autorizate pot avea acces la date.
6. Obligația din partea furnizorului de a sprijini clientul în facilitarea exercitării de către persoanele vizate a drepturilor lor ținând de accesul, rectificarea sau ștergerea datelor acestora.
7. Contractul ar trebui să stabilească explicit faptul că furnizorul de cloud computing nu poate comunica datele către terți, inclusiv în scopul păstrării, decât dacă este prevăzută în contract implicarea unor subcontractanți. Contractul ar trebui să specifice faptul că subcontractanții pot fi angajați numai pe baza unui acord care poate fi acordat, de manieră generală, de către operator cu condiția obligației clare a persoanei împuternicite de a informa operatorul cu privire la oricare modificare pe care intenționează să o facă în acest sens, operatorul având posibilitatea în orice moment de a se opune unor astfel de schimbări sau de a înceta contractul. Ar trebui să existe obligația clară din partea furnizorului de servicii de a numi toți subcontractanții contractați (de exemplu, într-un registru digital public). Trebuie să se garanteze faptul că contractele încheiate între furnizorul de servicii de cloud computing și subcontractant reflectă prevederile contractuale dintre clientul serviciilor de cloud

computing și furnizor (și anume, faptul că subcontractanții sunt supuși acelorași obligații contractuale ca și furnizorul de servicii). În special, trebuie să se garanteze faptul că atât furnizorul, cât și toți subcontractanții acestuia acționează numai la instrucțiunile clientului. Astfel cum s-a explicat în capitolul privind subcontractarea serviciilor de prelucrare, răspunderea juridică ar trebui stabilită clar în contract. Acesta ar trebui să stabilească obligația din partea persoanei împuternicite de a crea un cadru pentru realizarea transferurilor internaționale, de exemplu prin semnarea de contracte cu subcontractanții, pe baza clauzelor contractuale standard din Directiva 2010/87/UE.

8. Clarificarea responsabilităților furnizorului de servicii de cloud computing de a notifica clientul în cazul oricărei încălcări care afectează datele clientului serviciilor de cloud computing.
9. Obligația furnizorului de a furniza o listă a locațiilor în care ar putea fi prelucrate datele.
10. Dreptul operatorului de a monitoriza și obligația corespunzătoare a furnizorului de servicii de a coopera.
11. Ar trebui stabilit prin contract faptul că furnizorul de servicii de cloud computing trebuie să informeze clientul cu privire la modificările relevante aduse respectivului serviciu de cloud computing precum implementarea de funcții adiționale.
12. Contractul ar trebui să prevadă arhivarea și auditul operațiunilor relevante de prelucrare a datelor cu caracter personal efectuate de către furnizorul de servicii sau de către subcontractanți.
13. Notificarea clientului cu privire la orice solicitare, obligatorie din punct de vedere juridic, de a divulga date cu caracter personal, prezentată de o autoritate de aplicare a legii, cu excepția cazului în care aceasta face obiectul altei interdicții, de exemplu interdicția, în cadrul dreptului penal, de a păstra confidențialitatea unei investigații urmărind aplicarea legii.
14. O obligație generală din partea furnizorului de a acorda asigurările necesare potrivit cărora organizarea internă și dispozițiile sale privind prelucrarea datelor (și cele ale subcontractanților săi, dacă este cazul) sunt în conformitate cu cerințele și standardele legale naționale și internaționale aplicabile.

În cazul unei încălcări de către operator, orice persoană care suferă prejudicii ca urmare a prelucrării ilegale are dreptul de a primi compensații din partea operatorului pentru prejudiciile cauzate. În cazul în care persoanele împuternicite utilizează datele în oricare alt scop, le comunică sau le utilizează într-un mod care încalcă prevederile contractuale, acestea vor fi, de asemenea, considerați operatori și vor fi făcuți răspunzători pentru încălcările în care au fost implicați personal.

Trebuie notat faptul că, în multe cazuri, furnizorii de servicii de cloud computing oferă servicii și contracte standard spre a fi semnate de către operatori, care prezintă un format standard pentru prelucrarea datelor cu caracter personal. Această diferență între puterea contractuală a unui mic operator de date în raport cu marii furnizori de servicii nu ar trebui să justifice acceptarea de către operator a unor clauze și condiții contractuale neconforme cu legislația privind protecția datelor.

3.4.3 Măsuri tehnice și organizaționale privind protecția și securitatea datelor

Articolul 17 alineatul (2) din Directiva 95/46/CE prevede responsabilitatea exclusivă a clienților serviciilor de cloud computing (acționând în calitate de operatori) de a opta pentru furnizori de servicii care pun în aplicare măsuri de securitate tehnică și de organizare adecvate pentru protejarea datelor cu caracter personal și pentru a putea demonstra responsabilitatea.

Pe lângă obiectivele de securitate fundamentale legate de disponibilitate, confidențialitate și integritate, trebuie atrasă atenția, de asemenea, asupra obiectivelor complementare de protecție a datelor referitoare la transparență (a se vedea 3.4.1.1 mai sus), izolare[24], posibilitatea de intervenție, responsabilitate și portabilitate. Prezenta secțiune subliniază aceste obiective centrale în ceea ce privește protecția datelor, fără a aduce atingere altor analize complementare ale riscurilor vizând securitatea[25].

3.4.3.1 Disponibilitatea

Asigurarea disponibilității înseamnă garantarea accesului oportun și fiabil la datele cu caracter personal.

O amenințare gravă la adresa disponibilității în mediul de cloud computing o reprezintă pierderea accidentală a conectivității la rețeaua dintre client și furnizor sau a performanței serverului cauzată de acțiuni răuvoitoare precum atacurile prin blocarea accesului (de tip DoS)[26]. Alte riscuri privind disponibilitatea includ defecțiunile accidentale ale componentelor de hardware atât în rețea, cât și în sistemele de prelucrare și de stocare a datelor în mediul de cloud computing, întreruperi ale alimentării cu energie și alte probleme legate de infrastructură.

Operatorii de date ar trebui să verifice dacă furnizorul de servicii de cloud computing a adoptat măsuri rezonabile pentru a face față riscului de perturbări, cum ar fi conexiuni de siguranță la rețeaua de internet, stocare multiplă a datelor și mecanisme eficiente de efectuare a unor copii de rezervă ale datelor.

3.4.3.2 Integritatea

Integritatea poate fi definită ca fiind proprietatea conform căreia datele sunt autentice și nu au fost modificate, cu rea intenție sau accidental, în timpul prelucrării, stocării sau transmiterii. Noțiunea de integritate poate fi extinsă la sistemele informatice și presupune ca prelucrarea datelor cu caracter personal în cadrul acestor sisteme să rămână neschimbată.

Detectarea modificărilor aduse datelor cu caracter personal poate fi realizată prin mecanisme criptografice de autentificare precum coduri sau semnături de autentificare a mesajelor.

Interferența cu integritatea sistemelor de tehnologia informației în mediul de cloud computing poate fi prevenită sau detectată cu ajutorul sistemelor de detectare/prevenire a intruziunilor (IPS/IDS). Acest lucru este cu precădere important în tipul de mediu de rețea deschisă precum este cel în care cloud computing operează de obicei.

---

[24] În Germania, s-a introdus în legislație conceptul mai larg de „imposibilitate de stabilire a unei legături” („*unlinkability*”), acesta fiind promovat de către Conferința comisarilor pentru protecția datelor.

[25] Conform, de exemplu, ENISA la http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[26] Un atac de tip DoS reprezintă o încercare coordonată de a face ca un calculator sau un element din rețea să devină indisponibil pentru utilizatorii autorizați, temporar sau pe durată nedeterminată (de exemplu, prin intermediul a numeroase sisteme de atac care își paralizează ținta cu un număr foarte mare de cereri de comunicare externe).

3.4.3.3 Confidențialitatea

Într-un mediu de cloud computing, criptarea poate contribui în mod semnificativ la confidențialitatea datelor cu caracter personal dacă este implementată corect, deși aceasta nu anonimizează în mod ireversibil datele cu caracter personal[27]. Criptarea datelor cu caracter personal ar trebui folosită în toate cazurile atunci când acestea se află „în tranzit" și, atunci când este disponibilă, pentru datele „inactive"[28]. În unele cazuri (de exemplu, un serviciu de stocare de tip IaaS), este posibil ca un client al serviciilor de cloud computing să nu se poată baza pe o soluție de criptare oferită de către furnizor și atunci poate opta să cripteze datele cu caracter personal anterior trimiterii acestora în mediul de cloud computing. Criptarea datelor inactive necesită o atenție deosebită acordată gestionării cheilor criptografice deoarece securitatea datelor depinde în cele din urmă de confidențialitatea cheilor de criptare.

Comunicațiile dintre furnizorul de cloud computing și client, precum și cele dintre centrele de date ar trebui criptate. Administrarea de la distanță a platformei de cloud computing ar trebui să aibă loc numai prin intermediul unui canal de comunicare sigur. Dacă un client intenționează nu numai să stocheze, ci și să prelucreze ulterior datele cu caracter personal în mediul de cloud computing (de exemplu, căutând baze de date pentru înregistrări), acesta trebui să aibă în vedere faptul că criptarea nu poate fi menținută în timpul prelucrării datelor (cu excepția calculelor foarte specifice).

Alte măsuri tehnice destinate asigurării confidențialității includ mecanismele de autorizare și autentificarea puternică (de exemplu, autentificare cu doi factori). Clauzele contractuale ar trebui, de asemenea, să impună angajaților clientului serviciilor de cloud computing, furnizorilor de astfel de servicii și subcontractanților obligații privind confidențialitatea.

3.4.3.4 Transparența

Măsurile tehnice și organizaționale trebuie să susțină transparența pentru a permite revizuirea, a se vedea 3.4.1.1.

3.4.3.5 Izolarea (limitarea scopului)

În infrastructurile de cloud computing, resursele precum stocarea, memoria și rețelele sunt partajate între mai multe părți implicate (*tenants*). Acest fapt generează noi riscuri ca datele să fie divulgate și prelucrate în scopuri ilegale. Obiectivul de protecție referitor la „izolare" este destinat să abordeze acest aspect și să contribuie la garantarea faptului că datele nu sunt utilizate în alte scopuri în afara celui stabilit inițial [articolul 6 alineatul (1) litera (b) din Directiva 95/46/CE] și să mențină confidențialitatea și integritatea[29].

Atingerea acestui obiectiv necesită, în primul rând, o guvernanță adecvată a drepturilor și a funcțiilor de acces la datele cu caracter personal, revizuită în mod periodic. Implementarea de funcții cu privilegii excesive ar trebui evitată (de exemplu, niciun utilizator sau administrator nu ar trebui să fie autorizat să acceseze întregul mediu de cloud computing în cauză). În general, administratorii și utilizatorii trebuie să poată accesa numai informațiile necesare pentru scopurile lor legitime (principiul privilegiilor minime).

---

[27] Directiva 95/46/CE – considerentul 26: „(...) întrucât principiile protecției nu se aplică datelor anonime astfel încât persoana vizată să nu mai fie identificabilă; (...)". În aceeași linie, procesele tehnice de fragmentare a datelor care ar putea fi folosite în cadrul furnizării serviciilor de cloud computing nu conduc la anonimizarea ireversibilă și, prin urmare, nu implică neaplicarea obligațiilor privind protecția datelor.

[28] Acest lucru este valabil în special pentru operatorii de date care intenționează să transfere date sensibile în sensul articolului 8 din Directiva 95/46/CE (de exemplu, date privind sănătatea) în mediul de cloud computing sau care fac obiectul obligațiilor legale specifice privind secretul profesional.

[29] Cf. 3.4.1.2.

În al doilea rând, izolarea depinde, de asemenea, de măsuri tehnice precum întărirea managerilor de mașini virtuale și gestionarea adecvată a resurselor partajate dacă se utilizează mașini virtuale pentru partajarea resurselor fizice între diferiți clienți ai serviciilor de cloud computing.

3.4.3.5 Posibilitatea de intervenție

Directiva 95/46/CE oferă persoanelor de la care se colectează date dreptul de acces, rectificare, ștergere, blocare și de opoziție (conform articolelor 12 și 14). Clientul serviciilor de cloud computing trebuie să verifice dacă furnizorul nu impune obstacole tehnice sau organizaționale față de aceste cerințe, inclusiv în cazurile când datele sunt prelucrate ulterior de subcontractanți.

Contractul dintre client și furnizor ar trebui să stipuleze faptul că furnizorul de servicii de cloud computing este obligat să sprijine clientul în facilitarea exercitării de către persoanele vizate a drepturilor acestora și să asigure că acest lucru este valabil inclusiv în relația clientului cu oricare subcontractant[30].

3.4.3.6 Portabilitatea

În prezent, cei mai mulți furnizori de servicii de cloud computing nu utilizează formatele de date și interfețele de servicii standard care facilitează interoperabilitatea și portabilitatea între diferiți furnizori de astfel de servicii. Dacă un client al serviciilor de cloud computing decide să se transfere de la un furnizor la altul, lipsa interoperabilității ar putea avea ca rezultat imposibilitatea sau cel puțin dificultatea transferării datelor (cu caracter personal) ale clientului către noul furnizor (situație denumită blocaj de către furnizor). Același lucru este valabil pentru serviciile pe care clientul le-a dezvoltat pe o platformă oferită de către furnizorul inițial (PaaS). Clientul serviciilor de cloud computing ar trebui să verifice dacă și cum garantează furnizorul portabilitatea datelor și a serviciilor înainte de comandarea unui serviciu de cloud computing[31].

3.4.4.7 Responsabilitatea

În domeniul tehnologiei informației, responsabilitatea poate fi definită ca abilitatea de a stabili ce a făcut o anumită entitate la un anumit moment în trecut și cum. În domeniul protecției datelor, aceasta comportă deseori un sens mai larg și descrie abilitatea părților de a demonstra că au luat măsurile adecvate pentru a asigura faptul că au fost puse în aplicare principiile privind protecția datelor.

Responsabilitatea informatică este deosebit de importantă pentru a investiga încălcările în ceea ce privește securitatea datelor cu caracter personal în care clienții de servicii de cloud computing, furnizorii și subcontractanții ar putea să dețină fiecare un anumit grad de responsabilitate operațională. Capacitatea platformei bazate pe cloud computing de a furniza mecanisme fiabile de monitorizare și mecanisme de arhivare cuprinzătoare este de o importanță capitală în acest sens.

Mai mult, furnizorii de cloud computing ar trebui să prezinte documente doveditoare ale faptului că au fost adoptate măsuri adecvate și eficiente care oferă rezultatele urmărite de principiile privind protecția datelor subliniate în secțiunile anterioare. Procedurile pentru

---

[30] Cf. secțiunea 3.4.2 nr. 6 de mai sus. Furnizorul ar putea fi chiar instruit să răspundă solicitărilor în numele clientului.

[31] De preferat, furnizorul ar trebui să utilizeze interfețe și formate de date standardizate sau deschise. În orice caz, ar trebui consimțite clauze contractuale care să stipuleze formate sigure, menținerea relațiilor logice și toate costurile rezultate din migrarea către un alt furnizor de servicii.

garantarea identificării tuturor operațiunilor de prelucrare a datelor, pentru a răspunde solicitărilor de acces, alocarea resurselor, inclusiv numirea ofițerilor pentru protecția datelor care sunt responsabili pentru organizarea conformității protecției datelor sau procedurile de certificare independentă reprezintă exemple de astfel de măsuri. În plus, operatorii de date ar trebui să garanteze faptul că sunt pregătiți să demonstreze autorității de supraveghere competente, la cererea acesteia, adoptarea măsurilor necesare[32].

3.5 Transferuri internaționale

Articolele 25 și 26 din Directiva 95/46/CE prevăd libera circulație a datelor cu caracter personal către țările din afara SEE numai dacă țara sau destinatarul respectiv oferă un nivel adecvat de protecție a datelor. În caz contrar, trebuie luate măsuri de protecție de către operator și co-operatorii săi și/sau persoanele împuternicite. Cu toate acestea, cloud computing se bazează de cele mai multe ori pe o lipsă totală a unei locații stabile a datelor în cadrul rețelei furnizorului de cloud computing. Datele se pot afla într-un centru de date la ora 14.00 și în altă parte de pe glob la ora 16.00. Clientul serviciilor de cloud computing se află, prin urmare, foarte rar în poziția de a putea cunoaște în timp real unde sunt localizate, stocate sau transferate datele. În acest context, instrumentele legale tradiționale care furnizează un cadru de reglementare a transferurilor de date către țări terțe din afara UE care nu oferă o protecție adecvată au anumite limite.

3.5.1 „Sfera de siguranță" și țările adecvate

Mecanismele care atestă nivelul adecvat de protecție a datelor, inclusiv „sfera de siguranță", sunt limitate în ceea ce privește domeniul geografic de aplicare, prin urmare, acestea nu acoperă toate transferurile realizate în cadrul unui mediu de cloud computing.
Transferurile către organizații din SUA care aderă la aceste principii pot avea loc legal în temeiul legislației UE deoarece organizațiile destinatare sunt considerate ca oferind un nivel adecvat de protecție a datelor transferate.

Cu toate acestea, în opinia grupului de lucru, numai auto-certificarea aderării la „sfera de siguranță" nu poate fi considerată suficientă în absența unei aplicări solide a principiilor privind protecția datelor în mediul de cloud computing. În plus, articolul 17 din directiva UE prevede semnarea unui contract între operator și persoana împuternicită de acesta în scopul prelucrării datelor, cerință confirmată în FAQ 10 din documentele privind cadrul „sferei de siguranță" UE-SUA. Contractul nu face obiectul unei autorizări prealabile în conformitate cu autoritățile europene pentru protecția datelor (APD). Un astfel de contract menționează activitatea de prelucrare care urmează să fie efectuată și toate măsurile necesare pentru garantarea menținerii securității datelor. Legislațiile naționale diferite și APD pot stabili cerințe adiționale.

Grupul de lucru consideră că întreprinderile care exportă date nu ar trebui să se bazeze doar pe declarația importatorului de date care susține că deține o certificare de aderare la „sfera de siguranță". Dimpotrivă, întreprinderea care exportă date ar trebui să obțină dovezi care să ateste existența auto-certificărilor de aderare la „sfera de siguranță" și să solicite dovezi care să demonstreze că sunt respectate principiile acesteia. Acest lucru este important în special în

[32] Grupul de lucru a furnizat observații detaliate privind responsabilitatea în Avizul său nr. 3/2010 privind principiul responsabilității http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_ro.pdf.

ceea ce privește informațiile furnizate persoanelor vizate afectate de activitatea de prelucrare a datelor[33, 34].

Grupul de lucru consideră, de asemenea, că fiecare client al serviciilor de cloud computing trebuie să verifice dacă contractele standard elaborate de furnizorii de astfel de servicii sunt conforme cu cerințele naționale privind prelucrarea datelor. Legislația națională poate solicita definirea subcontractării activității de prelucrare a datelor în contract, ceea ce include locațiile și alte date privind subcontractanții și trasabilitatea datelor. În mod normal, furnizorii de cloud computing nu oferă clienților astfel de date – angajamentul lor la „sfera de siguranță" nu poate înlocui lipsa garanțiilor menționate mai sus atunci când acestea sunt prevăzute în legislația națională. În astfel de cazuri, exportatorul este încurajat să utilizeze alte instrumente legale disponibile, precum clauzele contractuale standard sau regulile corporatiste obligatorii (BCR).

În sfârșit, grupul de lucru consideră că este posibil, de asemenea, ca principiile „sferei de siguranță", în sine, să nu garanteze exportatorului de date mijloacele necesare pentru a asigura faptul că au fost aplicate măsuri de securitate adecvate de către furnizorul de cloud computing în SUA, astfel cum ar putea fi prevăzut în legislațiile naționale, în temeiul Directivei 95/46/CE[35]. În termeni de securitate a datelor, cloud computing prezintă câteva riscuri în ceea ce privește securitatea, specifice mediului de cloud computing, precum pierderea guvernanței, ștergerea nesigură și incompletă a datelor, piste insuficiente de audit sau deficiențe privind izolarea[36], care nu sunt suficient abordate de către principiile existente ale „sferei de siguranță" privind securitatea datelor[37]. Prin urmare, pot fi introduse garanții suplimentare referitoare la securitatea datelor, de exemplu, înglobând expertiza și resursele părților terțe capabile să evalueze caracterul adecvat al furnizorilor de cloud computing prin diferite sisteme de audit, standardizare și certificare[38]. Din aceste motive, ar putea fi recomandabil să se completeze angajamentul importatorului de date la „sfera de siguranță" cu garanții suplimentare având în vedere natura specifică a mediului de cloud computing.

3.5.2 Derogări

Derogările prevăzute la articolul 26 din Directiva 95/46/CE permit exportatorilor de date să transfere date în afara UE fără a prezenta garanții suplimentare. Cu toate acestea, WP29 a adoptat un aviz în care consideră că derogările trebuie să se aplice doar în cazul în care transferurile nu sunt recurente, masive sau de ordin structural[39].

Pe baza unor astfel de interpretări, este aproape imposibilă utilizarea unor astfel de derogări în contextul cloud computing.

---

33 A se vedea APD din Germania: http://www.datenschutzberlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

34 Pentru cerințe privind contractarea subcontractanților, a se vedea 3.3.2.

35 A se vedea avizul oferit de APD din Danemarca: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution.

36 Descrisă în detaliu în lucrarea ENISA „Cloud Computing: avantaje, riscuri și recomandări pentru securitatea informației" disponibilă la: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

37 „Organizațiile trebuie să adopte precauții rezonabile în vederea protejării informațiilor cu caracter personal împotriva pierderii, utilizării inadecvate și accesului neautorizat, divulgării, modificării și distrugerii acestora."

38 A se vedea secțiunea 4.2 de mai jos.

39 Documentul de lucru nr. 12/1998: „Transferuri de date cu caracter personal către țările terțe: punerea în aplicare a articolelor 25 și 26 din Directiva UE privind protecția datelor", document adoptat de grupul de lucru la 24 iulie 1998 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf).

3.5.3 Clauze contractuale standard

Clauzele contractuale standard adoptate de către Comisia UE în scopul creării unui cadru pentru transferurile internaționale de date între doi operatori sau un operator și o persoană împuternicită se bazează pe o abordare bilaterală. Atunci când furnizorul de cloud computing este considerat ca fiind persoana împuternicită, clauzele model prevăzute în Decizia 2010/87/CE a Comisiei constituie un instrument care poate fi folosit între persoana împuternicită și operator ca temei pentru mediul de cloud computing pentru a oferi garanții adecvate în contextul transferurilor internaționale.

Pe lângă clauzele contractuale standard, grupul de lucru consideră că furnizorii de cloud computing ar putea prezenta cumpărătorilor dispoziții elaborate pe baza experiențelor lor practice atât timp cât acestea nu contrazic, direct sau indirect, clauzele contractuale standard aprobate de către Comisie sau nu aduc atingere drepturilor și libertăților fundamentale ale persoanelor de la care se colectează date[40]. Cu toate acestea, întreprinderile nu pot să aducă nicio modificare clauzelor contractuale standard, fără ca acest lucru să implice faptul că acestea nu vor mai fi „standard”[41].

Atunci când furnizorul de cloud computing acționând în calitate de persoană împuternicită de operator este stabilit în UE, situația ar putea fi mai complexă deoarece clauzele tip se aplică, în general, numai în cazul transferului de date de la un operator din UE către o persoană împuternicită din afara UE (a se vedea considerentul 23 din Decizia 2010/87/UE a Comisiei privind clauzele tip, precum și WP 176).

În ceea ce privește relația contractuală dintre persoana împuternicită de operator stabilită în afara UE și subcontractanți, ar trebui elaborat un acord scris care să impună subcontractantului aceleași obligații ca cele impuse persoanei împuternicite în clauzele tip.

3.5.4 Regulile corporatiste obligatorii (BCR): către o abordare globală

BCR constituie un cod de conduită pentru întreprinderile care transferă date în cadrul propriului grup. O astfel de soluție va fi oferită, de asemenea, și în contextul cloud computing, atunci când furnizorul este și persoană împuternicită. Într-adevăr, WP29 lucrează, în prezent, la reguli corporatiste obligatorii pentru persoanele împuternicite care vor permite transferul în cadrul grupului în beneficiul operatorilor fără a mai presupune semnarea de contracte per client între persoana împuternicită și subcontractanți[42].

Astfel de BCR destinate persoanelor împuternicite de operator ar permite clientului furnizorului să-și încredințeze datele cu caracter personal persoanei împuternicite, fiind asigurat că datele transferate în sfera de competență profesională a furnizorului ar beneficia de un nivel adecvat de protecție.

---

40 A se vedea FAQ IV B1.9, Pot întreprinderile să includă clauzele contractuale standard într-un contract mai extins și să adauge clauze specifice? Publicat de CE la http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

41 A se vedea FAQ IV B1.10, Pot întreprinderile să modifice sau să schimbe clauzele contractuale standard aprobate de către Comisie?

42 A se vedea Documentul de lucru nr. 02/2012 de elaborare a unui tabel cu elementele și principiile care urmează să se regăsească în regulile corporatiste obligatorii destinate persoanelor împuternicite de operator, adoptat la 6 iunie 2012: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

4. Concluzii și recomandări

Întreprinderile și administrațiile care doresc să utilizeze servicii de cloud computing ar trebui, într-o primă etapă, să efectueze o analiză cuprinzătoare și detaliată a riscurilor. Analiza trebuie să vizeze riscurile asociate prelucrării datelor în mediul de cloud computing (lipsa controlului și informații insuficiente – a se vedea secțiunea 2 de mai sus) având în vedere tipul de date prelucrate într-un astfel de mediu[43]. O atenție deosibită ar trebui, de asemenea, acordată evaluării riscurilor legale privind protecția datelor care privesc, în special, obligațiile de securitate și transferurile internaționale. Prelucrarea datelor sensibile prin intermediul cloud computing dă naștere unor motive de preocupare suplimentare. Prin urmare, fără a aduce atingere legilor naționale, prelucrarea datelor de acest tip presupune furnizarea de garanții suplimentare[44]. Concluziile de mai jos sunt destinate să ofere o listă de verificare pentru conformitatea în ceea ce privește protecția datelor de către clienții serviciilor de cloud computing și furnizorii de astfel de servicii pe baza cadrului juridic actual; se oferă, de asemenea, o serie de recomandări în vederea evoluțiilor viitoare ale cadrului de reglementare la nivelul UE și în afara acesteia.

4.1 Orientări pentru clienții și furnizorii de servicii de cloud computing

- Relația operator – persoană împuternicită de operator: prezentul aviz se axează pe relația client – furnizor ca relație operator – persoană împuternicită de operator (a se vedea punctul 3.3.1); cu toate acestea, pe baza unor circumstanțe concrete, ar putea exista situații în care furnizorul de servicii de cloud computing acționează și în calitate de operator, de exemplu, atunci când furnizorul re-prelucrează unele date cu caracter personal în scopuri proprii. În acest caz, furnizorul este pe deplin (colectiv) responsabil pentru activitatea de prelucrare și trebuie să îndeplinească toate obligațiile legale stipulate în Directiva 95/46/CE și în Directiva 2002/58/CE (dacă este cazul);
- Responsabilitatea clientului serviciilor de cloud computing în calitate de operator: clientul, în calitate de operator, trebuie să accepte responsabilitatea respectării legislației privind protecția datelor și este supus tuturor obligațiilor legale menționate în Directiva 95/46/CE și în Directiva 2002/58/CE, dacă este cazul, în special în raport cu persoanele vizate (a se vedea 3.3.1). Clientul ar trebui să opteze pentru un furnizor de servicii de cloud computing care garantează conformitatea cu legislația UE privind protecția datelor, astfel cum este reflectată de garanțiile contractuale corespunzătoare sintetizate mai jos;
- Garanții privind subcontractarea: orice contract încheiat între furnizorul de servicii și clienții serviciilor de cloud computing ar trebui să includă dispoziții privind subcontractanții. Contractul ar trebui să menționeze faptul că subcontractanții pot fi contractați numai pe baza consimțământului care poate fi acordat, de manieră generală, de către operator, cu condiția obligației clare din partea persoanei împuternicite de a informa operatorul cu privire la orice modificare pe care intenționează să o facă în acest sens, operatorul având posibilitatea în orice moment de a se opune unor astfel de modificări sau de a înceta contractul. Ar trebui să existe obligația clară a furnizorului de servicii de a numi toți subcontractanții contractați. Furnizorul de servicii ar trebui să semneze un contract cu fiecare subcontractant în parte care să reflecte prevederile din contractul său încheiat cu clientul serviciilor de

[43] ENISA prezintă o listă a riscurilor care trebuie luate în considerare http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[44] A se vedea Memorandumul de la Sopot, cf. nota de subsol 2 de mai sus.

cloud computing; clientul trebuie să se asigure că are posibilități contractuale de remediere în cazul încălcării prevederilor contractuale de către subcontractanții furnizorului (a se vedea 3.3.2);

- Conformitatea cu principiile fundamentale privind protecția datelor:
    - Transparența (a se vedea 3.4.1.1): furnizorii de servicii de cloud computing ar trebui să-și informeze clienții cu privire la toate aspectele relevante (privind protecția datelor) ale serviciilor acestora în cadrul negocierii contractului; în special, clienții ar trebui să fie informați cu privire la toți subcontractanții care contribuie la furnizarea respectivului serviciu de cloud computing și la toate locațiile în care ar putea fi stocate sau prelucrate datele de către furnizorul de servicii și/sau subcontractanții acestuia [în special dacă unele sau toate locațiile se află în afara Spațiului Economic European (SEE)]; clientul ar trebui să dețină informații relevante privind măsurile tehnice și organizaționale implementate de către furnizor; ca bună practică, clientul ar trebui să informeze persoanele vizate cu privire la furnizorul de servicii de cloud computing și toți subcontractanții (dacă există), precum și cu privire la locațiile în care ar putea fi stocate sau prelucrate datele de către furnizorul de servicii și/sau subcontractanții acestuia;
    - Specificarea și limitarea scopului (3.4.1.2): clientul ar trebui să garanteze conformitatea cu principiile referitoare la specificarea și limitarea scopului și să se asigure că datele nu sunt prelucrate în alte scopuri de către furnizor sau oricare dintre subcontractanți. Angajamentele în acest sens ar trebui incluse în măsurile contractuale adecvate (inclusiv garanțiile tehnice și organizatorice);
    - Păstrarea datelor (3.4.1.3): clientul este responsabil pentru garantarea faptului că datele sunt șterse (de către furnizor sau oricare dintre subcontractanți) de oriunde sunt stocate imediat ce acestea nu mai sunt necesare pentru scopurile specifice; mecanisme sigure de ștergere (distrugere, demagnetizare, suprascriere) ar trebui prevăzute în contract;
- Garanții contractuale (a se vedea 3.4.2, 3.4.3 și 3.5):
    - În general: contractul încheiat cu furnizorul (și cele care urmează să fie stipulate între furnizor și subcontractanți) ar trebui să permită suficiente garanții în termeni de măsuri de securitate tehnică și de organizare [în conformitate cu articolul 17 alineatul (2) din directivă] și ar trebui să fie elaborat în scris sau în altă formă echivalentă. Contractul ar trebui să detalieze instrucțiunile clientului către furnizor, inclusiv obiectul și perioada serviciului, niveluri obiective și măsurabile ale serviciilor și sancțiunile relevante (financiare sau de altă natură); acesta ar trebui să menționeze măsurile de securitate care trebuie respectate în funcție de riscurile activității de prelucrare și natura datelor, în conformitate cu cerințele prevăzute mai jos și făcând obiectul unor măsuri mai stricte, stabilite în temeiul legislației naționale a clientului; dacă furnizorii de servicii de cloud computing urmăresc să utilizeze termenii contractuali standard, atunci aceștia trebuie să se asigure că termenii respectivi respectă cerințele referitoare la protecția datelor (a se vedea 3.4.2); în cadrul termenilor respectivi ar trebui specificate, în special, măsurile tehnice și de organizare implementate de către furnizor;
    - Accesul la date: numai persoanele autorizate ar trebui să aibă acces la date; o clauză de confidențialitate ar trebui inclusă în contract în ceea ce privește furnizorul și angajații acestuia;

- Divulgarea datelor către terți: acest aspect ar trebui reglementat numai prin intermediul contractului, care ar trebui să includă obligația din partea furnizorului de a numi toți subcontractanții acestuia – de exemplu, într-un registru digital public – și de a asigura accesul clientului la informații referitoare la orice schimbare pentru a-i permite acestuia să se opună schimbărilor respective sau să înceteze contractul; de asemenea, prin contract ar trebui să i solicite furnizorului să notifice orice solicitare, obligatorie din punct de vedere juridic, de a divulga date cu caracter personal, prezentată de o autoritate de aplicare a legii, cu excepția cazului în care aceasta face obiectul altei interdicții; clientul ar trebui să garanteze faptul că furnizorul va respinge toate solicitările care nu sunt obligatorii din punct de vedere juridic de a divulga date;
- Obligațiile de a coopera: clientul trebuie să se asigure că furnizorul este obligat să coopereze în ceea ce privește dreptul clientului de a monitoriza operațiunile de prelucrare, să faciliteze exercitarea de către persoanele vizate a drepturilor acestora legate de accesarea/corectarea/ștergerea datelor referitoare la acestea, și (dacă este cazul) să notifice clientului serviciilor de cloud computing orice încălcare a securității datelor care afectează datele clientului;
- Transferurile transfrontaliere de date: clientul serviciilor de cloud computing ar trebui să verifice dacă furnizorul de astfel de servicii poate să garanteze legalitatea transferurilor transfrontaliere de date și să limiteze transferurile la țările selectate de către client, dacă este posibil. Transferurile de date către țări terțe neadecvate necesită furnizarea unor garanții specifice prin intermediul utilizării acordurilor de aderare la „sfera de siguranță”, a clauzelor contractuale standard (SCC) sau a regulilor corporatiste obligatorii (BCR), după caz; utilizarea SCC în cazul persoanelor împuternicite (în temeiul Deciziei 2010/87/CE a Comisiei) presupune anumite adaptări la mediul de cloud computing (pentru a preveni încheierea de contracte separate per client între un furnizor și subcontractanții acestuia), fapt care ar putea implica necesitatea unei autorizări prealabile din partea APD competente; o listă a locațiilor în care ar putea fi furnizat serviciul ar trebui inclusă în contract;
- Arhivarea și auditul prelucrării: clientul ar trebui să solicite arhivarea operațiunilor de prelucrare efectuate de către furnizor și subcontractanții acestuia; clientul ar trebui să fie împuternicit să efectueze auditul operațiunilor de prelucrare, însă auditurile efectuate de terți selectați de către operator și certificarea ar putea fi, de asemenea, acceptabile cu condiția garantării transparenței depline (de exemplu, prevăzând posibilitatea obținerii unei copii a certificatului de audit efectuat de terți sau a unei copii a raportului de audit prin care s-a verificat certificarea);
- Măsuri tehnice și organizaționale: acestea ar trebui să vizeze remedierea riscurilor implicate de lipsa controlului și de lipsa informațiilor care caracterizează cel mai adesea mediul de cloud computing. Prima categorie include măsuri destinate asigurării disponibilității, integrității, confidențialității, izolării, posibilității de intervenție și portabilității astfel cum au fost definite în prezentul document, în timp ce a doua se axează pe transparență (a se vedea 3.4.3 pentru detalii complete).

4.2 Certificări privind protecția datelor eliberate de terți

- Verificarea sau certificarea independentă de către o parte terță cu o reputație solidă poate constitui o modalitate credibilă pentru furnizorii de servicii de cloud computing de a demonstra conformitatea acestora cu obligațiile care le revin conform prezentului aviz. O astfel de certificare ar indica, cel puțin, faptul că controalele privind protecția datelor au fost supuse unor proceduri de audit sau de revizuire derulate de către o organizație terță cu o reputație solidă în raport cu un standard recunoscut care îndeplinește cerințele stabilite în prezentul aviz[45]. În contextul cloud computing, cumpărătorii potențiali ar trebui să verifice dacă furnizorii de servicii de cloud computing pot prezenta o copie a unui certificat de audit eliberat de o parte terță sau chiar o copie a raportului de audit prin care s-a verificat certificarea inclusiv cu privire la cerințele stabilite în prezentul aviz.

- Auditurile individuale ale datelor găzduite într-un mediu virtualizat și colectiv al serverului ar putea fi imposibil de pus în practică din punct de vedere tehnic și pot contribui, în anumite situații, la creșterea riscurilor controalelor fizice și logice ale securității rețelei efectuate. În astfel de cazuri, un audit relevant efectuat de o parte terță selectată de către operator ar putea fi considerat suficient în locul dreptului unui operator individual de a efectua misiuni de audit.

- Adoptarea de standarde și certificări specifice în ceea ce privește confidențialitatea este esențială pentru stabilirea unei relații de încredere între furnizorii de servicii de cloud computing, operatori și persoanele vizate.

- Standardele și certificările ar trebui să vizeze măsuri tehnice (precum localizarea datelor sau criptarea), precum și procesele din cadrul organizației furnizorilor de servicii care garantează protecția datelor (precum politicile de control al accesului, controlul accesului sau mecanisme de siguranță).

4.3 Recomandări: Evoluții viitoare

Grupul de lucru este pe deplin conștient de faptul că aspectele complexe ale cloud computing nu pot fi abordate complet prin intermediul garanțiilor și soluțiilor subliniate în prezentul aviz, care oferă, cu toate acestea, o bază solidă pentru securizarea prelucrării datelor cu caracter personal pe care clienții stabiliți în cadrul SEE le transmit furnizorilor de servicii de cloud computing. Această secțiune este destinată să sublinieze o serie de aspecte care trebuie soluționate pe termen scurt și mediu pentru a consolida garanțiile existente, asistând industria cloud computing cu privire la aspectele subliniate și garantând în același timp respectul pentru drepturile fundamentale la viață privată și protecția datelor.

- O mai bună echilibrare a responsabilităților între operator și persoana împuternicită de acesta: grupul de lucru salută dispozițiile cuprinse în articolul 26 din propunerea Comisiei (Proiect de Regulament general al UE privind protecția datelor), care vizează să facă persoanele împuternicite mai răspunzătoare față de operatori prin asistarea acestora în vederea garantării conformității, în special, în ceea ce privește securitatea și obligațiile asociate. Articolul 30 din propunere introduce obligația legală din partea persoanei împuternicite de a implementa măsuri tehnice și organizaționale adecvate. Proiectul de propunere clarifică faptul că o persoană împuternicită care nu respectă instrucțiunile operatorului se califică drept operator și este supusă regulilor specifice privind controlul

[45] Astfel de standarde ar include standardele emise de Organizația Internațională pentru Standardizare, Comitetul internațional pentru asigurare și standarde de audit și Comitetul pentru standarde de audit al Institutului American al contabililor publici autorizați, în măsura în care aceste organizații furnizează standarde care îndeplinesc cerințele stabilite în prezentul aviz.

comun. Grupul de lucru instituit în temeiul articolului 29 consideră că propunerea urmează direcția corectă în ceea ce privește remedierea dezechilibrului care reprezintă deseori o caracteristică a mediului de cloud computing, în care poate fi dificil pentru client (mai ales dacă este un IMM) să-și exercite controlul deplin prevăzut de legislația privind protecția datelor asupra modului în care furnizorul prestează serviciile solicitate. Mai mult, având în vedere poziția juridică asimetrică a persoanelor de la care se colectează date și a utilizatorilor întreprinderi mici în raport cu marii furnizori de servicii de cloud computing, se recomandă un rol mai proactiv al consumatorilor și al organizațiilor economice interesate în vederea negocierii unor termeni și condiții mai echilibrate pentru astfel de întreprinderi.

- Accesul la datele cu caracter personal în scopuri de securitate națională și aplicare a legii: este deosebit de important să se adauge în viitorul regulament faptul că operatorilor care operează în UE li se interzice divulgarea datelor cu caracter personal unei țări terțe în cazul în care acest lucru este solicitat de către o autoritate judiciară sau administrativă a unei țări terțe, exceptând cazul în care acest lucru este autorizat explicit printr-un acord internațional sau prevăzut în tratate de asistență judiciară reciprocă sau aprobat de o autoritate de supraveghere. Regulamentul (CE) nr. 2271/96 al Consiliului constituie un exemplu adecvat de temei juridic în acest sens[46]. Grupul de lucru este preocupat de această lacună din propunerea Comisiei deoarece aceasta implică o pierdere considerabilă în termeni de siguranță juridică pentru persoanele vizate ale căror date cu caracter personal sunt stocate în centre de date localizate peste tot în lume. Din acest motiv, grupul de lucru ar dori să sublinieze[47] necesitatea de a include în regulament utilizarea obligatorie a tratatelor de asistență judiciară reciprocă în cazul divulgărilor neautorizate de legislația UE sau a statelor membre.

- Precauții speciale din partea sectorului public: trebuie adăugată o mențiune specială referitoare la necesitatea ca un organism public să evalueze mai întâi dacă comunicarea, prelucrarea și stocarea datelor în afara teritoriului național pot expune securitatea și viața privată a cetățenilor, precum și securitatea și economia națională la riscuri inacceptabile – în special dacă sunt implicate baze de date (de exemplu, date de recensământ) și servicii (de exemplu, de sănătate) care implică date sensibile[48]. Această atenție deosebită ar trebui acordată, oricum, de fiecare dată când sunt prelucrate date sensibile în contextul unui mediu de cloud computing. Din acest punct de vedere, guvernele naționale și instituțiile Uniunii Europene ar putea lua în considerare investigarea suplimentară a conceptului de „mediu de cloud computing guvernamental european" ca spațiu virtual supra-național în care ar putea fi aplicat un set de reguli coerente și armonizate.
- Parteneriatul european privind cloud computing: grupul de lucru sprijină strategia Parteneriatului european privind cloud computing (*European Cloud Partnership, ECP*)

---

46 Regulamentul (CE) nr. 2271/96 al Consiliului din 22 noiembrie 1996 de protecție împotriva efectelor aplicării extrateritoriale a unei legislații adoptate de către o țară terță, precum și a acțiunilor întemeiate pe aceasta sau care rezultă din aceasta, Jurnalul Oficial L 309 , 29/11/1996 P. 0001 - 0006, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:10:01:31996R2271:RO:PDF

47 Conform WP 191 – Avizul nr. 01/2012 privind propunerile de reformă referitoare la protecția datelor, pagina 23.

48 În acest sens, ENISA formulează următoarea recomandare în lucrarea sa privind „Securitatea și reziliența în mediul cloud guvernamental" (http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport): „În termeni de arhitectură, pentru aplicațiile care prelucrează date sensibile, mediile de cloud computing private și comunitare par să fie soluția care se potrivește în prezent cel mai bine cu nevoile administrațiilor publice deoarece acestea oferă cel mai înalt nivel de guvernanță, control și vizibilitate, chiar dacă în momentul planificării unui mediu de cloud computing privat sau comunitar ar trebui acordată o atenție specială amplitudinii infrastructurii."

prezentată de d-na Kroes, vicepreședinte al Comisiei Europene, în ianuarie 2012, la Davos[49]. Această strategie implică achiziții publice de tehnologia informației în vederea stimulării unei piețe europene a serviciilor de cloud computing. Transferul de date către un furnizor european de servicii de cloud computing, guvernat în mod suveran de legislația europeană privind protecția datelor, ar putea aduce avantaje importante pentru clienți în ceea ce privește protecția datelor, în special prin intensificarea adoptării de standarde comune (mai ales în ceea ce privește interoperabilitatea și portabilitatea datelor), precum și prin siguranța juridică.

[49] Neelie Kroes, vicepreședinte al Comisiei Europene responsabil cu Agenda digitală, Stabilirea Parteneriatului european privind cloud computing (*Setting up the European Cloud Partnership*) Forumul Economic Mondial Davos, Elveția, 26 ianuarie 2012, URL: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/1 23.

ANEXĂ

a) Modele de implementare

Mediu de cloud computing privat[50] descrie o infrastructură de tehnologia informației dedicată unei organizații individuale; acesta este localizat la sediul organizațiilor sau gestionarea acestuia este externalizată către o parte terță (de obicei, prin intermediul găzduirii serverului) care se află sub autoritatea strictă a operatorului. Un mediu de cloud computing privat poate fi comparat cu un centru de date convențional – diferența constând în faptul că măsurile tehnologice sunt implementate pentru a optimiza utilizarea resurselor disponibile și pentru a consolida resursele respective prin intermediul investițiilor mici realizate treptat, în timp.

Mediu de cloud computing public, pe de altă parte, este o infrastructură deținută de un furnizor specializat în furnizarea de servicii care pune la dispoziție –, prin urmare, partajează – sistemele sale pentru/în rândul unor utilizatori, întreprinderi și/sau organisme administrative publice. Serviciile pot fi accesate prin intermediul internetului, fapt care implică transferarea operațiunilor de prelucrare a datelor sau a datelor către sistemele furnizorului de servicii. Prin urmare, furnizorul de servicii își asumă un rol cheie în ceea ce privește protecția efectivă a datelor încredințate sistemelor sale. Împreună cu datele, un utilizator este obligat să transfere o mare parte din controlul său asupra datelor respective.

Pe lângă mediile de cloud computing „publice" și „private", există așa-numitele medii de cloud computing „intermediare" sau „hibride" în care serviciile furnizate de infrastructurile private coexistă cu serviciile achiziționate din mediile publice. Ar trebui făcută referire, de asemenea, la „mediile de cloud computing comunitare", în care infrastructura de tehnologia informației este partajată de mai multe organizații în beneficiul unei comunități specifice de utilizatori.

Flexibilitatea și simplitatea în configurarea sistemelor de cloud computing permit dimensionarea „elastică" a acestora, însemnând că aceste sisteme pot fi ajustate în funcție de cerințe specifice în conformitate cu o abordare bazată pe tipul utilizării. Utilizatorii nu trebuie să gestioneze sistemele de tehnologia informației care stau la baza acordurilor de externalizare, acestea fiind, prin urmare, administrate integral de partea terță în a cărui mediu de cloud computing sunt stocate datele. Deseori intervin furnizori mari cu infrastructuri complexe; prin urmare, mediul de cloud computing ar putea include mai multe locații și este posibil ca utilizatorii să nu mai știe unde exact sunt stocate datele acestora.

---

[50] Institutul Național de Standarde și Tehnologie (*National Institute of Standards and Technology, NIST*) din SUA, care lucrează de câțiva ani în domeniul standardizării tehnologiilor bazate pe medii de cloud computing și ale cărui definiții sunt, de asemenea, menționate în documentul ENISA:
Mediu de cloud computing privat.
Infrastructura de *cloud computing* este operată exclusiv pentru o organizație. Aceasta poate fi gestionată de către organizația respectivă sau de o parte terță și poate exista la sediul acesteia sau la distanță. Trebuie subliniat faptul că un „mediu de cloud computing privat" se bazează cel puțin pe anumite tehnologii care sunt, de asemenea, tipice „mediilor de cloud computing publice" – inclusiv, în special, tehnologii de virtualizare care intensifică reorganizarea (sau revizuirea) arhitecturii de prelucrare a datelor, astfel cum a fost explicată mai sus.
Mediu de cloud computing public.
Infrastructura de cloud computing publică este pusă la dispoziția publicului general sau a unui mare grup industrial și este deținută de o organizație care furnizează servicii de cloud computing.

b) Modele de furnizare a serviciilor

În funcție de cerințele utilizatorilor, există mai multe soluții de cloud computing disponibile pe piață; acestea pot fi grupate în trei categorii mari sau „modele de servicii". Aceste modele se aplică, de obicei, atât soluțiilor de cloud computing private, cât și celor publice:

- **IaaS (Cloud Infrastructure as a Service):** Un furnizor închiriază o infrastructură tehnologică, și anume servere virtuale la distanță pe care utilizatorul final se poate baza în conformitate cu mecanisme și măsuri astfel încât să facă simplă, eficientă precum și avantajoasă opțiunea de a înlocui sistemele corporatiste de tehnologia informației de la sediul întreprinderii și/sau să utilizeze infrastructura închiriată împreună cu sistemele corporatiste. Furnizorii sunt, de obicei, actori specializați care operează pe piață și se pot baza, de altfel, pe o infrastructură fizică complexă care cuprinde deseori mai multe zone geografice.
- **SaaS (Cloud Software as a Service):** Un furnizor oferă, prin intermediul internetului, diferite servicii de aplicații pe care le pune la dispoziția utilizatorilor finali. Serviciile sunt deseori destinate să înlocuiască aplicațiile convenționale instalate de utilizatori în sistemele lor locale; prin urmare, utilizatorii sunt în cele din urmă obligați să-și externalizeze datele către furnizorul individual. Acest lucru este valabil, de exemplu, în cazul aplicațiilor de birou tipice bazate pe internet precum fișiere, instrumente de editare a textelor, registre și agende computerizate, calendare partajate etc.; cu toate acestea, serviciile în cauză includ, de asemenea, aplicații e-mail bazate pe medii de cloud computing.
- **PaaS (Cloud Platform as a Service):** Un furnizor oferă soluții pentru dezvoltarea și găzduirea avansată de aplicații. Serviciile se adresează, de regulă, actorilor care operează pe piață care le utilizează pentru a dezvolta și găzdui soluții bazate pe aplicații proprietare pentru a îndeplini cerințe stabilite la nivel intern și/sau pentru a furniza servicii către terți. Din nou, serviciile furnizate de către un furnizor PaaS fac inutil recursul unui utilizator la componente hardware sau soluții informatice specifice și/sau adiționale la nivel intern.

Se pare că o tranziție veritabilă către un sistem de cloud computing public total nu este posibilă pe termen scurt din mai multe motive, care țin în special de entitățile mari precum întreprinderile sau organizațiile importante care trebuie să îndeplinească obligații specifice – de exemplu, bănci importante, organisme guvernamentale, municipalități mari etc. Acest lucru poate fi susținut, în principal, de două motive: în primul rând, există un factor de tip impuls în ceea ce privește investițiile necesare realizării unei astfel de tranziții; în al doilea rând, trebuie avute în vedere informațiile care prezintă un interes particular și/sau cu caracter sensibil care urmează să fie prelucrate în cazuri specifice.

Un alt factor care militează în favoarea utilizării mediilor de cloud computing private (cel puțin în cazurile menționate mai sus) se referă la faptul că adeseori niciun furnizor public de servicii de cloud computing nu poate asigura o calitate a serviciului (astfel cum se prevede în acordurile privind nivelul serviciilor) pentru a ține pasul cu natura critică a serviciului pe care operatorul îl furnizează – cauzat probabil de faptul că lățimea benzii și fiabilitatea rețelei nu sunt încă suficiente sau adecvate într-o anumită regiune sau în ceea ce privește conexiunile specifice utilizator-furnizor. Pe de altă parte, se poate presupune în mod rezonabil că mediile de cloud computing private pot fi închiriate sau pot face obiectul unui contract de leasing în câteva dintre cazurile de mai sus (deoarece acest lucru s-ar putea dovedi mai eficient din punct de vedere al costurilor) sau pot fi introduse modele de cloud computing hibride (incluzând componente publice și private). Implicațiile relevante ar trebui analizate cu atenție în toate cazurile.

În absența unor standarde stabilite la nivel internațional, există riscul apariției de soluții de cloud computing proprii (de tipul „do-it-yourself") sau partajate, care ar implica creșterea numărului de riscuri de blocaj (precum și a așa-numitelor „monoculturi de viață privată" („privacy monocultures")[51] și împiedicarea controlului total asupra datelor fără a asigura interoperabilitatea. Atât interoperabilitatea, cât și portabilitatea datelor constituie, într-adevăr, factori cheie în dezvoltarea tehnologiei bazate pe cloud computing, precum și pentru a permite exercitarea deplină a drepturilor privind protecția datelor acordate persoanelor vizate (precum cele de acces sau rectificare).

Din acest punct de vedere, dezbaterea actuală privind tehnologiile de cloud computing constituie un exemplu semnificativ referitor la tensiunea care există între abordările orientate înspre costuri și cele orientate înspre drepturi, astfel cum s-a evidențiat succint în secțiunea 2 de mai sus. În timp ce utilizarea de medii de cloud computing private poate fi realizabilă și chiar recomandabilă din perspectiva protecției datelor având în vedere circumstanțele specifice ale prelucrării, aceasta ar putea să nu fie viabilă pe termen lung în cazul organizațiilor, în special dintr-o perspectivă orientată înspre costuri. Este necesară o evaluare atentă a intereselor implicate, deoarece, în prezent, nu poate fi indicată o soluție universală în domeniu.

[51] A se vedea studiul realizat de Parlamentul European, „Ajutor sau piedică? Promovarea inovației pe internet și dreptul cetățenilor la viață privată" („Does it Help or Hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy"), publicat în decembrie 2011.