GRUPUL DE LUCRU „ARTICOLUL 29” PENTRU PROTECȚIA DATELOR

18/RO

WP 254 rev. 01

Grupul de lucru „articolul 29”

Criterii de referință privind caracterul adecvat al nivelului de protecție

Adoptate la 28 noiembrie 2017

Astfel cum au fost revizuite ultima dată și adoptate la 6 februarie 2018

Introducere

Grupul de lucru al autorităților UE pentru protecția datelor[1] (GL29) a publicat deja un document de lucru cu privire la transferurile de date cu caracter personal către țări terțe (WP12)[2]. Odată cu înlocuirea directivei prin Regulamentul general privind protecția datelor (RGPD)[3] al UE, GL29 revizuiește WP12, orientările sale anterioare, pentru a le actualiza în contextul noii legislații și al jurisprudenței recente a Curții de Justiție a Uniunii Europene (CJUE)[4].

Prezentul document de lucru urmărește să actualizeze capitolul 1 din WP12 cu privire la întrebarea centrală privind nivelul adecvat de protecție a datelor într-o țară terță, un teritoriu sau unul sau mai multe sectoare specificate din respectiva țară terță sau într-o organizație internațională (denumite în continuare „țări terțe sau organizații internaționale"). Documentul va fi revizuit continuu și, dacă este necesar, va fi actualizat în anii următori, pe baza experienței practice acumulate prin aplicarea RGPD. Capitolul 2 (*Aplicarea abordării în cazul țărilor care au ratificat Convenția 108*) și capitolul 3 (*Aplicarea abordării pentru autoreglementarea industriei*) din documentul WP12 ar trebui actualizate într-o etapă ulterioară.

Prezentul document de lucru se concentrează exclusiv asupra deciziilor privind caracterul adecvat al nivelului de protecție, care sunt acte de punere în aplicare[5] ale Comisiei Europene, în conformitate cu articolul 45 din RGPD. Alte aspecte legate de transferurile de date cu caracter personal către țări terțe și organizații internaționale vor fi examinate în următoarele documente de lucru care vor fi publicate separat (reguli corporatiste obligatorii, derogări).

Prezentul document urmărește să ofere orientări Comisiei Europene și GL29 în temeiul RGPD pentru evaluarea nivelului de protecție a datelor în țări terțe și organizații internaționale, stabilind principalele principii de protecție a datelor care trebuie să fie prezente în cadrul juridic al unei țări terțe sau al unei organizații internaționale în scopul de a asigura echivalența esențială cu cadrul UE. În plus, acesta ar putea ghida țările terțe și organizațiile internaționale interesate să obțină un caracter adecvat al nivelului de protecție. Cu toate acestea, principiile enunțate în prezentul document de lucru nu sunt adresate direct operatorilor de date sau persoanelor împuternicite de către operatori.

Prezentul document conține 4 capitole:

Capitolul 1: Unele informații generale referitoare la conceptul de caracter adecvat al nivelului de protecție

Capitolul 2: Aspecte procedurale pentru constatările privind caracterul adecvat al nivelului de protecție în temeiul RGPD

Capitolul 3: Principii generale privind protecția datelor. Acest capitol include principalele principii generale privind protecția datelor pentru a asigura că nivelul de protecție a datelor într-o țară terță sau organizație internațională este, în esență, echivalent cu cel stabilit de legislația UE.

Capitolul 4: Garanții esențiale cu privire la acces în scopul asigurării respectării legii și în scopul securității naționale pentru a limita interferențele cu drepturile fundamentale Acest capitol include garanțiile esențiale cu privire la acces în scopul asigurării respectării legii și în scopul securității naționale în urma hotărârii CJUE în cauza Schrems din 2015 și se bazează pe documentul de lucru al GL29 privind garanțiile esențiale adoptat în 2016.

---

[1] Astfel cum este stabilit în temeiul articolului 29 din Directiva UE privind protecția datelor 95/46/CE

2 WP12 , „Documentul de lucru: Transferurile de date cu caracter personal către țările terțe: aplicarea articolelor 25 și 26 din Directiva UE privind protecția datelor", adoptat de grupul de lucru la 24 iulie 1998.

3 Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE).

4 Inclusiv cauza C-362/14, Maximillian Schrems/Comisarul pentru protecția datelor, 6 octombrie 2015.

[5] Pentru informații suplimentare privind actele de punere în aplicare, a se vedea articolul 45 alineatul (3) și articolul 93 alineatul (2) din RGPD.

Capitolul 1: Informații generale referitoare la conceptul de caracter adecvat al nivelului de protecție

Articolul 45 alineatul (1) din RGPD stabilește principiul conform căruia transferurile de date către o țară terță sau o organizație internațională au loc numai în cazul în care țara terță, teritoriul acesteia sau unul sau mai multe sectoare specificate din țara terță respectivă sau organizația internațională în cauză asigură un nivel adecvat de protecție.

Acest concept de „nivel adecvat de protecție", care exista deja în cadrul Directivei 95/46, a fost dezvoltat în continuare de Curtea de Justiție a Uniunii Europene. În acest moment, este important de reamintit standardul stabilit de CJUE în cauza Schrems, și anume că, deși „nivelul de protecție" din țara terță trebuie să fie „în esență, echivalent" cu cel garantat în UE, „mijloacele la care această țară terță a recurs, în această privință, pentru a asigura un astfel de nivel de protecție pot fi diferite de cele puse în aplicare în cadrul [UE]"[6]. Prin urmare, obiectivul nu este de a reflecta punct cu punct legislația europeană, ci de a stabili cerințele principale – esențiale ale legislației respective.

Scopul deciziilor privind caracterul adecvat al nivelului de protecție luate de Comisia Europeană este de a confirma în mod oficial, cu efecte obligatorii asupra statelor membre[7], că nivelul de protecție a datelor într-o țară terță sau o organizație internațională este, în esență, echivalent cu nivelul de protecție a datelor din Uniunea Europeană[8]. Caracterul adecvat al nivelului de protecție poate fi obținut prin intermediul unei combinații de drepturi pentru persoanele vizate și obligații pentru cei care prelucrează date sau care exercită control asupra prelucrării, precum și prin supravegherea de către organisme independente. Cu toate acestea, normele de protecție a datelor sunt eficace numai dacă sunt executorii și sunt respectate în practică. Prin urmare, este necesar să se ia în considerare nu numai conținutul normelor aplicabile transferului de date cu caracter personal către o țară terță sau o organizație internațională, ci și sistemul existent pentru asigurarea eficacității unor astfel de norme. Mecanismele eficiente de punere în aplicare sunt de o importanță fundamentală pentru eficacitatea normelor de protecție a datelor.

Articolul 45 alineatul (2) din RGPD stabilește elementele de care Comisia Europeană trebuie să țină seama atunci când evaluează caracterul adecvat al nivelului de protecție dintr-o țară terță sau o organizație internațională.

De exemplu, Comisia ține seama de statul de drept, de respectarea drepturilor omului și a libertăților fundamentale, de legislația relevantă, de existența și funcționarea efectivă a uneia sau a mai multor autorități de supraveghere independente și de angajamentele internaționale asumate de țara terță sau de organizația internațională.

Prin urmare, este clar că orice analiză pertinentă a nivelului adecvat de protecție trebuie să includă cele două elemente fundamentale: conținutul normelor aplicabile și mijloacele pentru asigurarea aplicării efective a acestora. Comisiei Europene îi revine să verifice – în mod regulat – că normele în vigoare sunt eficace în practică.

„Nucleul" principiilor privind „conținutul" protecției datelor și cerințele „procedurale/de asigurare a respectării", care ar putea fi considerate o cerință minimă pentru ca nivelul de protecție să fie adecvat, sunt derivate din Carta drepturilor fundamentale a Uniunii Europene și din RGPD. În plus, ar trebui să se ia în considerare, de asemenea, alte acorduri internaționale în materie de protecție a datelor, de exemplu Convenția 108[9].

De asemenea, este necesar să se acorde atenție cadrului juridic pentru accesul autorităților publice la datele cu caracter personal. Orientări suplimentare cu privire la acest aspect sunt prevăzute în

---

[6] Cauza C-362/14, Maximillian Schrems/Comisarul pentru protecția datelor, 6 octombrie 2015 (punctele 73, 74).

[7] Articolul 288 alineatul (2) din TFUE.

[8] Cauza C-362/14, Maximillian Schrems/Comisarul pentru protecția datelor, 6 octombrie 2015 (punctul 52).

9 Considerentul 105 din RGPD.

documentul de lucru 237 (și anume, documentul privind garanțiile esențiale)[10] cu privire la garanțiile în contextul supravegherii.

Nu este suficientă existența unor dispoziții generale privind protecția datelor și a vieții private în țara terță. În cadrul juridic al țării terțe sau al organizației internaționale trebuie să fie incluse, de asemenea, dispoziții specifice care să abordeze nevoile concrete privind aspectele relevante din punct de vedere practic ale dreptului la protecția datelor. Aceste dispoziții trebuie să fie executorii.

Capitolul 2: Aspecte procedurale pentru constatările privind caracterul adecvat al nivelului de protecție în temeiul RGPD

Pentru ca CEPD (Comitetul european pentru protecția datelor) să își îndeplinească misiunea de consiliere a Comisiei Europene în conformitate cu articolul 70 alineatul (1) litera (s) din RGPD, acestuia ar trebui să i se pună la dispoziție documentația relevantă, inclusiv corespondența relevantă și constatările Comisiei Europene. În cazul în care cadrul legislativ este complex, aceasta ar trebui să includă orice raport întocmit cu privire la nivelul de protecție a datelor n țara terță sau organizația internațională. În orice caz, informațiile furnizate de Comisia Europeană ar trebui să fie exhaustive și să acorde CEPD posibilitatea de a efectua o evaluare proprie în ceea ce privește nivelul de protecție a datelor în țara terță. CEPD va furniza un aviz cu privire la constatările Comisiei Europene în timp util și, dacă este cazul, va identifica deficiențe ale cadrului privind caracterul adecvat al nivelului de protecție. De asemenea, CEPD va face tot posibilul pentru a propune modificări sau amendamente în scopul de a remedia eventualele deficiențe.

În conformitate cu articolul 45 alineatul (4) din RGPD, Comisiei Europene îi revine sarcina de a monitoriza – în mod permanent – evoluțiile care ar putea afecta funcționarea unei decizii privind caracterul adecvat al nivelului de protecție.

Articolul 45 alineatul (3) din RGPD prevede că trebuie să se efectueze o revizuire periodică cel puțin o dată la patru ani. Acesta este însă un interval de timp general care trebuie să fie ajustat pentru fiecare țară terță sau organizație internațională cu o decizie privind caracterul adecvat al nivelului de protecție. În funcție de circumstanțele specifice ale fiecărui caz, ar putea fi justificat un ciclu de revizuire mai scurt. De asemenea, incidentele sau alte informații despre cadrul juridic din țara terță sau organizația internațională în cauză sau schimbări ale acestuia ar putea determina necesitatea unei revizuiri înainte de termen. În plus, pare adecvat ca o primă analiză a unei decizii complet noi privind caracterul adecvat al nivelului de protecție să fie efectuată destul de curând și ca ciclul de revizuire să fie adaptat progresiv în funcție de rezultat.

Având în vedere mandatul de a furniza Comisiei Europene un aviz cu privire la faptul că țara terță, un teritoriu sau unul sau mai multe sectoare specificate din țara terță sau o organizație internațională asigură sau nu mai asigură un nivel adecvat de protecție, CEPD trebuie să primească, în timp util, informații semnificative privind monitorizarea evoluțiilor relevante din respectiva țară terță sau organizație internațională de la Comisia Europeană. Prin urmare, CEPD ar trebui să fie informat cu privire la orice proces de revizuire și misiune de evaluare în țara terță sau la organizația internațională. CEPD ar aprecia invitația de a participa la aceste procese de revizuire și misiuni de evaluare.

De asemenea, ar trebui remarcat că, în conformitate cu articolul 45 alineatul (5) din RGPD, Comisia Europeană are dreptul să abroge, să modifice sau să suspende deciziile existente privind caracterul adecvat al nivelului de protecție. Procedura de abrogare, de modificare sau de suspendare ar trebui, în consecință, să implice CEPD, prin solicitarea avizului său în conformitate cu articolul 70 alineatul (1) litera (s).

În plus, astfel cum se recunoaște în prezent la articolul 58 alineatul (5) din RGPD și în conformitate cu hotărârea CJUE în cauza Schrems, autoritățile pentru protecția datelor trebuie să aibă posibilitatea de a acționa în justiție în cazul în care constată că o sesizare făcută de către o persoană împotriva unei decizii privind caracterul adecvat este întemeiată: „În această privință, revine legiuitorului național sarcina de a prevedea căi de atac care să permită autorității naționale de supraveghere în cauză să

[10] Documentul de lucru 01/2016 privind justificarea interferențelor cu drepturile fundamentale la viață privată și protecția datelor prin măsuri de supraveghere atunci când se transferă date cu caracter personal (Garanții esențiale europene), 16/EN WP 237, 13 aprilie 2016.

invoce motivele pe care le consideră întemeiate în fața instanțelor naționale, astfel încât acestea din urmă să efectueze, dacă împărtășesc îndoielile acestei autorități în ceea ce privește validitatea deciziei Comisiei, o trimitere preliminară în vederea examinării validității acestei decizii”[11].

[11] Cauza C-362/14, Maximillian Schrems/Comisarul pentru protecția datelor, 6 octombrie 2015 (punctul 65).

Capitolul 3: Principii generale în materie de protecție a datelor pentru a garanta că nivelul de protecție dintr-o țară terță, un teritoriu sau unul sau mai multe sectoare specificate din țara terță sau o organizație internațională este, în esență, echivalent cu cel garantat de legislația UE

Sistemul unei țări terțe sau al unei organizații internaționale trebuie să conțină următoarele principii și mecanisme fundamentale de protecție a datelor referitoare la conținut și la procedură/asigurarea respectării:

A. <u>Principii referitoare la conținut:</u>

1) Concepte

Ar trebui să existe concepte și/sau principii de bază în materie de protecție a datelor. Acestea nu trebuie să corespundă terminologiei RGPD, dar ar trebui să reflecte conceptele consacrate în legislația europeană privind protecția datelor și să fie în concordanță cu acestea. De exemplu, RGPD include următoarele concepte importante: „date cu caracter personal", „prelucrarea datelor cu caracter personal", „operator de date", „persoană împuternicită de către operator", „destinatar" și „date sensibile".

2) Motive care justifică prelucrarea legală și echitabilă în scopuri legitime

Datele trebuie să fie prelucrate în mod legal, echitabil și legitim.

Temeiurile legitime, în baza cărora datele cu caracter personal pot fi prelucrate în mod legal, echitabil și legitim, ar trebui să fie stabilite într-un mod suficient de clar. Cadrul european recunoaște mai multe astfel de temeiuri legitime incluzând, de exemplu, dispozițiile din dreptul național, consimțământul persoanei vizate, executarea unui contract sau un interes legitim al operatorului de date sau al unui terț care nu prevalează asupra intereselor persoanei.

3) Principiul limitării scopului

Datele ar trebui să fie prelucrate într-un scop anume și să fie utilizate ulterior numai în măsura în care acest lucru nu este incompatibil cu scopul prelucrării.

4) Principiul calității datelor și al proporționalității

Datele ar trebui să fie exacte și, dacă este necesar, actualizate. Datele ar trebui să fie adecvate, relevante și neexcesive în raport cu scopurile în care sunt prelucrate.

5) Principiul privind păstrarea datelor

Ca regulă generală, datele nu ar trebui să fie păstrate o perioadă mai îndelungată decât este necesar în vederea atingerii scopurilor pentru care sunt prelucrate datele cu caracter personal.

6) Principiul confidențialității și al securității

Orice entitate care prelucrează date cu caracter personal ar trebui să se asigure că datele sunt prelucrate într-un mod care asigură securitatea datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării

accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare. Nivelul de securitate ar trebui să ia în considerare stadiul actual al tehnologiei și costurile aferente.

7) Principiul transparenței

Fiecare persoană ar trebui să fie informată cu privire la toate elementele principale ale prelucrării datelor sale cu caracter personal într-o formă clară, ușor accesibilă, concisă, transparentă și comprehensibilă. Astfel de informații ar trebui să includă scopul prelucrării, identitatea operatorului de date, drepturile de care dispune și alte informații în măsura în care acest lucru este necesar pentru a asigura o procedură echitabilă. În anumite condiții, pot exista unele excepții de la acest drept la informații, cum ar fi, de exemplu, pentru a proteja anchetele penale, securitatea națională, independența judiciară și procedurile judiciare sau alte obiective importante de interes public general, astfel cum se prevede la articolul 23 din RGPD.

8) Dreptul de acces, la rectificare, la ștergere și la opoziție

Persoana vizată ar trebui să aibă dreptul de a i se confirma dacă se desfășoară sau nu o prelucrare a datelor care o privesc, precum și de a obține acces la datele sale, inclusiv de a obține o copie a tuturor datelor care o privesc, care sunt prelucrate.

Persoana vizată ar trebui să aibă dreptul de a obține rectificarea datelor care o privesc, după caz, pentru anumite motive, de exemplu dacă acestea se dovedesc a fi inexacte sau incomplete, precum și ștergerea datelor sale cu caracter personal, de exemplu atunci când prelucrarea acestora nu mai este necesară sau este ilegală.

Persoana vizată ar trebui să aibă dreptul de a se opune în orice moment, din motive întemeiate și legitime legate de situația sa particulară, prelucrării datelor care o privesc, conform condițiilor specifice stabilite în cadrul juridic al țării terțe. În RGPD, de exemplu, aceste condiții includ cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini executate în interes public sau cazul în care aceasta este necesară pentru exercitarea autorității publice cu care este învestit operatorul de date sau atunci când prelucrarea este necesară în scopul intereselor legitime urmărite de operatorul de date sau de o parte terță.

Exercitarea acestor drepturi nu ar trebui să fie excesiv de greoaie pentru persoana vizată. Ar putea exista eventuale restricții cu privire la aceste drepturi, de exemplu, pentru a proteja anchetele penale, securitatea națională, independența judiciară și procedurile judiciare sau alte obiective importante de interes public general, astfel cum se prevede la articolul 23 din RGPD.

9) Restricții privind transferurile ulterioare de date

Transferurile ulterioare de date cu caracter personal efectuate de destinatarul inițial al transferului de date ar trebui să fie autorizate numai în cazul în care noul destinatar (și anume, destinatarul transferului ulterior) face, de asemenea, obiectul unor norme (inclusiv norme contractuale) care asigură un nivel adecvat de protecție și urmează instrucțiunile relevante atunci când prelucrează date în numele operatorului de date. Nivelul de protecție a persoanelor fizice ale căror date sunt transferate nu trebuie să fie subminat de transferul ulterior. Destinatarul inițial al datelor transferate din UE este responsabil să asigure faptul că sunt prevăzute garanții adecvate pentru transferurile ulterioare de date în absența unei decizii privind caracterul adecvat al nivelului de protecție. Astfel de transferuri ulterioare de date ar trebui să se realizeze numai pentru scopuri specificate și limitate și în măsura în care există un temei juridic pentru prelucrarea respectivă.

B. Exemple de principii suplimentare privind conținutul care trebuie aplicate anumitor tipuri de prelucrare:

1) Categorii speciale de date

Ar trebui să existe garanții specifice în cazul în care sunt implicate „categorii speciale de date”[12]. Aceste categorii ar trebui să le reflecte pe cele prevăzute la articolele 9 și 10 din RGPD. Această protecție ar trebui să fie instituită prin intermediul unor cerințe mai stricte pentru prelucrarea datelor, cum ar fi, de exemplu, ca persoana vizată să își dea consimțământul explicit pentru prelucrare, sau prin măsuri de securitate suplimentare.

2) Marketing direct

Atunci când datele sunt prelucrate în scopuri de marketing direct, persoana vizată ar trebui să aibă posibilitatea de a obiecta gratuit, în orice moment, ca datele sale cu caracter personal să fie prelucrate în acest scop.

3) Procesul decizional automatizat și crearea de profiluri

Deciziile bazate exclusiv pe prelucrarea automată (procesul decizional individual automatizat), inclusiv crearea de profiluri, care produc efecte juridice sau care afectează în mod semnificativ persoana vizată pot avea loc numai în anumite condiții stabilite în cadrul juridic al țării terțe. În cadrul european, aceste condiții includ, de exemplu, necesitatea de a obține consimțământul explicit al persoanei vizate sau necesitatea unei astfel de decizii pentru încheierea unui contract. În cazul în care decizia nu respectă astfel de condiții stabilite în cadrul juridic al țării terțe, persoana vizată ar trebui să aibă dreptul de a nu face obiectul deciziei respective. Legislația țării terțe ar trebui, în orice caz, să prevadă garanțiile necesare, inclusiv dreptul de a fi informat cu privire la motivele specifice care stau la baza deciziei și logica implicată, de a corecta informațiile inexacte sau incomplete, precum și de a contesta decizia în cazul în care aceasta a fost adoptată în baza unui temei de fapt incorect.

C. Mecanismele procedurale și de aplicare:

Chiar dacă mijloacele la care țara terță a recurs pentru a asigura un nivel adecvat de protecție pot fi diferite de cele puse în aplicare în cadrul Uniunii Europene[13], un sistem coerent cu cel european trebuie să fie caracterizat prin existența următoarelor elemente:

1) Autoritatea independentă competentă de supraveghere

Ar trebui să existe una sau mai multe autorități independente de supraveghere, însărcinate cu monitorizarea, asigurarea și impunerea respectării dispozițiilor privind protecția datelor și a vieții private în țara terță. Autoritatea de supraveghere beneficiază de independență și imparțialitate deplină în îndeplinirea sarcinilor sale și în exercitarea competențelor sale și, în acest sens, nu solicită și nici nu acceptă instrucțiuni. În acest context, autoritatea de supraveghere ar trebui să dețină toate competențele necesare și disponibile și să desfășoare misiuni pentru a asigura conformitatea cu drepturile în materie de protecție a datelor și a promova creșterea gradului de sensibilizare. Ar trebui

[12] Astfel de categorii speciale sunt denumite, de asemenea, „date sensibile” în considerentul 10 din RGPD.

[13] Cauza C-362/14, Maximillian Schrems/ Comisarul pentru protecția datelor, 6 octombrie 2015, punctul 74.

acordată atenție, de asemenea, personalului și bugetului autorității de supraveghere. De asemenea, autoritatea de supraveghere poate, din proprie inițiativă, să efectueze investigații.

2) Sistemul de protecție a datelor trebuie să asigure un bun nivel de conformitate

Sistemul unei țări terțe ar trebui să asigure un nivel ridicat de responsabilitate și de sensibilizare în rândul operatorilor de date și al celor care prelucrează datele cu caracter personal în numele acestora cu privire la obligațiile, sarcinile și responsabilitățile care le revin, precum și în rândul persoanelor vizate cu privire la drepturile lor și la mijloacele de exercitare a acestora. Existența unor sancțiuni eficace și disuasive poate juca un rol important în asigurarea respectării normelor, la fel ca sistemele de verificare directă de către autorități, auditori sau funcționari independenți însărcinați cu protecția datelor.

3) Responsabilitate

Cadrul de protecție a datelor al unei țări terțe ar trebui să oblige operatorii de date și/sau pe cei care prelucrează datele cu caracter personal în numele acestora să îl respecte și să fie în măsură să își dovedească conformitatea în special în fața autorității de supraveghere competente. Astfel de măsuri pot include, de exemplu, evaluări ale impactului asupra protecției datelor, păstrarea de evidențe sau fișiere-jurnal ale activităților de prelucrare a datelor pentru o perioadă de timp corespunzătoare, desemnarea unui responsabil cu protecția datelor sau protecția datelor din faza de concepție și protecția implicită a datelor.

4) Sistemul de protecție a datelor trebuie să furnizeze asistență și sprijin persoanelor individuale vizate în exercitarea drepturilor acestora și mecanisme adecvate de recurs

Fiecare persoană ar trebui să aibă posibilitatea de a acționa pentru a-și exercita drepturile în mod rapid și eficace, fără costuri prohibitive, precum și de a asigura respectarea acestora. În acest scop, trebuie să existe mecanisme de supraveghere care să permită investigarea independentă a plângerilor și identificarea și sancționarea în practică a tuturor încălcărilor dreptului la protecția datelor și la respectarea vieții private.

În cazul în care normele nu sunt respectate, ar trebui să se pună la dispoziția persoanei vizate și căi de atac administrative și judiciare eficiente, inclusiv în vederea despăgubirii pentru daunele suferite în urma prelucrării ilegale a datelor sale cu caracter personal. Acesta este un element esențial care trebuie să implice un sistem independent de adjudecare sau arbitraj care să permită plata de despăgubiri și impunerea de sancțiuni, după caz.

Capitolul 4: Garanții esențiale în țările terțe cu privire la accesul în scopuri legate de asigurarea respectării legii și de securitatea națională pentru a limita interferențele cu drepturile fundamentale

Atunci când evaluează caracterul adecvat al nivelului de protecție, în temeiul articolului 45 alineatul (2) litera (a) Comisia trebuie să ia în considerare „legislația relevantă, atât generală, cât și sectorială, inclusiv privind securitatea publică, apărarea, securitatea națională și dreptul penal, precum și accesul autorităților publice la datele cu caracter personal, precum și punerea în aplicare a acestei legislații [...]".

În hotărârea în cauza Schrems, CJUE a remarcat că „expresia «nivel de protecție adecvat» trebuie înțeleasă în sensul că impune ca această țară terță să asigure efectiv, în temeiul legislației interne sau al angajamentelor sale internaționale, un nivel de protecție a drepturilor și libertăților fundamentale în esență echivalent cu cel garantat în cadrul Uniunii în temeiul Directivei 95/46, interpretată în lumina cartei". Chiar dacă mijloacele la care țara terță a recurs, în această privință, pot fi diferite de cele utilizate în cadrul Uniunii Europene, aceste mijloace trebuie totuși să se dovedească, în practică, eficace[14].

În acest context, Curtea a remarcat, de asemenea, că decizia anterioară privind sfera de siguranță „nu cuprinde nicio constatare în privința existenței în Statele Unite a unor norme cu caracter statal destinate să limiteze eventualele ingerințe în drepturile fundamentale ale persoanelor ale căror date sunt transferate din Uniune către Statele Unite, ingerințe pe care entități de stat din această țară ar fi autorizate să le practice atunci când urmăresc scopuri legitime precum securitatea națională"

GL29 a identificat în avizul WP 237, adoptat la 13 aprilie 2016, garanțiile esențiale care reflectă jurisprudența CJUE și CEDO în domeniul supravegherii. În timp ce recomandările detaliate din WP237 rămân valabile și ar trebui să fie luate în considerare atunci când se evaluează caracterul adecvat al nivelului de protecție al unei țări terțe în domeniul supravegherii, aplicarea acestor garanții poate fi diferită în domeniile asigurării respectării legii și al securității naționale în materie de acces la date. Cu toate acestea, cele patru garanții trebuie să fie respectate pentru accesul la date, fie în scopuri legate de securitatea națională sau în scopuri de asigurare a respectării legii, de către toate țările terțe, pentru ca nivelul de protecție să fie considerat adecvat:

1) **Prelucrarea trebuie să se bazeze pe norme clare, precise și accesibile (temei juridic)**

2) **Trebuie să se demonstreze necesitatea și proporționalitatea în ceea ce privește obiectivele legitime urmărite**

3) **Prelucrarea trebuie să fie supusă unui control independent**

4) **Trebuie să se pună la dispoziția persoanelor fizice căi de atac eficiente**

[14] Cauza C 362/14, Maximilian Schrems/Comisarul pentru protecția datelor, 6 octombrie 2015, punctul 74.