GRUPUL DE LUCRU „ARTICOLUL 29“ PRIVIND PROTECȚIA DATELOR

00379/13/RO
WP 201

Avizul 01/2013 de furnizare de informații suplimentare pentru discutarea proiectului de directivă privind protecția datelor în domeniul poliției și al justiției penale

Adoptat la 26 februarie 2013

1. Introducere

La 25 ianuarie 2012, Comisia Europeană a adoptat o propunere de *Directivă privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și la libera circulație a acestor date* (denumită în continuare „Directiva privind protecția datelor în domeniul poliției și al justiției penale" sau „directiva"). Propunerea a fost prezentată în paralel cu proiectul de regulament general privind protecția datelor. Ulterior, atât Consiliul, cât și Parlamentul European au demarat procedurile lor respective în procesul legislativ pentru ambele instrumente cu scopul de a ajunge la un acord privind pachetul complet înainte de alegerile europene din 2014. Cu toate acestea, se înregistrează progrese lente în dezbaterea legislativă privind directiva.

Grupul de lucru „articolul 29" și-a exprimat prima reacție generală la propunerile Comisiei în avizul său din 23 martie 2012, în care a evidențiat aspectele care suscită motive de preocupare și a formulat o serie de sugestii de îmbunătățire.

Grupul de lucru „articolul 29" salută așa-numita abordare bazată pe un pachet de măsuri, utilizată de către raportorii Parlamentului European în proiectele lor de rapoarte către Comisia LIBE și are convingerea că toate grupurile politice vor continua să acorde o atenție deosebită tuturor elementelor pachetului, precum și coerenței atât de necesare între cele două propuneri în vederea îmbunătățirii ulterioare a acestora. De asemenea, grupul de lucru salută intensificarea dezbaterii legislative din cadrul Consiliului, declanșată la inițiativa atât a președinției cipriote, cât și a celei irlandeze.

În urma primului aviz de furnizare de informații suplimentare pentru discutarea regulamentului adoptat de grupul de lucru „articolul 29" la 5 octombrie 2012, grupul de lucru prezintă acum orientări suplimentare cu privire la o serie de elemente specifice directivei propuse privind protecția datelor în domeniul poliției și al justiției penale. Deși există mai multe aspecte care s-ar putea discuta în continuare, grupul de lucru a decis, având în vedere stadiul negocierilor, să se concentreze asupra a patru aspecte considerate în prezent a fi cele mai importante. Acestea includ utilizarea datelor persoanelor care nu sunt suspectate, drepturile persoanelor vizate, utilizarea analizelor de impact asupra confidențialității, precum și competențele autorităților pentru protecția datelor, în special în ceea ce privește informațiile confidențiale sau clasificate.

2. Privind utilizarea datelor persoanelor care nu sunt suspectate

Articolul 5 din proiectul de directivă prevede obligația operatorilor de a face o distincție clară între datele cu caracter personal ale diferitelor categorii de persoane și definește cinci categorii de persoane vizate. În conformitate cu considerentul 23, o astfel de distincție este inerentă prelucrării datelor cu caracter personal în domeniul cooperării judiciare în materie penală și cel al cooperării polițienești. GL29 subliniază faptul că o astfel de distincție este, de asemenea, necesară pentru a se asigura punerea în aplicare corespunzătoare a principiilor referitoare la prelucrarea datelor cu caracter personal astfel cum sunt definite la articolul 4.

Articolul 5 face distincție între diversele categorii de persoane care au legătură directă sau indirectă (posibilă) cu o anumită infracțiune sau anumiți suspecți [categoriile (a) - (d)] și alte persoane [categoria (e)]. Având în vedere descrierea legăturii persoanelor menționate la categoriile (a) - (d) cu o infracțiune sau o investigație, este clar că persoanele care se

încadrează în categoria (e) pot fi descrise ca fiind persoane care nu au nicio legătură cunoscută cu o infracțiune sau cu suspecți, astfel cum se menționează la celelalte categorii.

Prin urmare, în 2005, tocmai acest grup de persoane a determinat autoritățile europene pentru protecția datelor[1] să sublinieze necesitatea de a se face o distincție între prelucrarea datelor cu caracter personal ale persoanelor care nu sunt suspectate și cele ale persoanelor care au legătură cu o anumită infracțiune. Prelucrarea datelor persoanelor care nu sunt suspectate de săvârșirea unei infracțiuni (altele decât victime, martori, informatori, persoane de contact și asociați) „ar trebui să fie permisă numai în anumite condiții specifice și atunci când este absolut necesar, în scop legitim, bine definit și specific". În plus, o astfel de prelucrare ar trebui (în opinia autorităților pentru protecția datelor) „să fie permisă doar pe o perioadă limitată, iar utilizarea ulterioară a acestor date în alte scopuri ar trebui să fie interzisă". În același timp, directiva ar trebui să clarifice faptul că limitările și garanțiile suplimentare se aplică victimelor sau altor părți terțe, astfel cum se menționează la articolul 5 alineatul (1) litera (c) din propunerea actuală. Trebuie să se recunoască, din punct de vedere legislativ, faptul că este necesară diferențierea între prelucrarea datelor cu caracter personal ale infractorilor condamnați și cele ale victimelor unei infracțiuni, în special în bazele de date create în scopuri preventive sau pentru urmărirea penală a infracțiunilor în viitor.

Evoluția tehnicilor și metodelor de aplicare a legislației din ultimul deceniu demonstrează în mod clar că toate aceste categorii care se încadrează în categoria largă de „persoane care nu sunt suspectate" necesită protecție specială. Acest lucru este valabil în special în cazul în care prelucrarea nu se efectuează în cadrul unei urmăriri sau a unei anchete penală specifice. Trebuie să se facă diferența între informațiile pe care autoritățile pentru aplicarea legislației „trebuie să le cunoască" și informațiile pe care „ar fi bine să le dețină".

În scopul de a proteja „persoanele care nu sunt suspectate", grupul de lucru recomandă cu convingere introducerea unui nou articol 7a, în plus față de articolul 5. Prin noul articol 7a, astfel cum se propune mai jos, s-ar asigura faptul că diferențierea categoriilor de date nu reprezintă o sarcină administrativă sau un scop în sine, cum ar putea fi interpretată propunerea actuală. Acest lucru este necesar pentru a se asigura faptul că statele membre pot prelucra datele „persoanelor care nu sunt suspectate" numai în cazul în care sunt îndeplinite cerințele specifice și că este necesară protecția suplimentară în cazul prelucrării datelor „persoanelor care nu sunt suspectate". De aceea, este mai logic să se includă noua dispoziție în contextul articolului 7, care reglementează legalitatea prelucrării.

Grupul de lucru este conștient de caracterul specific al prelucrării datelor într-un mediu de aplicare a legislației și înțelege că prelucrarea datelor „persoanelor care nu sunt suspectate" poate fi necesară în situații specifice. De asemenea, propunerea ține cont de scopurile diferite în care autoritățile de aplicare a legislației pot prelucra datele „persoanelor care nu sunt suspectate" și recomandă norme extrem de stricte pentru situațiile în care prelucrarea nu se efectuează în scopul unei urmăriri sau anchete penale specifice. Numai în aceste situații se permite prelucrarea datelor „persoanelor care nu sunt suspectate", în cazul în care această operațiune este indispensabilă pentru un scop legitim, bine definit și specific. Prelucrarea se limitează la evaluarea relevanței pentru una dintre categoriile indicate la articolul 7a alineatul 1 literele (a) - (d) și se permite doar pe o perioadă de timp limitată, iar utilizarea ulterioară a datelor respective este interzisă.

---

[1] Documentul de poziție privind aplicarea legislației şi schimbul de informații în UE, adoptat la Conferința de primăvară a autorităților europene pentru protecția datelor - Cracovia (Polonia), 25-26 aprilie 2005

În scopul de a evita discuțiile semantice privind diferența dintre „necesar” (astfel cum se utilizează în prezent în proiectul de directivă) și „absolut necesar” (astfel cum se utilizează în documentul de poziție de la Cracovia), grupul de lucru a utilizat cuvântul „indispensabil” în amendamentul său propus. Această formulare urmărește să reflecte necesitatea unei condiții mai stricte pentru prelucrarea datelor unei persoane care nu este suspectată, din cauza faptului că nu există o relație directă sau indirectă între persoana respectivă și o anumită anchetă sau infracțiune.

Amendamentul propus pentru introducerea unui nou articol

Articolul 7a - Diferitele categorii de persoane vizate

1. Statele membre prevăd că autoritățile competente, pentru scopurile menționate la articolul 1 alineatul (1), să prelucreze datele cu caracter personal ale următoarelor categorii diferite de persoane vizate:

(a) persoane în privința cărora există motive serioase să se creadă că au săvârșit sau că urmează să săvârșească o infracțiune;

(b) persoane condamnate pentru săvârșirea unei infracțiuni;

(c) victime ale unei infracțiuni penale sau persoane în privința cărora, în baza anumitor fapte, există motive să se creadă că ar putea fi victimele unei infracțiuni penale;

(d) părți terțe la infracțiunea penală, de exemplu persoane care ar putea fi chemate să depună mărturie în cadrul cercetărilor legate de infracțiuni penale sau în cadrul procedurilor penale ulterioare sau persoane care pot oferi informații cu privire la infracțiuni penale sau persoane care sunt în legătură sau asociate cu persoanele menționate la literele (a) și (b);

2. Datele cu caracter personal ale altor persoane vizate decât cele menționate la alineatul (1) pot fi prelucrate numai în următoarele cazuri:

(a) atât timp cât este necesar pentru cercetarea sau urmărirea penală a unei infracțiuni penale specifice, în scopul de a evalua relevanța datelor pentru una dintre categoriile indicate la alineatul (1) sau

(b) atunci când o astfel de prelucrare este indispensabilă pentru un scop precis, preventiv, sau pentru efectuarea analizei penale, dacă și atâta timp cât scopul este legitim, bine definit și specific, iar prelucrarea se limitează la evaluarea relevanței datelor pentru una dintre categoriile indicate la alineatul (1). Acest lucru face obiectul unor revizuiri periodice, care vor avea loc cel puțin o dată la șase luni. Orice utilizare ulterioară este interzisă.

3. Statele membre prevăd că, în ceea ce privește prelucrarea ulterioară a datelor cu caracter personal referitoare la persoanele vizate menționate la alineatul (1) literele (c) și (d) se aplică limitări și garanții suplimentare, în conformitate cu legislația națională.

3. Privind drepturile persoanelor vizate

Diferitele elemente ale legislației privind protecția datelor sunt grupate în jurul a trei actori principali: operatorii de date/agenții care prelucrează datele, autoritățile de supraveghere și persoanele vizate. În cazul ultimei categorii, atât regulamentul, cât și directiva prevăd o serie de drepturi care pot fi exercitate la cerere, inclusiv dreptul la informare, dreptul de acces și dreptul de a rectifica sau de a șterge datele prelucrate în mod eronat sau ilegal. În cadrul regulamentului, aceste drepturi au fost puse în aplicare mai degrabă în mod liber, cu un număr limitat de excepții posibile. În privința directivei, situația este diferită, fiind determinată, de asemenea, de natura sectorului de aplicare a legislației. Este foarte ușor de înțeles faptul că autoritățile polițienești și judiciare nu pot asigura întotdeauna transparența modalităților în care prelucrează datele, precum și a tipului de date cu caracter personal pe care le dețin în evidențele acestora, întrucât acest lucru ar putea pune în pericol anchetele în curs de desfășurare.

În același timp, grupul de lucru subliniază faptul că excluderile și limitările actuale ale drepturilor persoanelor vizate au un domeniu excesiv de larg. Fără alte explicații, nu se justifică în special motivul pentru care ar trebui să li se permită statelor membre să excludă categorii întregi de date cu caracter personal de la dreptul de acces. În consecință, ar trebui să fie eliminate articolul 11 alineatul (5) și articolul 13 alineatul (2). Grupul de lucru subliniază faptul că limitarea drepturilor persoanelor vizate ar trebui să fie întotdeauna o decizie luată în funcție de caz, ținând seama de circumstanțele specifice ale cererii. De exemplu, acest lucru ar putea conduce, de asemenea, la decizia de a refuza cererea doar parțial. În plus, grupul de lucru își menține opinia potrivit căreia excepțiile de la un anumit drept fundamental trebuie să fie interpretate în permanență într-un mod restrictiv.

4. Privind analizele de impact asupra confidențialității în sectorul aplicării legislației

În cadrul primului său răspuns oferit la proiectul de directivă, grupul de lucru a îndemnat deja legiuitorul european să introducă în directivă dispoziții care să impună analizele de impact privind protecția datelor (DPIA), inclusiv în procedura legislativă. Efectuarea analizelor de impact privind protecția datelor este deosebit de importantă în domeniul prelucrării datelor cu caracter personal din sectorul aplicării legislației, având în vedere în special riscurile sporite pentru persoanele supuse prelucrării datelor. GL29 nu înțelege care este diferența majoră dintre sectorul de aplicare a legislației și sectoarele care intră sub incidența regulamentului, în cazul cărora se impun analizele de impact privind protecția datelor în vederea evaluării riscurilor noilor operațiuni de prelucrare a datelor avute în vedere. Atunci când este vorba despre date cu caracter personal, existența unor garanții temeinice prezintă o importanță deosebită în acest domeniu al legislației. Prin urmare, garanțiile ar trebui să fie luate în considerare și puse în aplicare înainte de demararea operațiunii de prelucrare a datelor.

Prin urmare, grupul de lucru este mulțumit de amendamentele 27, 28, 110 și 113 propuse de către raportorul Parlamentului European, care introduce astfel cerințe de efectuare a analizelor de impact privind protecția datelor în sectorul aplicării legislației, comparabile, într-o foarte mare măsură, cu cele care sunt deja în vigoare în regulament. De asemenea, acest pas important în asigurarea unei protecții mai bune a drepturilor de bază ale persoanelor fizice, chiar și într-un mediu bogat din punct de vedere informațional precum sectorul de aplicare a legislației, ar trebui să fie inclus în abordarea generală a Consiliului privind proiectul de directivă.

Cu toate acestea, opinia grupului de lucru diferă de cea a raportorului în privința unui singur punct. Atât în considerentul modificat 41, cât și în articolul 25 alineatul (2), raportorul introduce obligația autorităților pentru protecția datelor de a evalua toate analizele de impact privind protecția datelor și de a face „propuneri adecvate pentru a remedia (...) nerespectarea". GL29 consideră că evaluarea analizelor de impact privind protecția datelor de către autoritățile pentru protecția datelor ar trebui să se efectueze doar dacă este cazul.

5. Privind competențele autorităților pentru protecția datelor

Decizia-cadru în temeiul celui de-al treilea pilon, aplicabilă în prezent, conține un număr redus de dispoziții privind atribuțiile și competențele autorităților pentru protecția datelor, precum și posibilitățile și/sau obligațiile acestora de a coopera în momentul îndeplinirii sarcinilor de supraveghere și de punere în aplicare care le revin. În acest sens, proiectul de directivă reprezintă un important pas înainte. Acesta include atât dispoziții privind necesitatea existenței unei autorități independente de supraveghere pentru toate operațiunile de prelucrare a datelor care au loc în cadrul domeniului de aplicare a directivei, cât și un capitol specific privind cooperarea dintre autoritățile pentru protecția datelor. Grupul de lucru „articolul 29" salută ideea de bază a acestor dispoziții.

Din păcate, dispozițiile incluse în directivă sunt mult mai puțin specifice decât cele din proiectul de regulament. Prin urmare, în avizul său general privind pachetul legislativ, grupul de lucru „articolul 29" a afirmat deja necesitatea de a permite accesul autorităților de supraveghere în toate incintele. De asemenea, s-a subliniat necesitatea de a strânge legăturile dintre dispozițiile ambelor instrumente pentru a se asigura coerența în cadrul juridic al protecției datelor. Acest aspect este deosebit de important în ceea ce privește cooperarea impusă între autoritățile pentru protecția datelor. În cazul în care autoritățile respective nu au competențe similare în întreaga Uniune Europeană, asigurarea protecției drepturilor cetățenilor noștri riscă să devină foarte dificilă. Astfel, ar putea exista situații în care o autoritate, în baza legislației naționale puse în aplicare, are permisiunea de a intra în incinta unei agenții de aplicare a legislației în vederea efectuării unei inspecții fără acordul prealabil al agenției implicate, în timp ce altă autoritate pentru protecția datelor dintr-o țară învecinată nu deține această competență și, prin urmare, nu are acces în incinta agenției de aplicare a legislației.

Referitor la situația autorităților pentru protecția datelor în ceea ce privește informațiile, cooperarea se poate dovedi chiar mai dificilă în cazul în care nu există o armonizare a competențelor autorităților, astfel cum se întâmplă în situația actuală. Un sondaj realizat de grupul de lucru „articolul 29" indică faptul că unele autorități pentru protecția datelor, în temeiul unei dispoziții specifice în conformitate cu legislația națională, au acces la toate informațiile și documentele, indiferent dacă acestea sunt disponibile publicului, confidențiale sau clasificate, necesare în vederea îndeplinirii sarcinilor de supraveghere privind prelucrarea datelor în domeniul aplicării legislației. În cazul altor autorități pentru protecția datelor, membrii personalului beneficiază de acces similar numai după obținerea unei autorizații de securitate de la serviciile de informații relevante. Cu toate acestea, alte autorități pentru protecția datelor nu au niciun fel de acces la informațiile confidențiale și/sau clasificate.

Prin urmare, în cazul în care autoritățile pentru protecția datelor sunt obligate să coopereze în temeiul directivei, este foarte important ca toate autoritățile implicate să aibă acces la aceleași informații. În caz contrar, există posibilitatea ca acestea să nu aibă imaginea completă asupra situației unui caz specific și să ajungă la o concluzie diferită, aducând astfel atingere

intereselor persoanei vizate. Prin urmare, grupul de lucru „articolul 29” propune identificarea în directivă a informațiilor accesibile autorităților pentru protecția datelor atunci când informațiile respective sunt necesare pentru îndeplinirea atribuțiilor de supraveghere care le revin. Prezenta propunere nu are intenția de a reduce nivelul de acces la informațiile clasificate deținute în prezent de către autoritățile pentru protecția datelor.

La un nivel mai general, grupul de lucru salută propunerile făcute de raportorul Parlamentului European privind competențele autorităților pentru protecția datelor și susține descrierea mai detaliată a competențelor recomandate de acesta. Următorul amendament trebuie considerat ca un element suplimentar la aceste propuneri.

Amendamentul propus

Articolul 46 – Competențe (alineate care urmează să fie adăugate)

1. Statele membre se asigură că fiecare autoritate de supraveghere deține competența de investigare necesară pentru a obține, de la operatorul sau de la agentul care prelucrează datele, acces la oricare dintre incintele sale, inclusiv la orice echipament sau mijloc de prelucrare a datelor.
2. Statele membre se asigură că fiecare autoritate de supraveghere are la dispoziție toate informațiile și documentele necesare pentru exercitarea competențelor de investigare ale acesteia. Nu se pot invoca cerințele legate de necesitatea păstrării secretului pentru a refuza solicitările autorităților de supraveghere, cu excepția cerințelor de păstrare a secretului profesional menționate la articolul 43.
3. Statele membre pot prevedea necesitatea unui control de securitate suplimentar, în conformitate cu legislația națională, pentru accesul la informațiile clasificate, cu un nivel similar cu nivelul RESTREINT UE sau mai ridicat. În cazul în care legislația statului membru al autorității de supraveghere nu impune un control de securitate suplimentar, acest aspect trebuie să fie recunoscut de către toate celelalte state membre.

Adoptat la Bruxelles, la 26 februarie 2013

Pentru Grupul de lucru
Președintele
Jacob KOHNSTAMM