Parlamentul României
Camera Deputaților

Nr. ref. M.69

ROMANIA

Deputat Ștefan Mușoiu

Circumscripția nr.23 Ialomița

Informare - Bruxelles, 15 Mai - REUNIUNE INTERPARLAMENTARĂ LA NIVEL DE COMISII – Punerea în aplicare a pachetului legislativ privind protecția datelor, organizata de Comisia LIBE a Parlamentului European

În data de 15 mai, la sediul Parlamentului European, a avut loc dezbaterea "Punerea în aplicare a pachetului legislativ privind protecția datelor", în ajunul aplicării acesteia.

Din partea țării noastre au participat Ștefan Mușoiu, vicepreședinte al Comisiei pentru Afaceri Europene și Cătălin Drulă, președintele Comisiei pentru Tehnologia Informației și Comunicațiilor, reprezentanți ai Camerei deputaților și din partea Senatului Robert Cazanciuc, președinte al Comisiei juridice, denumiri, disciplină, imunități și validări și Ionuț Sibinescu, președinte al Comisiei pentru Constituționalitate, libertăți civile și monitorizare a executării hotărârilor Curții europene a drepturilor omului.

Scopul conferinței a fost reprezentat de implementarea Regulamentului General privind Protecția Datelor (2016/679) începând cu data de 25 mai 2018 și transpunerea Directivei europene (2016/680) privind protecția datelor în activitățile desfășurate de autoritățile de aplicare a legii.

Reuniunea a fost structurată în jurul a patru sesiuni principale și anume: Aspectele instituționale, Impactul asupra sectorului privat, inclusiv asupra IMM-urilor, Inovarea tehnologică și impactul RGPD și, în cele din urmă, "Directiva privind asigurarea aplicării legii".

ROMANIA

Parlamentul României
Camera Deputaților

Deputat Ștefan Mușoiu

Circumscripția nr.23 Ialomița

Panel 1 – Punerea în aplicare a Regulamentului general privind protecția datelor – Aspecte instituționale

Dna. Andrea Jelinek, șefa Autorității pentru protecția datelor din Austria și președinta grupului de lucru "Articolul 29", a susținut că atât Autoritatea pentru protecția datelor, cât și întreprinderile au desfășurat în ultimii doi ani o activitate de îmbunătățire a acestui domeniu. În Austria au fost organizate workshopuri care puneau întreprinderi reale în situații fictive legate de domeniul protecției datelor și pentru rezolvarea acestora s-a folosit implementarea RGDP, ceea ce a dus la constatarea că există o diferență între forma scriptică și modul de aplicare efectivă a RGDP. Structura Autorității pentru protecția datelor a fost modificată și adaptată în acest sens și au fost stabilite noi norme și proceduri atât la nivel național cât și la nivel intern, au fost recrutați noi angajați și a fost creată "Lista albă" care specifică părțile din RGDP care sunt considerate mai puțin necesare în a fi implementate. Va exista o cooperare cu celelalte Autorități europene în domeniu pentru a se realiza o implementare cât mai eficientă a ghișeului unic de protecție a datelor. S-a realizat informarea atât în limba germană cât și în limba engleză și a fost pregătit secretariatul Comitetului European pentru Protecția Datelor care reprezintă entitatea care sprijină Autoritatea pentru protecția datelor în realizarea funcțiilor sale, iar Comitetul pentru protecția datelor este o entitate nouă cu competențe decizionale și au fost organizate reuniuni atât în plen cât și în cadrul unor grupuri de lucru pentru a pregăti intrarea în vigoare a RGDP.

Dna. Katarzyna Szymielewicwz, reprezentanta Fundației Panoptykon și vicepreședinta EDRI, a susținut că au fost efectuate îmbunătățiri majore ale RGDP în comparație cu anii anteriori fapt ce va duce la o mai mare transparență în domeniul online și cel al publicității. Cetățenii vor putea să descopere cum sunt colectate datele personale, atât cele observabile cât și cele ascunse, și vor avea dreptul de a obține copii ale datelor proprii. Vor apărea conflicte juridice în ceea ce privește asigurarea transparenței, deoarece companiile fie vor stabili din start

ce date sunt colectate, fie vor introduce ulterior mecanisme ce au ca scop colectarea în plus a unor date mai semnificative. O altă provocare o reprezintă înțelegerea logicii pe baza căreia este creat profilul utilizatorului, deoarece prezentarea acesteia nu se poate face într-un mod facil și ușor de înțeles de toți. Portabilitatea datelor crează și ea un obstacol în sensul că există un prag între datele care au fost oferite de persoana vizată prin utilizarea serviciului și datele care au fost deduse. Procedurile de despăgubire vor crea o revoluție deoarece RGDP se aplică tuturor companiilor care prelucrează datele cetățenilor europeni indiferent unde se află aceștia și este foarte important să existe mecanisme așa cum este Comitetul European pentru Protecția Datelor. Cetățenii vor putea să se ducă în instanță direct fără a se adresa mai întâi Autorității pentru protecția datelor, iar acest lucru în practică va depinde de cât de rapide, competente și bine finanțate vor fi instituțiile naționale.

Dna. Christine Hennion, membră a Parlamentului Franței, a susținut că RGDP fundamentează garanția libertăților în lumea digitală a sec. 21. Evoluțiile tehnologice impun o supraveghere permanentă și tot mai crescută a vieții personale. Textul RGDP este unul hibrid care lasă fiecărei țări peste 50 de marje de implementare și trebuie evitată o dispersie normativă prea mare sau modul prin care concurența poate fi distorsionată împiedicând autoritățile competente să își facă treaba în mod eficient. Textul votat de Parlamentul francez folosește această marjă la minim pentru a se realiza o armonizare cât mai mare cu legislația europeană. În Franța vor fi permise acțiunile colective pentru daune, acțiuni care, până acum, vizau doar încetarea procesării. Franța este prima țară Europeană care, încă din 1978, are o instituție dedicată protecției datelor personale - Comisia Națională pentru Informatică și Libertăți care cooperează cu alte autorități de la nivel european prevăzute prin lege. Eficiența activităților de control, de instrucție, de investigație și de sancțiune în ceea ce privește procesarea transfrontalieră a datelor personale este garantată prin instituirea unei organizații de control care stabilește care este entitatea pricipală responsabilă pentru procesarea datelor care poate face controlul cu privire la modalitatea de utilizare a acestor date. Deciziile sunt luate prin consens în termenul impus de lege, normele franceze prevăzând adaptarea la aceste noi modalități de

cooperare transfrontalieră în domeniu, membrii autorității naționale de control acționând alături de membri ai Comisiei Naționale pentru Informatică și Libertăți. În timp ce întreprinderile mari consideră RGDP drept o ocazie de dezvoltare, IMM-urile susțin că este dificil de implementat. Legea franceză a modificat compoziția și atribuțiile CNIL pentru a-l adapta noilor misiuni care îi revin. RGDP reprezintă un mecanism important pentru asigurarea responsabilizării actorilor din domeniul digital și este necesar ca Europa să redevină lider în ceea ce privește protecția drepturilor omului și în special a datelor personale.

Panel 2 - Punerea în aplicare a Regulamentului general privind protecția datelor – Impactul asupra sectorului privat, inclusiv asupra IMM-urilor

Dl. Judicael Phan, consilier general asociat în cadrul Global DPO Ubisoft, a susținut că RGDP conține valori democratice intrinsece și anume protecția datelor personale sau respectarea vieții private. Ubisoft consideră RGDP ca o oportunitate atât pentru cetățeni cât și pentru cei care procesează date. Abordarea problematicii datelor personale devine tot mai omogenă, acestea începând să fie considerate o valoare în sine și nu doar bunuri imateriale. În ceea ce privește activitatea companiei, datele personale sunt indispensabile pentru a putea oferi o experiență a produsului finit cât mai bună, astfel că RGDP este considerat o oportunitate de consolidare a propriei reputații și pentru o mai bună cartografiere a datelor folosite în vederea gestionării mai bune a acestora și pentru a îmbunătăți competențele concurențiale. A fost consolidată echipa și a fost realizată o mai bună situație efectivă a datelor deținute, se pregătesc noi instrumente de îmbunătățire a transparenței și a controalelor, s-a creat un grup de lucru intern, și au fost consolidate foarte mult echipele care se ocupă de date personale, dar acest lucru este mult mai dificil de realizat de către IMM-uri.

ROMANIA

Parlamentul României
Camera Deputaților

Deputat Ștefan Mușoiu

Circumscripția nr.23 Ialomița

Dl. Luc Hendrickx, director pentru politica întreprinderii și afacerile externe în cadrul UEAPME, a susținut că IMM-urile reprezintă peste 99% din întreprinderile vizate din sistemul privat. Este necesar să se țină cont de noile evoluții tehnologice ceea ce necesită un nivel înalt de protecție a consumatorului dar și o abordare echilibrată care să preîntâmpine poverile administrative suplimentare pentru IMM-uri, și în acest sens este nevoie de dispoziții ușor de înțeles precum și campanii de informare cu privire la protecția datelor cu caracter personal sprijinite de Uniunea Europeană împreună cu organizațiile reprezentative la nivelul UE și național. Inițiativa a fost văzută ca favorizând marile întreprinderi fără a ține cont de interesele IMM-urilor. Au fost organizate ample campanii de informare și au fost elaborate instrumente care să asiste IMM-urile atât la nivel național cât și la nivel sectorial pentru că și sectoarele au nevoie de o abordare specifică. La nivel național există o cooperare bună cu Autoritățile pentru protecția datelor. Toate aceste norme și reglementări au presupus atât costuri suplimentare cât și nesiguranță în ceea ce privește rezultatele obținute, dificultăți în punerea în aplicare a RGDP, lipsa personalului necesar, structura mult prea largă a Regulamentului și folosirea doar a limbii engleze pentru mai mult de 50% din documentele emise, precum și înțelegerea deficitară a legislației fiind solicitată, în acest sens, o perioadă de grație de 1 an de zile pentru IMM-uri pentru implementarea RGDP-ului.

Dna Pascale Gelly, responsabilă a grupului cu protecția datelor, finanțe, control-afaceri juridice în cadrul Schneider Electric, a susținut necesitatea elaborării de marile companii a unui program care să se conformeze cu specificațiile RGDP. La nivelul central, compania pe care o reprezintă, a aprobat organizarea unui comitet care să emită un astfel de program și să elaboreze politici pentru a-i ajuta pe ceilalți angajați să pună în aplicare aceste norme. Se dorește diseminarea, prin intermediul structurilor de resurse umane și de marketing, a instrucțiunilor de implementare. Acest program este conceput pe baza unor domenii de interes care decurg din RGDP. Este necesară prezența unui ofițer de protecție a datelor la toate sediile externe ale marilor companii pentru a asigura conformarea și respectarea regulilor, precum și a unei comisii reprezentative pentru toate sediile și care poate să ofere îndrumări cu privire la politicile

companiei. Sunt recomandate campanii de informare pentru a familiariza persoanele cu privire la ce reprezintă și cum funcționează în practică RGDP. Este important să nu existe diferențe majore între structura Regulamentului aprobată la nivel național și cea de la nivel european.

Panel 3 - Regulamentul general privind protecția datelor și inovarea tehnologică

Dl. Eric Leandrin, reprezentatnt al QWANT, a susținut că motorul de căutare european cu același nume, nu colectează datele personale și au asigurat protecția acestora, conform cu art. 25 din RGDP. Istoricul căutărilor reprezintă informații personale care spun multe despre utilizator (venituri, nivel de educație, orientare religioasă etc), iar cei de la QWANT sunt primii care pot oferi rezultate fără a folosi datele personale. Aceste date pot fi mascate sau anonimizate. Google susține că nu sunt afectați de RGDP, deoarece o mare parte din veniturile lor provin din publicitate. Marile corporații trebuie să se conformeze regulilor și trebuie să înceteze în a mai folosi datele personale pentru a oferi informații simple. În Franța utilizatorii pot alege deja ce motor de căutare vor folosi.

Dna Ninja Marnau, expert în dezvoltare I.T. din cadrul Universității din Saarland, susține că Regulamentul pune un accent important pe modalitatea în care sunt colectate datele și se cere implementarea unor măsuri tehnice și de organizare, conform art. 25 și art. 32. Art. 26 susține că RGDP nu se aplică datelor anonime, iar art. 11 permite controlorului să proceseze mai bine anumite date personale dacă procesează doar date care nu permit identificarea subiectului. Industria și știința ar trebui ca împreună să avanseze în ceea ce privește privacy engineering, tehnologiile din domeniul protecției vieții private. Interesul față de acestea a crescut în ultimii ani și s-au înregistrat mai multe progrese științifice în ceea ce privește avansarea în domeniul tehnicilor de anonimizare, proces de care sunt interesate și IMM-urile. Din păcate IMM-urile

încă sunt în urmă, interesul pentru acest subiect venind mai mult din partea marilor companii. Sunt necesare noi metode criptografice de ștergere a datelor. E nevoie de mai multă cercetare interdisciplinară și măsurători standardizate de risc. Protecția vieții private trebuie incorporată la toate nivelurile de căutare. Autoritățile pentru protecția datelor trebuie să fie proactive. Trebuie să existe un model de bune practici în acest domeniu, pe baza căruia să se orienteze toate părțile interesate. Există multe inițiative legislative în sensul combaterii abuzului de date și a cyber-criminalității.

Dl. Paul Breitbarth, reprezentant al societății de consultanță pentru întreprinderi Nymity, a spus că prima fază de reformă a cadrului pentru protecția datelor personale a fost încheiată. Se încearcă respectarea cât mai acurată în toate domeniile a RGDP. Tot mai multe companii înțeleg semnificația acestuia și faptul că trebuie să ia măsurile necesare pentru respectarea acestuia, chiar dacă acest lucru presupune un efort mai mare. RGDP trebuie considerat o evoluție, nu o revoluție în domeniu. Organizațiile trebuie să își incorporeze protecția datelor în practicile lor operaționale și trebuie să dovedească respectarea prevederilor RGDP la toate nivelurile organizației. S-au dezvoltat în acest sens noi soluții de software inteligente. Sistemul Privacy by design a fost incorporat deja de 23% din organizații, în vreme ce 43% lucrează în acest moment pentru a realiza incorporarea, iar 27% doresc sa treacă la acest sistem și doar 2% au spus că nu li se aplică, iar în ceea ce privește procesarea datelor 23% dintre organizații au confirmat că este necesară, 27% au implementat deja acest proiect, iar 14% sunt în curs de implementare. La momentul actual sunt dezvoltate soluții pentru păstrarea evidenței activităților de procesare a datelor.

Panel 4 – Punerea în aplicare a Directivei privind protecția datelor de către autoritățile polițienești

Dl. Christian Wiese Svanberg, inspector-şef pentru protecția confidențialității și șeful Unității pentru protecția datelor din Poliția națională daneză, a susținut că Directiva pentru protecția datelor de către autoritățile polițienești a fost o precondiție pentru ca Danemarca să poată menține o legătură strânsă cu EUROPOL. Poliția daneză a înregistrat progrese importante în ceea ce privește protecția confidențialității și a datelor cu caracter personal, fapt necesar atât pentru desfășurarea anchetelor cât și pentru a se asigura protecția individului. Autoritățile polițienești au întreprins măsuri în vederea inovării în acet domeniu, cu respectarea nevoii de a informa cetățenii. În Danemarca au fost efectuate verificări pentru a se vedea cum sunt procesate datele de către agenții de poliție. O mare provocare la acest moment o reprezintă procesarea pachetelor mari de date, Directiva având o serie de efecte pozitive în acest sens. În ceea ce privește procesarea datelor personale ca parte a unei cooperări europene apar dificultăți în transferul de date, deoarece trebuie știut dacă el se face pe baza RGDP, a Directivei sau a unor norme suplimentare dintru-un alt act legislativ. Este necesară o interpretare concretă a regulilor și trebuie știut cu exactitate de ce anumite date sunt procesate și trebuie văzut în ce scop pot fi folosite acestea de către autoritățile implicate. Ca soluție, poliția sau autoritățile competente, împreună cu autoritățile pentru protecția datelor trebuie să colaboreze și să găsească un răspuns practic și transparent la această problemă.

Dl. Olivier Micol, șeful Unității pentru protecția datelor din cadrul DG Justiție – Comisia Europeană, a susținut că obiectivele principale au rămas aceleași: un nivel ridicat de protecție a datelor personale ținând cont de contextul specific polițienesc și al justiției și promovarea unui schimb optim de informații între justiție și organele polițienești, precum și cooperarea în domeniul prevenirii și combaterii terorismului în Europa. Directiva introduce noi elemente similare cu RGDP: protecția datelor by desing și by default, responsabilitatea autorităților de a face o evaluare a impactului pentru persoana vizată, obligația de a numi un ofițer pentru protecția datelor, notificarea încălcărilor cu privire la date și obligația de a avea registre. În ceea ce privește transferul internațional acesta se va face pe baza unei cereri între autoritățile competente sau direct prin intermediul furnizorilor de servicii dar pe baza unor condiții prestabilite. Directiva

se aplică autorităților care răspund de urmărirea penală, și dă posibilitatea statelor membre să aibă aceleași autorități de protecție a datelor.

Dna. Maja Smoltczyk, comisar pentru protecția datelor și libertatea de informare – Berlin, a susținut că în Germania Directiva a avut 16 interpretări diferite și, de aceea, este foarte important ca la nivel european să aibă loc aceleași dezbateri și același mod de implementare pentru a se realiza o mai bună armonizare în domeniul protecției datelor, Comisia Europeană trebuind să aibă un rol integrator în acest sens. În Berlin Directiva nu a fost încă implementată, aceasta aflându-se, la ora actuală, în dezbatere parlamentară și este necasar ca toate normele să fie reglementate unitar și pentru anumite autorități ar trebui să fie specificate câteva norme speciale, deoarece la nivel național nu există expertiza prezentă la nivel european. Anumite puncte din inițiativa legislativă s-au dovedit a fi problematice: art. 47 alin. 2 din Directivă, privind acțiunile corective în cazul în care se încalcă protecția datelor, lipsa reglementărilor de executare, definiția ineficientă a sancțiunilor și măsurilor ce trebuie luate în caz de încălcare a protecției datelor, reglementarea în ceea ce privește studiul și impactul în ceea ce privește protecția datelor (modul în care se va acționa atunci când apar constrângeri), transparența și normele juridice, precum și lipsa de dotare în ceea ce privește echipamentul și personalul necesar pentru protecția datelor.

Deputat,

Ștefan Mușoiu