**Instruirea angajaților și revizuirea procedurilor interne, aspecte importante în protecția datelor cu caracter personal**

*Material de opinie de Sergiu Zaharia, Director, Cyber Strategy Advisory, Deloitte România, și Silvia Axinescu, Senior Managing Associate, Reff & Asociații | Deloitte Legal*

Protecția datelor cu caracter personal reprezintă o preocupare continuă a autorităților, atât la nivel local, cât și european, în special în contextul dezvoltărilor din economia digitală, astfel că operatorii din domeniu trebuie să țină pasul cu reglementările și cu recomandările acestora pentru a se conforma cerințelor legale în vigoare. În România, autoritatea competentă recomandă, pe baza aspectelor constatate în cadrul controalelor din 2021, intensificarea măsurilor organizatorice interne pentru asigurarea securității datelor prelucrate. Printre acestea se numără pregătirea periodică a angajaților, revizuirea soluțiilor tehnice, dar și respectarea regulilor privind transferul internațional al datelor cu caracter personal.

Autoritatea Națională de Supraveghere privind Prelucrarea Datelor cu Caracter Personal (ANSPDCP) a înregistrat, în 2021, peste 5.000 de plângeri, sesizări și notificări privind incidentele de securitate cu privire la protecția datelor, pe baza cărora a derulat 691 de investigații. Pe parcursul anului, autoritatea a aplicat 36 de amenzi, în cuantum total de aproximativ 75.000 de euro. Dincolo de cifre, însă, din raportul instituției se desprind și câteva aspecte importante de care operatorii ar trebui să țină cont în perioada următoare.

**Neregulile constate de autoritate**

Unul dintre acestea se referă la **instruirea permanentă a angajaților** responsabili cu gestionarea datelor personale colectate de un operator. Factorul uman se dovedește a fi, în continuare, cel mai relevant în ceea ce privește asigurarea conformării privind protecția datelor cu caracter personal. Este extrem de important ca angajații societăților să cunoască și să înțeleagă foarte bine atribuțiile pe care le au în legătură cu protejarea datelor, să aplice în cadrul activității regulile și politicile care guvernează acest domeniu și să respecte măsurile de securitate adoptate la nivelul societății. De altfel, instruirea angajaților se numără printre măsurile corective impuse de ANSPDCP în urma constatării unor încălcări ale legislației, alături de revizuirea procedurilor sau de aplicarea unor politici interne pentru asigurarea respectării cadrului legal în domeniu (precum gestionarea procesului de soluționare a cererilor persoanelor vizate etc.).

Printre neregulile constate de autoritate se numără și încălcarea măsurilor de securitate și confidențialitate a prelucrării de date cu caracter personal. Așadar, un alt aspect important desprins din raportul autorității este cel legat de necesitatea **intensificării controalelor interne,** astfel încât societățile să se asigure că aplică măsuri tehnice și organizaționale corespunzătoare pentru garantarea securității datelor.

În plus, ANSPDCP a analizat un număr impresionant de reguli corporatiste obligatorii, în calitate de autoritate principală sau autoritate de cooperare, precum și recomandările emise în legătură cu acestea. Această analiză ar putea indica faptul că autoritatea intenționează să evalueze, în perioada următoare, **transferul de date către state terțe** și maniera în care sunt încheiate clauzele standard obligatorii adoptate de Comisia Europeană, în vigoare de la 27 septembrie 2021, acestea reprezentând, de altfel, cel mai des întâlnit instrument pentru fundamentarea unor astfel de transferuri.

**Prevenția, armă împotriva atacurilor cibernetice**

În plus, pentru viitor, organizațiile trebuie să își exerseze capacitatea de a anticipa și de a răspunde rapid la atacurile cibernetice sau la erorile interne care intervin în procesul de protecție a datelor cu caracter personal, astfel încât să reducă riscul de compromitere a datelor. În acest sens, este important să desfășoare exerciții de testare a proceselor de management al crizelor, având în vedere că incidentele de securitate cibernetică sunt deja percepute ca având cel mai mare risc asupra afacerii.

Nu în ultimul rând, analiza preventivă a nivelului de maturitate în domeniul securității datelor, inclusiv a celor cu caracter personal, și identificarea unui parcurs pentru sporirea acestuia rămân măsuri clasice, dar extrem de aplicate, menite să reducă riscul de exploatare a unor vulnerabilități tehnice, organizatorice și umane, și implicit riscul unui impact major asupra operațiunilor, asupra reputației și, în final, de natură financiară.