protecția datelor cu caracter personal - modificări legislative publicate în aprilie 2021

I. România – sancțiuni

1. ANSPDCP. Tip Top Food Industry S.R.L a fost sancționată pentru încălcarea Regulamentul General privind Protecția Datelor cu amendă în cuantum de 24.362,50 lei (echivalentul în lei al sumei de 5.000 Euro).

În urma investigației, Autoritatea Națională de Supraveghere a constatat că **operatorul a prelucrat imaginea angajaților săi, în mod excesiv, prin intermediul camerelor video instalate în spații cu destinația de vestiare și în zona destinată servirii mesei,** invocând scopul protejării bunurilor și a produselor societății, precum și al descurajării furtului.

Pe de altă parte, în investigația efectuată, având în vedere relația angajator-angajat, s-a reținut faptul că nu a putut fi considerat liber exprimat consimțământul persoanei vizate și nici nu a putut fi identificat alt temei legal de prelucrare, operatorul neputând face dovada respectării principiilor de prelucrare, prin raportare și la art. 5 alin. (2) din Regulamentul General privind Protecția Datelor.

De asemenea, operatorului respectiv i-au fost aplicate și următoarele **măsuri corective**:

- măsura corectivă de a asigura conformitatea operațiunilor de prelucrare a datelor personale în activitatea de monitorizare video, cu respectarea principiului „reducerii la minimum a datelor", raportat la art. 5 alin. (1) lit. c);
- să reanalizeze orientarea unghiului de captare a imaginilor video astfel încât acestea să nu monitorizeze activitatea angajaților săi în spații cu destinația de vestiare și în sala de mese, raportat la scopul prelucrării.

Investigația a fost demarată ca urmare a unei sesizări a unei persoane fizice care a semnalat faptul că societatea TIP TOP FOOD INDUSTRY SRL prelucrează date cu caracter personal (respectiv imaginea), prin intermediul camerelor video instalate în birourile angajaților, în vestiare și în sala de mese.

2. ANSPDCP. Lugera & Makler Broker S.R.L. a fost sancționată cu amendă în cuantum de 7.331,85 lei (echivalentul sumei de 1500 EURO)

Investigația a fost demarată ca urmare a unei sesizări primite din partea unei persoane fizice și a unei notificări de încălcare a securității datelor cu caracter personal transmisă de Raiffeisen Bank SA. din care a rezultat că Lugera & Makler Broker S.R.L (persoană împuternicită de operatorul Raiffeisen Bank SA) nu a predat Raiffeisen Bank SA documentele aferente activităților de prescoring efectuate de un angajat al său, pe motiv că acestea au fost distruse.

De asemenea, ca urmare a efectuării a 1372 de prescoringuri de către un agent de vânzări, angajat al Lugera & Makler Broker S.R.L., au fost afectate de incidentul de securitate 1058 de persoane fizice vizate, întrucât documentația originală aferentă prescoringurilor nu a fost predată de agent, ci distrusă, ceea ce a generat incidentul de securitate notificat de

Raiffesien Bank la ANSPDCP, încălcându-se astfel prevederile art. 29, art. 32 alin.(2) și (4) din Regulamentul General privind Protecția Datelor.

II. UNIUNEA EUROPEANĂ – reglementări

1. A patruzeci și opta Plenară a Comitetului European pentru Protecția Datelor

În cadrul Plenarei Comitetului European pentru Protecția Datelor, desfășurată on-line pe data de 13 aprilie 2021, în principal, au fost adoptate:

- Opinia nr. 14/2021 privind proiectul Deciziei Comisiei Europene de recunoaștere a unui nivel adecvat de protecție în Marea Britanie, în temeiul Regulamentului General privind Protecția Datelor
- Opinia nr. 15/2021 privind proiectul Deciziei Comisiei Europene de recunoaștere a unui nivel adecvat de protecție în Marea Britanie, în temeiul Directivei 680/2018
- Ghidul nr. 8/2020 privind evidențierea utilizatorilor în mediile sociale (forma finală)
- Ghidul nr. 3/2021 privind aplicarea art. 65 alin. (1) lit. a) din Regulamentul General privind Protecția Datelor – în consultare publică timp de 6 săptămâni

Mai multe informații sunt disponibile la adresa: https://edpb.europa.eu/news/news_en

III. UNIUNEA EUROPEANĂ – sancțiuni

1. Autoritatea olandeză pentru protecția datelor a amendat municipalitatea Enschede cu amendă în cuantum de 600.000 EUR pentru că a utilizat urmărirea Wi-Fi în centrul orașului

Urmărirea Wi-Fi a făcut posibilă monitorizarea cumpărătorilor și a persoanelor care locuiesc sau lucrează în centrul orașului. În 2017, municipalitatea Enschede a decis să măsoare cât de aglomerat era centrul orașului, folosind senzori. A contractat o companie specializată în efectuarea numărului de persoane.

Echipament de senzori a fost plasat pe străzile comerciale care detectau semnalele Wi-Fi de pe telefoanele mobile ale trecătorilor. Fiecare telefon a fost înregistrat separat și a primit un cod unic.

2. Autoritatea portugheză pentru protecția datelor a ordonat INE (Institutul Național de Statistică) să suspende trimiterea de date cu caracter personal din Recensământul 2021 către Statele Unite.

Autoritatea a emis o decizie adresată INE pentru suspendarea în termen de 12 ore de la orice transfer internațional de date cu caracter personal către Statele Unite sau alte țări terțe fără un nivel adecvat de protecție în contextul chestionarului recensământului 2021.

După o serie de reclamații referitoare la condițiile de colectare a datelor online, Autoritatea a efectuat o investigație rapidă și a concluzionat că INE a externalizat către Cloudflare, Inc. funcționarea chestionarului recensământului, printr-un acord de prelucrare a datelor care prevede transferul de date personale către Statele Unite.

Cloudflare este o întreprindere stabilită în California. Prin tipul de servicii pe care le oferă, este supus direct legislației SUA de supraveghere în scopul securității naționale, care îi impune obligația legală de a oferi autorităților Statelor Unite acces nelimitat la datele cu caracter personal deținute sau păstrate de Cloudflare, fără putându-și informa clienții despre acest fapt.

3. Autoritatea olandeză pentru protecția datelor a sancționat Booking.com cu amendă de 475.000 EUR deoarece compania a notificat foarte târziu o încălcare a datelor cu caracter personal.

Când a avut loc încălcarea, infractorii au obținut datele personale ale peste 4.000 de clienți. De asemenea, au avut acces la informațiile despre cardul de credit a aproape 300 de persoane.

Într-o înșelătorie telefonică vizând 40 de hoteluri din Emiratele Arabe Unite în decembrie 2018, infractorii au convins personalul hotelului să dezvăluie detaliile de conectare pentru conturile dintr-un sistem Booking.com. În acest fel, infractorii au obținut acces la datele a 4.109 de persoane care rezervaseră o cameră de hotel în EAU. Datele includeau numele, adresele și numerele de telefon, precum și detalii despre rezervarea lor.

Infractorii au putut accesa, de asemenea, informațiile despre cardul de credit a 283 de persoane. În 97 de cazuri, a fost obținut și codul de securitate al cardului de credit. Infractorii au încercat, de asemenea, să obțină informațiile despre cardul de credit ale altor victime, prezentându-se ca personal al Booking.com în e-mailuri sau la telefon.