

**Nr…………./…………..2021**

 **Avizat Primar,**

 **RADU-NICOLAE MIHAIU**

**INFORMARE**

În urma participării, în data de 27 ian.2021, la Conferinţa intitulată “ Constatări şi recomandări pentru operatorii din sectorul public“, organizată on-line cu ocazia Zilei Europene a Protecţiei Datelor de Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, vă informăm cu privire la cele discutate în cadrul evenimentului:

Ziua Europeană a Protecției Datelor se celebrează în data de 28 ianuarie 2021 de către toate statele membre ale Consiliului Europei și marchează 40 de ani de la adoptarea, în anul 1981, la Strasbourg, a Convenției 108 pentru protecția persoanelor referitoare la prelucrarea automatizată a datelor cu caracter personal.

Convenţia 108 defineşte o serie de principii universale şi conţine prevederi de natură să asigure protecţia vieţii private a persoanelor fizice în raporturile acestora cu autorităţile publice sau entităţile private.

Modernizarea Convenției 108 s-a realizat în luna mai 2018, când Comitetul de Miniștri al Consiliului Europei a adoptat Protocolul modificat cunoscut sub numele de „Convenția 108+”.

Sărbătorirea anuală a acestei zile constituie un prilej de a aduce în atenţia publicului importanța respectării principiilor de prelucrare a datelor cu caracter personal, a dreptului la viață privată și a dreptului la protecția datelor personale, consacrate ca drepturi fundamentale.

Pentru celebrarea Zilei Europene a Protecţiei Datelor, Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal organizează două evenimente on-line destinate informării corecte a operatorilor cu privire la aplicarea adecvată a regulilor de protecție a datelor personale, statuate de Regulamentul General privind Protecția Datelor.

Astfel, **pe data de 27 ianuarie 2021**, instituția noastră a fost reprezentată de Responsabilul cu Protecţia Datelor la conferinţa on-line, o conferință dedicată autorităților și instituțiilor publice, intitulată „Constatări și recomandări pentru operatorii din sectorul public”, în care s-au prezentat și dezbătut aspecte practice specifice de aplicare a principiilor de prelucrare a datelor personale. La acest eveniment au fost invitate, în principal, autoritățile și instituțiile publice centrale reprezentative.

Evenimentul a fost livrat de:

Doamna Anca OPRE - președinte ANSPDCP Prezentări si discuții

Doamna Adina Diaconescu – director Direcția Plângeri ANSPDCP Constatări și recomandări pentru operatorii din sectorul public

Doamna Țuicu Carmen Camelia, chestor de poliție, adjunct al inspectorului general al Poliției Române Alocuțiune IGPR

Doamna Ecaterina MIREA, secretar de stat Instituția Avocatul Poporului Cazuistica instituției Avocatul Poporului în m a t e ria p r o t e c ția d a t elo r c u caracter personal

Domnul Aurel-Cătălin Giulescu, director DEPABD Scurte considerații cu privire la aplicarea dispozițiilor art. 23 din GDPR, prin prisma dreptului la informare al persoanei vizate .

Domnul Cristian LEAHU – director Departamentul Legislativ Autoritatea Electorală Permanentă

 Procesele electorale şi protecţia datelor personale .

Doamna Carmen Iordache - Consiliul Național de Studiere a Arhivelor Securității - mesajul președintelui CNSAS

Domnul Savu Ionuț - șeful Oficiului pentru Protecția Datelor din Ministerul Afacerilor Interne Principiul limitărilor legate de scop - adesea neglijat

Domnul Emil DRĂGHICI, președinte Asociația Comunelor din România.

Doamna Amelia DONDERA– consilier Consiliul Legislativ Protecția datelor cu caracter personal. Măsuri organizatorice implementate la nivelul Consiliului Legislativ.

Domnul Sergiu-Răzvan Malița, subinspector Inspectoratul General al Poliției de Frontieră Prelucrarea Datelor cu Caracter Personal în cadrul Poliției de Frontieră Române

**OBIECTIVE**

Din 25 mai 2018 s-au produs schimbări importante în legislaţia privind protecţia datelor personale în Europa, odată cu intrarea în vigoare a Regulamentului (UE) 679/2016, cunoscut drept Regulamentul General privind Protecţia Datelor Personale (RGPD).

 Evenimentul s-a adresat autorităţilor publice centrale şi locale, inclusiv companiilor de drept public şi privat, organizaţiilor/firmelor private, sindicate, ONG-urilor care procesează date cu caracter personal, pentru adaptarea la noile cerinţe legislative şi implementarea noilor măsuri tehnice şi organizatorice menite să asigure o protecţie adecvată a acestora, referindu-ne la: datele angajaţilor, datelor clienţilor în scopuri de marketing, a datelor de sănătate, cazier fiscal sau judiciar etc., toate aceste situaţii transformând organizaţia/compania/instituţia într-un subiect al RGPD.

**SUBIECTE în dezbatere**:

Obligațiile pe care le au operatorii de date cu caracter personal sunt reglementate în Capitolul IV din Regulamentul (UE) 2016/679.

Printre principalele obligații ale operatorilor în aplicarea Regulamentului (UE) 2016/679 se numără:

 ¬ respectarea principiilor de prelucrare a datelor (art. 5 din Regulamentul (UE) 2016/679);

¬ respectarea drepturilor persoanelor fizice (art. 12-23 din Regulamentul (UE) 2016/679);

¬ asigurarea securității datelor (art. 25 și art. 32 din Regulamentul (UE) 2016/679);

¬ desemnarea unui responsabil cu protecția datelor (art. 37-39 din Regulamentul (UE) 2016/679), după caz; ¬ notificarea încălcărilor de securitate (art. 33 din Regulamentul (UE) 2016/679), după caz; ¬ evaluarea impactului asupra protecției datelor (art. 35 din Regulamentul (UE) 2016/679), după caz;

¬ cartografierea prelucrărilor de date cu caracter personal (art. 30 din Regulamentul (UE) 2016/679).

Desemnarea responsabilului cu protecția datelor (DPO)

Este obligatorie atunci când:

 ¬ prelucrarea este efectuată de o autoritate sau un organism public (definite de art. 2 alin. (1) lit. a) din Legea nr. 190/2018), cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;

 ¬ se realizează, ca activități principale, operațiuni de prelucrare care, prin natura, domeniul de aplicare şi/sau scopurile lor, necesită o monitorizare periodică şi sistematică a persoanelor vizate pe scară largă;

¬ se realizează, ca activități principale, prelucrarea pe scară largă a unor categorii speciale de date în temeiul articolului 9 sau a unor date cu caracter personal referitoare la condamnări penale şi infracțiuni, menționată la articolul 10.

Responsabilul cu protecția datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să îşi îndeplinească sarcinile în baza unui contract de servicii (art. 37 din Regulamentul (UE) 2016/679).

**Un subiect foarte important ( îndelung disputat cu Direcţia Audit Public Intern din cadrul Primăriei Sectorului 2) a fost legat de situațiile în care se impune realizarea unei evaluări a impactului asupra protecției datelor cu caracter personal de către operatori ;i care sunt prevăzute în Decizia președintelui Autorității Naționale de Supraveghere nr. 174/2018**, astfel:

♣ prelucrarea datelor cu caracter personal efectuată în vederea realizării unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

♣ prelucrarea pe scară largă a datelor cu caracter personal privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate, a datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea, viața sexuală sau orientarea sexuală ale unei persoane fizice sau a datelor cu caracter personal referitoare la condamnări penale şi infracțiuni;

♣ prelucrarea datelor cu caracter personal având ca scop monitorizarea sistematică pe scară largă a unei zone accesibile publicului, cum ar fi supravegherea video în centre comerciale, stadioane, piețe, parcuri sau alte asemenea spații;

 ♣ prelucrarea pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile, în special ale minorilor şi ale angajaților, prin mijloace automate de monitorizare şi/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfășurării activităților de reclamă, marketing şi publicitate;

1. Aspecte generale

♣ prelucrarea pe scară largă a datelor cu caracter personal prin utilizarea inovatoare sau implementarea unor tehnologii noi, în special în cazul în care operațiunile respective limitează capacitatea persoanelor vizate de a-şi exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaștere facială în vederea facilitării accesului în diferite spații;

♣ prelucrarea pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace (aplicații "Internetul lucrurilor", cum ar fi smart TV, vehicule conectate, contoare inteligente, jucării inteligente, orașe inteligente sau alte asemenea aplicații);

♣ prelucrarea pe scară largă şi/sau sistematică a datelor de trafic şi/sau de localizare a persoanelor fizice (cum ar fi monitorizarea prin Wi-Fi, prelucrarea datelor de localizare geografică a pasagerilor în transportul public sau alte asemenea situații) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată. C. Spre a veni în sprijinul persoanelor vizate și operatorilor de date cu caracter personal Autoritatea națională de supraveghere a pus la dispoziția publicului: - Ghidul orientativ de aplicare a Regulamentului General privind protecția datelor destinat operatorilor; - Ghid Întrebări și răspunsuri cu privire la aplicarea Regulamentului (UE) 2016/679. Acestea sunt accesibile pe site-ul www.dataprotection.ro, alături de alte documente și materiale informative.

**Activitatea de monitorizare și control a Autorității de Supraveghere**

În anul 2020, Autoritatea de Supraveghere a primit un număr total de 5480 de plângeri, sesizări și notificări privind incidente de securitate, pe baza cărora au fost deschise 694 investigații.

Ca urmare a investigațiilor, au fost aplicate 29 de amenzi în cuantum total de 892115,95 lei. De asemenea, au mai fost aplicate 64 de avertismente și au fost dispuse 65 de măsuri corective.

 Activitatea de soluționare a plângerilor

În anul 2020, în ceea ce privește activitatea de soluționare a plângerilor, Autoritatea de Supraveghere a primit un număr total de 5082 plângeri, pe baza cărora au fost demarate 296 de investigații. Plângerile primite de Autoritatea de Supraveghere în anul 2020 au vizat, în principal, următoarele:

• încălcarea drepturilor și a principiilor prevăzute de Regulamentul (UE) 2016/679; • dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate;

• prelucrarea imaginilor prin intermediul sistemelor de supraveghere video;

 • primirea de mesaje comerciale nesolicitate;

• încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date personale prin neadoptarea de către operatori a măsurilor tehnice și organizatorice adecvate privind asigurarea securității prelucrărilor;

• raportarea de date personale la Biroul de Credit. Urmare a investigațiilor efectuate pe baza plângerilor, au fost aplicate următoarele sancţiuni contravenţionale :

¬ 20 amenzi, dintre care 18 în baza Regulamentului (UE) 2016/679, în cuantum total de 220.096,45 lei (echivalentul sumei de 45.500 Euro) și 2 amenzi în baza Legii nr. 506/2004, în cuantum total de 20.000 lei;

 ¬ 55 de avertismente;

¬ 47 măsuri corective în baza dispozițiilor art. 58 alin. (2) lit. c) și d) din Regulamentul (UE) 2016/679.

Activitatea de control ca urmare a primirii de notificări privind încălcărea securității datelor și sesizări.

 În anul 2020, în ceea ce privește incidentele de securitate, operatorii de date au transmis, atât în temeiul Regulamentului (UE) 2016/679, cât și al Legii nr. 506/2004, un număr de 194 de notificări, iar sesizările privind posibile neconformități cu dispozițiile Regulamentul (UE) 2016/679 s-au ridicat la un număr de 204.

Încălcările de securitate au vizat, în principal, următoarele aspecte:

¬ Confidențialitatea/disponibilitatea/integritatea datelor cu caracter personal afectate ca urmare a dezvăluirilor neautorizate ori ca urmare a unui software malițios, de tip ransomware;

 ¬ Accesul ilegal la datele cu caracter personal ale clienților din sistemul bancar; ¬ Accesul neautorizat la sistemele de supraveghere video cu circuit închis (CCTV);

¬ Dezvăluirea de date cu caracter personal în sistemul medical.

Sesizările primite au vizat, în principal, următoarele aspecte:

• Lipsa măsurilor de securitate, inclusiv la nivelul website-urilor;

• Publicarea/dezvăluirea datelor cu caracter personal în mediul on-line, în special pe retelele sociale.

Ca urmare a sesizărilor primite și încălcărilor de securitate notificate de către operatorii de date cu caracter personal, pe parcursul anului 2020, la nivelul Autorității de Supraveghere au fost demarate un număr de 398 de investigații din oficiu.

În cadrul investigațiilor efectuate din oficiu, în anul 2020 au fost aplicate 9 amenzi în cuantum total de 652.019,5 RON (139.000 Euro), 9 avertismente și 18 măsuri corective

**Măsurile corective dispuse în urma plângerilor și a investigațiilor din oficiu au vizat, în special, următoarele:**

**⎫ Asigurarea conformității operațiunilor de prelucrare cu dispozițiile Regulamentului (UE) 2016/679;**

**⎫ Respectarea principiilor de prelucrare a datelor, în special cele privind legalitatea, transparența și proporționalitatea;**

**⎫ Respectarea drepturilor persoanelor vizate prevăzute de Regulamentul (UE) 2016/679;**

**⎫ Realizarea informării persoanelor vizate potrivit art. 12 din Regulamentul (UE) 2016/679, inclusiv prin utilizarea de pictograme standardizate în spațiile/locurile monitorizate video, poziționate la o distanță rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere;**

**⎫ Punerea în aplicare a unor măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător, cum ar fi verificarea periodică, prin sondaj, a datelor înregistrate în aplicațiile informatice, pentru a identifica accesările neautorizate;**

 **⎫ Instruirea personalului cu privire la măsurile luate de operator, astfel ca utilizatorii să aibă acces numai la datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu;**

**⎫ Revizuirea şi actualizarea procedurilor de lucru referitoare la protecția datelor cu caracter personal.**

Organizat sub forma unui panel de discuții cu reprezentanţii autorităţilor şi instituţiilor publice centrale reprezentative, evenimentul şi-a propus să ofere răspunsuri la cele mai importante întrebări legate de modificările pe care le-a adus Regulamentul GDPR precum şi sprijin pentru asigurarea aplicării adecvate a Regulamentului UE 2016/679, în contextul specific fiecărui domeniu de activitate.

De asemenea, recomandările experţilor precum şi ale Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal sunt următoarele:

* Este indicat, pe lângă numirea unui DPO, să avem un consultant extern;
* Instruirea întregului personal în mod corespunzător;
* Aplicarea GDPR şi a legislaţiei subsecvente la locul de muncă;
* Angajaţii trebuie să evite utilizarea infrastructurii profesionale pentru scop personal;
* Ca şi măsuri de salvgardare, recomandat este să:
* Limităm tipurile de date prelucrate precum şi limitarea dreptului de retenţie întrucât, lipsa referitoare la durata de stocare precum şi termenul specific de ştergere generează amenzi.
* Anual este indicat să avem un audit de securitate.

Participanți la eveniment din partea Primăriei Sectorului 2:

Maria Ionescu – Consilier juridic, DPO