Conferinţa de analiză a riscului – Ediţia a VI-a

*OPTIMIZARE **ȘI PERFORMANȚĂ ÎN REDUCEREA** RISCURILOR DE SECURITATE*

PANEL IV

Tendinte si influente în practicile evaluatorilor

Eveniment **online şi**

pe Youtube & Facebook

PANEL SPONSORIZAT DE:

MAGUS
PROTECT TECHNOLOGIES

Impactul GDPR asupra securitatii fizice

Agenda

- Cadrul legal
  Legislatie specifica de securitate si legislatie complementara ce trebuie avuta in vedere la evaluarea de risc
- Date cu caracter personal (DCP)
  Ce sunt datele cu caracter personal si ce trebuie sa stim despre ele?
- DCP si securitatea fizica
  Exista date cu caracter personal in securitatea fizica ?
- DCP si evaluarea de risc la securitatea fizica
  Cum ne influenteaza legislatia si cerintele pe zona de privacy in intocmirea evaluarii de risc ?

PANEL SPONSORIZAT DE:

Cadrul legal

La intocmirea ERSF, evaluatorul de risc trebuie sa tina cont de mai multe acte normative si nu doar de Legea 333/2003, HG 1010/2013 cu modificarile si completarile ulterioare si Instructiunile nr. 9/2013.

Legislatia din alte domenii are impact pe masurile de securitate fizica, ca de exemplu:

- Infrastructuri critice nationale / europene (ICN/ICE)
- Documente clasificate
- Diferite domenii economice (cum ar fi cel bancar sau petrolier) care impun reguli suplimentare pe zona de securitate.

Chiar daca autoritatea competenta nu este IGPR, masurile de securitate au caracter unitar si toate cerintele legale trebuie considerate in intocmirea ERSF.

Impactul GDPR asupra securitatii fizice

Legislatie date cu caracter personal

Anterior GDPR, in Romania exista legislatie cu impact pe securitatea fizica (inclusive amenzi applicate Politiei Romane), si anume:

- Legea 677/2001 privind protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date
- Decizia nr. 52/2012 a ANSPDCP privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video

Arges: Amenda pentru supravegherea video a angajatilor

Serviciul de Evidenţă a Populaţiei Argeş a fost amendat cu 4.000 de lei, pentru că angajaţii sunt supravegheaţi de camere video, din ordinul conducerii instituţiei.

Supravegherea este considerată abuz de către Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

https://news.securityportal.ro/stiri/business-si-tehnologie/arges-amenda-pentru-supravegherea-video-a-angajatilor/

Impactul GDPR asupra securitatii fizice

Legislatie date cu caracter personal

Odata cu aparitia GDPR, legislatia nationala in vigoare a fost abrogata si noi acte normative au fost emise pentru a asigura corelarea cu cadrul european. Legislatia complete se gaseste pe site-ul ANSPDCP (https://www.dataprotection.ro/?page=legislatie_primara&lang=ro)

Cele mai importante texte de lege care trebuie considerate in zona securitatii sunt:

- GDPR – Regulamentul General pentru Protectia Datelor cu Caracter Personal
- Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR
- Ghidul nr. 3/2019 privind supravegherea video (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en)

Nu este interzis sa se prelucreze date cu caracter personal insa acest lucru trebuie facut tinandu-se cont de o serie de cerinte si anume:

- Principiile generale de prelucrare a datelor cu caracter personal
- Privacy by default si privacy by design
- Analiza pe zona de privacy care poate fi sub forma de:
  - Data Protection Impact Analysis
  - Gap Analysis

PANEL SPONSORIZAT DE:

Impactul GDPR asupra securitatii fizice

Principiile de procesare a DCP

PANEL SPONSORIZAT DE:

Impactul GDPR asupra securitatii fizice

Caracterul special al zonei de privacy

Spre deosebire de alte cerinte legale pe alte zone, in cazul datelor cu caracter personal exista doua elemente care fac ca acest domeniu sa fie tratat cu foarte mare atentie de catre orice companie.

“Povara dovezii” (the burden of proof)	Cuantumul amenzilor
• Art. 5, alin. 1 din GDPR specifica cele 6 principii generale de prelucrare legala a DCP • Art. 5, alin. 2 din GDPR specifica faptul ca pica in sarcina operatorului sa faca dovada ca respecta alin. 1 ***Operatorul este responsabil de respectarea alineatului (1) şi poate demonstra această respectare ("responsabilitate")*** Acest lucru inseamna ca nu se aplica principiul “nevinovat pana la proba contrarie” deoarece sarcina dovezii pica “by default” in raspunderea operatorului de date cu caracter personal.	• GDPR prevede cele mai mari amenzi din UE ce pot duce pana la 20 milioane de euro sau 4% din cifra de afaceri agregata a grupului de firme (si nu a firmei unde s-a constatat problema) – ***se aplica cea mai mare dintre ele*** • In ianuarie 2021, a fost aplicata o amenda de 10,4 milioane euro pentru probleme legate de supravegherea video (https://dataprivacymanager.net/10-4-million-euro-gdpr-fine-for-video-surveillance/) • In octombrie 2020 H&M a primit o amenda de 32 milioane euro pentru un cumul de probleme, inclusive in ceea ce priveste supravegherea video a angajatilor (https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren)

PANEL SPONSORIZAT DE:

Impactul GDPR asupra securitatii fizice

Amenzi GDPR Romania

DATA PROTECTION AUTORITHY ACTIVITY

Number of total GDPR fines by country

SPAIN	212	DENMARK	8
ITALY	67	THE NETHERLANDS	8
ROMANIA	52	SLOVAKIA	6
HUNGARY	38	IRELAND	6
GERMANY	31	FINLAND	5
BELGIUM	25	ESTONIA	5
NORWAY	24	LATVIA	5
POLAND	23	LITHUANIA	5
BULGARIA	20	UNITED KINGDOM	4
SWEDEN	17	PORTUGAL	4
CYPRUS	15	ICELAND	2
GREECE	14	CROATIA	2
CZECH REPUBLIC	14	ISLE OF MAN	1
FRANCE	14	MALTA	1
AUSTRIA	10		

Evidentele publice arata ca Romania este una dintre cele mai active tari pe acest domeniu, clasandu-se pe locul 3 dupa numarul total de amenzi aplicate, dupa Spania (212) si Italia (67) dar mult inaintea locului 4 ocupat de Ungaria (38).

Din totalul de 52 de amenzi aplicate, 5 sunt pe zona de securitate fizica (supraveghere video), adica aproximativ 10%.

Impactul GDPR asupra securitatii fizice

Amenzi GDPR Romania

DATA PROTECTION AUTORITHY ACTIVITY

Total amount of GDPR fines by country

ITALY	€ 76.065.307	PORTUGAL	€ 424.000
GERMANY	€ 63.686.833	DENMARK	€ 375.750
FRANCE	€ 54.661.300	ESTONIA	€ 300.548
UNITED KINGDOM	€ 44.221.000	LATVIA	€ 243.250
SPAIN	€ 25.368.910	CYPRUS	€ 224.000
SWEDEN	€ 12.332.430	FINLAND	€ 207.500
THE NETHERLANDS	€ 4.405.000	CZECH REPUBLIC	€ 140.566
BULGARIA	€ 3.210.690	LITHUANIA	€ 106.500
POLAND	€ 1.816.498	SLOVAKIA	€ 90.000
NORWAY	€ 1.257.650	AUSTRIA	€ 70.950
BELGIUM	€ 918.000	ICELAND	€ 29.600
IRELAND	€ 785.000	ISLE OF MAN	€ 13.500
GREECE	€ 769.000	MALTA	€ 5.000
HUNGARY	€ 752.361	CROATIA	UNKNOWN
ROMANIA	€ 687.650		

Aceleasi evidente publice arata ca Romania se claseaza pe locul 15 din 29 dupa valoarea totala a amenzilor aplicate, cu un cuantum total de 687.650 euro.

Din aceasta suma, 18.500 euro reprezinta amenzi pe zona de securitate (supraveghere video), adica aproximativ 2.70% din cuantumul total al amenzilor aplicate de ANSPDCP.

Impactul GDPR asupra securitatii fizice

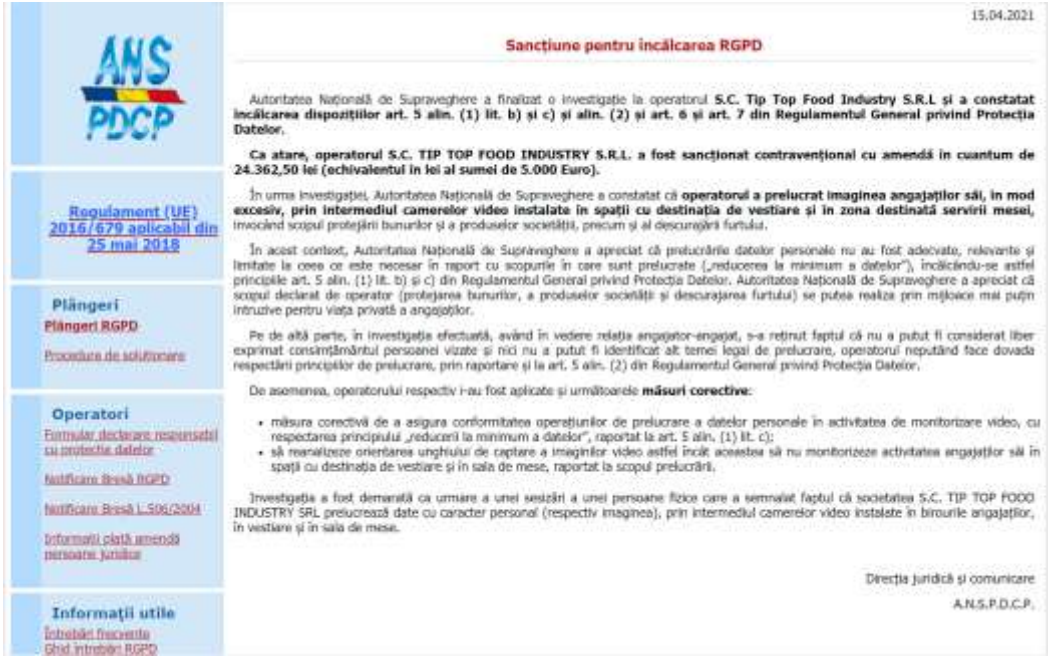
Amenzi GDPR Romania

Conform enforcementtracker.com (https://www.enforcementtracker.com/), in Romania au fost applicate 54 de amenzi pe GDPR dintre care 5 au legatura cu sistemele de supraveghere video si au amenzi cuprinse intre 500 si 5000 euro.

PANEL SPONSORIZAT DE:

Impactul GDPR asupra securitatii fizice

Amenda GDPR – Tip Top Food Industry SRL



ANS PDCP

Regulament (UE) 2016/679 aplicabil din 25 mai 2018

Plângeri
Plângeri RGPD
Procedura de soluționare

Operatori
Formular declarare responsabil cu protecția datelor
Notificare Breșă RGPD
Notificare Breșă L.506/2004
Informații plată amendă persoane juridice

Informații utile
Întrebări frecvente
Ghid întrebări RGPD

15.04.2021

Sancțiune pentru încălcarea RGPD

Autoritatea Națională de Supraveghere a finalizat o investigație la operatorul **S.C. Tip Top Food Industry S.R.L și a constatat încălcarea dispozițiilor art. 5 alin. (1) lit. b) și c) și alin. (2) și art. 6 și art. 7 din Regulamentul General privind Protecția Datelor.**

Ca atare, operatorul S.C. TIP TOP FOOD INDUSTRY S.R.L. a fost sancționat contravențional 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.

În acest context, Autoritatea Națională de Supraveghere a apreciat că prelucrările datelor personale nu au fost adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor"), încălcându-se astfel principiile art. 5 alin. (1) lit. b) și c) din Regulamentul General privind Protecția Datelor. Autoritatea Națională de Supraveghere a apreciat că scopul declarat de operator (protejarea bunurilor, a produselor societății și descurajarea furtului) se putea realiza prin mijloace mai puțin intruzive pentru viața privată a angajaților.

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 aceastea 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 S.C. 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.

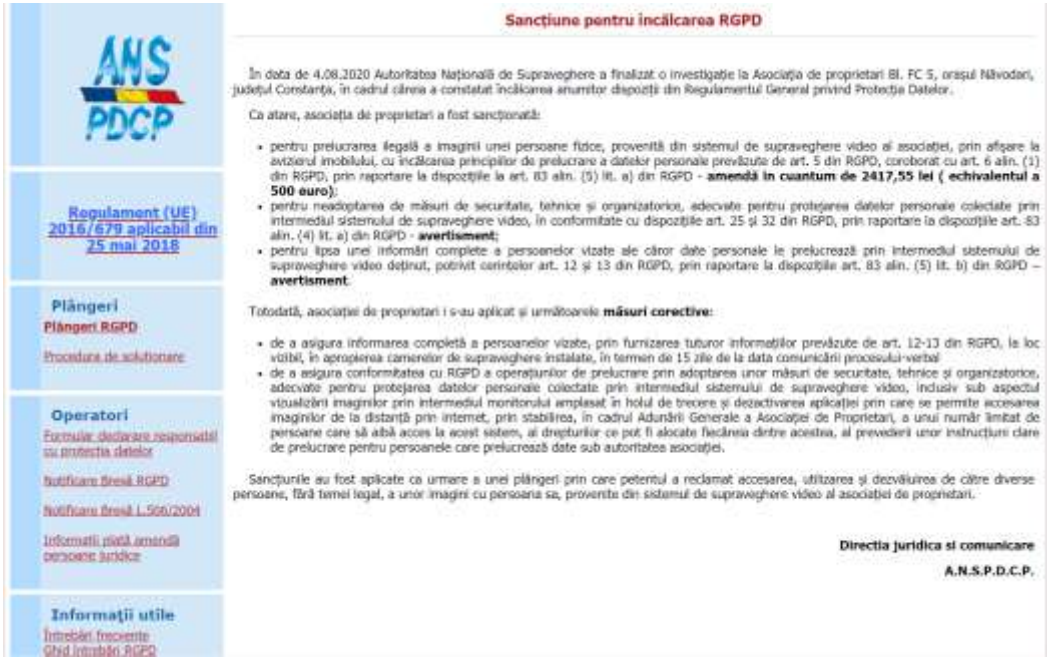
Direcția juridică și comunicare
A.N.S.P.D.C.P.

- Supraveghere excesiva a unor zone sensibile (vestiar, sala de mese)
- nerespectarea principiului minimarii datelor
- Interesul persoanei prevaleaza interesului de securitate
- Interzicerea monitorizarii activitatii angajatilor

https://www.dataprotection.ro/?page=Comunicat_Presa_15_/_04_/_2021&lang=ro

Impactul GDPR asupra securitatii fizice

Amenda GDPR – Asociatie de proprietari Navodari



ANS PDCP

Regulament (UE) 2016/679 aplicabil din 25 mai 2018

Plângeri

Plângeri RGPD

Procedura de soluționare

Operatori

Formular declarare responsabil cu protecția datelor

Notificare breșă RGPD

Notificare breșă L 506/2004

Informații plată amendă persoane juridice

Informații utile

Întrebări frecvente

Ghid întrebări RGPD

Sancțiune pentru încălcarea RGPD

În data de 4.08.2020 Autoritatea Națională de Supraveghere a finalizat o investigație la Asociația de proprietari Bl. FC 5, orașul Năvodari, județul Constanța, în cadrul căreia a constatat încălcarea anumitor dispoziții din Regulamentul General privind Protecția Datelor.

Ca atare, asociația de proprietari a fost sancționată:

- pentru prelucrarea ilegală a imaginii unei persoane fizice, provenită din sistemul de supraveghere video al asociației, prin afișare la avizierul imobilului, cu încălcarea principiilor de prelucrare a datelor personale prevăzute de art. 5 din RGPD, coroborat cu art. 6 alin. (1) din RGPD, prin raportare la dispozițiile la art. 83 alin. (5) lit. a) din RGPD - **amendă în cuantum de 2417,55 lei (echivalentul a 500 euro)**;
- pentru neadoptarea de măsuri de securitate, tehnice și organizatorice, adecvate pentru protejarea datelor personale colectate prin intermediul sistemului de supraveghere video, în conformitate cu dispozițiile art. 25 și 32 din RGPD, prin raportare la dispozițiile art. 83 alin. (4) lit. a) din RGPD - **avertisment**;
- pentru lipsa unei informări complete a persoanelor vizate ale căror date personale le prelucrează prin intermediul sistemului de supraveghere video deținut, potrivit cerințelor art. 12 și 13 din RGPD, prin raportare la dispozițiile art. 83 alin. (5) lit. b) din RGPD – **avertisment**.

Totodată, asociației de proprietari i s-au aplicat și următoarele **măsuri corective**:

- de a asigura informarea completă a persoanelor vizate, prin furnizarea tuturor informațiilor prevăzute de art. 12-13 din RGPD, la loc vizibil, în apropierea camerelor de supraveghere instalate, în termen de 15 zile de la data comunicării procesului-verbal
- de a asigura conformitatea cu RGPD a operațiunilor de prelucrare prin adoptarea unor măsuri de securitate, tehnice și organizatorice, adecvate pentru protejarea datelor personale colectate prin intermediul sistemului de supraveghere video, inclusiv sub aspectul vizualizării imaginilor prin intermediul monitorului amplasat în holul de trecere și dezactivarea aplicației prin care se permite accesarea imaginilor de la distanță prin internet, prin stabilirea, în cadrul Adunării Generale a Asociației de Proprietari, a unui număr limitat de persoane care să aibă acces la acest sistem, al drepturilor ce pot fi alocate fiecăreia dintre acestea, al prevederii unor instrucțiuni clare de prelucrare pentru persoanele care prelucrează date sub autoritatea asociației.

Sancțiunile au fost aplicate ca urmare a unei plângeri prin care petentul a reclamat accesarea, utilizarea și dezvăluirea de către diverse persoane, fără temei legal, a unor imagini cu persoana sa, provenite din sistemul de supraveghere video al asociației de proprietari.

Directia juridica si comunicare

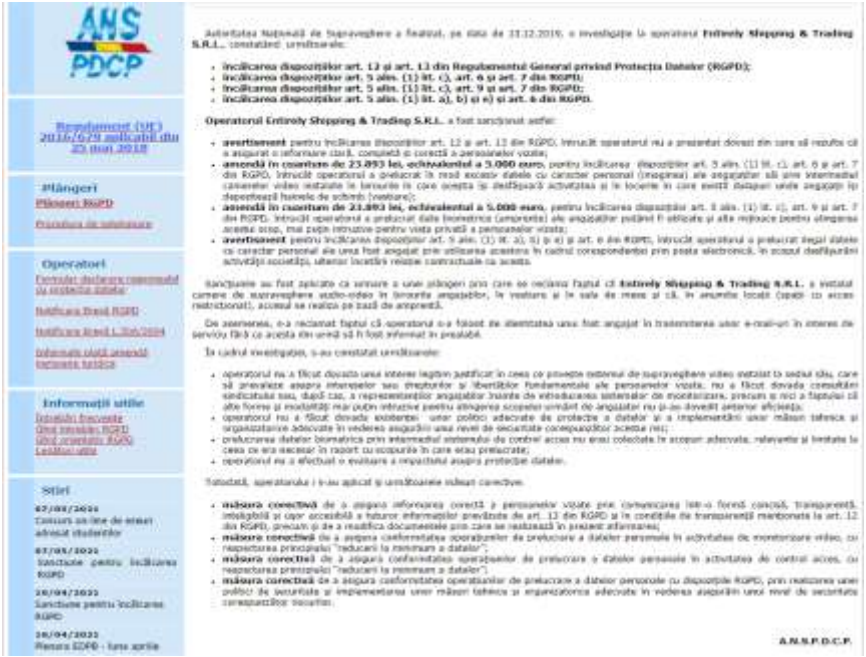
A.N.S.P.D.C.P.

- Neefectuarea analizei privind procesarea DCP
- Neinformarea corespunzatoare a persoanelor vizate
- Masuri pentru limitarea supravegherii video
- Interzicerea monitorizarii la distanta (pe telefon)

https://www.dataprotection.ro/?page=Comunicat_Presa_01_09_2020&lang=ro

Impactul GDPR asupra securitatii fizice

Amenda GDPR – Entirely Shipping & Trading SRL



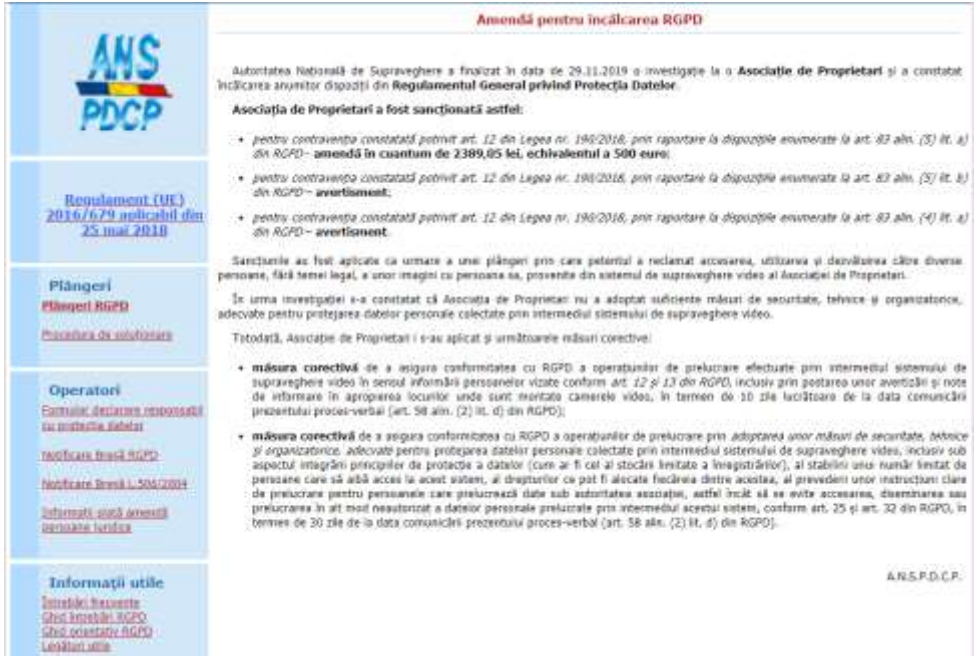
- 4 nereguli identificate din care 2 pe zona de securitate
- 2 nereguli non-security sanctionate cu avertisment
- 2 reguli security sanctionate cu 10.000 euro
- Supravegherea excesiva a angajatilor
- Folosirea de metode biometrice

https://www.dataprotection.ro/index.jsp?page=O_noua_sanctiune_pentru_incalcarea_RGPD_2020_3&lang=ro

PANEL SPONSORIZAT DE:

Impactul GDPR asupra securitatii fizice

Amenda GDPR – Asociatie de proprietari



ANS PDCP

Regulament (UE) 2016/679 aplicabil din 25 mai 2018

Plângeri

Plângeri RGPD

Procedura de soluționare

Operatori

Formular declarare responsabil cu protecția datelor

Notificare breșă RGPD

Notificare Breșă L 506/2004

Informații despre anumite persoane juridice

Informații utile

Întrebări frecvente

Ghid legislație RGPD

Ghid orientativ RGPD

Legături utile

Amendă pentru încălcarea RGPD

Autoritatea Națională de Supraveghere a finalizat în data de 29.11.2019 o investigație la o **Asociație de Proprietari** și a constatat încălcarea anumitor dispoziții din **Regulamentul General privind Protecția Datelor**.

Asociația de Proprietari a fost sancționată astfel:

- *pentru contravenția constatată potrivit art. 12 din Legea nr. 190/2018, prin raportare la dispozițiile enumerate la art. 83 alin. (5) lit. a) din RGPD* – **amendă în cuantum de 2389,05 lei, echivalentul a 500 euro**;
- *pentru contravenția constatată potrivit art. 12 din Legea nr. 190/2018, prin raportare la dispozițiile enumerate la art. 83 alin. (5) lit. b) din RGPD* – **avertisment**;
- *pentru contravenția constatată potrivit art. 12 din Legea nr. 190/2018, prin raportare la dispozițiile enumerate la art. 83 alin. (4) lit. a) din RGPD* – **avertisment**.

Sancțiunile au fost aplicate ca urmare a unei plângeri prin care petentul a reclamat accesarea, utilizarea și dezvăluirea către diverse persoane, fără temei legal, a unor imagini cu persoana sa, provenite din sistemul de supraveghere video al Asociației de Proprietari.

În urma investigației s-a constatat că Asociația de Proprietari nu a adoptat suficiente măsuri de securitate, tehnice și organizatorice, adecvate pentru protejarea datelor personale colectate prin intermediul sistemului de supraveghere video.

Totodată, Asociația de Proprietari i s-au aplicat și următoarele măsuri corective:

- **măsura corectivă** de a asigura conformitatea cu RGPD a operațiunilor de prelucrare efectuate prin intermediul sistemului de supraveghere video în sensul informării persoanelor vizate conform *art. 12 și 13 din RGPD*, inclusiv prin postarea unor avertizări și note de informare în apropierea locurilor unde sunt montate camerele video, în termen de 10 zile lucrătoare de la data comunicării prezentului proces-verbal (art. 58 alin. (2) lit. d) din RGPD);
- **măsura corectivă** de a asigura conformitatea cu RGPD a operațiunilor de prelucrare prin *adoptarea unor măsuri de securitate, tehnice și organizatorice, adecvate* pentru protejarea datelor personale colectate prin intermediul sistemului de supraveghere video, inclusiv sub aspectul integrării principiilor de protecție a datelor (care ar fi cel al stocării limitate a înregistrărilor), al stabilirii unui număr limitat de persoane care să aibă acces la acest sistem, al drepturilor ce pot fi alocate fiecăreia dintre acestea, al prevederii unor instrucțiuni clare de prelucrare pentru persoanele care prelucrează date sub autoritatea asociației, astfel încât să se evite accesarea, diseminarea sau prelucrarea în alt mod neautorizat a datelor personale prelucrate prin intermediul acestui sistem, conform art. 25 și art. 32 din RGPD, în termen de 30 zile de la data comunicării prezentului proces-verbal (art. 58 alin. (2) lit. d) din RGPD).

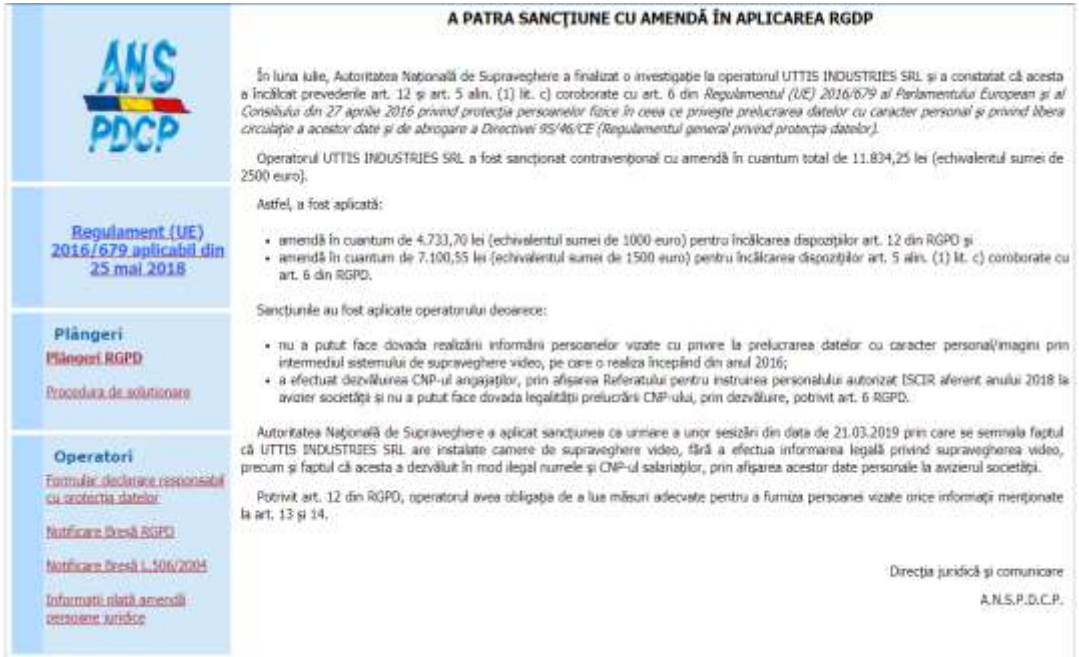
A.N.S.P.D.C.P.

- Transferul datelor cu caracter personal (imagini CCTV) realizat fara respectarea GDPR
- Masuri pentru limitarea accesului la, prelucarii sau diseminarii imaginilor rezultate din CCTV

https://www.dataprotection.ro/?page=Amenda_asociatie_proprietari&lang=ro

Impactul GDPR asupra securitatii fizice

Amenda GDPR – Uttis Industry SRL



ANS PDCP

Regulament (UE) 2016/679 aplicabil din 25 mai 2018

Plângeri

Plângeri RGPD

Procedura de soluționare

Operatori

Formular declarare responsabil cu protecția datelor

Notificare Breșă RGPD

Notificare Breșă L.506/2004

Informații plată amendă persoane juridice

A PATRA SANCȚIUNE CU AMENDĂ ÎN APLICAREA RGDP

În luna iulie, Autoritatea Națională de Supraveghere a finalizat o investigație la operatorul UTTIS INDUSTRIES SRL și a constatat că acesta a încălcat prevederile art. 12 și art. 5 alin. (1) lit. c) coroborate cu art. 6 din *Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).*

Operatorul UTTIS INDUSTRIES SRL a fost sancționat contravențional cu amendă în cuantum total de 11.834,25 lei (echivalentul sumei de 2500 euro).

Astfel, a fost aplicată:

- amendă în cuantum de 4.733,70 lei (echivalentul sumei de 1000 euro) pentru încălcarea dispozițiilor art. 12 din RGPD și
- amendă în cuantum de 7.100,55 lei (echivalentul sumei de 1500 euro) pentru încălcarea dispozițiilor art. 5 alin. (1) lit. c) coroborate cu art. 6 din RGPD.

Sancțiunile au fost aplicate operatorului deoarece:

- nu a putut face dovada realizării informării persoanelor vizate cu privire la prelucrarea datelor cu caracter personal/imagini prin intermediul sistemului de supraveghere video, pe care o realiza începând din anul 2016;
- a efectuat dezvăluirea CNP-ul angajaților, prin afișarea Referatului pentru instruirea personalului autorizat ISCIR aferent anului 2018 la avizier societăți și nu a putut face dovada legalității prelucrării CNP-ului, prin dezvăluire, potrivit art. 6 RGPD.

Autoritatea Națională de Supraveghere a aplicat sancțiunea ca urmare a unor sesizări din data de 21.03.2019 prin care se semnala faptul că UTTIS INDUSTRIES SRL are instalate camere de supraveghere video, fără a efectua informarea legală privind supravegherea video, precum și faptul că acesta a dezvăluit în mod ilegal numele și CNP-ul salariaților, prin afișarea acestor date personale la avizierul societății.

Potrivit art. 12 din RGPD, operatorul avea obligația de a lua măsuri adecvate pentru a furniza persoanei vizate orice informații menționate la art. 13 și 14.

Direcția juridică și comunicare

A.N.S.P.D.C.P.

- Lipsa indeplinirii obligatiilor legale pe zona de informare a persoanelor vizate
- Afisarea publica a unor informatii sensibile

https://www.dataprotection.ro/?page=A_patra_amenda&lang=ro

PANEL SPONSORIZAT DE:

MAGUS
PROTECT TECHNOLOGIES

Impactul GDPR asupra securitatii fizice

Date cu caracter personal

DCP = inseamna orice informatii privind o persoană fizica identificata sau identificabila ("persoana vizata"); o persoana fizica identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un numar de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identitatii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

Anumite date cu caracter personal intra in categoria celor sensibile (ex: date genetice, date biometrice, date privind sanatatea, etc.

Impactul GDPR asupra securitatii fizice

Sistem de evidenta a datelor

inseamna orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate dupa criterii functionale sau geografice.

Prelucrare

inseamna orice operatiune sau set de operatiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fara utilizarea de mijloace automatizate, cum ar fi colectarea, inregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispozitie in orice alt mod, alinierea sau combinarea, restrictionarea, stergerea sau distrugerea.

Impactul GDPR asupra securitatii fizice

Date cu caracter personal sensibil in securitate

In securitatea fizica, se intalnesc de obicei 2 tipuri de date cu caracter personal din categoria celor sensibile, si anume:

- Date biometrice (ex: recunoastere faciala, amprenta etc)
- Date din documentele de identitate (ex: CNP, serie si numar CI, pasaport, permis sau orice alt) - https://www.dataprotection.ro/servlet/ViewDocument?id=742

Art. 1

(1) Codul numeric personal reprezintă un număr semnificativ care individualizează în mod unic o persoană fizică, constituind un instrument de verificare a stării civile a acesteia şi de identificare în anumite sisteme informatice de către persoanele autorizate.

(2) Datele cu caracter personal cu funcţie de identificare de aplicabilitate generală sunt acele numere prin care se identifică o persoană fizică în anumite sisteme de evidenţă şi care au aplicabilitate generală, cum ar fi: codul numeric personal, seria şi numărul actului de identitate, numărul paşaportului, al permisului de conducere, numărul de asigurare socială sau de sănătate.

(3) Datele prevăzute la alin. (1) şi (2) fac parte din categoria datelor cu caracter special supuse regulilor specifice de prelucrare.

PANEL SPONSORIZAT DE:

Impactul GDPR asupra securitatii fizice

Date cu caracter personal in securitate

Toate celelalte date cu care se lucreaza in zona prestarii de servicii de securitate nu intra in mod normal in categoria celor sensibile dar ar putea in anumite conditii, ca de exemplu:

- Triajul epidemiologic nu reprepzinta nici macar o procesare de date cu caracter personal daca datele medicale procesate nu pot fi asociate cu o persoana anume.
- Daca insa datele respective pot fi asociate cu o anumita persoana, atunci prelucrarea se incadreaza in categoria datelor cu caracter sensibil. Spre exemplu, acest lucru ar putea aparea daca:
  - Temperatura citita este salvata impreuna cu imaginea in cazul camerelor care fac automat acest lucru
  - Temperatura citita cu termometrul este vizibila pe o alta camera sau poate fi asociata pe baza unor detalii cum ar fi timestamping.

Impactul GDPR in ERSF

Exista doua paliere prin care GDPR impacteaza evaluarea de risc si anume:

Calitatea partilor	Instructiunea nr. 9/2013
• Obligatiile legale privind realizarea securitatii revin clientului final de unde rezulta ca acesta are calitatea de ***operator*** conform GDPR iar firmele prestatoare de servicii au calitatea de ***persoane imputernicite***. • Evaluatorul de risc are calitatea de operator doar in ceea ce priveste procesul tehnic de realizare a evaluarii de risc (ce fotografii realizeaza, ce date consulta etc). • Firma de securitate are calitatea de operator pentru prelucrarile rezultate de activitatile ce ii sunt impuse prin lege (ex: recrutare, instruire etc)	• Art. 5 prevede ca prima etapa a analizei de risc consta in ***definirea parametrilor interni si externi care genereaza si/sau modifica riscurile la securitatea fizica a unitatii*** • Art. 7, alin. 2 prevede ca evaluatorul trebuie sa faca referire in cadrul raportului de evaluare la ***amplasarea geografica a unitatii, vecinatati, cai de acces, alti factori externi cu impact asupra activitatii unitatii***

Impactul GDPR asupra securitatii fizice

Prelucrarea datelor de acces

- Exista obligatia legala a mentinerii unor evidente (ex: registru de acces) care include date cu carater personal sensibil (seria si nr documentelor de identitate)
- Nivelul de protectie asigurat datelor cu caracter personal trebuie sa fie:
  - Adecvat sensibilitatii datelor
  - Implementat by default si by design
- Registrul de evidenta a accessului nu indeplineste cerintele pe linie de privacy (vezi anexa)
- Posibile solutii sunt:
  - Implementarea unor registre electronice care permit eliminarea vulnerabilitatilor celor in format hard-copy
  - Pastrarea registrelor in anumite conditii
  - Minimizarea volumetriei prin folosirea de registre cu numar limitat de pagini
  - Minimizarea riscurilor de access neautorizat la date prin folosirea unor formulare cu o singura persoana / pagina (atunci cand este necesar de exemplu sa captam o semnatura)

Impactul GDPR asupra securitatii fizice

Prelucrarea imaginilor CCTV

Ghidul nr. 3 / 2019 privind prelucrarea datelor cu caracter personal prin intermediul imaginilor sistemelor de supraveghere ne ofera cadrul de interpretare al GDPR precum si o serie de exemple practice in acest sens.

Exemplu: Proprietarul unui magazin dorește să deschidă un nou magazin și vrea să instaleze un sistem de supraveghere video pentru a preveni vandalismul. Prin prezentarea de statistici, el poate demonstra că există o mare probabilitate de vandalism în vecinătate. De asemenea, este utilă experiența magazinelor din vecinătate. Nu este necesar ca operatorul în cauză să fi suferit un prejudiciu, de vreme ce prejudiciile înregistrate în vecinătate sugerează un pericol sau ceva asemănător și, prin urmare, pot indica un interes legitim. Cu toate acestea, nu este suficientă prezentarea statisticilor privind criminalitatea la nivel național sau general fără analizarea zonei în cauză sau a pericolelor la adresa magazinului respectiv.

Impactul GDPR asupra securitatii fizice

Exemplu: O librărie dorește să-și protejeze sediul împotriva vandalismului. În general, camerele trebuie să filmeze doar spațiul respectiv deoarece nu este necesară supravegherea spațiilor învecinate sau a zonelor publice din împrejurimile sediului librăriei în acest scop.

Exemplu: Proprietarul unui magazin înregistrează imagini la intrare. În imagini se vede o persoană care fură portofelul alteia. Poliția solicită operatorului să predea materialul pentru a fi folosit în anchetă. În acest caz, proprietarul magazinului ar utiliza temeiul juridic prevăzut la articolul 6 alineatul (1) litera (c) (obligația legală) interpretat în coroborare cu dreptul intern relevant pentru prelucrarea prin transfer.

Exemplu: Într-un magazin se instalează o cameră de luat vederi din motive de securitate. Proprietarul magazinului consideră că a surprins ceva suspect în materialele înregistrate și decide să le trimită poliției (fără niciun indiciu că ar exista o anchetă în curs, de orice natură). În acest caz, proprietarul magazinului trebuie să evalueze dacă sunt îndeplinite condițiile prevăzute, în majoritatea cazurilor, la articolul 6 alineatul (1) litera (f). De obicei, acest lucru este valabil dacă proprietarul magazinului are o suspiciune rezonabilă legată de comiterea unei infracțiuni.

Impactul GDPR asupra securitatii fizice

Exemplu: Opiniile politice ar putea fi deduse, de exemplu, din imagini care prezintă persoane vizate identificabile participând la un eveniment, luând parte la o grevă, etc. Această situație ar intra sub incidența articolului 9.

Exemplu: Instalarea unei camere video de către un spital pentru a monitoriza starea de sănătate a unui pacient ar fi considerată prelucrare de categorii speciale de date cu caracter personal (articolul 9).

Exemplu: Un angajator nu poate să folosească înregistrări ale supravegherii video care prezintă o demonstrație cu scopul de a identifica greviștii.

Exemplu: Supravegherea video care surprinde o biserică nu intră în sine sub incidența articolului 9. Cu toate acestea, operatorul trebuie să efectueze o evaluare deosebit de atentă în baza articolului 6 alineatul (1) litera (f), ținând seama de natura datelor, precum și de riscul de înregistrare a altor date cu caracter special (dincolo de sfera articolului 9) atunci când sunt evaluate interesele persoanei vizate.

Impactul GDPR asupra securitatii fizice

3. Exemplu: Un operator gestionează accesul la clădirea sa folosind o metodă de recunoaștere facială. Oamenii pot utiliza acest mod de acces numai dacă și-au dat în prealabil consimțământul explicit și în cunoștință de cauză [în conformitate cu articolul 9 alineatul (2) litera (a)]. Cu toate acestea, pentru a se asigura că nu se captează imaginea niciunei persoane care nu și-a dat anterior consimțământul, metoda recunoașterii faciale ar trebui utilizată chiar de către persoana vizată, de exemplu prin apăsarea unui buton. Pentru a asigura legalitatea prelucrării datelor, operatorul trebuie să ofere întotdeauna o modalitate alternativă de acces în clădire, fără prelucrare biometrică, cum ar fi legitimații sau chei.

5. Exemplu: Proprietarul unui magazin dorește să-și personalizeze oferta pe baza caracteristicilor de gen și vârstă ale clientelei înregistrare de un sistem de supraveghere video. Dacă acest sistem nu generează modele biometrice pentru a identifica în mod unic persoanele, ci doar detectează caracteristicile fizice necesare pentru a clasifica persoanele, atunci prelucrarea nu intră sub incidența articolului 9 (atâta timp cât nu sunt prelucrate alte tipuri de categorii speciale de date).

Impactul GDPR asupra securitatii fizice

Exemplu: Dacă o persoană vizată solicită o copie a datelor sale personale prelucrate prin supraveghere video la intrarea într-un centru comercial cu 30 000 de vizitatori pe zi, persoana vizată trebuie să specifice când a trecut prin zona monitorizată într-un interval de aproximativ o oră. Dacă operatorul prelucrează încă materialul, trebuie să i se pună la dispoziție o copie a înregistrării video. Dacă alte persoane vizate pot fi identificate în același material, atunci acea parte a materialului trebuie anonimizată (de exemplu, prin estomparea copiei sau a unor părți ale acesteia) înainte de transmiterea copiei către persoana vizată care a depus cererea.

Exemplu: Dacă operatorul șterge automat toate înregistrările video, de exemplu în termen de 2 zile, nu este în măsură să furnizeze înregistrarea persoanei vizate după cele 2 zile. Dacă operatorul primește o solicitare după cele 2 zile, persoana vizată trebuie informată în consecință.

Impactul GDPR asupra securitatii fizice

Exemplu: Un magazin de proximitate care are probleme cu vandalismul, în special la exterior, și, prin urmare, folosește supraveghere video pe partea exterioară a intrării, în legătură directă cu pereții. Un trecător solicită ca datele sale personale să fie șterse chiar din acel moment. Operatorul este obligat să răspundă cererii fără întârzieri nejustificate și în termen de cel mult o lună. Întrucât înregistrările în cauză nu mai îndeplinesc scopul pentru care au fost stocate inițial (nu a avut loc niciun act de vandalism în perioada în care persoana vizată a trecut prin zonă), la momentul solicitării nu există niciun interes legitim de a stoca datele care să prevaleze asupra intereselor persoanelor vizate. Operatorul trebuie să șteargă datele cu caracter personal.

Exemplu: O companie întâmpină dificultăți constând în încălcări ale securității la intrarea publică și folosește supraveghere video pe motive de interes legitim, cu scopul de a-i surprinde pe cei care intră ilegal. Un vizitator se opune prelucrării datelor sale prin sistemul de supraveghere video din motive legate de situația sa particulară. Totuși, în acest caz, compania respinge cererea explicând că înregistrările stocate sunt necesare pentru o anchetă internă aflată în curs, având astfel motive legitime imperioase pentru a continua prelucrarea datelor cu caracter personal.

PANEL SPONSORIZAT DE:

Impactul GDPR asupra securitatii fizice

Supravegherea video

Live	Trigger based	Black box
• Pentru zonele cu infrastructura critica ce ar putea afecta continuitatea afacerii (ex: server, TEG etc.) • Pentru zona de access sau zone in care se concentreaza valori inseminate • Pentru alte zone unde in mod normal accesul persoanelor este interzis (ex: scari de evacuare)	• Pentru zone cu activitati intermitente (ex: zona de arpovizionare) • Pentru zone in care se primesc semnale de la diferiti senzori etc	• Este cea mai putin invaziva metoda de supraveghere si presupune accesul post eveniment la imagini • Este metoda “by default” ceea ce inseamna ca celelalte metode de supraveghere trebuie justificate

PANEL SPONSORIZAT DE:

Impactul GDPR asupra securitatii fizice

Greseli frecvente

- **Minimzarea datelor** – excesul pe linie de securitate este un element care creste nivelul de protectie insa acest lucru este in contradictie cu principiile de procesare a datelor. Chiar daca monitorizarea are loc in regim “black box”, evaluatorul este raspunzator pentru solutia generate sau pentru reperele pe care le ofera proiectantului
- **Limitarea scopului** – nu pot fi instalate camera in mod preventive (in caz ca …) si nici nu pot fi folosite imaginile pentru alte scopuri decat cele declarate
- **Limitarea accesului si procesarii** – trebuie implementate roluri de utilizatori bazate pe principiu “need to know”
- **Transferul datelor** – trebuie sa se faca in conditiile impuse de legislatie
- **Stocarea datelor** – exista o cantitate extrem de mare de date nenecesare care raman in sistem, accesibile multor persoane, neprotejate etc.
- **Trasabilitate operatii** – folosirea aceluiasi utilizator de mai multe persoane, lipsa loguri (in special pe zona evidentelor pe hartie)
- **Securitate datelor** – parole default, lipsa politica parole, lipsa securizare conexiune, lipsa criptare date etc.

Vă mul**ț**u**m**esc!

Razvan Ionescu

razvan@securityportal.ro