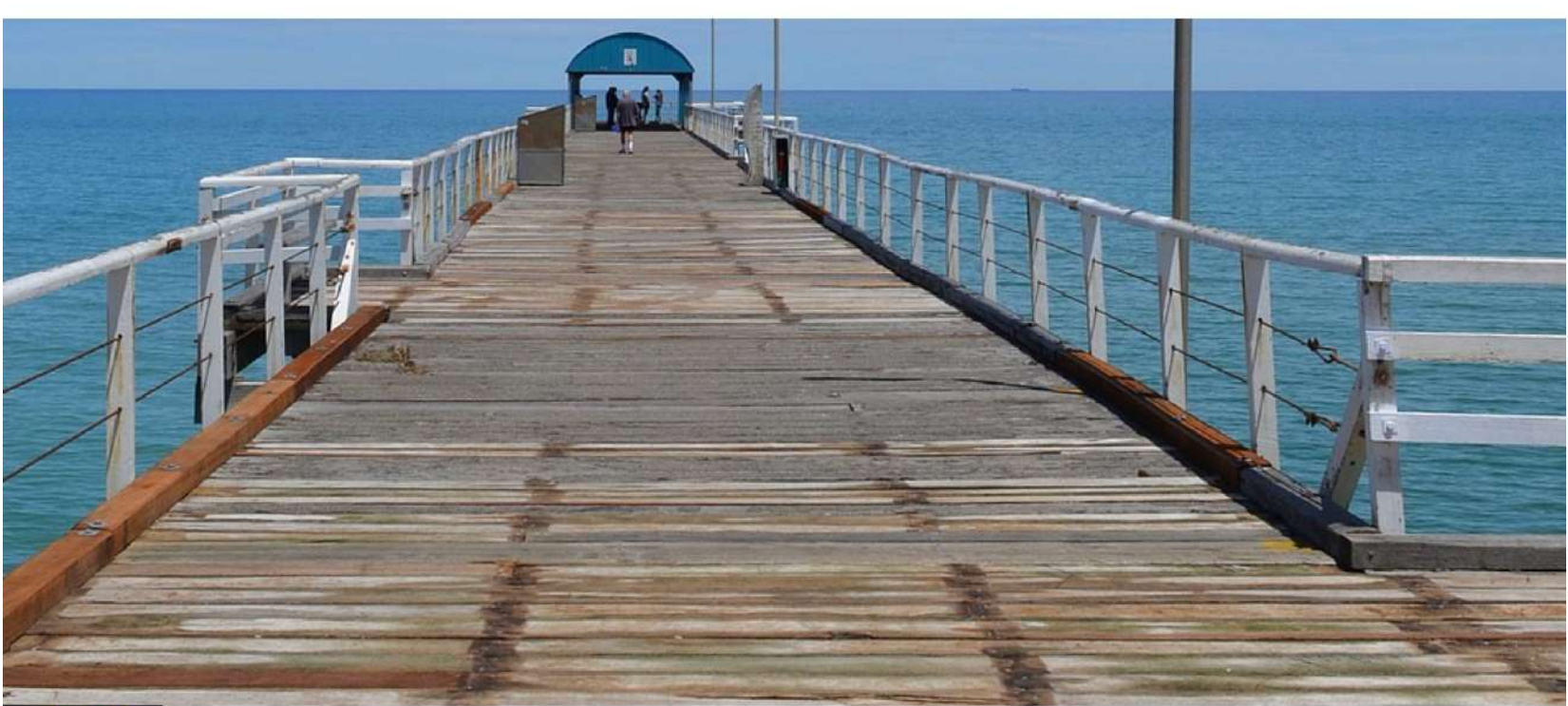
GDPR
SUPRAVEGHEREA VIDEO

GHID ILUSTRAT
pentru societățile specializate în domeniul sistemelor de alarmare împotriva efracției și a celor din domeniul pazei şi protecției



Autor: Ion Iordache
PECB Certified Data Protection Officer

CONȚINUT

INTRODUCERE

Ce înseamnă Regulamentul General privind Protecţia Datelor (GDPR) pentru supravegherea video?

Chiar dacă s-a făcut destul de multă informare, pe toate căile, pe unii apariția Regulamentul eneral privind protecţia datelor (GDPR) în 2018 i-a luat prin surprindere și din păcate și după trei ani de la intrarea sa în vigoare ca obligativitate legală mulți se află tot în zona de surprindere.

Când spun acest lucru mă refer atât la beneficiarii (operatorii) cât și la furnizorii serviciilor de securitate (împuterniciții acestora) adică cei care asigură instalarea și/sau întreținerea sistemelor de supraveghere video.

Observ foartă multă confuzie, derută sau chiar o anumită îndârjire din partea ambelor părți în a susține puncte de vedere care încalcă flagrant cerințele Regulamentului.

Acest lucru este, oarecum de înțeles atâta timp cât circulă o serie de informații care alimentează aceste confuzii.

De exemplu, este amintită și se face referire foarte des la "Decizia preşedintelui Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video".

Decizia nr. 52/2012 a fost abrogată prin DECIZIA nr. 99 din 18 mai 2018 privind încetarea aplicabilităţii unor acte normative cu caracter administrativ emise în aplicarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.

DECIZIA nr. 52/2012
privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video a fost ABROGATĂ

LEGEA nr. 677/2001
pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date a fost ABROGATĂ.

Nici unele autorități, cum ar fi Poliția Română nu ajută mai mult cu informarea corectă asupra protecției datelor cu caracter personal deoarece în modelele de "documente privind activitatea poliției în domeniul sistemelor de securitate private" fac referire la Legea nr. 677/2001 abrogată și aceasta tot în 2018.

Scopul acestui ghid este acela de a crea un instrument de informare atât pentru societăţile specializate în domeniul sistemelor de alarmare împotriva efracţiei şi a celor din domeniul pazei şi protecţiei cât și pentru beneficiarii serviciilor lor.

IMPORTANT! Acest ghid se bazează atât pe cerințele **"Regulamentului (UE) 2016/679** privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor) cât și pe **"Ghidul 3/2019** privind prelucrarea datelor cu caracter personal prin mijloace video" Versiunea 2.0, adoptat la 29 ianuarie 2020 de către Comitetul European pentru Protecția Datelor care oferă, printre altele, mai multe exemple privind asigurarea conformității GDPR cu principiile de prelucrare a datelor și cu drepturile persoanei vizate cu privire la utilizarea dispozitivelor video.

Concluzia principală a acestui ghid este accea că operatorii trebuie să-și revizuiască prelucrarea datelor cu caracter personal prin intermediul dispozitivelor video pentru a se asigura că sunt respectate cerințele GDPR iar societăţile specializate în domeniul sistemelor de alarmare împotriva efracţiei și a celor din domeniul pazei şi protecţiei să-și ia în serios rolurile lor de împuterniciți ai clienților lor (operatorii de date cu caracter personal).

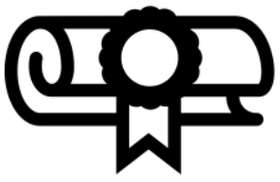
AUTORUL

Ion Iordache
PECB Certified Data Protection Officer

Numele meu este **Ion Iordache** și sunt Data Protection Officer (DPO) și Training & Development Manager la RQM Cert, CEO și fondator la Iordache Quality Services, companii care oferă servicii de consultanță și cursuri de formare în managementul securității, GDPR și sisteme de management bazate pe standardele internaționale ISO.

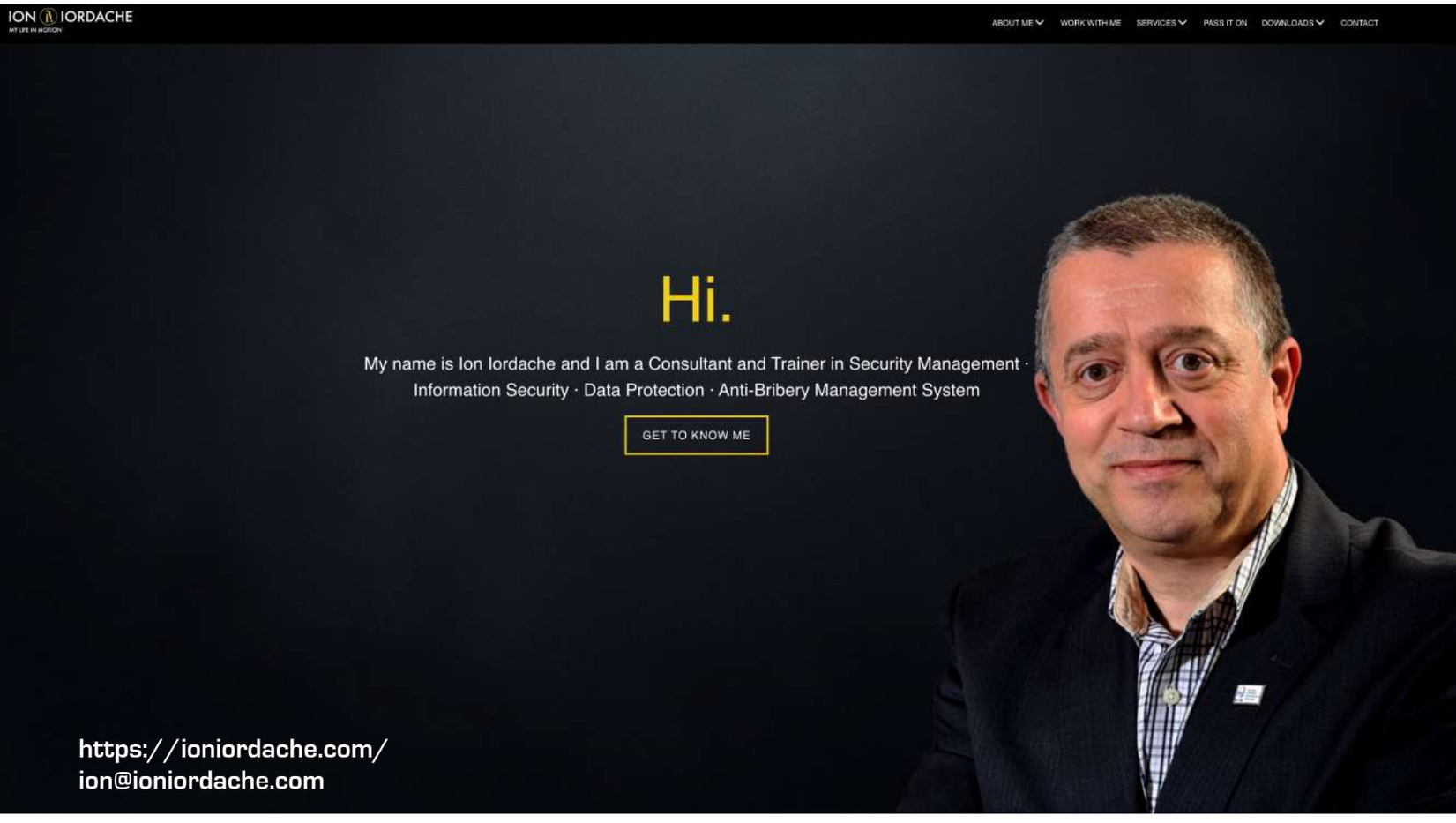
În ultimii 20 de ani am coordonat și/sau livrat in mod direct consultanță și formare profesionala pentru mai mult de 18.000 de persoane în România și Australia.

Sunt inițiatorul și autorul standardului ocupațional "Consultant de securitate" cu codul COR 242113, am creat metodologia "Security Management Solutions" care este o alternativă la modelul tradițional de management al securității ce oferă o soluție eficientă la asigurarea securității persoanelor, bunurilor și informațiilor și metodologia "iQS GDPR Approach" de implementare a cerințelor GDPR.



Dețin o serie de certificări internaționale bazate pe cunoștiințe și experiență practică:

- PECB Certified Trainer
- PECB Certified Data Protection Officer (DPO)
- PECB Certified ISO/IEC 27001 Lead Implementer
- PECB Certified ISO/IEC 27001 Lead Auditor
- PECB Certified ISO 37001 Lead Implementer
- PECB Certified ISO 28000 Lead Implementer
- PECB Certified ISO 9001 Lead Auditor



GDPR
REGULAMENTUL GENERAL PRIVIND PROTECTIA DATELOR

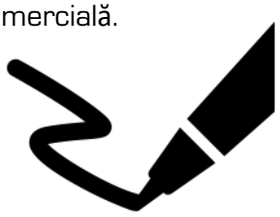
Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE.

Parlamentul European și Consiliul au adoptat, în data de 27 aprilie 2016, Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulaţie a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor - GDPR) prevederile lui fiind direct aplicabile în toate statele membre ale Uniunii Europene, începând cu data de 25 mai 2018.

GDPR se aplică prelucrării datelor cu caracter personal, efectuată total sau parţial prin mijloace automatizate, precum şi prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă a datelor sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor.

GDPR nu se aplică prelucrării datelor cu caracter personal efectuate de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice.

În considerentul 18 din GDPR se precizează că activităţile personale sau domestice nu ar trebui să aibă legătură cu activtatea profesională sau comercială.



Activităţile personale sau domestice pot include corespondenţa şi repertoriul de adrese sau activităţile din cadrul reţelelor sociale şi activităţile online desfăşurate în contextul respectivelor activităţi.

DATELE CU CARACTER PERSONAL

Datele cu caracter personal includ orice informații despre o persoană identificată sau identificabilă (subiectul datelor).

Printre datele cu caracter personal se numără:

- numele
- adresa
- numărul cărții de identitate/pașaportului
- venitul
- profilul cultural
- adresa IP (Internet Protocol)
- înregistrarile video deținute de o companie (care identifică o persoană în scopuri de control acces)

GDPR SE APLICĂ:

Prelucrării datelor cu caracter personal în cadrul activităţilor derulate la sediul unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.

Prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activităţile de prelucrare sunt legate de:

- oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăţi de către persoana vizată; sau
- monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.

Prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internaţional public.

DEFINIȚII

2) **"prelucrare"** înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

(3) **"restricționarea prelucrării"** înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora.

(7) **"operator"** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern.

(8) **"persoană împuternicită de operator"** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

(1) **"date cu caracter personal"** înseamnă orice informații privind o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică 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 număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

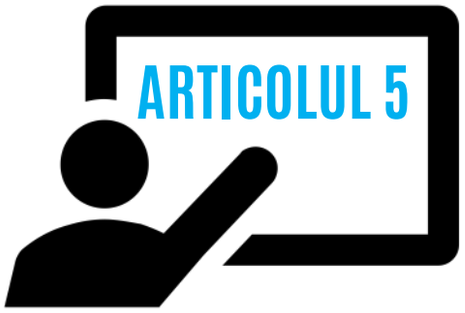
(9) **"destinatar"** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță;

(10) **"parte terță"** înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal

(11) **"consimțământ"** al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.

(12) **"încălcarea securității datelor cu caracter personal"** înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.

PRINCIPIILE GDPR
și supravegherea video



Supravegherea video nu este reglementată în mod expres de GDPR deși aceasta este un dintre cele mai utilizate metode de colectare și procesare a datelor cu caracter personal. Există însă prevederi punctuale în LEGEA nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 la Art.5: Prelucrarea datelor cu caracter personal în contextul relaţiilor de muncă.

Utilizarea pe scară largă a supravegherii video influențează comportamentul cetățenilor iar implicațiile pentru protecția datelor sunt uriașe deoarece în prezent se utilizează numeroase instrumente pentru exploatarea imaginilor captate și transformarea camerelor tradiționale în camere inteligente.

Riscurile legate de păstrarea confidențialității sau chiar de utilizare abuzivă sunt mai mari ca oricând; de acea ori de câte ori se utilizează supravegherea video, trebuie luate, foarte atent, în considerare **"Principiile generale"** prevăzute în Art.5 al GDPR.

1 Legalitate, echitate şi transparenţă
datele cu caracter personal sunt prelucrate în mod legal, echitabil și transparent față de persoana vizată.

2 Limitări legate de scop
datele cu caracter personal sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri.

3 Reducerea la minimum a datelor
datele cu caracter personal sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate.

4 Exactitatea informațiilor
datele cu caracter personal sunt exacte și, în cazul în care este necesar, actualizate.

5 Limitarea stocării
datele cu caracter personal sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele.

6 Integritate și confidențialitate
datele cu caracter personal sunt prelucrate într-un mod care le asigură securitatea adecvată, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

DEROGAREA privind activitățile domestice

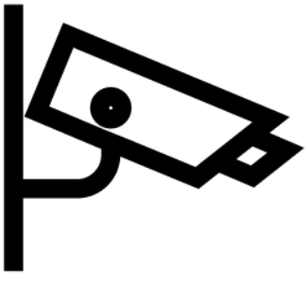
Prevederile GDPR nu se aplică prelucrării datelor cu caracter personal de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice și care, prin urmare, nu are legătură cu o activitate profesională sau comercială. (Art.2, al.(2), litera (c).

Activitățile personale sau domestice ar putea include corespondența și repertoriul de adrese sau activitățile din cadrul rețelelor sociale și activitățile online desfășurate în contextul respectivelor activități.

Cu toate acestea, prevederile GDPR se aplică operatorilor sau persoanelor împuternicite de operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activități personale sau domestice *(ex. **societatea care instalează sistemul de supraveghere video și/sau asigură mentenanța acestuia**).*

Potrivit Curții de Justiție a Uniunii Europene, așa-numita „derogare privind activitățile domestice” trebuie „interpretată ca referindu-se doar la activitățile care se desfășoară în cadrul vieții private sau de familie a persoanelor, ceea ce în mod evident nu este cazul prelucrării de date cu caracter personal care constă în publicarea pe internet, astfel încât aceste date să devină accesibile unui număr nedeterminat de persoane”.

Dacă un sistem de supraveghere video, în măsura în care implică înregistrarea continuă și stocarea de date cu caracter personal și acoperă, „chiar și parțial, un spațiu public și este, ca atare, direcționat spre exterior din cadrul privat al persoanei care prelucrează datele în acest mod, aceasta nu poate fi considerată o activitate exclusiv personală sau domestică" *(Curtea de Justiție a Uniunii Europene, Hotărârea în cauza C-212/13)*



Exemplu: Cineva își monitorizează și înregistrează activitățile din grădina proprie.

Proprietatea este împrejmuită și numai operatorul și familia sa intră în grădină în mod regulat.

Aceasta ar intra sub incidența derogării privind activitățile domestice, cu condiția ca supravegherea video să nu se extindă nici măcar parțial la un spațiu public sau la o proprietate învecinată.

LEGALITATEA prelucrării

Operatorul trebuie să specifice [Art. 5, al.(1) litera (b)] și să documenteze în scris [Art. 5, al.(2)], în detaliu, scopurile prelucrării prin sistemul de supraveghere video, scopuri care ar putea fi, de exemplu, asigurarea protejării proprietății și a altor bunuri și/sau asigurarea protejării vieții și a integrității fizice a persoanelor.

Atenție! scopurile monitorizării trebuie specificate pentru fiecare cameră de supraveghere care se utilizează (camerele care sunt utilizate în același scop de un singur operator pot fi documentate împreună).

Persoanele vizate trebuie să fie informate cu privire la scopul (scopurile) prelucrării în conformitate cu articolul 13 (secțiunea 7 - Obligații privind transparența și informarea).

NOTĂ: supravegherea video având ca scop doar „siguranța" sau „pentru siguranța dumneavoastră" nu este suficient de specifică [Art.5 alineatul (1) litera (b)].

În plus, acest lucru contravine principiului potrivit căruia datele cu caracter personal trebuie prelucrate în mod legal, echitabil și transparent în raport cu persoana vizată [Art.5 alineatul (1) litera (a)].

Existența intereselor legitime

Supravegherea video este legală dacă este necesară pentru a îndeplini scopul unui interes legitim urmărit de un operator sau de o parte terță, cu excepția cazului în care interesele sau drepturile și libertățile fundamentale ale persoanei vizate prevalează asupra acestor interese [Art.6 al.(1) litera (f)]. Interesele legitime urmărite de un operator sau de o parte terță pot fi interese juridice, economice sau morale.

De exemplu, în cazul unei situații reale și periculoase, scopul protejării proprietății împotriva spargerii, furtului sau vandalismului poate constitui un interes legitim pentru supravegherea video.

Având în vedere principiul răspunderii, ar fi indicat ca operatorii să documenteze incidentele relevante (data, modalitatea, pierderea financiară) și acuzațiile de natură penală aferente. Aceste incidente documentate pot fi o dovadă solidă a existenței unui interes legitim.

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.

[Sursa: Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video]

Conform principiului "**Reducerea la minimum a datelor**", datele cu caracter personal trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate.

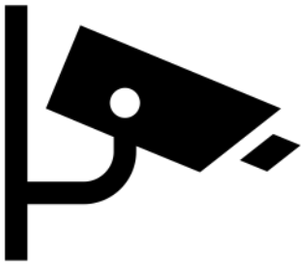
Exemplu: O librărie dorește să-și protejeze sediul împotriva vandalismului. În general, camerele trebuie să filmeze doar spațiul respectiv deoarece nu este necesară supravegherea spațiilor învecinate sau a zonelor publice din împrejurimile sediului librăriei în acest scop.

[Sursa: Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video]

În principiu, oricare dintre temeiurile juridice prevăzute la Art.6 - "Legalitatea prelucrării" alineatul (1) poate constitui un temei juridic pentru prelucrarea datelor provenite din supravegherea video.

De exemplu, Art.6 alineatul (1) litera (c) se aplică în situațiile în care legislația națională prevede obligația de a efectua supraveghere video. [Obligații derivate din HG 301 din 2012, Anexa 1 - Cerinţe minimale de securitate, pe zone funcţionale şi categorii de unităţi].

LEGALITATEA prelucrării



În general, necesitatea utilizării supravegherii video pentru protejarea spațiilor operatorului nu depășește limitele proprietății dar pot exista cazuri în care supravegherea proprietății nu este suficientă pentru o protecție eficientă. În acest context, operatorul trebuie să ia în considerare mijloace fizice și tehnice, de exemplu blocarea sau pixelarea zonelor nerelevante.

Asigurarea unui echilibru între interese și evaluarea comparativă a intereselor este obligatorie în conformitate cu GDPR, decizia trebuie luată de la caz la caz [Art.6 alineatul (1) litera (f)] iar drepturile și libertățile fundamentale, pe de o parte, și interesele legitime ale operatorului, pe de alta, trebuie evaluate și comparate cu atenție.

Exemplu: O firmă de parcare privată a documentat problemele recurente constând în furturi din mașinile parcate. Zona de parcare este un spațiu deschis și poate fi accesată cu ușurință de oricine, dar este semnalizată în mod clar cu indicatoare și blocante rutiere care delimitează spațiul. Firma de parcare are un interes legitim (prevenirea furturilor din mașinile clienților) de monitorizare a zonei în intervalul din zi în care se confruntă cu probleme. Persoanele vizate sunt monitorizate într-un interval de timp limitat, nu se află în zonă în scop recreativ și, de asemenea, este în interesul lor ca furturile să fie prevenite. În acest caz, interesul legitim al operatorului prevalează asupra interesului persoanelor vizate de a nu fi monitorizate.

(Sursa: Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video)

AȘTEPTĂRILE REZONABILE ALE PERSOANELOR VIZATE

Potrivit GDPR. Considerentului 47, existența unui interes legitim necesită o evaluare atentă.

Aici trebuie incluse așteptările rezonabile ale persoanei vizate din momentul și în contextul prelucrării datelor sale cu caracter personal.

Semnele care informează persoana vizată cu privire la supravegherea video nu au nicio relevanță atunci când se stabilește la ce se poate aștepta în mod obiectiv o persoană vizată.

Aceasta înseamnă că, de exemplu, proprietarul unui magazin nu poate miza pe așteptarea rezonabilă pe care clienții ar avea-o în mod obiectiv de a fi monitorizați doar pentru că există un semn la intrare care îi informează cu privire la supraveghere.

Consimțământul, Art.6 alineatul (1) litera (a). Consimțământul trebuie să fie acordat în mod liber, specific, în cunoștință de cauză și lipsit de ambiguitate.

În ceea ce privește monitorizarea sistematică, consimțământul persoanei vizate nu poate servi ca temei juridic în conformitate cu Art.7 (considerentul 43) decât în cazuri excepționale.

Având în vedere dezechilibrul de putere dintre angajatori și angajați, în majoritatea cazurilor, angajatorii nu trebuie să se bazeze pe consimțământ atunci când prelucrează date cu caracter personal, deoarece este puțin probabil ca acesta să fie acordat în mod liber.

DIVULGAREA

înregistrărilor video către părți terțe

În principiu, în cazul divulgării înregistrărilor video către părți terțe se aplică reglementările generale ale GDPR.

Divulgarea este definită la Art.4 alineatul (2) ca transmitere (de exemplu, comunicare individuală), diseminare (de exemplu, publicare online) sau punere la dispoziție în orice alt mod. Părțile terțe sunt definite la Art.4 alineatul (10). Orice divulgare a datelor cu caracter personal este un mod separat de prelucrare a datelor cu caracter personal pentru care operatorul trebuie să aibă un temei juridic prevăzut la Art.6.

Conform Art.6 alineatul (1) litera (c), prelucrarea este legală dacă este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului.

Deși legislația aplicabilă poliției se află sub controlul exclusiv al statelor membre, cel mai probabil există norme generale care reglementează transferul probelor către autoritățile de aplicare a legii în fiecare stat membru.

Prelucrarea constând în transmiterea datelor de către operator este reglementată de GDPR.

Dacă legislația națională impune operatorului să coopereze cu autoritățile de aplicare a legii (de exemplu, în cadrul unei anchete), temeiul juridic pentru transmiterea datelor este obligația legală prevăzută la Art.6 alineatul (1) litera (c).

Exemplu: *(Un operator care dorește să încarce o înregistrare pe internet trebuie să se bazeze pe un temei juridic pentru prelucrarea respectivă, de exemplu, obținând consimțământul persoanei vizate în conformitate cu Art.6 alineatul (1) litera (a).*

Sursa: Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video)

Transmiterea înregistrărilor video către părți terțe în alt scop decât cel pentru care au fost culese datele este posibilă în conformitate cu normele prevăzute la Art.6 alineatul (4).

Divulgarea înregistrărilor video către autoritățile de aplicare a legii

În HG 301 din 2012 este prevăzut la Art.67 alineatul (4) că **"Beneficiarul subsistemului de televiziune cu circuit închis are obligaţia punerii la dispoziţia organelor judiciare, la solicitarea scrisă a acestora, a înregistrărilor video şi/sau audio în care este surprinsă săvârşirea unor fapte de natură penală."**

(Nerespectarea acestei obligații constituie contravenție și se sancționează cu amendă de la 5.000 la 10.000 lei)

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 Art.6 alineatul (1) litera (c) (obligația legală) interpretat în coroborare cu dreptul intern relevant pentru prelucrarea prin transfer.

(Sursa: Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video)

Exemplu: *Supravegherea video a unei bariere (la o parcare) este instalată în scopul soluționării daunelor. Înregistrarea este publicată online, exclusiv pentru amuzement. În acest caz, scopul s-a schimbat și nu este compatibil cu scopul* inițial.

Sursa: Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video)

PRELUCRAREA de categorii speciale de date

Sistemele de supraveghere video colectează de obicei cantități masive de date cu caracter personal, care pot dezvălui informații extrem de personale și chiar categorii speciale de date.

Cu toate acestea, supravegherea video nu este întotdeauna considerată prelucrare de categorii speciale de date cu caracter personal.

Exemplu: *Înregistrările video în care se vede o persoană vizată purtând ochelari sau utilizând un fotoliu rulant nu sunt considerate în sine categorii speciale de date cu caracter personal.*

Dacă un sistem de supraveghere video este utilizat pentru a prelucra categorii speciale de date, operatorul de date trebuie să identifice atât o excepție pentru prelucrarea categoriilor speciale de date în baza articolului 9 (adică o excepție de la regula generală conform căreia nu trebuie prelucrate categoriile speciale de date), cât și un temei juridic în conformitate cu articolul 6.

EXEMPLU

Art.9 al.(2) litera(c)

(„[...] prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice [...]") ar putea, în mod teoretic și excepțional, să fie utilizat, dar operatorul de date ar trebui să justifice prelucrarea prin necesitatea absolută de a proteja interesele vitale ale unei persoane și să demonstreze că această „[...] persoană vizată se află în incapacitate fizică sau juridică de a-și da consimțământul".

În plus, operatorul de date nu va avea permisiunea să folosească sistemul pentru orice alt motiv.

În general, ca principiu, de fiecare dată când se instalează un sistem de supraveghere video trebuie să ia în considerare principiul reducerii la minimum a datelor.

EXEMPLU:

Prin urmare, chiar și în cazurile în care nu se aplică Art.9 al.(1), operatorul de date trebuie să încerce întotdeauna să reducă la minimum riscul de a capta imagini care dezvăluie alte date cu caracter special indiferent de scop.

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 Art.6 al.(1) litera (f), ținând seama de natura datelor, precum și de riscul de înregistrare a altor date cu caracter special (dincolo de sfera Art.9) atunci când sunt evaluate interesele persoanei vizate.

Pentru prelucrarea categoriilor speciale de date este necesară o vigilență sporită și permanentă față de anumite obligații; de exemplu, un nivel ridicat de securitate și o evaluare a impactului asupra protecției datelor, dacă este necesar (un angajator nu poate să folosească înregistrări ale supravegherii video care prezintă o demonstrație cu scopul de a identifica greviștii.)

LEGEA nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679

CAPITOLUL II: Reguli speciale privind prelucrarea unor categorii de date cu caracter personal

Art. 3: Prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea

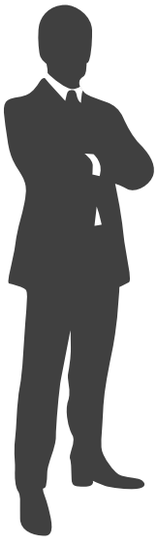
(1) Prelucrarea datelor genetice, biometrice sau a datelor privind sănătatea, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri, este permisă cu consimţământul explicit al persoanei vizate sau dacă prelucrarea este efectuată în temeiul unor dispoziţii legale exprese, cu instituirea unor măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate.

PRELUCRAREA de categorii speciale de date
considerații generale la prelucrarea datelor biometrice

GDPR-ul ne spune că **"datele biometrice"** înseamnă date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice." *(GDPR, Art.4, al.14)*

Chiar dacă utilizarea datelor biometrice și, în special, recunoașterea facială pot fi percepute ca deosebit de eficiente, acestea implică riscuri crescute pentru drepturile persoanelor vizate iar acest lucru impune operatorilor să evalueze, în primul rând, impactul asupra drepturilor și libertăților fundamentale și să ia în considerare mijloace mai puțin invazive pentru a-și atinge scopul legitim al prelucrării.

Criterii de luat în considerare



Natura datelor

date referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice

Mijloacele și modul de prelucrare

date care „rezultă în urma unor tehnici de prelucrare specifice"

Scopul prelucrării

datele trebuie să fie utilizate pentru identificarea unică a unei persoane fizice

Pentru a se încadra ca "date" biometrice așa cum sunt definite în GDPR, prelucrarea datelor brute, cum ar fi caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, trebuie să implice măsurarea acestor caracteristici.

ATENȚIE! Înregistrările video ale unei persoane nu pot fi considerate în sine date biometrice în conformitate cu Art.9 dacă nu au fost prelucrate prin tehnici specifice pentru a contribui la identificarea unei persoane.

Pentru a putea fi considerată prelucrare de categorii speciale de date cu caracter personal, datele biometrice trebuie să fie prelucrate „pentru identificarea unică a unei persoane fizice".

Utilizarea supravegherii video, inclusiv funcționalitatea de recunoaștere biometrică instalată de către entități private în scopuri proprii (de exemplu, marketing, statistică sau chiar securitate) va necesita, în cele mai multe cazuri, consimțământul explicit din partea tuturor persoanelor vizate [Art.9 al.(2) litera(a)].

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 Art.9 al.(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.*

DREPTURILE PERSOANELOR VIZATE

Având în vedere caracterul prelucrării datelor toate drepturile prevăzute în GDPR se aplică prelucrării datelor cu caracter personal prin supraveghere video.

La Capitolul III din GDPR sunt reglementate drepturle persoanelor vizate.
În pagina următoare voi prezenta mai pe larg trei dintre acestea, cele pe care pune accent și Ghidul 3/2019.

Dreptul la informare (art. 13 și art. 14)
Acest drept se referă exclusiv la persoana vizată și se realizează prin obligațiile operatorului de a informa persoana vizată despre ce se întâmplă cu date sale personale, de ce si cum i le prelucrează, pentru ce perioadă de timp și dacă le dă uni terțe părți.

Dreptul de acces (art.15)
Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu, date cu caracter personal care o privesc.

Dreptul la rectificare (art.16)
Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc.

Dreptul la ștergere („dreptul de a fi uitat” – art.17)
Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate.

Dreptul la restricționarea prelucrării (art.18)
Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării.

Dreptul la portabilitatea datelor (art.20)
Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat.

Dreptul la opoziție (art.21)
În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situația particulară în care se află, prelucrării datelor cu caracter personal care o privesc.

Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată (art.22)
Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri.

Dreptul de a depune o plângere la o autoritate de supraveghere (art.77)
Orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere.

DREPTURILE PERSOANELOR VIZATE

Având în vedere caracterul prelucrării datelor toate drepturile prevăzute în GDPR se aplică prelucrării datelor cu caracter personal prin supraveghere video.

Dreptul de acces

În cazul supravegherii video, faptul că o persoană vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal înseamnă că, dacă datele nu sunt stocate sau transferate în niciun fel, după ce a trecut momentul monitorizării în timp real, operatorul nu poate să furnizeze decât informația că nu mai sunt prelucrate date cu caracter personal.

Dacă însă la momentul solicitării încă se prelucrează date (adică dacă datele sunt stocate sau prelucrate în continuare în orice alt mod), persoana vizată trebuie să primească acces și să fie informată în conformitate cu Art.15.

Dacă operatorul poate demonstra că nu este în măsură să identifice persoana vizată, trebuie să informeze persoana respectivă în consecință, dacă este posibil. În această situație, în răspunsul său către persoana vizată, operatorul trebuie să furnizeze informații cu privire la zona exactă a monitorizării, verificarea camerelor care erau în funcțiune etc., pentru ca persoana vizată să înțeleagă pe deplin ce date personale este posibil să fi fost prelucrate.

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.

Dreptul la ștergerea datelor

La cerere, operatorul este obligat să șteargă datele cu caracter personal fără întârzieri nejustificate dacă se aplică una dintre circumstanțele enumerate la Art.17 alineatul (1) din GDPR [și dacă nu se aplică niciuna din excepțiile enumerate la Art.17 alineatul (3) din GDPR]. În acest caz este inclusă obligația de a șterge datele cu caracter personal când nu mai sunt necesare pentru îndeplinirea scopului pentru care au fost stocate inițial sau când prelucrarea este ilegală (vezi și Secțiunea 8 – Perioadele de stocare și obligația de ștergere a datelor).

Pe lângă obligația de a șterge datele cu caracter personal la solicitarea persoanei vizate, operatorul este obligat să limiteze datele cu caracter personal stocate, în conformitate cu principiile generale ale GDPR.

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.

Dreptul la opoziție

În cazul supravegherii video bazate pe interesul legitim sau pe necesitatea de a îndeplini o sarcină care servește unui interes public, persoana vizată are dreptul, în orice moment, să se opună prelucrării, din motive legate de situația sa particulară, în conformitate cu articolul 21 din GDPR.

Cu excepția cazului în care operatorul demonstrează motive legitime imperioase care prevalează asupra drepturilor și intereselor persoanei vizate, prelucrarea datelor persoanei care s-a opus trebuie să înceteze. Operatorul trebuie să fie obligat să răspundă cererilor persoanei vizate fără întârzieri nejustificate și în termen de cel mult o lună.
În contextul supravegherii video, această opoziție ar putea fi formulată la intrarea, în timpul petrecut în interior sau la părăsirea zonei monitorizate. În practică, acest lucru înseamnă că, exceptând cazul în care operatorul are motive legitime imperioase, monitorizarea unei zone în care persoanele fizice ar putea fi identificate este legală numai dacă:

1. operatorul este capabil să oprească imediat camera de la prelucrarea datelor cu caracter personal la cerere, sau
2. zona monitorizată este restricționată în detaliu, astfel încât operatorul poate asigura aprobarea persoanei vizate înainte de a intra în zonă și nu este o zonă la care persoana vizată ca cetățean are drept de acces.

Atunci când se utilizează supravegherea video în scopul marketingului direct, persoana vizată are dreptul să se opună prelucrării în mod discreționar, întrucât dreptul de opoziție este absolut în acest context.

OBLIGAȚII
PRIVIND TRANSPARENȚA ȘI INFORMAREA

Potrivit GDPR, obligațiile generale privind transparența și informarea sunt stabilite la Art.12 "Transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate".

Informații din primul nivel (mesajul de avertizare)
Exemplu:

Având în vedere volumul informațiilor care trebuie furnizate persoanei vizate, operatorii de date pot adopta o abordare pe mai multe niveluri atunci când optează pentru utilizarea unei combinații de metode pentru asigurarea transparenței.
În ceea ce privește supravegherea video, cele mai importante informații trebuie afișate pe semnul de avertizare (**primul nivel**), în timp ce alte detalii obligatorii pot fi furnizate prin alte mijloace (**al doilea nivel**).

Poziționarea mesajului de avertizare
Informațiile trebuie poziționate astfel încât persoana vizată să poată recunoaște cu ușurință circumstanțele supravegherii înainte de a intra în zona monitorizată (aproximativ la nivelul ochilor). Nu este necesar să se divulge poziția camerei, atâta timp cât nu există niciun dubiu asupra zonelor supuse monitorizării, iar contextul supravegherii este clarificat fără ambiguitate.Persoana vizată trebuie să poată estima zona captată de o cameră de luat vederi, ca să poată evita supravegherea sau să-și adapteze comportamentul, dacă este necesar.

Informațiile din cel de-al doilea nivel trebuie furnizate persoanei vizate într-un loc ușor accesibil, de exemplu sub forma unei fișe cu informații complete disponibilă într-un loc central (de exemplu, birou de informații, recepție sau casierie) sau afișate pe un panou ușor accesibil.
Informațiile din cel de-al doilea nivel trebuie să poată fi accesate fără a intra în zona supravegheată, în special dacă informațiile sunt furnizate digital (acest lucru se poate realiza, de exemplu, printr-un link). Indiferent de modul în care sunt furnizate, informațiile trebuie să conțină tot ce este obligatoriu în conformitate cu **Art.13 "Informații care se furnizează în cazul în care datele cu caracter personal sunt colectate de la persoana vizată"** din GDPR.

Exemplu: Proprietarul unui magazin își monitorizează magazinul. Pentru a respecta Art.13 este suficient să amplaseze un mesaj de avertizare, care să conțină informațiile din primul nivel, într-un punct ușor vizibil la intrarea în magazin.
În plus, trebuie să afișeze o fișă cu informații care să conțină informațiile din al doilea nivel la casierie sau în alt loc central și ușor accesibil din magazin.

PERIOADELE
DE STOCARE ȘI OBLIGAȚIA DE ȘTERGERE

Datele cu caracter personal nu pot fi stocate pe o perioadă care depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate [Art.5 al.(1) literele (c) și (e) din GDPR].

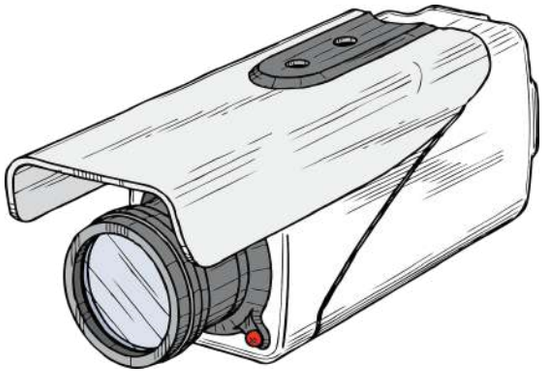
În România există dispoziții specifice pentru perioadele de stocare cu privire la supravegherea video în conformitate cu Art.6 al.(2) din GDPR.

HOTĂRÂREA nr. 301 din 2012

Echipamentele de televiziune cu circuit închis trebuie să asigure preluarea de imagini din zona de acces, atât din exterior, cât şi din interior, zona de lucru cu publicul, traseele de vehiculare şi acces în spaţiul de depozitare a valorilor, asigurând stocarea imaginilor pe o perioadă de **20 de zile**.

LEGEA nr. 190 din 2018

Durata de stocare a datelor cu caracter personal este proporţională cu scopul prelucrării, dar nu mai mare de **30 de zile**, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate.



Pentru a facilita demonstrarea conformității cu cadrul de protecție a datelor, este în interesul operatorului să facă aranjamente organizatorice în prealabil (de exemplu, să desemneze, dacă este necesar, un reprezentant pentru vizualizarea și securizarea materialului video).

Având în vedere principiile prevăzute la Art.5 al.(1) literele(c) și (e) din GDPR, și anume reducerea la minimum a datelor și limitările legate de stocare, datele cu caracter personal trebuie șterse în mod ideal automat, după perioada impusă de legislația incidentă domeniului sistemelor de securitate private din România, în majoritatea cazurilor (de exemplu, în scopul depistării actelor de vandalism).

Exemplu: Proprietarul unui magazin mic ar observa, în mod normal, un act de vandalism în aceeași zi în care a avut loc. În consecință, ar fi suficientă o perioadă de stocare obișnuită de 24 de ore dar legislația incidentă domeniului sistemelor de securitate private din România impune stocarea imaginilor pe o perioadă de 20 de zile. Dacă se constată o pagubă, poate fi necesar să se păstreze înregistrările video pentru o perioadă mai lungă pentru a se lua măsuri legale împotriva infractorului.

GDPR prevede că datele vor fi păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele

Trebuie verificat într-un interval scurt dacă este necesar ca datele cu caracter personal să fie stocate. În general, scopurile legitime pentru supravegherea video sunt adesea protejarea proprietății sau păstrarea dovezilor.

Perioada ar trebui să țină seama de motivele pentru care operatorul trebuie să prelucreze datele, precum și de eventuale obligații juridice de a păstra datele o perioadă fixă de timp (de exemplu, legile privind ocuparea forței de muncă, legile fiscale sau legile antifraudă naționale care vă impun păstrarea datelor cu caracter personal despre angajații dvs. pentru o perioadă determinată, durata garanției produselor etc.).

Societatea/organizația ar trebui să stabilească termene pentru ștergerea sau revizuirea datelor stocate.

Ca excepție, datele cu caracter personal pot fi păstrate o perioadă mai îndelungată în scopuri de arhivare în interes public ori în scopuri de cercetare științifică sau istorică, cu condiția să fie puse în aplicare măsuri de ordin tehnic și organizatoric adecvate (precum anonimizare, criptare etc.).

De asemenea, societatea/organizația dvs. trebuie să se asigure că datele pe care le deține sunt exacte și să le actualizeze.

Operatorului i se conferă posibilitatea de a avea diferite termene de stocare a datelor, în funcție de scopul/scopurile prelucrării și pe durata necesară realizării lor, fie prin stabilirea din proprie inițiativă a unei durate maxime de păstrare, cu respectarea principiului proporționalității, fie prin respectarea unor termene prevăzute în diferite acte normative specifice.

CERINȚE legale în România privind supravegherea video

LEGISLAȚIA INCIDENTĂ DOMENIULUI SISTEMELOR DE SECURITATE PRIVATĂ

În România, activitățile de proiectare, instalare, modificare sau întreţinere a componentelor sau sistemelor de supraveghere video intră sub incidența legislației speciale, respectiv a **LEGII nr. 333 din 8 iulie 2003** (republicată și actualizată în 2015) privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor unde, la Art.4 se precizează că **"răspunderea pentru luarea măsurilor de asigurare a pazei bunurilor şi valorilor deţinute cu orice titlu revine conducătorilor unităţilor".**

Activitățile de proiectare, instalare, modificare sau întreţinere a componentelor sau sistemelor de supraveghere video se efectueză doar de către societăți licențiate de Inspectoratului General al Poliţiei Române ce au personal calificat și avizat.

IMPORTANT! În Legea 333 la ART. 32 al.(1) se precizează foarte clar că **"societăţilor specializate în domeniul sistemelor de alarmare le sunt interzise culegerea de informaţii, înregistrările audio sau video care excedează obiectului de activitate pentru care li s-a acordat licenţă, precum şi instalarea de echipamente disimulate care să le permită executarea acestor activităţi".**

Prevederi specifice sistemelor video de supraveghere găsim în **HOTĂRÂREA nr. 301 din 11 aprilie 2012(actualizată) pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003** unde găsim o serie de cerințe obligatorii pentru beneficiari de dotare cu sisteme de supraveghere video a diferitelor categorii de unități de asigurare a întreținerilor periodice a acestora, obligativitatea societăților licențiate de a utiliza ca elemente componente în sistemele de supraveghere video doar echipamente fabricate conform standardelor europene şi certificate de laboratoare acreditate într-un stat membru al Uniunii Europene sau al Spaţiului Economic European dar și precizarea că:

Echipamentele de televiziune cu circuit închis trebuie să asigure preluarea de imagini din zona de acces, atât din exterior, cât şi din interior, zona de lucru cu publicul, traseele de vehiculare şi acces în spaţiul de depozitare a valorilor, asigurând stocarea imaginilor pe o perioadă de 20 de zile.

LEGEA nr. 190 din 18 iulie 2018

privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor).

La Art.5 găsim cerințe punctuale unde "**prelucrarea datelor cu caracter personal în contextul relaţiilor de muncă în cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicaţii electronice şi/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaţilor, în scopul realizării intereselor legitime urmărite de angajator**" este permisă numai dacă:

a) interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate;

b) angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaţilor;

c) angajatorul a consultat sindicatul sau, după caz, reprezentanţii angajaţilor înainte de introducerea sistemelor de monitorizare;

d) alte forme şi modalităţi mai puţin intruzive pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficienţa; şi

e) durata de stocare a datelor cu caracter personal este proporţională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate.

INSTALAREA unui sistem de supraveghere video de către asociația de proprietari

Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (A.N.S.P.D.C.P) a dat publicității următoarele::

Prin prisma rolului pe care îl îndeplinesc și a atribuțiilor legale, asociațiile de proprietari au calitatea de operatori de date cu caracter personal și, în consecință, obligația de a respecta dispozițiile Regulamentului (UE) 679/2016 – Regulamentul general privind protecția datelor (RGPD). Astfel, în contextul prelucrării (inclusiv al dezvăluirii) datelor personale, asociațiile de proprietari trebuie să identifice temeiul legal al efectuării acesteia, prevăzut de dispozițiile RGPD prin raportare la prevederile legale din domeniul lor de activitate.

Scopul și mijloacele prelucrării datelor de către asociațiile de proprietari pot fi în mod expres stabilite prin actele normative care le reglementează înființarea, organizarea și funcționarea sau pot fi stabilite de către asociație, fiind justificate de interesul legitim al său. De asemenea, în unele situații, prelucrările de date se pot baza pe consimțământul persoanelor fizice vizate.

În ceea ce privește instalarea unui sistem de supraveghere video de către asociația de proprietari, întrucât sistemele de televiziune cu circuit închis au posibilitatea de înregistrare şi stocare a imaginilor şi datelor, această activitate se supune atât prevederilor Regulamentului (UE) 679/2016, cât şi ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, modificată şi completată și Normelor metodologice de aplicare a acesteia, mai ales raportat la instalarea şi utilizarea sub aspect tehnic a echipamentelor şi elementelor componente ale sistemului de supraveghere video.

Măsura instalării unui sistem de supraveghere video poate fi luată de către asociația de proprietari în baza interesului legitim al asociaţiei, de ex. pentru asigurarea pazei şi protecției persoanelor, bunurilor și valorilor, a imobilelor și a instalațiilor de utilitate publică, precum și a împrejmuirilor afectate acestora, dar și în zona de acces în imobil sau lifturi.

Argumentele privind justificarea interesului legitim trebuie să se regăsească într-o documentație la nivelul asociației de proprietari și, ulterior, hotărârea de a instala un astfel de sistem trebuie adoptată în cadrul adunării generale a asociaţiei de proprietari, potrivit legii.

Referitor la obligația de informare a persoanei vizate, în spaţiile monitorizate prin camerele de supraveghere video, trebuie instalată o pictogramă adecvată, care să conţină o imagine reprezentativă, poziţionată la o distanţă rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere, astfel încât să poată fi văzută de orice persoană.

În ceea ce privește **perioada de stocare a datelor cu caracter personal** (imaginea) prelucrate de asociaţie ca urmare a instalării sistemului de supraveghere video, Autoritatea de supraveghere recomandă ca aceasta să nu depăşească 30 zile.

Excepție pot face situațiile temeinic justificate în care s-au produs evenimente ce necesită stocarea doar a imaginilor relevante pe o perioadă mai mare de timp necesară îndeplinirii scopurilor respective (de ex. până la soluționarea definitivă a unei cauze penale de către organele judiciare).

Referitor la imaginile captate și înregistrate de camerele video, instalate în zonele stabilite potrivit hotărârii adunării generale a proprietarilor, cu respectarea echilibrului dintre interesul legitim al asociației și drepturile și libertățile persoanelor, în vederea respectării principiului proporționalității, se poate apela la echipamente care din punct de vedere tehnic pot fi orientate astfel încât să focalizeze zonele necesare a fi supravegheate.

În ceea ce privește prelucrarea datelor prin altă persoană (cum ar fi de ex. societatea care instalează sistemul de videosupraveghere și asigură mentenanța acestuia, efectuează și prelucrarea datelor), potrivit art. 4 pct. 8 din RGPD aceasta este „persoana împuternicită de operator" întrucât prelucrează datele cu caracter personal în numele operatorului.

ATENȚIE! prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract, ce trebuie să conțină și instrucțiuni documentate din partea operatorului pe baza cărora împuternicitul va prelucra datele cu caracter personal.

MĂSURI organizatorice și măsuri tehnice

La Art.32 al.(1) din GDPR, prelucrarea datelor cu caracter personal în timpul supravegherii video nu trebuie să fie doar permisă din punct de vedere legal, ci și securizată corespunzător de către operatori și persoanele împuternicite de aceștia.

Măsurile organizatorice și tehnice puse în aplicare trebuie să fie proporționale cu riscurile la adresa drepturilor și libertăților persoanelor fizice care sunt generate, în mod accidental sau ilegal, din distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele obținute prin supraveghere video.

Conform Art.24 și 25 din GDPR, operatorii trebuie să pună în aplicare măsuri tehnice și organizatorice inclusiv pentru a garanta toate principiile de protecție a datelor în timpul prelucrării, precum și să stabilească mijloace prin care persoanele vizate să-și exercite drepturile definite la articolele 15-22 din GDPR.

Operatorii trebuie să adopte cadrul și politicile interne care să asigure această punere în aplicare atât la momentul stabilirii mijloacelor de prelucrare, cât și la momentul prelucrării în sine, inclusiv prin efectuarea de evaluări ale impactului asupra protecției datelor dacă este necesar.

"Politica de prelucrare a datelor cu caracter personal prin mijloace video" și limitarea accesului la date prin controlarea accesului sunt doar două asemenea masuri.

Operatorul trebuie să ia în considerare și tehnologii favorabile confidențialității.

(ex. sistemele care permit mascarea sau distorsionarea zonelor irelevante pentru supraveghere).

Măsuri organizatorice

Operatorii trebuie să ia în considerare următoarele subiecte atunci când își formulează propriile politici și proceduri privind supravegherea video:

- cine răspunde de gestionarea și funcționarea sistemului de supraveghere video;
- scopul și sfera de cuprindere a proiectului de supraveghere video;

- utilizarea adecvată și cea interzisă (unde și când este permisă supravegherea video, unde și când nu este permisă;
- măsurile privind transparența;
- modul de înregistrare și durata materialului video, inclusiv stocarea în arhive a înregistrărilor video referitoare la incidente de securitate;
- cine trebuie să beneficieze de instruire tematică și când;
- cine are acces la înregistrările video și în ce scopuri;
- procedurile operaționale (de exemplu, de către cine și de unde este monitorizată supravegherea video, ce trebuie făcut în cazul unui incident de încălcare a securității datelor);
- procedurile pe care trebuie să le urmeze părțile externe pentru a solicita înregistrări video și procedurile pentru respingerea sau aprobarea acestor cereri;
- procedurile de achiziție, instalare și întreținere a SSV;
- procedurile de gestionare a incidentelor și de recuperare a datelor.

Măsuri tehnice

Securitatea sistemului înseamnă securitatea fizică a tuturor componentelor sistemului și integritatea sistemului, adică protecția împotriva interferențelor intenționate și neintenționate în funcționarea sa obișnuită și reziliența față de acestea, precum și controlul accesului.

Securitatea datelor înseamnă confidențialitate (datele sunt accesibile doar persoanelor cărora li s-a acordat acces), integritate (prevenirea pierderilor de date sau a manipulării datelor) și disponibilitate (datele pot fi accesate atunci când este necesar).

- protecția întregii infrastructuri SSV (inclusiv camerele de la distanță, cablarea și alimentarea cu energie electrică) împotriva manipulării fizice frauduloase și a furtului fizic;
- protecția transmiterii înregistrărilor împotriva interceptării prin canale de comunicare sigure;
- criptarea datelor;
- utilizarea de soluții bazate pe hardware și software, cum ar fi sisteme firewall, antivirus sau de detectare a intruziunilor împotriva atacurilor cibernetice;
- detectarea disfuncționalităților la nivel de componente, software și interconectări.

Securitatea fizică

este o parte esențială a protecției datelor și prima linie de apărare, deoarece protejează echipamentele SSV de furt, vandalism, catastrofe naturale, catastrofe provocate de om și daune accidentale (de exemplu, supratensiuni electrice, temperaturi extreme și cafea vărsată). În cazul sistemelor de tip analog, securitatea fizică are rol principal în protecția lor.

CONTRACTUL

încheiat între operator și persoana împuternicită de operator

Așa cum am precizat anterior, Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (A.N.S.P.D.C.P) a specificat foarte clar, în comunicatul său că *"societatea care instalează sistemul de videosupraveghere și asigură mentenanța acestuia, efectuează și prelucrarea datelor"* este **„persoana împuternicită de operator"** întrucât prelucrează datele cu caracter personal în numele operatorului.

Prelucrarea efectuată de către o persoană împuternicită în numele unui operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul şi care stabileşte obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate şi obligaţiile şi drepturile operatorului.

Contractul încheiat între operator și persoana împuternicită trebui să prevadă că persoana împuternicită de operator:

O persoana împuternicită trebuie să fie conștientă că:

- poate fi supusa verificării potrivit competențelor de investigare și corectare a A.N.S.P.D.C.P (Art.58 din GDPR);
- în cazul în care nu își îndeplinește obligațiile, poate fi supus unei amenzi administrative (Art.83 din GDPR);
- în cazul în care nu îndeplinește obligațiile GDPR, aceasta poate fi supusă unei sancțiuni (Art.84 din GDPR) și să plătească despăgubiri.

ATENȚIE! Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligațiile din GDPR care revin în mod specific persoanelor împuternicite de operator sau a acționat în afara sau în contradicție cu instrucțiunile legale ale operatorului. [Art.82 al.(2)]

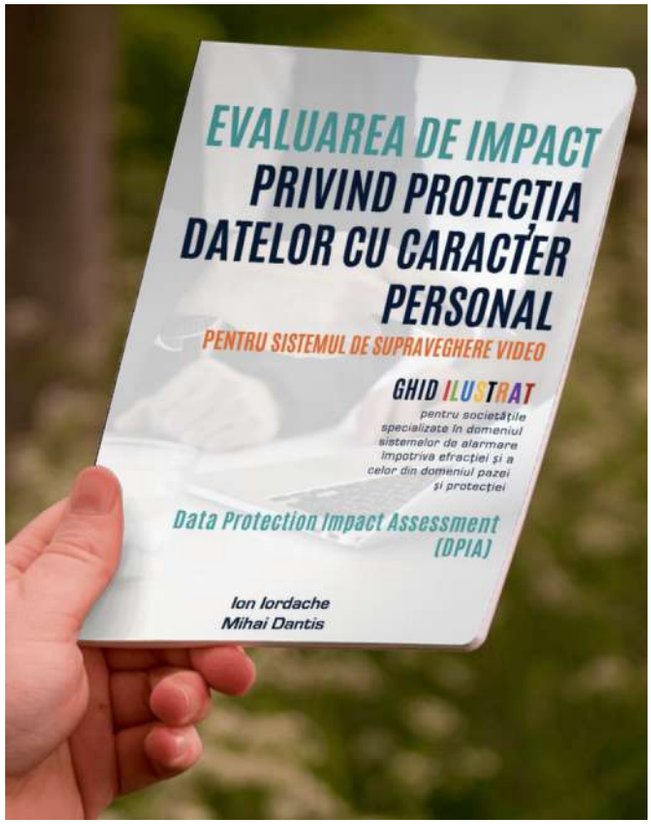
- **prelucrează datele cu caracter personal numai pe baza unor instrucţiuni documentate din partea operatorului**, inclusiv în ceea ce priveşte transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, cu excepţia cazului în care această obligaţie îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică;
- se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte **confidenţialitatea** sau au o obligaţie statutară adecvată de confidenţialitate și respectă condiţiile privind recrutarea unei alte persoane împuternicite de operator;
- **adoptă măsuri tehnice şi organizatorice** adecvate și oferă asistenţă operatorului prin măsuri tehnice şi organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligaţiei operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor sale;
- ajută operatorul să asigure **respectarea obligaţiilor** pe care acesta le are, în aplicarea GDPR;
- **şterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor** legate de prelucrare şi elimină copiile existente, cu excepţia cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;
- **pune la dispoziţia operatorului toate informaţiile necesare pentru a demonstra respectarea obligaţiilor sale**, permite desfăşurarea auditurilor, inclusiv a inspecţiilor, efectuate de operator sau alt auditor mandatat şi contribuie la acestea.

În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, **aceleași obligații** privind protecția datelor prevăzute în contractul încheiat între operator și persoana împuternicită de operator **revin celei de a doua persoane împuternicite**, prin intermediul unui contract sau al unui alt act juridic.

EVALUAREA impactului asupra protecției datelor în privința monitorizării video

Conform Art.35 al.(1) din GDPR, operatorii au obligația de a efectua evaluări ale impactului asupra protecției datelor atunci când un tip de prelucrare a datelor este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice.

Art.35 al.(3) litera(c) din GDPR prevede că operatorii au obligația de a efectua evaluări ale impactului asupra protecției datelor dacă prelucrarea constituie o monitorizare sistematică pe scară largă a unei zone accesibile publicului.



În **GHIDUL ilustrat "Evaluarea de impact privind protecția datelor cu caracter personal pentru sistemul de supraveghere video"** am prezentat pe larg acest subiect.

DOWNLOAD GRATUIT PE
www.ioniordache.com

Lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal

Autoritatea română de supraveghere a adoptat Decizia nr. 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal, publicată în Monitorul Oficial al României, Partea I, nr. 919 din 31 octombrie 2018 care prevede, printre altele că evaluarea impactului asupra protecției datelor cu caracter personal de către operatori este obligatorie în special în cazurile:

- prelucrării 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, și
- prelucrării 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-și exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaștere facială în vederea facilitării accesului în diferite spații.

Este important de menționat că, în cazul în care rezultatele DPIA indică faptul că prelucrarea ar genera un risc mare în pofida măsurilor de securitate prevăzute de operator, atunci va trebui consultată autoritatea de supraveghere relevantă înainte de prelucrare.

iQS GDPR APPROACH
Compliance Methodology

Vă pot ajuta să respectați și să implementați cerințele Regulamentului General privind Protecția Datelor (GDPR).

Pentru aceasta, am creat o metodologie simplă, în patru pași, pe care am denumit-o "iQS GDPR Approach".

Metodologia "iQS GDPR Approach" utilizează următorii patru pași: Conștientizarea, Evaluarea, Implementarea și Întreținerea.

Fiecare pas este alcătuit dintr-o serie de activități de sprijin. Cerința principală este ca fiecare etapă să fie finalizată într-o secvență iterativă cu scopul de a îndeplini obiectivul principal: executarea cu succes a fiecărei operațiuni.

Scopul final al metodologiei este implementarea cu succes a cerințelor GDPR.

Această metodologie este integrată într-un plan general. Serviciile mele pot fi angajate pentru întregul pachet "iQS GDPR Approach"; situație în care vom aborda planul general complet sau doar pentru unul sau mai mulți pași din planul general.

Este important să ne amintim de principiul responsabilității prevăzut de Art.5 paragraful(2) din GDPR care impune organizațiilor să dovedească conformitatea cu cerințele GDPR.

CONSULTANȚĂ ȘI SPECIALIZARE

SPECIALIZARE
ca "Responsabil cu protecția datelor cu caracter personal"
(COR 242231)

Acest curs de 180 de ore vă oferă posibilitatea de a înțelege toate cerințele Regulamentului general privind protecţia datelor (GDPR) și de a vă reorienta profesional în acest domeniu.

Un element de noutate pe care acest act normativ european îl aduce în peisajul juridic românesc îl reprezintă instituirea obligativității desemnării la nivelul operatorului sau persoanei împuternicite de operator, în anumite cazuri, a unui responsabil cu protecția datelor. Una dintre aceste situații este aceea în care "activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrarea care necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă."

ATENȚIE! Deși în unele cazuri nu este necesară desemnarea unui responsabil cu protecția datelor, Autoritatea de Supraveghere recomandă numirea unei astfel de persoane, întrucât este utilă operatorului pentru respectarea obligațiilor în domeniul protecției datelor cu caracter personal.

Eu am expertiza și experiența pentru a te ajuta să înțelegi și să utilizezi în mod corect cerințele Regulamentului general privind protecţia datelor (GDPR).

Evită amenzile GDPR care sunt, nu numai foarte mari dar și foarte ușor de luat.

STABILEȘTE ACUM O ÎNTÂLNIRE!

Vom discuta toate așteptările, nevoile, obiectivele tale și cum pot să te ajut.

Mă poți contacta pe *ion@ioniordache.com*

Ion Iordache
PECB Certified Data Protection Officer

BIBLIOGRAFIE
surse de informare

- **Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)**
- **Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video, Versiunea 2.0 Adoptat la 29 ianuarie 2020,** Comitetul European pentru Protecția datelor
- **Ghidul orientativ de aplicare a Regulamentului General privind Protecţia Datelor destinat operatorilor, emis de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal,** A.N.S.P.D.C.P
- **Ghid Întrebări și răspunsuri cu privire la aplicarea Regulamentului (UE) 2016/679, A.N.S.P.D.C.P**
- **Prelucrarea datelor de către asociațiile de proprietari,** A.N.S.P.D.C.P
- **Decizia nr. 174 din 18 octombrie 2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal,** A.N.S.P.D.C.P
- **LEGEA nr. 333 din 8 iulie 2003** (**republicată**)(*actualizată*) privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor*) (actualizată la data de 1 decembrie 2015*)
- **HOTĂRÂREA nr. 301 din 11 aprilie 2012** (*actualizată*) pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor (actualizată până la data de 29 ianuarie 2016*)
- **LEGEA nr. 190 din 18 iulie 2018** privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)
- **LEGEA nr. 129 din 15 iunie 2018** pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
- **DECIZIA nr. 99 din 18 mai 2018** privind încetarea aplicabilităţii unor acte normative cu caracter administrativ emise în aplicarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
- **GDPR Aplicat - instrument de lucru pentru implementarea Regulamentului UE 679/2016,** Autori: Daniela Simionovici, Daniela-Irina Cireașă, Cătălina Pantilimon, Marius-Florian Dan, Wolters Kluwer Romania, 2020
- **Metodologia "iQS GDPR Approach",** Ion Iordache
- **Responsabil cu protecția datelor cu caracter personal** (COR 242231), curs specializare, Ion Iordache

DATA ȘI VERSIUNEA: 10.06.2021, V.00

AUTOR: Acest ghid a fost elaborat de Ion Iordache.

Copii ale celei mai recente versiuni ale acestui ghid pot fi descărcate de pe https://ioniordache.com.

Dacă aveți nevoie de informații suplimentare, asistență sau recomandări cu privire la conținutul acestui document, vă rog să mă contactați la ion@ioniordache.com.