

NOTA DE INFORMARE

privind monitorizarea prin mijloace sisteme de supraveghere video cu circuit închis

Scopul documentului este informarea personalului din cadrul **Direcției de Prestări Servicii Timiș** cu privire la utilizarea de sisteme de supraveghere video cu circuit închis (sistem supraveghere CCTV) utilizate în sediul direcției în scopul realizării intereselor legitime urmărite .

1. Prezentare generală:

- Prezentarea scopului declarat al activității de supraveghere prin intermediul sistemului de supraveghere video cu circuit închis:
 - a) prevenirea și combaterea săvârșirii infracțiunilor;
 - b) asigurarea pazei și protecției persoanelor, bunurilor și valorilor, a imobilelor și a instalațiilor de utilitate publică, precum și a întreprinderilor afectate acestora;
 - c) realizarea unor interese legitime, cu condiția ca acesata să nu se prejudicieze drepturile și libertățile fundamentale sau interesul persoanelor vizate;
- Proiectarea, instalarea sistemului de supraveghere și monitorizare a fost efectuată/se va face prin intermediul unei/unor firme autorizate în condițiile prevăzute de lege;
- Preluarea, gestionarea, arhivarea imaginilor captate, durata de stocare a datelor obținute prin intermediul sistemului de supraveghere video cu circuit închis (sistem supraveghere CCTV) sunt reglementate și asigură îndeplinirea cerințelor de securitate, confidențialitate și disponibilitate;
- Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video se realizează doar de către persoanele autorizate de **Direcția de Prestări Servicii Timiș** (personal propriu sau persoane împuternicite de către operator), instruite cu privire la legislația referitoare la protecția datelor cu caracter personal și obligate să se supună acesteia;
- Durata de stocare a datelor obținute prin intermediul sistemului de supraveghere video este proporțională cu scopul pentru care se prelucrează datele, dar nu mai mare de 30 de zile, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate. La expirarea termenului stabilit, înregistrările se distrug sau șterg, după caz, în funcție de suportul pe care s-au stocat.
- Existența sistemului de supraveghere video este semnalată prin intermediul unei pictograme care conține o imagine reprezentativă cu vizibilitate suficientă și poziționată la o distanță rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere video:



2. Definiții în sensul regulament GDPR:

- ❖ *"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;*
- ❖ *"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;*
- ❖ *"restricționarea prelucrării" înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;*
- ❖ *"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;*
- ❖ *"date biometrice" înseamnă o 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;*
- ❖ *Imaginile obținute prin utilizarea sistemelor de supraveghere video reprezintă date cu caracter personal.*

3. Referinte legislative:

- ❖ **Legea nr. 102/2005** privind infiintarea, organizarea si functionarea Autoritatii Nationale de Supraveghere a Prelucrării Datelor cu Caracter Personal, publicata in Monitorul Oficial al Romaniei, Partea I, nr. 391 din 9 mai 2005, republicata;
- ❖ **Legea nr. 129/2018**, pentru modificarea si completarea Legii nr. 102/2005 privind infiintarea, organizarea si functionarea Autoritatii Nationale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum si pentru abrogarea Legii nr. 677/2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date.

Art. 3:

Atributiile Autoritatii nationale de supraveghere sunt, in principal, reglementate prin Regulamentul (UE) 2016/679 al Parlamentului European si al Consiliului din 27 aprilie 2016 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE (Regulamentul general privind protectia datelor), publicat in Jurnalul Oficial al Uniunii Europene, seria L, nr. 119 din 4 mai 2016, denumit in continuare Regulamentul general privind protectia datelor, si prin legislatia nationala de transpunere a Directivei (UE) 2016/680 a Parlamentului European si a Consiliului din 27 aprilie 2016 privind protectia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de catre autoritatile competente in scopul prevenirii, depistarii, investigarii sau urmaririi penale a infractiunilor sau al executarii pedepselor si privind libera circulatie a acestor date si de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, publicata in Jurnalul Oficial al Uniunii Europene seria L nr. 119 din 4 mai 2016.

- ❖ **Legea nr. 190 din 18 iulie 2018** privind măsuri de punere în aplicare a Regulamentului (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);

În cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaților, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă:

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

b)angajatorul a realizat informarea prealabilă obligatorie, completă și în mod explicit a angajaților;

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

d)alte forme și modalități mai puțin intruzive pentru atingerea scopului urmărit de angajator nu și-au dovedit anterior eficiența;

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

Legea nr. 190, Art. (47):

Interesele legitime ale unui operator, inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terțe părți, pot constitui un temei juridic pentru prelucrare, cu condiția

să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate, luând în considerare așteptările rezonabile ale persoanelor vizate bazate pe relația acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relație relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia.

...

Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor constituie, de asemenea, un interes legitim al operatorului de date în cauză.

Legea nr. 190, Art. (83):

În vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezentul regulament, operatorul ar trebui să evalueze riscurile inerente prelucrării și să implementeze măsuri pentru atenuarea acestor riscuri. Măsurile respective ar trebui să asigure un nivel corespunzător de securitate, inclusiv confidențialitatea, luând în considerare stadiul actual al dezvoltării și costurile implementării în raport cu riscurile și cu natura datelor cu caracter personal a căror protecție trebuie asigurată. La evaluarea riscului pentru securitatea datelor cu caracter personal, ar trebui să se acorde atenție riscurilor pe care le prezintă prelucrarea datelor, cum ar fi distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, în mod accidental sau ilegal, care pot duce în special la prejudicii fizice, materiale sau morale.

Legea nr. 190, Art. (76):

Probabilitatea de a se materializa și gravitatea riscului pentru drepturile și libertățile persoanei vizate ar trebui să fie determinate în funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor cu caracter personal. Riscul ar trebui apreciat pe baza unei evaluări obiective prin care se stabilește dacă operațiunile de prelucrare a datelor prezintă un risc ridicat. În aceste condiții se impune efectuarea unei evaluări a impactului asupra protecției datelor, care să estimeze, în special, originea, natura, specificitatea și gravitatea acestui risc, conf. Art.(84). Evaluarea impactului ar trebui să includă, în special, măsurile, garanțiile și mecanismele avute în vedere pentru atenuarea riscului respectiv, pentru asigurarea protecției datelor cu caracter personal.

Legea nr. 190, Art. (90):

În astfel de cazuri, operatorul ar trebui să efectueze, înainte de prelucrare, o evaluare a impactului asupra protecției datelor, în scopul evaluării gradului specific de probabilitate a materializării riscului ridicat și gravitatea acestuia, având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și sursele riscului. Respectiva evaluare a impactului ar trebui să includă, în special, măsurile, garanțiile și mecanismele avute în vedere pentru atenuarea riscului respectiv, pentru asigurarea protecției datelor cu caracter personal și pentru demonstrarea conformității cu prezentul regulament.

Legea nr. 190, Art.(80) :

prelucrarea are caracter ocazional nu include prelucrarea pe scară largă a unor categorii speciale de date cu caracter personal și nici prelucrarea de date referitoare la condamnări penale și la infracțiuni, și este puțin susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice, având în vedere natura, contextul, domeniul de aplicare și scopurile prelucrării, precum și a cazului în care operatorul este o autoritate publică sau un organism public.

EXTREM CONSULT S.R.L. Timisoara
Ing. Vasile Radulescu