EVALUAREA DE IMPACT PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL

PENTRU SISTEMUL DE SUPRAVEGHERE VIDEO

GHID ILUSTRAT

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

Data Protection Impact Assessment (DPIA)

Ion Iordache
Mihai Dantis

Nota autorilor:

Am elaborat acest ghid ilustrat pentru a veni atât în sprijinul operatorilor de date cu caracter personal cât și al împuterniciților acestora, societățile specializate în domeniul sistemelor de alarmare împotriva efracției și a celor din domeniul pazei şi protecției de a înțelege utilitatea și în unele situații obligativitatea ca operatorul de date date să efectueze o "Evaluarea de impact privind protecția datelor cu caracter personal pentru sistemul de supraveghere video".

Pentru a nu exista confuzii în interpretarea textului acestui ghid, am utilizat doar resursele oficiale (prezentate în bibliografie) care tratează acest proces, metodologia propusă fiind una adaptată cerințelor Regulamentului General privind Protecţia Datelor.

Am ales să utilizăm următoarele prescurtări:

- **DPIA** - acronim al Data Protection Impact Assessment pentru "Evaluarea de impact privind protecția datelor cu caracter personal pentru sistemul de supraveghere video".
- **GDPR** - acronim al General Data Protection Regulation pentru " 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".
- **SSV** - acronim pentru Sistem de Supraveghere Video numit până la intrarea în vigoare a seriei de standarde IEC 62676 pentru sisteme de supraveghere video, televiziune cu circuit închis (TVCI).
- **DPO** - acronim pentru Data Protection Officer pentru Responsabilul cu Protecția Datelor Personale.

CUPRINS:

I. INTRODUCERE

GDPR include o cerință de a efectua o evaluare a impactului asupra protecției datelor (DPIA) pentru anumite proiecte care implică prelucrarea datelor cu caracter personal.

Deși DPIA este o cerință a GDPR, statele individuale din SEE pot avea cerințe suplimentare, inclusiv „liste negre" de activități care declanșează un DPIA iar Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal din România a emis DECIZIA nr. 174 din 18 octombrie 2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal. Vom prezenta, pe scurt această decizie în Capitolul III.

GDPR introduce noi cerințe pentru operatorii de date responsabilitatea fiind deosebit de relevantă deoarece doar respectarea cerințelor GDPR nu este suficientă mai trebuie să și demonstrezi că faci asta.

În acest sens, evaluările impactului asupra protecției datelor (DPIA) sunt un instrument cheie pentru a demonstra prelucrarea responsabilă a datelor iar pentru ca rezultatele DPIA să fie obiective, repetabile și comparabile, acestea trebuie să se bazeze pe metode sistematice.

GDPR adoptă o abordare bazată pe risc a protecției datelor, care necesită efectuarea unei analize de risc și, dacă riscurile sunt prea mari, o reducere a riscului. Putem clasifica riscurile asociate procesării datelor în două tipuri: riscurile inerente prelucrării datelor *(așa cum a fost proiectat)* și riscurile asociate securității datelor.

Un „risc" este un scenariu care descrie un eveniment și consecințele acestuia, estimate în ceea ce privește gravitatea și probabilitatea. Astfel, „gestionarea riscului" poate fi definită ca activitățile coordonate pentru conducerea și controlul unei organizații în ceea ce privește riscurile.

Atunci când riscurile inerente procesării datelor sunt prea mari, trebuie să le modificăm pentru a le reduce.

De exemplu, pentru a evita complet prelucrarea unor tipuri de date care sunt sensibile *(imaginile colectate de sistemele de supraveghere video)* sau pentru a restricționa accesul la astfel de date.

Riscurile asociate securității datelor sunt cele care rezultă din pierderea confidențialității, integrității și disponibilității datelor. Metodologiile standard de analiză a riscurilor sunt complexe, iar organizațiile mici pot avea dificultăți în implementarea lor.

În acest ghid, vă propun o metodologie de realizare a DPIA pentru sistemul de supraveghere video.

ATENȚIE! Conform GDPR, neconformitatea cu cerințele DPIA poate conduce la aplicarea de amenzi de către autoritatea de supraveghere competentă. Neefectuarea unei DPIA atunci când prelucrarea face obiectul unei DPIA [articolul 35 alineatul (1) și alineatele (3)-(4)], efectuarea unei DPIA într-un mod incorect [articolul 35 alineatul (2) și alineatele (7) - (9)] sau neconsultarea autorității de supraveghere competente atunci când este necesar [articolul 36 alineatul (3) litera (e)] poate conduce la aplicarea unei amenzi administrative de până la 10 milioane EUR sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare.

II. DPIA EXPLICATĂ PE SCURT

Conform articolului 35 alineatul (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.

Articolul 35 alineatul (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 plus, în conformitate cu articolul 35 alineatul (3) litera (b) din GDPR, o evaluare a impactului asupra protecției datelor se impune, de asemenea, atunci când operatorul intenționează să prelucreze pe scară largă categorii speciale de date.

DPIA este un proces conceput pentru a descrie prelucrarea, a evalua necesitățile și proporționalitățile acesteia și a contribui la gestionarea riscurilor la adresa drepturilor și libertăților persoanelor fizice care rezultă din prelucrarea datelor cu caracter personal, prin evaluarea acestora și stabilirea de măsuri pentru soluționarea lor.

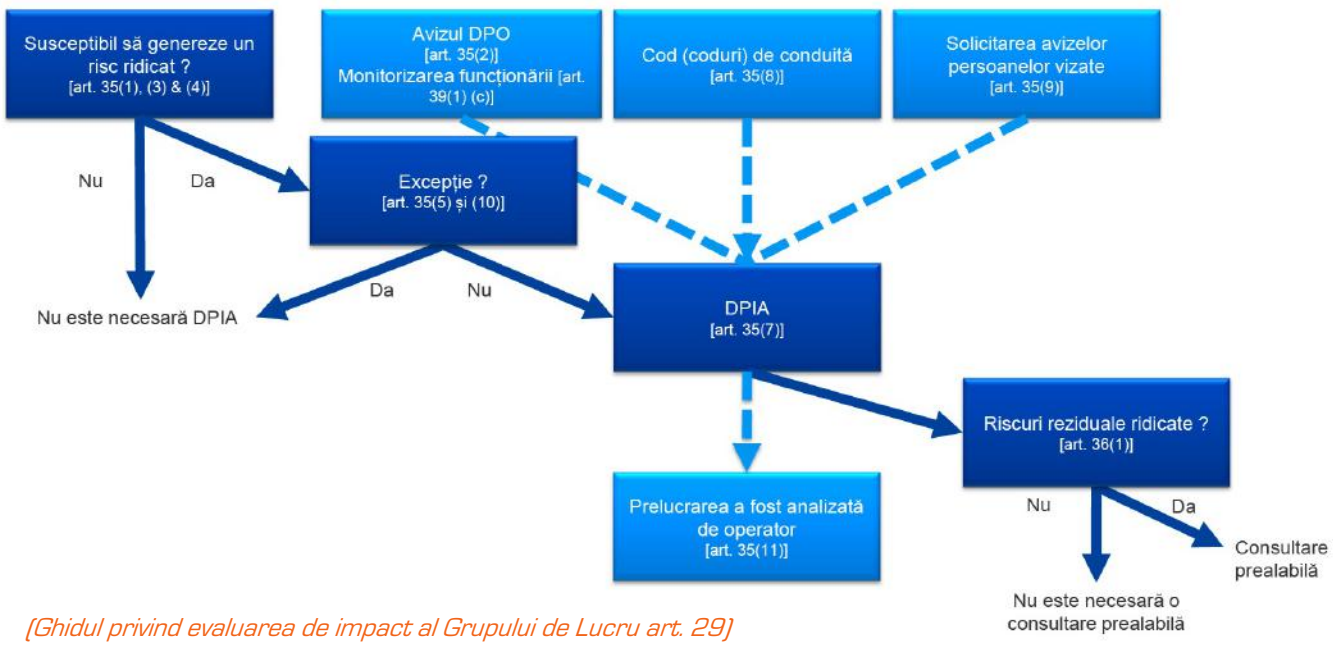
DPIA sunt instrumente importante pentru asumarea răspunderii, întrucât acestea ajută operatorii să respecte cerințele GDPR, dar și să demonstreze că au fost luate măsurile corespunzătoare în vederea asigurării conformității cu regulamentul (a se vedea, de asemenea, articolul 24)5.

Cu alte cuvinte, o DPIA este un proces de consolidare și demonstrare a conformității.

(Ghidul privind evaluarea de impact al Grupului de Lucru art. 29)

În conformitate cu abordarea bazată pe risc prevăzută de GDPR, efectuarea unei DPIA nu este obligatorie pentru fiecare operațiune de prelucrare. În schimb, o DPIA este necesară numai în cazul în care un tip de prelucrare este *„susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice”* [articolul 35 alineatul (1)].

Figura de mai jos ilustrează principiile de bază legate de DPIA din GDPR



(Ghidul privind evaluarea de impact al Grupului de Lucru art. 29)

O DPIA poate fi utilă pentru a evalua impactul unui produs al tehnologiei asupra protecției datelor, de exemplu, al unui element de hardware sau software, atunci când este posibil ca acesta să fie utilizat de diferiți operatori de date pentru a efectua diferite operațiuni de prelucrare.

Sistemul de supraveghere video, de exemplu, unde operatorul și persoana împuternicită de operator ar trebui să facă schimb de informații utile, fără a compromite secrete și fără a genera riscuri de securitate prin divulgarea vulnerabilităților.

DPIA ar putea să vizeze o singură operațiune de prelucrare a datelor. Cu toate acestea, articolul 35 alineatul (1) prevede că *„o evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare”.*

Ar putea fi utilizată o singură DPIA pentru a evalua mai multe operațiuni de prelucrare similare în ceea ce privește natura, domeniul de aplicare, contextul, scopul și riscurile.

Într-adevăr, evaluările DPIA urmăresc în mod sistematic studierea unor situații noi care ar putea conduce la riscuri ridicate pentru drepturile și libertățile persoanelor fizice și nu este necesar să se efectueze o DPIA în cazurile (și anume, operațiunile de prelucrare efectuate într-un context specific și pentru un anumit scop) care au fost deja studiate.

GDPR nu solicită efectuarea unei DPIA pentru fiecare operațiune de prelucrare care poate genera riscuri pentru drepturile și libertățile persoanelor fizice.

Efectuarea unei DPIA este obligatorie numai în cazul în care prelucrarea este ***„susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice”*** [articolul 35 alineatul (1), ilustrat de articolul 35 alineatul (3) și completat de articolul 35 alineatul (4)].

Atunci când operațiunea de prelucrare implică operatori asociați, aceștia trebuie să definească obligațiile lor respective în mod exact.

Notă: În cazurile în care nu este clar dacă este necesară o DPIA, se recomandă efectuarea, cu toate acestea, a unei DPIA, întrucât o DPIA este un instrument util pentru a sprijini operatorii să respecte legislația în materie de protecție a datelor.

III. CÂND, CINE ȘI CUM EFECTUEAZĂ O DPIA

1. Când este o DPIA obligatorie

În afară de cazul în care operațiunea de prelucrare constituie o excepție, DPIA trebuie efectuată dacă o operațiune de prelucrare este *„susceptibilă să genereze un risc ridicat”.*

Cu toate că o DPIA ar putea fi solicitată și în alte împrejurări, articolul 35 alineatul (3) prevede o serie de exemple atunci când o operațiune de prelucrare este „susceptibilă să genereze riscuri ridicate”:

a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă”;

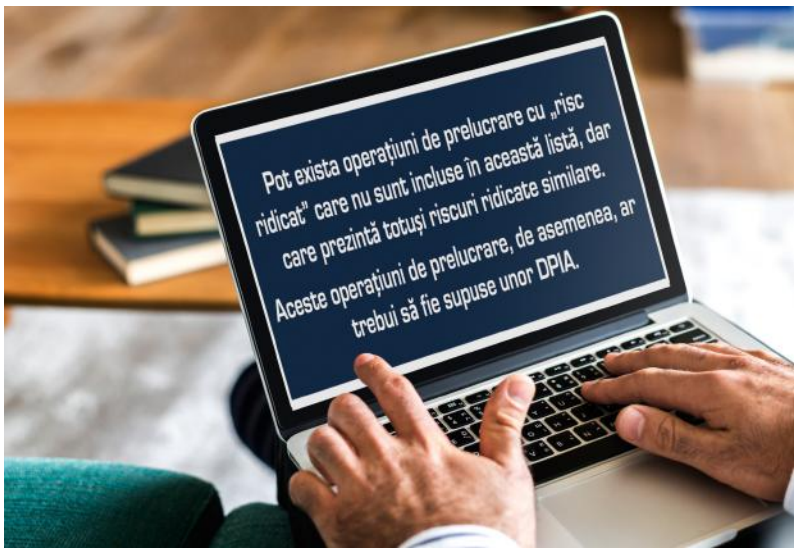
b) prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10; sau

c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului”.

În ce moment ar trebui să fie efectuată o DPIA?

DPIA ar trebui să fie efectuată „înaintea prelucrării”.

Aceasta este în concordanță cu asigurarea protecției datelor începând cu momentul conceperii și în mod implicit. DPIA ar trebui să fie văzută ca un instrument pentru sprijinirea procesului decizional în ceea ce privește prelucrarea.



Notă: **Faptul că DPIA ar putea necesita actualizare odată ce prelucrarea a început efectiv nu reprezintă un motiv valabil pentru amânarea sau neefectuarea unei DPIA.**

De exemplu, raportul evaluatorului de risc la securitatea fizică ar putea să ducă la această actualizare.

DPIA este un proces continuu, nu un exercițiu unic, în special în cazul în care o operațiune de prelucrare este dinamică și în continuă schimbare.

1.1. Criterii de luat în considerare pentru a determina dacă o operațiune de prelucrare este susceptibilă să genereze un risc ridicat

1. **Evaluarea sau punctarea**, inclusiv crearea de profiluri și preconizarea, în special de la *„aspecte privind randamentul la locul de muncă al persoanei vizate, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările”*.
2. **Luarea de decizii în mod automat cu un efect juridic sau similar semnificativ:** prelucrarea care are ca scop luarea deciziilor privind persoanele vizate care produc *„efecte juridice privind persoana fizică”* sau care *„o afectează în mod similar într-o măsură semnificativă”* Exemplu: prelucrarea poate conduce la excluderea sau discriminarea persoanelor.
3. **Monitorizarea sistematică:** prelucrarea utilizată pentru observarea, monitorizarea sau controlul persoanelor vizate, inclusiv datele colectate prin intermediul rețelelor sau al „unei monitorizări sistematice pe scară largă a unei zone accesibile publicului”.
4. **Date sensibile sau date foarte personale**: acestea includ categorii speciale de date cu caracter personal *(de exemplu, informații cu privire la opiniile politice ale persoanelor)*, precum și date cu caracter personal referitoare la condamnări penale sau infracțiuni. Faptul că datele cu caracter personal *(imaginile video, de exemplu)* sunt puse la dispoziția publicului poate fi considerat un factor în cadrul evaluării, în cazul în care se preconiza că datele urmau să fie utilizate în continuare în anumite scopuri.
5. **Datele prelucrate pe scară largă:** Se recomandă ca, în special, următorii factori să fie luați în considerare atunci când se stabilește dacă prelucrarea se efectuează pe scară largă: numărul de persoane vizate în cauză; volumul de date și/sau gama de diferite elemente de date care sunt prelucrate; durata sau persistența activității de prelucrare a datelor și extinderea geografică a activității de prelucrare.
6. **Corelarea sau combinarea seturilor de date**, de exemplu care provin din două sau mai multe operațiuni de prelucrare a datelor efectuate în scopuri diferite și/sau de către diferiți operatori de date într-un mod care ar depăși așteptările rezonabile ale persoanei vizate.
7. **Date privind persoanele vizate vulnerabile:** prelucrarea acestui tip de date reprezintă un criteriu din cauza dezechilibrului de putere crescut dintre persoanele vizate și operatorul de date, ceea ce înseamnă că persoanele pot să nu fie în măsură a-și da consimțământul sau a respinge cu ușurință prelucrarea datelor lor sau a-și exercita drepturile.
8. **Utilizarea inovatoare sau aplicarea unor soluții tehnologice sau organizaționale noi,** cum ar fi combinarea utilizării amprentei digitale și recunoașterea facială pentru îmbunătățirea controlului accesului fizic etc.
9. **Atunci când prelucrarea în sine „împiedică persoanele vizate să exercite un drept sau să utilizeze un serviciu ori un contract”** Acest lucru include operațiunile de prelucrare care au ca obiectiv permiterea, modificarea sau refuzul accesului persoanelor vizate la un serviciu sau la angajarea într-un contract.

Următorul exemplu ilustrează modul în care criteriile ar trebui să fie utilizate pentru a evalua dacă o anumită operațiune de prelucrare necesită o DPIA:

Utilizarea unui sistem de camere pentru a monitoriza comportamentul de conducere pe autostrăzi.

Operatorul intenționează să utilizeze un sistem inteligent de analiză video pentru a identifica autoturismele și pentru a recunoaște în mod automat plăcuțele de înmatriculare.

Criterii relevante posibile: monitorizare sistematică și utilizarea inovatoare sau aplicarea unor soluții tehnologice sau organizaționale.

Este DPIA susceptibilă să fie necesară?

DA!

2. Cine este obligat să efectueze o DPIA

Operatorului îi revine responsabilitatea de a asigura efectuarea DPIA.

Efectuarea DPIA ar putea fi realizată de altă persoană, din interiorul sau din exteriorul organizației, însă operatorul rămâne responsabil în cele din urmă de această sarcină.

Operatorul trebuie să solicite, de asemenea, avizul responsabilului cu protecția datelor (DPO) în cazurile desemnate iar acest aviz și deciziile luate de către operator ar trebui să fie documentate în cadrul DPIA.

De asemenea, DPO ar trebui să monitorizeze funcționarea DPIA.

ATENȚIE! În cazul în care prelucrarea este efectuată integral sau parțial de către o persoană împuternicită de operator, persoana împuternicită de operator ar trebui să asiste operatorul în efectuarea DPIA și să furnizeze toate informațiile necesare *[în conformitate cu articolul 28 alineatul (3) litera (f)]*.

Operatorul trebuie „să solicite avizul persoanelor vizate sau al reprezentanților acestora acolo unde este cazul"

Respectivele avize ar putea fi urmărite printr-o varietate de mijloace, în funcție de context (de exemplu, un studiu generic legate de scopul și mijloacele operațiunii de prelucrare.

În cazul în care decizia finală a operatorului de date diferă de avizele persoanelor vizate, motivele acestuia de a continua sau nu ar trebui să fie documentate.

Operatorul ar trebui să își documenteze justificarea pentru nesolicitarea avizelor persoanelor vizate, în cazul în care decide că acest lucru nu este necesar.

O bună practică este aceea de a defini și a documenta alte roluri și responsabilități specifice, în funcție de politica, procesele și normele interne, de exemplu:

În cazul în care anumite unități operaționale (Ex. Departamentul intern de securitate) pot propune efectuarea unei DPIA, respectivele unități ar trebui să furnizeze ulterior date DPIA și ar trebui să fie implicate în procesul de validare a DPIA;

După caz, **se recomandă solicitarea avizelor de la experți independenți** din diferite profesii (avocați, experți IT, experți în securitatea fizică, evaluatori de risc la securitatea fizică, etc.).

Rolurile și responsabilitățile persoanelor împuternicite de către operator trebuie să fie definite prin contract; iar DPIA trebuie să fie efectuată cu sprijinul persoanei împuternicite de către operator, ținând seama de natura prelucrării și de informațiile aflate la dispoziția persoanei împuternicite de operator.

2.1. Decizia ANSPDCP privind lista operațiunilor pentru care este obligatorie realizarea DPIA

În Monitorul Oficial al României, partea I, nr. 919 din data de 31 octombrie 2018, a fost publicată Decizia nr. 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal.

Decizia Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) are ca temei art. 35 alin. (4) din GDPR: "Autoritatea de supraveghere întocmește și publică o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor, în conformitate cu alineatul (1)."

Art. 1 (1) Evaluarea impactului asupra protecției datelor cu caracter personal de către operatori este obligatorie în special în următoarele cazuri:

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

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

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

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

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

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

g) prelucrarea pe scară largă și/sau sistematică a datelor de trafic și/sau de localizare a persoanelor fizice (cum ar fi monitorizarea prin Wi-Fi, prelucrarea datelor de localizare geografică a pasagerilor în transportul public sau alte asemenea situații) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

3. Beneficiile efectuării unei DPIA

Efectuarea unei DPIA poate îmbunătăți gradul de conștientizare a riscurilor de protecție a datelor asociate unui proiect

(De exemplu, efectuarea avaluarii riscurilor la securitatea fizică pentru a asigura viața și bunurile organizației).

Acest lucru va ajuta organizația să îmbunătățească comunicarea privind protecția datelor cu părțile interesate relevante.

Unele dintre beneficiile efectuării unui DPIA includ:

Asigurarea și demonstrarea faptului că organizația respectă cerințele GDPR și evită sancțiunile.

Inspirarea încrederii clienților prin îmbunătățirea comunicărilor cu privire la problemele de protecție a datelor.

Asigurarea că angajații și clienții organizației nu riscă să le fie încălcate drepturile de protecție a datelor.

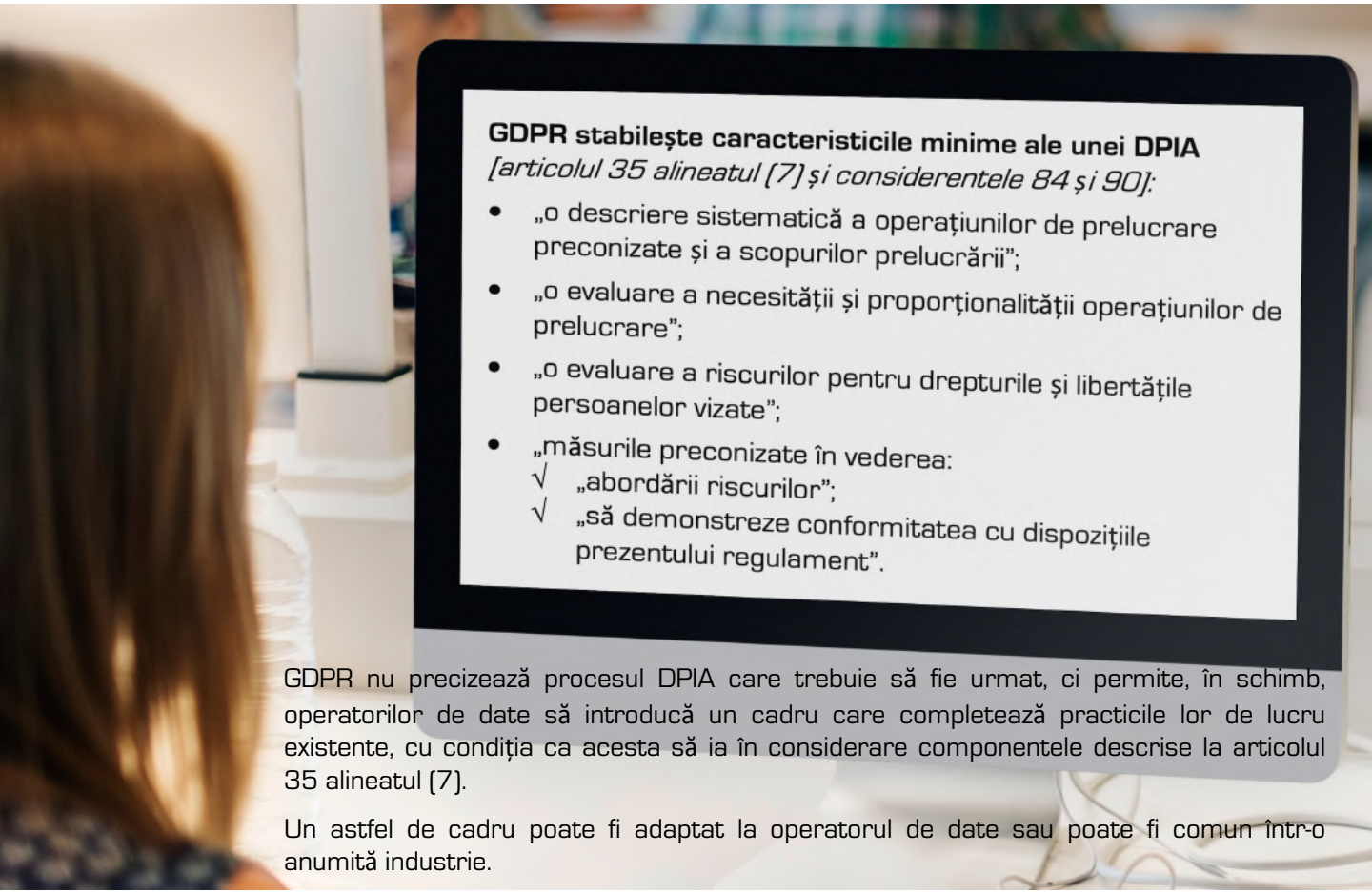
Esențial pentru creșterea gradului de conștientizare a confidențialității între organizații.

Reducerea costurilor operaționale prin optimizarea fluxurilor de informații în cadrul unui proiect și eliminarea colectării și prelucrării inutile a datelor.

Un sprijin excelent acordat evaluatorilor de risc la securitatea fizică și proiectanților sistemelor de securitate (SSV) care au obligații legale pe care trebuie să le respecte și pe care, la rândul lor, sunt obligați să le comunice operatorului de date.

4. Metodologia de efectuare a unei DPIA

Metodologiile de efectuare a DPIA pot fi diferite, dar criteriile sunt aceleași.

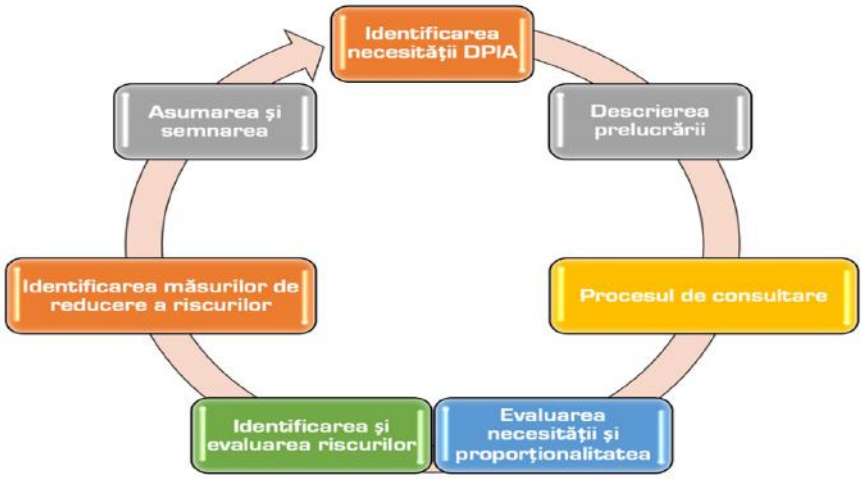


GDPR nu precizează procesul DPIA care trebuie să fie urmat, ci permite, în schimb, operatorilor de date să introducă un cadru care completează practicile lor de lucru existente, cu condiția ca acesta să ia în considerare componentele descrise la articolul 35 alineatul (7).

Un astfel de cadru poate fi adaptat la operatorul de date sau poate fi comun într-o anumită industrie.

ISO/IEC 29134:2017 Tehnologia informației - Tehnici de securitate - Evaluarea impactului asupra vieții private este un standard internațional care furnizează orientări pentru metodologiile utilizate pentru efectuarea unei DPIA.

Metodologia propusă de noi la Capitolul IV are următorii pași:



Indiferent de forma sa, o DPIA trebuie să fie o veritabilă evaluare a riscurilor, care permite operatorilor să ia măsuri pentru soluționarea acestora.

5. Criterii pentru o DPIA acceptabilă

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL WP29 propune o serie de criterii pe care operatorii de date le pot utiliza pentru a determina dacă o DPIA sau o metodologie pentru efectuarea unei DPIA este suficient de cuprinzătoare pentru a respecta GDPR:

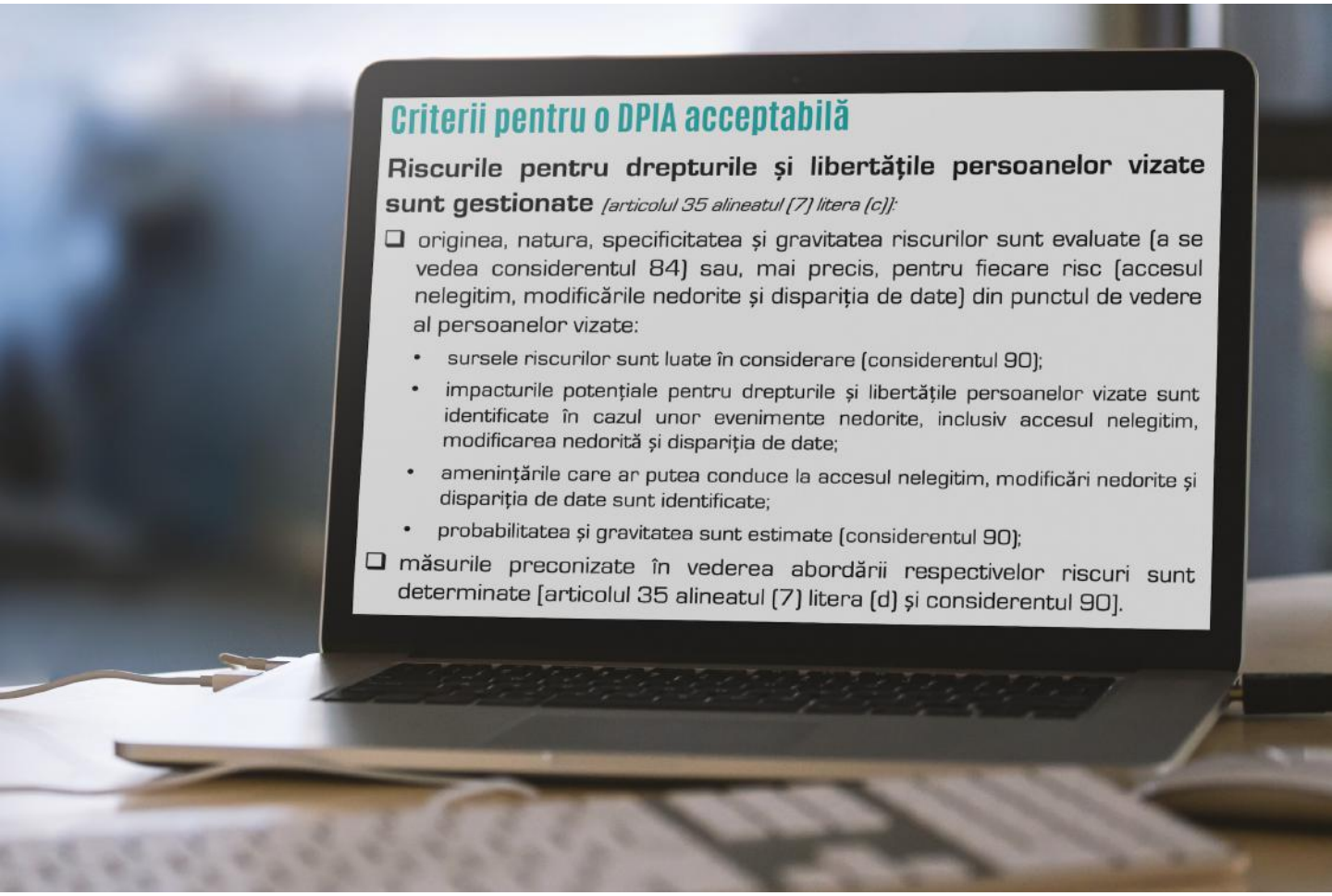
- **necesitatea și proporționalitatea sunt evaluate [articolul 35 alineatul (7) litera (b)]:**
  - √ sunt stabilite măsurile avute în vedere pentru respectarea regulamentului [articolul 35 alineatul (7) litera (d) și considerentul 90], luând în considerare:
    - măsurile care contribuie la proporționalitatea și necesitatea prelucrării pe baza:
      - √ scopului sau a scopurilor determinate, explicite și legitime [articolul 5 alineatul (1) litera (b)];
      - √ legalității prelucrării (articolul 6);
      - √ datelor adecvate, relevante și limitate la ceea ce este necesar [articolul 5 alineatul (1) litera (c)];
      - √ duratei limitate legate de stocare [articolul 5 alineatul (1) litera (e)];
    - măsurile care contribuie la drepturile persoanelor vizate:
      - √ informațiile furnizate persoanei vizate (articolele 12, 13 și 14);
      - √ dreptul de acces și dreptul la portabilitatea datelor (articolele 15 și 20);
      - √ dreptul la rectificare și dreptul la ștergere (articolele 16, 17 și 19);
      - √ dreptul la opoziție și la restricționarea prelucrării (articolele 18, 19 și 21);
      - √ relațiile cu persoanele împuternicite de operator (articolul 28);
      - √ garanțiile privind transferul (transferurile) internațional(e) (capitolul V);
      - √ consultarea prealabilă (articolul 36).

Criterii pentru o DPIA acceptabilă

Părțile interesate sunt implicate

Avizul DPO este solicitat
[articolul 35 alineatul (2)]

Avizele persoanelor vizate sau ale reprezentanților acestora sunt solicitate, dacă este cazul
[articolul 35 alineatul (9)].



IV. DPIA PENTRU SISTEMUL DE SUPRAVEGHERE VIDEO

AVIZAT,

Responsabil cu protecția datelor (DPO)

.....

EVALUAREA DE IMPACT
PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL PENTRU SISTEMUL DE SUPRAVEGHERE VIDEO
Data Protection Impact Assessment (DPIA)

(Exemplu)

Operatorul de date: UNIVERSITATEA BANAT - Centrul de consiliere și orientare în carieră (CCOC)

Numele proiectului: Instalarea unui sistem de supraveghere video (SSV) la Centrul de Consiliere și Orientare în Carieră (CCOC) din Timișoara, Str. Libertății, nr.202

Cine a întocmit "Evaluarea de impact privind protecția datelor cu caracter personal pentru sistemul de supraveghere video" (DPIA): această evaluare a fost realizată de către reprezentanții CCOC din management, securitate IT și juridic.

Avizul Responsabilului cu Protecția Datelor Personale (DPO): "Evaluarea de impact privind protecția datelor cu caracter personal pentru sistemul de supraveghere video" a fost realizată sub supravegherea și a fost avizată de către ..... (numele DPO)

1. Identificarea necesității DPIA

Explicați pe larg ce își propune să realizeze proiectul și ce tip de procesare implică. S-ar putea să vă fie de ajutor să faceți referire sau să legați alte documente, cum ar fi o propunere de proiect. Rezumați de ce ați identificat necesitatea unui DPIA.

Scopul prelucrării - Una dintre responsabilitățile de bază ale universității noastre este aceea de a oferii un mediu sigur personalului și studenților noștrii iar instalarea unui sistem de supraveghere video la Centrul de Consiliere și Orientare în Carieră (CCOC) completează o serie de alte măsuri de securitate existente deja sau care vor trebui implementate datorită unor cerințe legale *(punctul 6 de mai jos)*.

Sistemul de supraveghere video (SSV) va ajuta la realizarea următoarelor situații:

1. **Prevenirea incidentelor** - aceasta este o funcție importanta a oricărui sistem de supraveghere video deoarece prin plasarea camerelor de securitate în zonele critice ale CCOC, potențialii infractori vor fi descurajați să comită infracțiuni sau să se comporte neadecvat. Aceste imagini video pot fi folosite ca probe atunci când se aplică măsuri disciplinare iar prin integrări cu alte subsisteme de securitate *(alarmarea la efracție și/sau controlul accesului)* conducerea universității poate aborda aceste incidente rapid și precis.
2. ...
3. ...

EVALUAREA DE IMPACT

PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL PENTRU SISTEMUL DE SUPRAVEGHERE VIDEO

2. Descrierea prelucrării

Descrieți natura procesării: cum veți colecta, utiliza, stoca și șterge datele? Care este sursa datelor? Veți comunica date cu oricine? S-ar putea să fie util să vă uitati la o diagramă de flux sau alt mod de descriere a fluxurilor de date. Ce tipuri de prelucrare identificate ca riscuri susceptibile de risc sunt implicate?

2.1. Colectarea, utilizarea, stocarea și ștergerea datelor. - Sistemul de supraveghere video (SSV) va oferi CCOC imagini video de la cele 11 camere fixe iar imaginile vor fi capturate pe un sistem Digital Video Recorder (DVR) situat într-o încăpere securizată unde accesul este restricționat cu sistem de control acces și alarmare la efracție. Sistemul de supraveghere video (SSV) este operațional 24 de ore pe zi, 7 zile pe săptămână.

2.2. ...

2.3. Perioada de stocare a datelor cu caracter personal *(imaginile video)* colectate prin intermediul sistemului de supraveghere video (SSV) este de 30 de zile cu specificarea că Legea 333 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor obligă la un minim de 20 de zile.

2.4. ...

2.5. ...

3. Procesul de consultare

Luați în considerare modul de consultare cu părțile interesate relevante: descrieți momentul și modul în care veți căuta opiniile persoanelor - sau justificați motivul pentru care nu este adecvat să faceți acest lucru. Cine mai trebuie să se implice în organizația dvs.? Trebuie să cereți procesatorilor să vă ajute? Aveți de gând să consultați experții în domeniul securității informațiilor sau alți experți?

În procesul de consultare vor fi obținute opiniile personalului și ale studenților și se vor respecta prevederile Art. 5: Prelucrarea datelor cu caracter personal în contextul relațiilor de muncă din **"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).**

EVALUAREA DE IMPACT

PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL PENTRU SISTEMUL DE SUPRAVEGHERE VIDEO

4. Evaluarea necesității și proporționalitatea

Descrieți măsurile de conformitate și proporționalitate: care este baza dvs. legală pentru prelucrare? Procesarea îți atinge efectiv scopul? Există un alt mod de a obține același rezultat? Cum veți asigura calitatea datelor și minimizarea datelor? Ce informații le veți da persoanelor fizice? Cum vă veți ajuta să vă sprijiniți drepturile? Ce măsuri trebuie luate pentru a asigura respectarea procesorilor? Cum protejați orice transferuri internaționale?

Temeiul juridic al prelucrării - Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor precum și interesul legitim al CCOC de a supraveghea activitățile de acces în clădirea CCOC și **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).

Procesarea își atinge scopul. Camerele video sunt amplasate în zone în care studenții și personalul au acces. Camerele nu sunt amplasate în zone în care se așteaptă confidențialitatea.

5. Identificarea și evaluarea riscurilor

Notă: O DPIA trebuie să fie o evaluare autentică a riscurilor implicate într-un operațiune de prelucrare. Considerentul 76 din GDPR prevede că riscurile pentru persoanele vizate trebuie „evaluate în mod obiectiv". În același timp, domeniul de aplicare al termenului „risc" este larg și acoperă mult mai mult decât impactul asupra protecției datelor/vieții private a persoanelor fizice și include impact-uri asupra altor drepturi, libertăți și interese, care pot fi fizice, materiale sau emoționale.

În termeni simpli, utilizând matricea de mai jos, riscul este calculat după cum urmează:

Riscul = (severitatea x probabilitatea)

Severitatea impactului				
	Sever	Risc scăzut	Risc ridicat	Risc ridicat
	Semnificativ	Risc scăzut	Risc mediu	Risc ridicat
	Minim	Risc scăzut	Risc scăzut	Risc scăzut
		De la distanță	Posibil	Probabil
		Probabilitatea		

EVALUAREA DE IMPACT

PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL PENTRU SISTEMUL DE SUPRAVEGHERE VIDEO

6. Identificarea măsurilor de reduce a riscurilor

DPIA include măsurile pe care intenționează să le ia CCOC (sau, în cazul unei activități de prelucrare existente, măsurile pe care le-a luat) pentru a atenua riscurile identificate mai sus. Aceste măsuri pot include măsuri de securitate tehnică și organizațională, sau audituri periodice ale măsurilor de securitate.

Identificați măsurile suplimentare pe care le-ați putea lua pentru a reduce sau elimina riscurile identificate ca risc mediu sau ridicat la pasul 5				
Riscul	**Opțiuni de reducere sau eliminare a riscurilor**	**Efectul riscului**	**Riscuri reziduale**	**Măsuri aprobate**
		Eliminare Reducere Acceptare	Scăzut Mediu Ridicat	DA/NU
Pătrunderea apei în carcasele de protecție	Utilizarea carcaselor de calitate	Eliminare	Scăzut	DA
Mentenanța SSV				

7. Asumarea și semnarea de către persoanele responsabile a DPIA

Un extras din DPIA va fi pus la dispoziția angajaților, studenților și vizitatorilor prin afișare după ce va fi adus la cunoștiința tuturor angajaților și studenților precum și vizitatorilor care solicită mai multe informații cu privire la supravegherea video.

Datorită faptului că nu există riscuri reziduale, nu este necesară comunicare evaluării către ANSPDCP dar la cerere sau în caz de inspecție, aceasta poate fi comunicată integral ANSPDCP.

Articolul	Nume/Poziția	Data	Semnături
DPIA realizată de:			
Măsuri aprobate de:			
Aviz DPO:			

V. CONSULTANȚĂ ȘI FORMARE PROFESIONALĂ

CONSULTANȚĂ - GDPR

Vă putem ajuta să respectați și să implementați cerințele Regulamentului General privind Protecția Datelor (GDPR) cu o metodologie simplă în patru pași pe care am denumit-o **"iQS GDPR Approach"**.

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.

Această metodologie este integrată într-un plan general. Serviciile noastre 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.

Pentru informații complete despre acest serviciu, mă puteți contacta pe
ion@ioniordache.com
https://ioniordache.com/

V. CONSULTANȚĂ ȘI FORMARE PROFESIONALĂ

CONSULTANȚĂ - SECURITATE

iQuality Services

Metodologia de consultanță de securitate "Security Management Solutions" (SMS) propusa de **iQuality Services** este o alternativa la modelul traditional de management al securitatii ce ofera o serie de soluții la problemele companiilor de securitate.

Licentieri/autorizari (consultanta in intocmirea dosarelor)

Aceste servicii de consultanta sunt furnizate in contextul in care clientii nostrii doresc sa se licentieze/autorizeze in activitati specifice securitatii private, reglementate atat de catre IGPR cat si de IGSU respectiv:

- Licențierea societăților specializate în domeniul pazei și protecției
- Licențierea societăților specializate în domeniul sistemelor de alarmare împotriva efracției
- Autorizarea persoanelor care efectuează lucrări în domeniul apărării împotriva incendiilor:
- proiectarea sistemelor și instalațiilor de semnalizare, alarmare și alertare în caz de incendiu;
- instalarea și întreținerea sistemelor și instalațiilor de semnalizare, alarmare și alertare în caz de incendiu;
- proiectarea sistemelor și instalațiilor de limitare și stingere a incendiilor;
- instalarea și întreținerea sistemelor și instalațiilor de limitare și stingere a incendiilor, cu excepția celor care conțin anumite gaze fluorurate cu efect de seră;
- proiectarea sistemelor și instalațiilor de ventilare pentru evacuarea fumului și gazelor fierbinți, cu excepția celor de tip natural-organizat;
- instalarea și întreținerea sistemelor și instalațiilor de ventilare pentru evacuarea fumului și gazelor fierbinți.

Serviciile oferite constau in: informari cu privire la metodologiile de autorizare conform cerintelor legislatiei in vigoare, analiza si evaluarea conditiilor de licentiere/autorizare indeplinite de client in vederea pregatirii documentatiei de licentiere/autorizare, informare cu privire la continutul dosarului de licentiere/autorizare (incluxiv anexele acestuia), pregatirea profesionala specifica cerintelor legislative de licentiere/autorizare.

Proiecte tehnice pentru sistemele de securitate.

Aceste servicii de consultanta sunt furnizate clientilor nostrii de catre consultanti licentiati/autorizati in intocmirea proiectelor pentru:

- sisteme tehnice de detecție și semnalizare la efracție, control acces, TVCI și monitorizare;
- sisteme si instalatii de semnalizare, alarmare si alertare in caz de incendiu;
- sisteme si instalatii de limitare si stingere a incendiilor.

Serviciile oferite constau in: informari cu privire la cerintele legale ce trebuiesc indeplinite de aceste proiecte, realizarea efectiva a acestor proiecte conform legislatiei, normativelor si standardelor in vigoare.

Alegerea solutiilor tehnice de securitate electronica si/sau fizica

Aceste servicii de consultanta sunt furnizate clientilor nostrii de catre consultanti licentiati/autorizati și sunt furnizate in contextul in care clientii nostrii doresc sa implementeze o solutie de securitate prin utilizarea echipamentelor electronice de securitate si/sau a altor mijloace de protectie fizica (iluminat de siguranta, bariere mecanice, diferite tipuri de garduri etc.).

Serviciile oferite constau in alegerea celei mai bune solutii in:

- Controlul, admiterea si monitorizarea accesului (admitere acces pe baza de tastaturi cu cod, carduri, solutii biometrice, sisteme mecano-electrice de bariere si porti automate, sisteme de bariere antitero cu acționare hidraulică, pneumatică, electrică si control acces cu scanere X-Ray etc.)
- Sisteme de detectie/alarmare la efractie si monitorizare .
- Sisteme de Supraveghere Video, echipamente si solutii de inregistrare si gestionare video cu aplicatii in: supravegherea accesului în zone restrictionate, controlul traficului, controlul angajatilor, controlul mulțimilor, supravegherea parcarilor, supravegherea în banci, instituții guvernamentale, magazine, cazinouri, supravegherea reședințelor etc.
- Sisteme protectie perimetrala si detectie a intruziunilor (bariere cu infrarosu, bariere cu microunde, garduri etc.).
- Iluminatul de securitate (iluminatul de securitate permite personalului de paza si interventie sa observe activitatile din perimetrul asigurat minimalizand, in acelasi timp, prezenta lor. Un iluminat deadecvat si ineficient nu va descuraja intrarile neautorizate ci va crea premisele pentru acest lucru).
- Sisteme si instalatii de semnalizare, alarmare si alertare in caz de incendiu (integrarea acestora cu alte sisteme de control al cladirii).
- Sisteme si instalatii de limitare si stingere a incendiilor (integrarea acestora cu alte sisteme de control al cladirii).

Pentru informații complete despre acest serviciu, mă puteți contacta pe ion@ioniordache.com

https://ioniordache.com/

Managementul proiectelor de securitate fizică

Aceste servicii de consultanta sunt furnizate in contextul in care clientii nostrii accepta si inteleg importanta managementului de securitate fizică pe care le desfasoara si doresc sa faca acest lucru utilizand o metodologie moderna de management al proiectelor.

Serviciile oferite constau in consultanta si sprijin direct in urmatoarele grupe de procese:

1. initiere;
2. planificare;
3. executie;
4. monitorizare si control;
5. incheierea.

FORMAREA PROFESIONALĂ - GDPR

RQM CERT, furnizor de formare profesionala organizează în România atât cursuri acreditate de Autoritatea Națională pentru Calificări (ANC) în baza Standardelor Ocupaționale și a Programelor Cadru cât și cursuri ca provider pentru PECB („PECB Group Inc.“) care este un organism internațional de educație și certificare în conformitate cu ISO/IEC 17024 pentru programele de certificare a personalului.

https://rqmcert.com

Responsabil cu protecția datelor cu caracter personal

(Cod COR: 242231)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Cursul este recomandat persoanelor desemnate de organizațiile din sectorul public și/sau privat ca Responsabil cu Protectia Datelor cu Caracter Personal (DPO) conform cerințelor GDPR.

https://rqmcert.com

GDPR - Foundation

Certificat de absolvire eliberat de **PECB**.

Curs de formare introductiv care vă permite să înțelegeți conceptele de bază și cerințele GDPR.

- Înțelegeți conceptele de bază și componentele protecției datelor.
- Înțelegeți principiile, provocările, problemele de protecție a datelor și importanța unui responsabil cu protecția datelor, a unui operator și a unui procesator.
- Înțelegeți conceptele, abordările, metodele și tehnicile pentru protecția eficientă a datelor.

https://rqmcert.com

GDPR - Certified Data Protection Officer

Certificat de absolvire eliberat de **PECB**.

Cursul de formare vă permite să dobândiți cunoștințele și abilitățile necesare și să dezvoltați competența de a îndeplini rolul Responsabilului cu Protecția Datelor într-o implementare a programului de conformitate cu GDPR.

După ce ați trecut cu succes examenul, puteți solicita acreditarea ca PECB Certified Data Protection Officer.

FORMAREA PROFESIONALĂ - SECURITATE

În România, ocupațiile din domeniile sistemelor de securitate private și apărării împotriva incendiilor se află pe ˝Lista profesiilor și ocupațiilor pentru care există cerințe speciale la organizarea pregătirii profesionale˝ iar cursurile de formare profesională sunt organizate de către **RQM CERT**, furnizor de formare profesionala acredita de Autoritatea Națională pentru Calificări (ANC) în baza Standardelor Ocupaționale și a Programelor Cadru avizate de către Inspectoratul General al Poliției Române (I.G.P.R.) și/sau Inspectoratul General pentru Situații de Urgență (I.G.S.U.)

Certificatele de competențe profesionale, eliberate de către Ministerul Muncii și Protecției Sociale și Ministerul Educaţiei prin furnizorii de formare profesională acreditați de Autoritatea Națională pentru Calificări (ANC) fac parte din categoria actelor oficiale și sunt recunoscute la nivel național iar dacă sunt apostilate în cadrul instituției prefectului și traduse sunt recunoscute și la nivel internațional.


ROMÂNIA

Seria N Nr. 0079

CERTIFICAT
DE ABSOLVIRE

https://rqmcert.com

Manager de securitate
(Cod COR: 121306)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educaţiei.

Activitatea managerului de securitate cuprinde: Securitatea Fizică * Securitatea personalului * Securitatea documentelor clasificate * Securitatea Industrială * Securitatea Sistemelor Informatice și de Comunicații (INFOSEC) și Instruirea și educația preventivă a personalului.

https://rqmcert.com

Evaluator de risc la securitatea fizică
(Cod COR: 242115)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educaţiei.

Analiza de risc la securitatea fizică constituie fundamentul adoptării măsurilor de securitate a obiectivelor, bunurilor şi valorilor prevăzute de lege, transpuse în planul de pază şi proiectul sistemului de alarmare. Obținerea certificatului de absolvire vă va permite să solicitați înscrierea în Registrul Naţional al Evaluatorilor de Risc la Securitate Fizică (RNERSF)

FORMAREA PROFESIONALĂ - SECURITATE

RQM CERT

furnizor de formare profesionala acredit de Autoritatea Națională pentru Calificări (ANC)

Proiectant sisteme de securitate

(Cod COR: 215119)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Modulul I - Proiectarea sistemelor tehnice de detecție și semnalizare la afracție și control acces, TVCI și monitorizare/Proiectarea sistemelor tehnice de detecție și alarmare la incendiu.

Modulul II - Proiectarea instalațiilor pentru stingere automată a incendiului/Proiectarea sistemului de control și evacuare a fumului și gazelor fierbinți din construcții și de limitare a propagării fumului în caz de incendiu.

Tehnician Sisteme de Detecție, Supraveghere Video, Control Acces

(Cod COR: 352130)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Obținerea certificatului de absolvire este obligatorie dacă intenționați să vă licențiați/autorizați propria companie la I.G.P.R./I.G.S.U. sau să lucrați în cadrul unor companii licențiate de I.G.P.R. pentru ˝instalarea, modificarea, monitorizarea, întreținerea și utilizarea sistemelor de alarmare împotriva efracției˝ sau autorizate de I.G.S.U. pentru ˝instalarea și întreținerea sistemelor și instalațiilor de semnalizare, alarmare și alertare în caz de incendiu˝.

Tehnician sisteme și instalații de limitare și stingere a incendiilor

(Cod COR: 742106)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Obținerea certificatului de absolvire este obligatoriu dacă intenționați să vă autorizați propria companie la I.G.S.U. sau să lucrați în cadrul unor companii autorizate de I.G.S.U. pentru ˝instalarea si intretinere a sistemelor si instalatiilor de limitare si stingere a incendiilor, cu exceptia celor care contin anumite gaze fluorurate cu efect de sera.˝

VI. BIBLIOGRAFIE

- **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 privind evaluarea de impact al Grupului de Lucru art. 29.**
- **Decizia nr. 174 din 18 octombrie 2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal.**
- **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 şi răspunsuri cu privire la aplicarea Regulamentului (UE) 2016/679, A.N.S.P.D.C.P.**
- **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).
- **Metodologia "iQS GDPR Approach",** Ion Iordache.
- **Responsabil cu protecția datelor cu caracter personal** (COR 242231), curs specializare, Ion Iordache.

Autori:

Ion Iordache, BEc

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

www.ioniordache.com ion@ioniordache.com

Mihai Dantis, MEng

Lead auditor în domeniul securității informațiilor și DPO certificat international cu experiență dovedită de peste 20 de ani în managementul proiectelor, implementarea și auditul sistemelor de securitate informațională.
Specialități/certificări: Audit: ISO 27001, ISO 20000, ISO 22301, ISO 27032, ISO 27035, ISO 27701, ISO 31000, GDPR, NIS.

mihai@dantis.ro

DATA ȘI VERSIUNEA 01.09.2021, V.00

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.

RQM Certification

RQM Certification cu sediul în Timișoara este un furnizor de formare profesională cu o echipă excepțională de specialiști cu mare experiență în formare profesională, servicii de evaluare și audit. Compania are expertiză în domeniul sistemelor de management al calității, al mediului, al sănătății și securității la locul de muncă, al automobilelor, al securității fizice, al informațiilor și al serviciilor IT. Programele de formare sunt concepute pentru a sprijini învățarea activă în conformitate cu standardele internaționale și cerințele specifice fiecărei industrii.

www.rqmcert.com
office@rqmcert.com
+40 356 173 020