ARTS
Arta de a trăi în siguranță
Asociație de utilitate publică

&

Profesioniștii între ei
Conferințele Media Makers

Conferința
EVALUAREA RISCULUI – CELE MAI BUNE PRACTICI
Ediția a III-a

București, 29 martie 2018

Hotel Hilton Athénée Palace, Sala Regina Maria

Panel I

RISCUL DE SECURITATE ÎN CONTEXTUL GENERAL DE RISC

Managementul riscului

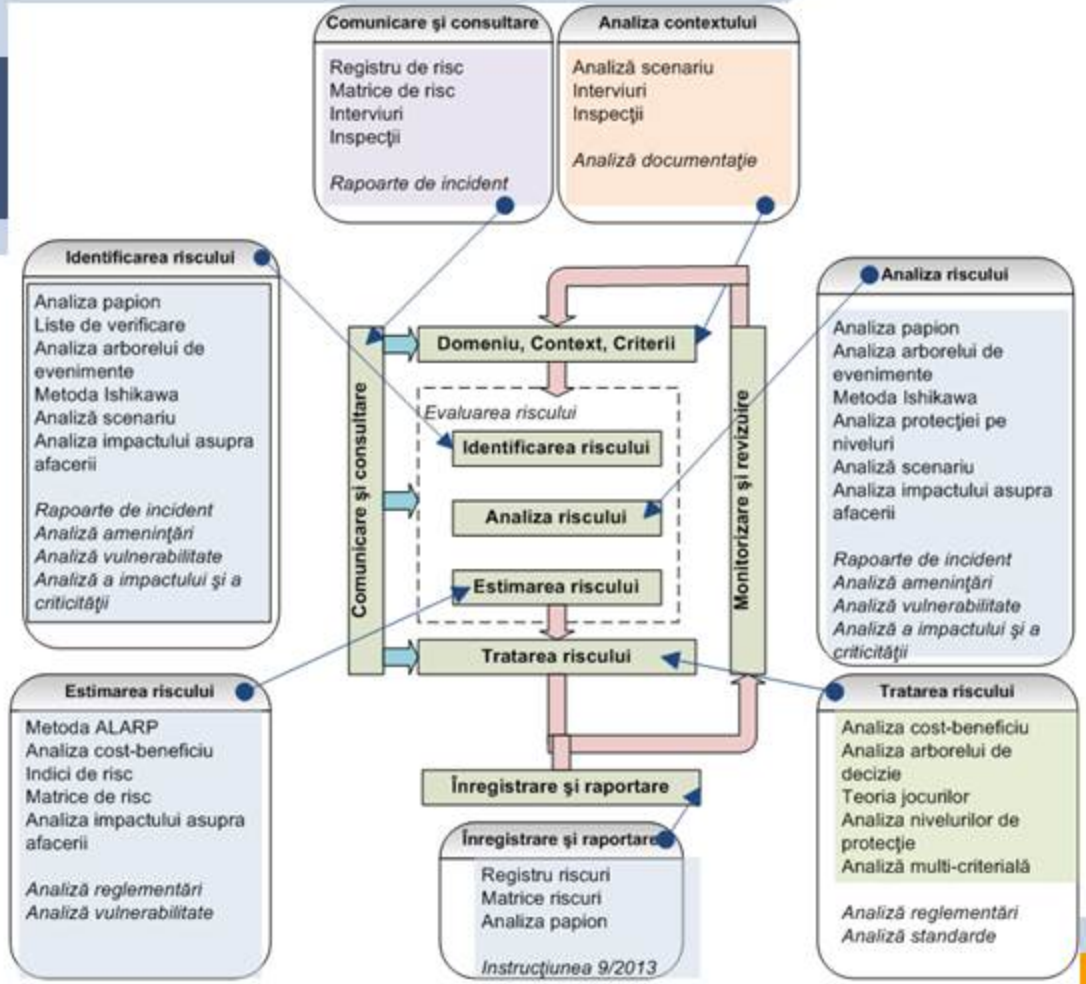
- Proces fundamental
- Securitate vs. Operațional
- Securitate fizică vs. securitatea informației, continuitate, hazarduri
- Noțiunea de reziliență
- Evaluatorul de risc

Analiza riscului de securitate

- Tehnici de analiză a riscului
- Evaluări de securitate
- Limitări in aplicarea mijloacelor de control
- Calitatea rapoartelor de evaluare

Tehnici de analiza a riscului de securitate

- Tehnici din SR/ISO 31010 adaptate
- *Metode din teoria riscului de securitate*
- *Istoricul incidentelor*



Securitatea informatiei si GDPR

- GDPR
- securitatea cibernetică a sistemelor de securitate fizică
- securitatea fizică a sistemelor de securitate cibernetică

Panelişti şi subiecte

- **Rene Pasculescu** – ASIS, Civitas
- **Marius Georgescu** – ASIS, Petrom
- **Andrei Hohan** – Fiatest, ASRO

- ASIS International Romania
- Evaluarea riscului in viziunea ASIS Intl
- Riscul pe lanțul de aprovizionare
- Aspecte prectice in aplicarea Instructiunii 9/2013
- Limitările și riscurile induse de GDPR
- Securitatea cibernetică a sistemelor de securitate fizică
- Tehnici de evaluare a riscului de securitate
- Calitatea rapoartelor ARSF și așteptări
- Viitorul profesiei de evaluator de risc de securitate fizică

ARIES & Profesioniștii între ei
Conferințele Media Makers

ASIS International

- Pune accent major pe educatie, oferind cursuri si seminarii cu diverse teme, specifice industriei de securitate (cursuri cu certificat: Risk, Threat and Vulnerability assessment si Executive Protection)
- Acorda trei dintre cele mai cunoscute certificari, la nivel global: Certified Protection Professional (CPP), Physical Security Professional (PSP) si Professional Certified Investigator (PCI)
- Organizeaza conferinte globale (ASIS Europe, ASIS Global, ASIS NY)
- Standarde (Risk Assessment, Resilience, Business Continuity, etc)
- Ofera burse de studiu (In 2017 au fost acordate 7 burse pentru Master in Security Management la universitati de prestigiu din US)
- Programe de mentoring
- www.asisonline.org

ASIS Romanian chapter

- A aparut in 2011
- Are 49 membri
- Are un board format din 4 membri
- Au loc intalniri de cel putin 6 ori pe an
- Urmareste strategia ASIS International
- Ofera suport pentru obtinerea certificarilor CPP si PSP
- Exista o taxa anuala care se plateste direct la ASIS International

Abordarea riscului din perspectiva ASIS

- ASIS promoveaza o perspectiva largita asupra security risk managementului, la nivel de intreprindere, cu focus pe toate componentele unei intreprinderi: resurse umane, asset-uri, informatii si procese.
- ESRM (Enterprise Security Risk Management) este, in viziunea ASIS, parte integranta a ERM (Enterprise Risk Management) si a SRM (Strategic Risk Management).
- Ca si ERM, ESRM se concentreaza pe managementul riscului la nivelul proceselor companiilor, dar din perspectiva securitatii.
- Prin ESRM creste semnificativ rolul managerului de securitate, ajungand sa fie un business driver in cadrul top managementului.

ESRM – Enterprise Security Risk Management

- ESRM este o filozofie de management care implica atat securitatea fizica cat si cyber security, information security sau investigations.

- Rolul managerului de securitate in cadrul ESRM este de a gestiona riscurile care pot afecta o intreprinde, acest lucru fiind facut intr-un strans parteneriat cu liderii din top management care raspund de integritatea aseturilor, a persoanelor, a informatiilor sau de continuitatea proceselor din responsabilitea lor.

- ESRM implica educarea liderilor din top management, astfel incat sa aiba o imagine realista a posibilului impact cauzat de riscurile indentificate, prezentand posibile strategii de diminuare a acestui impact, iar apoi participand la implementarea unor strategii/optiuni, alese in concordanta cu nivelul de toleranta la risc acceptat de intreprindere, care este strans legat de strategia de business a intreprinderii pe termen lung.

Procesul specific ESRM

- Se identifica si prioritizeaza asset-urile care trebuiesc protejate in cadrul unei intreprinderi, aici fiind incluse atat asset-urile fizice cat si informatiile sau resursele umane.

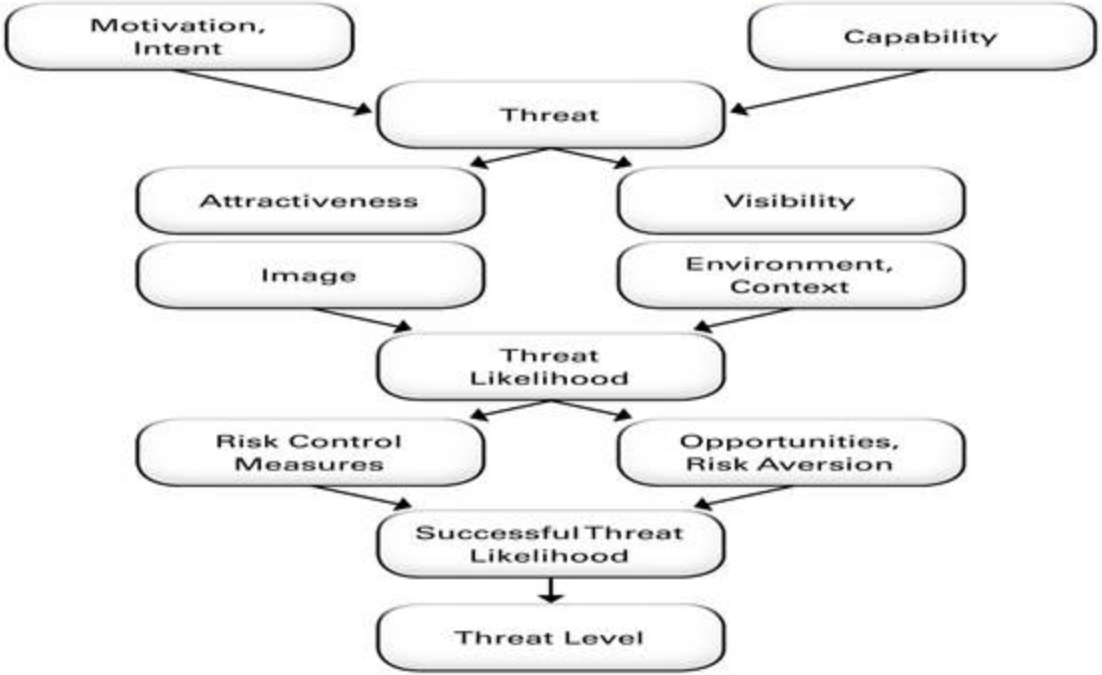
- Se identifica si prioritizeaza posibillele amenintari la adresa intreprinderii, atat cele existente cat si cele care pot aparea, si riscul asociat acestor amenintari (detaliere in slide-ul urmator).

- Se iau masurile necesare, corespunzatoare si realistice pentru a proteja si diminua cele mai importante amenintari si riscuri.

- Se monitorizeaza incidentul, se face o analiza post-eveniment si se aplica lectiile invatate , pentru a imbunatatii programul.

- ESRM acopera toate zonele de security si este un proces iterativ, care ajuta la dezvoltarea politicilor si a procedurilor de securitate, astfel incat acestea sa evolueze in timp si sa se transforme intr-un adevarat program de management.

ASIS Risk Assessment Standard – Determining threat levels



Strategic Risk Management Perspective

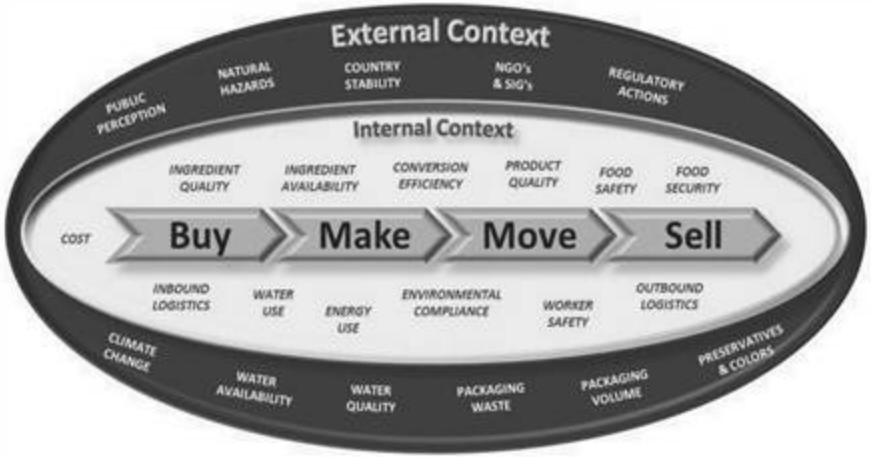
Supply chain Risk Management

- Riscuri interne, asociate proceselor si controlului intern.
- Riscuri externe:

- Riscuri externe intreprinderii, dar care sunt asociate lantului de aprovizionare.

- Riscuri externe atat intreprinderii cat si lantului de aprovizionare, dar care pot afecta major procesele de productie (dezastre naturale, vreme nefavorabila, instabilitate politica si alti factori asimilati modelului STEEP).

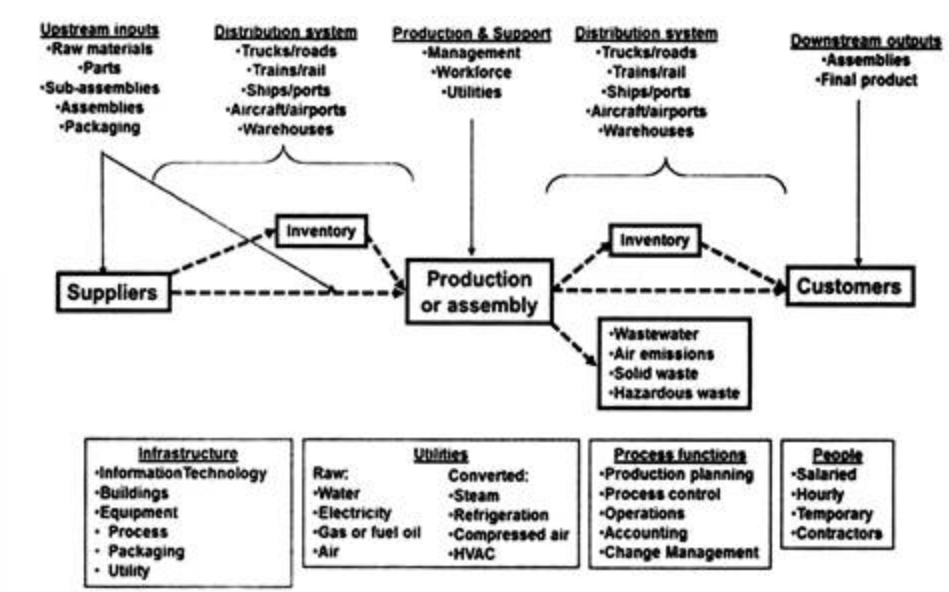
Supply chain Risk Management



- Supply chain risks fall into two categories:
  - External context, which are out of our direct control but must be factored into business planning
  - Internal context, which are within our direct control and must be factored into operations
- Different aspects of some risks may fall into both categories

Example of Internal and External Contexts for a Food/Beverage Company

Supply chain Risk Management



Notional Supply-Chain Process Flows

Evaluarea de risc - Istoric si provocari

Industria de petrol si gaze - obiective complexe

- ~ 12.000 km conducte
- ~ 1.000 km drumuri petroliere
- ~ 8.600 sonde
- ~ parcuri de productie, depozite, alte facilitati

- Rafinărie
- Peste 500 de statii de distributie carburanti

*peste **2800** obiective evaluate*

Grup de sonde

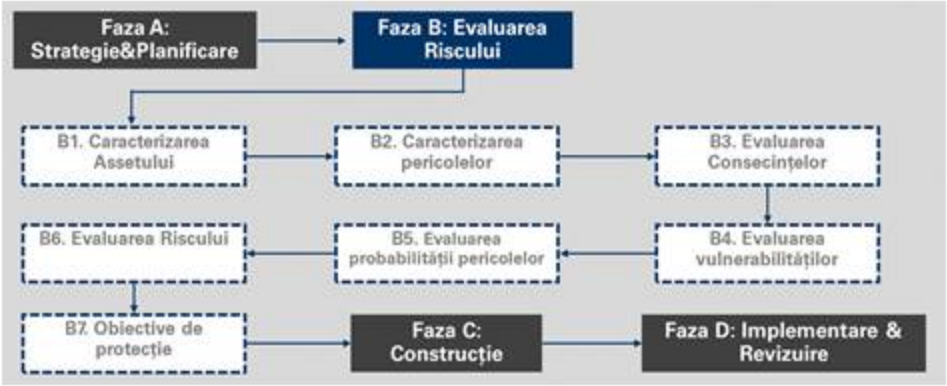
Grup de conducte

Grup statii de transformare

Obiective individuale

Evaluarea de risc - Abordare

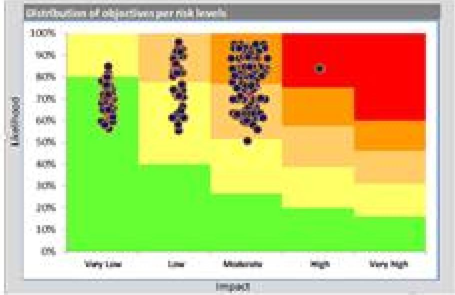
- Metodologie integrata de securitate bazata pe Risc si Performanta - PRISM®

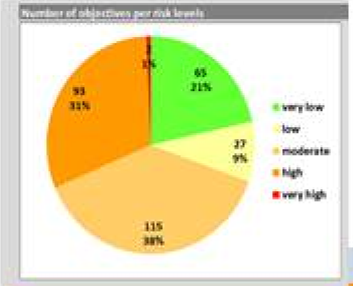


Evaluarea de risc - Abordare

- Elaboare documentatie (chestionare culegere date, tool evaluare, tipizate rapoarte)

Ref	Threat Assessment Score	Consequence Assessment Score	Vulnerability Assessment Score	Likelihood	Risk Score	Risk Level
1	9.00	20	8.33	55%	12	Very Low
2	12.00	60	10.17	77%	47	High
3	12.00	60	9.83	76%	46	High
4	12.00	20	7.67	69%	14	Very Low
5	9.50	60	10.67	67%	41	Moderate
6	12.00	60	9.83	76%	46	High
7	12.00	20	8.67	72%	15	Very Low
8	11.00	20	5.33	54%	11	Very Low
9	12.50	20	10.67	77%	16	Low
10	11.50	20	11.00	75%	15	Very Low
11	12.50	20	7.33	66%	14	Very Low
12	12.00	60	10.67	79%	48	High
13	12.00	60	8.33	71%	43	Moderate
14	12.50	60	9.67	77%	47	High
15	12.00	20	7.33	66%	14	Very Low
16	12.00	20	8.67	62%	13	Very Low
17	14.50	60	8.33	76%	46	High
18	12.00	20	7.67	69%	14	Very Low
19	12.00	20	10.67	79%	16	Low
20	12.00	20	7.67	69%	14	Very Low
21	12.00	20	11.33	81%	17	Low
22	12.00	20	9.83	76%	16	Low

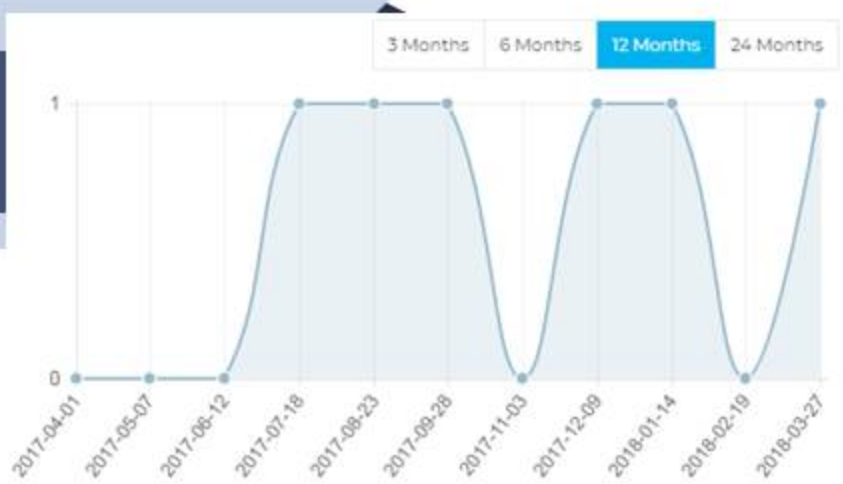




ARTS & Profesioniștii între ei
Conferințele Media Makers

Evaluarea de risc - Abordare

- Studiu al pietei de profil in vederea identificarii aplicatiilor software de evaluare a riscurilor la securitatea fizica
- Solutii pentru integrarea modulului de raportare a Incidentelor/ SRA/ Monitorizare implementare masuri/ Managementul Sistemelor Tehnice de Securitate intr-o platforma unica



Sisteme de securitate - Obiective individuale

Parcuri petroliere	Sonde	Transformatoare	Alte obiective
			
			
			

Concluzii

Grila 12?

Instructiunea 9 - promulgare/ prevederi/ termen aplicare…

Intrebari

Analiza de risc în contextul Regulamentului European privind Protecția Datelor Personale (GDPR)

Cerințele GDPR ⇔ Analiză risc

Art. 32: Securitatea prelucrării
(1) Având în vedere stadiul actual al dezvoltării, costurile implementării şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscul cu diferite grade de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul şi persoana împuternicită de acesta implementează măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc
Art. 25: Asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit
(1) Având în vedere stadiul actual al tehnologiei, costurile implementării, şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice pe care le prezintă prelucrarea, operatorul […] pune în aplicare măsuri tehnice şi organizatorice adecvate […] care sunt destinate să pună în aplicare în mod eficient principiile de protecţie a datelor […] şi a proteja drepturile persoanelor vizate.

Estimarea nivelului de impact

1) Neglijabil: persoanele vizate nu sunt afectate sau întâmpină probleme minore, care pot fi depășite fără probleme: timp consumat pentru reintroducerea informației, deranjare, iritare, etc.
2) Limitat: persoanele vizate pot întâmpina probleme semnificative, care pot fi depășite în ciuda unor dificultăți (costuri suplimentare, refuzul accesului la servicii, frică, neînțelegere, stres, daune fizice minore, etc.)
3) Semnificativ: persoanele vizate pot întâmpina probleme majore, pe care le pot depăși cu dificultăți majore (pierderea fondurilor, includerea pe liste de refuz al serviciilor esențiale, distrugerea proprietății, pierderea locului de muncă, chemarea în judecată, înrăutățirea stării de sănătate, etc.)
4) Maxim: persoanele vizate pot fi puse în fața unor consecințe semnificative sau ireversibile, pe care este posibil să nu le poată depăși (probleme financiare precum credite care nu pot fi plătite, incapacitatea de a munci, probleme psihologice sau fizice pe termen lung, deces, etc.)

Nivelul de impact poate fi modificat prin factori suplimentari:
-Date care identifică direct persoana
-Surse de risc semnificative
-Număr mare de interconectări sau destinatari

Exemplu de clasificare a impactului, în funcție de natura datelor

Categoria datelor cu caracter personal	Nivel de impact
DP accesibile public (de ex. in cărți de telefon, liste de adrese sau liste de selecție)	1
DP care necesită un interes legitim pentru acces (de ex. fișiere uz intern sau membrii unei liste de distribuție)	2
DP a căror dezvăluire neautorizată poate afecta reputația persoanei vizate (informații cu privire la venit, beneficii sociale, taxe sau amenzi)	3
DP a căror dezvăluire, modificare, pierdere sau distrugere pot afecta existența sau sănătatea, libertatea sau viața persoanelor vizate (de ex. informații privind apartenența la o instituție, sentințe, evaluări, date cu privire la sănătate, datorii, investigații legale)	4

Art. 35: Evaluarea impactului asupra protecţiei datelor

(1) […] în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal.[…]

(3) Evaluarea impactului asupra protecţiei datelor […] se impune mai ales în cazul:

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

b)prelucrării pe scară largă a unor categorii speciale de date[…] sau a unor date cu caracter personal privind condamnări penale şi infracţiuni, menţionată la articolul 10; sau

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

Art. 35: Evaluarea impactului asupra protecţiei datelor

(7)Evaluarea conţine cel puţin:
a)o descriere sistematică a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;
b)o evaluare a necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri;
c)o evaluare a riscurilor pentru drepturile şi libertăţile persoanelor vizate menţionate la alineatul (1); şi
d)măsurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor cu caracter personal şi să demonstreze conformitatea cu dispoziţiile prezentului regulament, luând în considerare drepturile şi interesele legitime ale persoanelor vizate şi ale altor persoane interesate.

“Discuții

Vă mulţumesc!

"I'm applying for the Information Security position.
Here is a copy of my resumé, encoded, encrypted and shredded."

ARTS & Profesioniștii între ei
Conferințele Media Makers