www.privacyromania.ro

29-30 Ianuarie 2021

PRIVACY ROMANIA 2021

Conferința Națională de Confidențialitate și Protecția Datelor

CONFLUENTE GDPR – ERSF

ASCPD

Asociația Specialiștilor în Confidențialitate și Protecția Datelor

Viorel PETCU

Vicepreședinte ANERSFR

Asociația Națională a Evaluatorilor de Risc

ANERSF

Confluențe GDPR - ERSF

Conferința Națională de Confidențialitate și Protecția Datelor

PR!VACY ROMANIA 2021

Viorel Petcu

29 Ianuarie 2021

ANERSF

Confluențe GDPR & ERSF

- Ce este ***Evaluarea riscurilor la securitatea fizică ?...***
- ***GDPR*** – o privire de ansamblu
- ***Confluențe*** ERSF - GDPR

ANERSF

Evaluarea Riscurilor la Securitatea Fizică

ANERSF

Evaluarea riscurilor la securitatea fizică

EN 16763: 2017 Servicii pentru sisteme de securitate la incendiu și sisteme de securitate / Planificare: ***Stabilirea specificațiilor obiectivelor de protecție și a domeniului de aplicare a sistemului (sistemelor) pe baza riscurilor identificate și a condițiilor limită cunoscute.***

Toate organizațiile se confruntă cu riscuri. Provocarea constă în a determina care este pragul de acceptabiltate a riscului în limitele rentabilității.

…Trebuie făcute alegeri cu privire la compromisul dintre

***resursele necesare pentru a genera produse, profituri și cote de piață*,**

și *mijloacele de control necesare pentru a le proteja*, *respectând în același timp legile aplicabile*

ANERSF

Evaluarea riscurilor la securitatea fizică - Contextul legal în Romania

Legea 333/2003, HG301/2012, Instrucțiunea 9/2013, HG 1002/2015

- **Adoptarea măsurilor de securitate …….. se realizează pe baza unei analize de risc la securitatea fizică (HG 301 Art 2)**
- **Elaborarea analizei de risc la securitate fizică se face potrivit instrucţiunilor emise de MAI. (HG 301 Art 2 Anexa)**
- **(3) Adoptarea măsurilor de securitate prevăzute la alin. (1) se realizează în conformitate cu analiza de risc efectuată …. prin structuri de specialitate sau prin experți abilitați, care dețin competențe profesionale dobândite pentru ocupația de evaluator de risc la securitatea fizică (I 9 Art 1)**
- **(2) Analiza de risc la securitatea fizică constituie fundamentul adoptării măsurilor de securitate ….., transpuse în planul de pază şi proiectul sistemului de alarmare.**

ANERSF

Evaluarea de risc la securitatea fizică ...

... Este, înainte de toate este o **măsură preventivă si pregătitoare pentru contracararea riscurilor la securitatea fizică:**

Implică **analiza proceselor de bussines** și ”identificarea, caracterizarea și evaluarea **resurselor** organizației, înțelese ca orice are valoare pentru organizație, în domeniul de aplicare al evaluării.

Nivelul riscului este determinat în etapa de analiză pornind în general de la analiza **amenințărilor** și a **oportunităților**, analiza **vulnerabilităților** și a capabilității, respectiv analiza **impactului** și a **criticității***.

Nivelul de risc, exprimat prin plauzibilitate si consecințe este ponderat prin nivelul de eficacitate al mijloacelor de control al riscului aplicate și funcționale”*.

... Este o **obligație legală**, însă este mai mult decât auditarea conformității cu cerințele legale.

**Stelian Arion, TENDINȚE ÎN EVALUAREA RISCULUI DE SECURITATE , Revista Alarma Nr. 1/2018*

ANERSF

GDPR

Regulamentul (UE) 2016/679 General privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date

Regulamentul pune accent pe transparența față de persoana vizată și responsabilizarea operatorului de date față de modul în care prelucrează datele cu caracter personal.

ANERSF

Regulamentul (UE) General privind Protecția Datelor -RGPD 2016/679

Legislatia aplicabila unitar pe intreg teritoriul UE incepand cu 28 Mai 2018

- ✓ **Transparență față de persoana vizată** și responsabilizarea operatorului de date față de modul în care prelucrează datele cu caracter personal
- ✓ Stabilește o serie de garanții specifice pentru a se proteja cât mai eficient **viața privată a minorilor**, în special în mediul online
- ✓ Introduce noi drepturi: **dreptul de a fi uitat, dreptul la portabilitatea datelor și dreptul la restricționarea prelucrării**.
- ✓ Introduce **sancțiuni severe** pentru operatorii de date cu caracter personal care nu respectă aceste reguli
- ✓ Dreptul persoanelor vizate de a fi **despăgubite** pentru orice prejudiciu cauzat de operatorul de date dar și de procesator.

ANERSF

Regulamentul (UE) General privind Protecția Datelor -RGPD 2016/679

GDPR stabilește niște reguli de conduită pentru toate departamentele unei companii.

- ✓ **IT** – *Instituirea măsurilor de securitate cibernetică. Alertarea autorităților în cazul unei breșe de securitate (care duce la compromiterea datelor cu caracter personal).*
- ✓ **Resurse umane** – *mecanisme de prelucrare a datelor cu caracter personal ale angajaților și în procesul de recrutare, reglementarea procesului de concediere; inclusiv informațiile medicale ale angajaților, diplomele de studii etc.*
- ✓ **Juridic** – *modificarea documentației prin intermediul căreia se colectează date personale (formulare, solicitări, acte) în vederea obținerii consimțământului în mod express și fără echivoc;*
- ✓ **Marketing** – *instrucțiuni clare privind modul în care se efectuează comunicarea cu clienții companiei sau cu potențialii clienți.*
- ✓ **Securitate** – *înregistrări de supraveghere video, pontaj, monitorizare GPS, date biometrice, etc. vor fi prelucrate în acord cu prevederile GDPR;*

ANERSF

Principiile GDPR

- ✓ **Legalitate, echitate și transparență**
- ✓ Limitarea la **scopul prelucrării**
- ✓ **Reducerea la minimum a datelor -** adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate.
- ✓ Asigurarea **acurateții** și **actualizării** datelor cu caracter personal
- ✓ **Accesul** persoanei vizate la datele personale

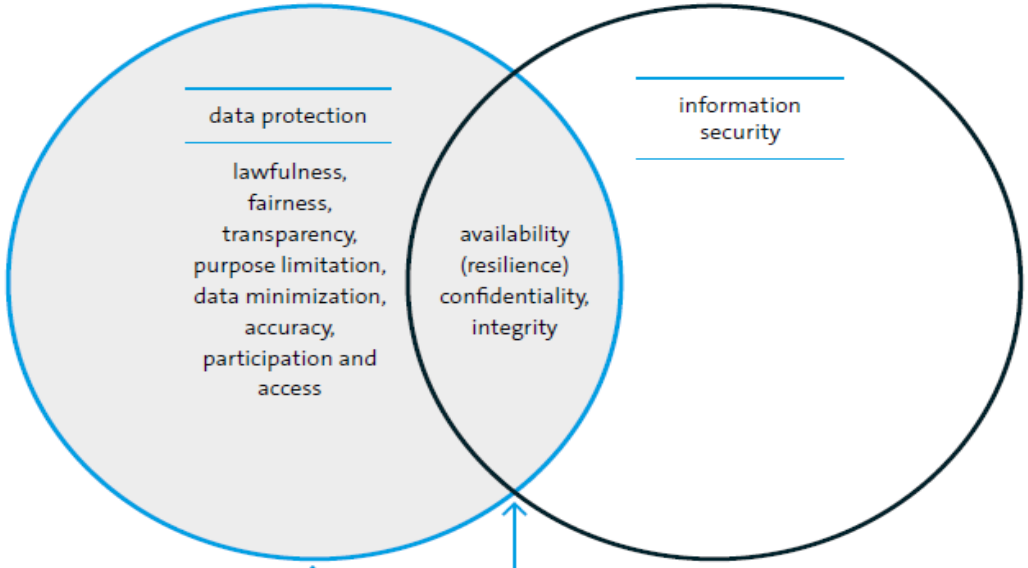
- ✓ Principiul **responsabilității**

ANERSF

Confluențe ERSF & GDPR

ANERSF

Principiile GDPR



Data Protection Impact Assessment – GDPR Art. 35

Security of Processing – GDPR Art. 32

security of processing

data protection impact assessment

Risk level for the rights and freedoms of data subjects	=	likelihood	×	severity (=potential damage)

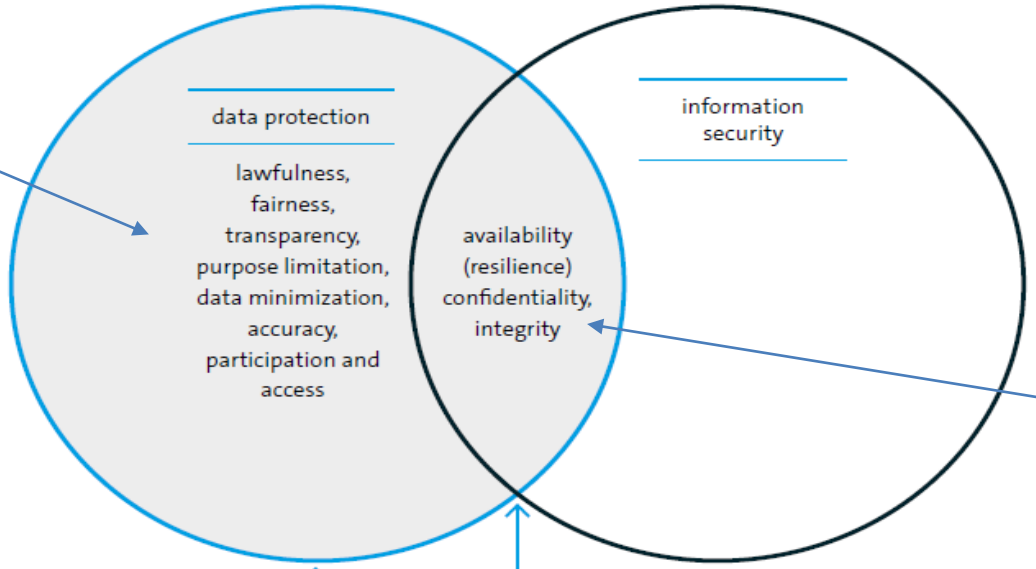
"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying **likelihood** and **severity** for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."

Sursa: Bitkom 2017 Risk Assessment & Data Protection Impact Assessment

ANERSF

GDPR & ERSF

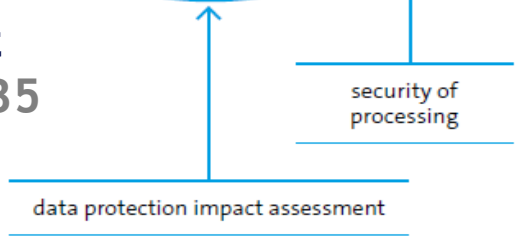
Datele utilizate



Mijloacele de control

Data Protection Impact Assessment – GDPR Art. 35

Security of Processing - GDPR Art. 32



Metodologia

Sursa: Bitkom 2017 Risk Assessment & Data Protection Impact Assessment

ANERSF

Date personale utilizate (și) în securitatea fizică

În procesul de evaluari și, implicit, la implementarea măsurilor pentru controlul riscurilor la securitatea fizică sunt utilizate și date personale - aflate sub incidenta GDPR:

- *Imagini preluate si stocate in sistemele de supraveghere video*
- *Date biometrice pentru autentificarea in sistemele de control acces*
- *Fotografie si/sau CNP folosite la inregistrarea accesului*

Este in scopul ERSF analiza conformității prelucrării datelor cu caracter personal ?... NU - este alt domeniu!... Însă...

- ...măsurile necesare încadrării într-un nivel de risc la securitatea fizică acceptabil trebuie să se raporteze și la principiile GDPR:
  - *interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate *;*
  - *a fost realizată informarea prealabilă obligatorie, completă şi în mod explicit a angajaţilor*;*
  - *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*.*
- ...sunt necesare prevederi explicite în procedura de securitate referitoare la regulile de acces și utilizare a datelor personale în sistemele de securitate

* Art. 5 LEGEA nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679

ANERSF

Mijloace pentru asigurarea...

Măsurile tehnice și organizatorice implementate pentru controlul riscurilor la securitatea fizică contribuie la asigurarea **disponibilității (rezilienței)**, **confidențialității** și **integrității** datelor cu caracter personal

Măsuri tehnice : controlul accesului, detecția și alarmarea la efracție etc.

Măsuri organizatorice : reguli de acces la informațiile video stocate, reguli de înregistrare a accesului etc

Completitudinea, eficiența mijloacelor de **securitate fizică** care concură la asigurarea disponibilității (rezilienței) și confidențialității datelor personale procesate de organizație se evaluează prin **analiza de risc la securitatea fizică** ....

ANERSF

Datele personale și securitatea fizică

Dacă evaluatorul de risc la securitatea fizică nu are competențe în domeniul GDPR, este necesară colaborarea cu un specialist conformitatea prelucrării datelor personale, astfel încât măsurile propuse să se încadreze în limitele GDPR.

&

De asemenea, la auditul GDPR este necesară consultarea ERSF în vederea unei evaluări cantitative și calitative a datelor personale implicate în implementarea măsurilor și mijloacelor pentru controlul riscurilor la securitatea fizică.

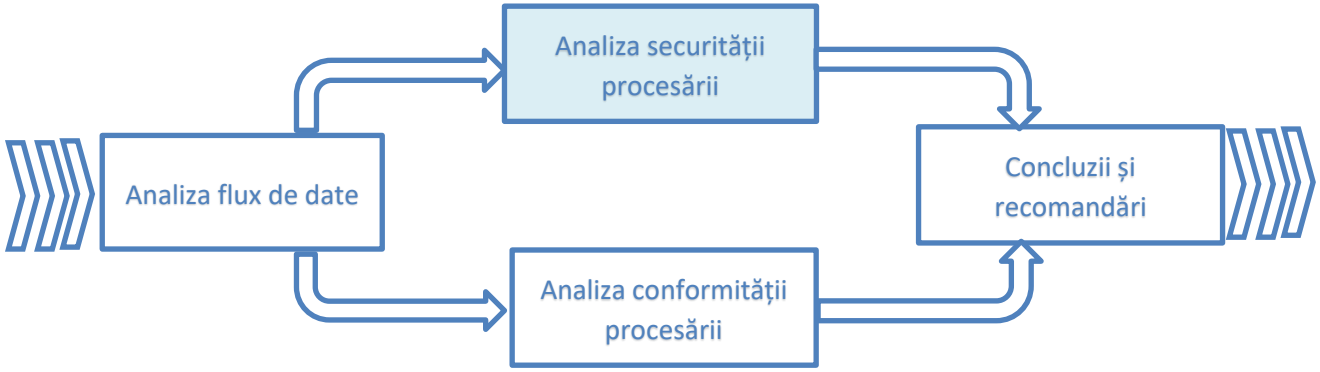
Implementarea unor măsuri (noi) de securitate fizică generează revizuirea (sau întocmirea dacă nu a fost deja realizată) analizei de impact asupra prelucrării datelor cu caracter personal.

ANERSF

Aspecte metodologice

Din interpretarea art. 30, para. 5 din Regulament, rezultă că obligația menținerii unei evidențe a activităților de prelucrare a datelor cu caracter personal incumbă, de principiu, organizațiile cu peste 250 de angajați sau atunci când prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date.

Evidența activităților de prelucrare a datelor cu caracter personal este indispensabilă pentru gestionarea protecției datelor. În acest sens, este necesară analiza proceselor de business, identificarea fluxurilor de prelucrarea a datelor cu caracter personal și maparea datelor personale în conformitate cu procesele.



Sursa: Ghid utilizare DECAN.pdf; https://onestsolutions.ro/ro#produse

ANERSF

Securitatea procesării datelor - Aspecte metodologice

Security of Processing - GDPR Art. 32

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying **likelihood** and **severity** for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."*

La evaluarea nivelului de securitate a procesării datelor personale sunt luate în considerare în special riscurile generate, accidental sau voit, de **accesarea**, **modificarea**, **transferul** (**divulgarea**) sau **ștergerea** (**distrugerea**) neautorizată a datelor cu caracter personal stocate, transmise sau prelucrate în alt mod.

Sursa: Bitkom 2017 Risk Assessment & Data Protection Impact Assessment

ANERSF

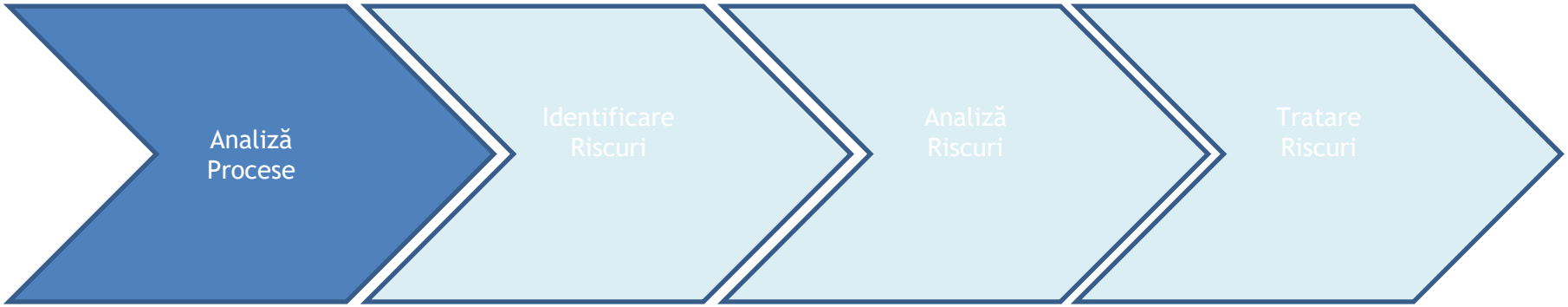
ERSF & GDPR - Aspecte metodologice

Security of Processing - GDPR Art. 32

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying **likelihood** and **severity** for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."*

ANERSF

ERSF & GDPR - Aspecte metodologice



Analiza proceselor de bussines

GDPR	• Active primare: datele personale ale persoanelor vizate • Identificarea activelor suport: suportul pe care aceste date sunt colectate/stocate/transferate (ersoane fizice, documente pe hârtie, transmiterea de documente pe suport de hârtie etc.) • Identificarea măsurilor tehnice și organizatorice existente • Evaluarea impactului (consecința materializării riscului)
ERSF	• Identificarea activelor relevante (oameni, valori materiale sau necorporale, informații), • Identificarea măsurilor tehnice și organizatorice existente • Evaluarea impactului (consecința materializării riscului)

ANERSF

ERSF & GDPR - Aspecte metodologice

Identificarea riscurilor

GDPR[1,2]

- Amenințări : acces nelegitim la date, modificare neautorizată, ștergere sau distribuire neautorizată
- Surse de amenințare :
  - Surse umane interne :Angajați, stagiari etc.
  - Surse umane externe: Beneficiarii datelor personale, terții autorizați etc
  - Surse non-umane: Malicious code (viruși, viermi etc.), dezastre naturale, animale etc.
- Identificarea măsurilor tehnice și organizatorice existente
- Evaluarea impactului : Impact general, Impact fizic, Impact material

ERSF[3]

Categorii și surse de amenințare: Furt (hoț intern, hoț extern, ...), Agresiune (vandal, harțuitor etc)
Analiza scenariilor de amenințare (pătrundere neautorizată în zone protejate, agresiune, vandalism etc.)

- Identificarea măsurilor tehnice și organizatorice existente
- Evaluarea impactului : Impact general, Impact fizic, Impact material

[1] *Bitkom 2017 Risk Assessment & Data Protection Impact Assessment*
[2] *Ghid utilizare DECAN.pdf; https://onestsolutions.ro/ro#produse*
[3] *MATRISK, http://www.matrisk.ro/download/TUTORIAL%20Matrisk%202017.pdf*

ANERSF

ERSF & GDPR - Aspecte metodologice

Analiza și cuantificarea riscurilor

Risk level for the rights and freedoms of data subjects = likelihood × severity (=potential damage)

...Utilizarea **plauzibilității** și a potențialelor **consecințe** pentru cuantificarea riscului este o tehnică folosită atât la estimarea riscului la securitatea fizică[1], cât și la evaluarea conformității securității prelucrării datelor cu caracter personal[2].

[1] Ghid utilizare DECAN.pdf; https://onestsolutions.ro/ro#produse
[2] Viorel Petcu, MATRISK, Keeping Security Secure, EURALARM SYMPOSIUM, Bucharest, 2018

ANERSF

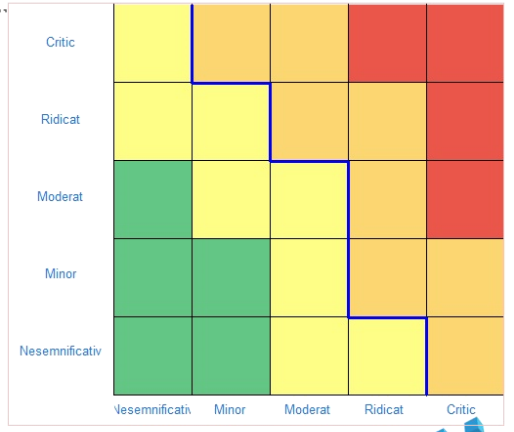
Aspecte metodologice

Security of Processing - GDPR Art. 32

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying **likelihood** and **severity** for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."[1]

Risk level for the rights and freedoms of data subjects	=	likelihood	×	severity (=potential damage)

...Utilizarea **plauzibilității** și a potențialelor **consecințe** pentru cuantificarea riscului este o tehnică folosită atât la estimarea riscului la securitatea fizică [2], cât și la evaluarea conformității securității prelucrării datelor cu caracter personal [3].



[1] *Bitkom 2017 Risk Assessment & Data Protection Impact Assessment*
[2] *Viorel Petcu, MATRISK, Keeping Security Secure, EURALARM SYMPOSIUM, Bucharest, 2018*
[3] *Ghid utilizare DECAN.pdf; https://onestsolutions.ro/ro#produse*

ANERSF

~~Influențe~~ Confluențe GDPR - ERSF

Evaluarea de risc la securitatea fizică este o componentă a **managementul riscurilor la securitatea fizică**, un proces continuu care urmărește, de asemenea, echilibrul între resursele necesare pentru a genera produse, profituri și cote de piață, și mijloacele de control necesare pentru a le proteja și pentru a se asigura respectarea legilor aplicabile.

Protecția datelor personale este un proces continuu, care vizează echilibrul între interesul legitim la viața privată a individului și interesele legitime ale altor indivizi sau organizații.

Evaluarea de risc la securitatea fizică și **conformitatea prelucrării datelor personale cu prevederile GDPR** sunt demersuri care se **sprijină reciproc** în favoarea **siguranței** și **securității** individului și a **dreptului la viață privată**.

ANERSF

ASOCIAȚIA NAȚIONALĂ A EVALUATORILOR DE RISC LA SECURITATEA FIZICĂ DIN ROMANIA

www.anersf.ro

Viorel Petcu

General Manager
ONEST SOLUTIONS
Vicepresedinte ANERSFR

OSPA WINNER 2016