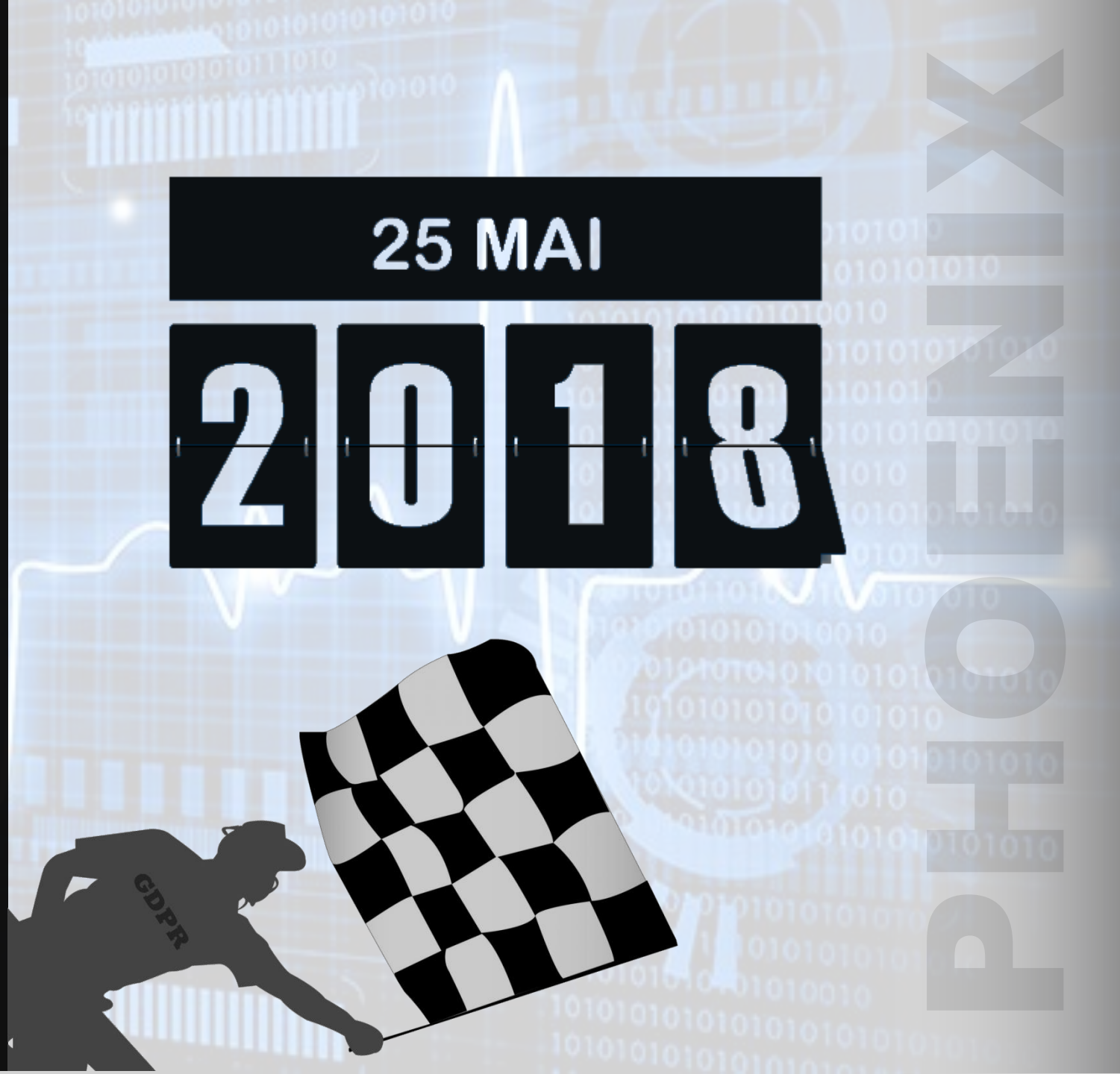
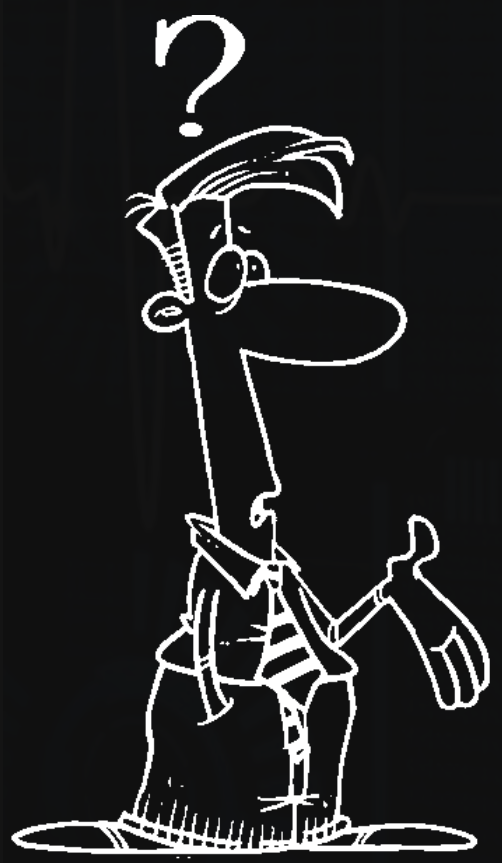
REGULAMENT nr. 679/2016
privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date

GDPR

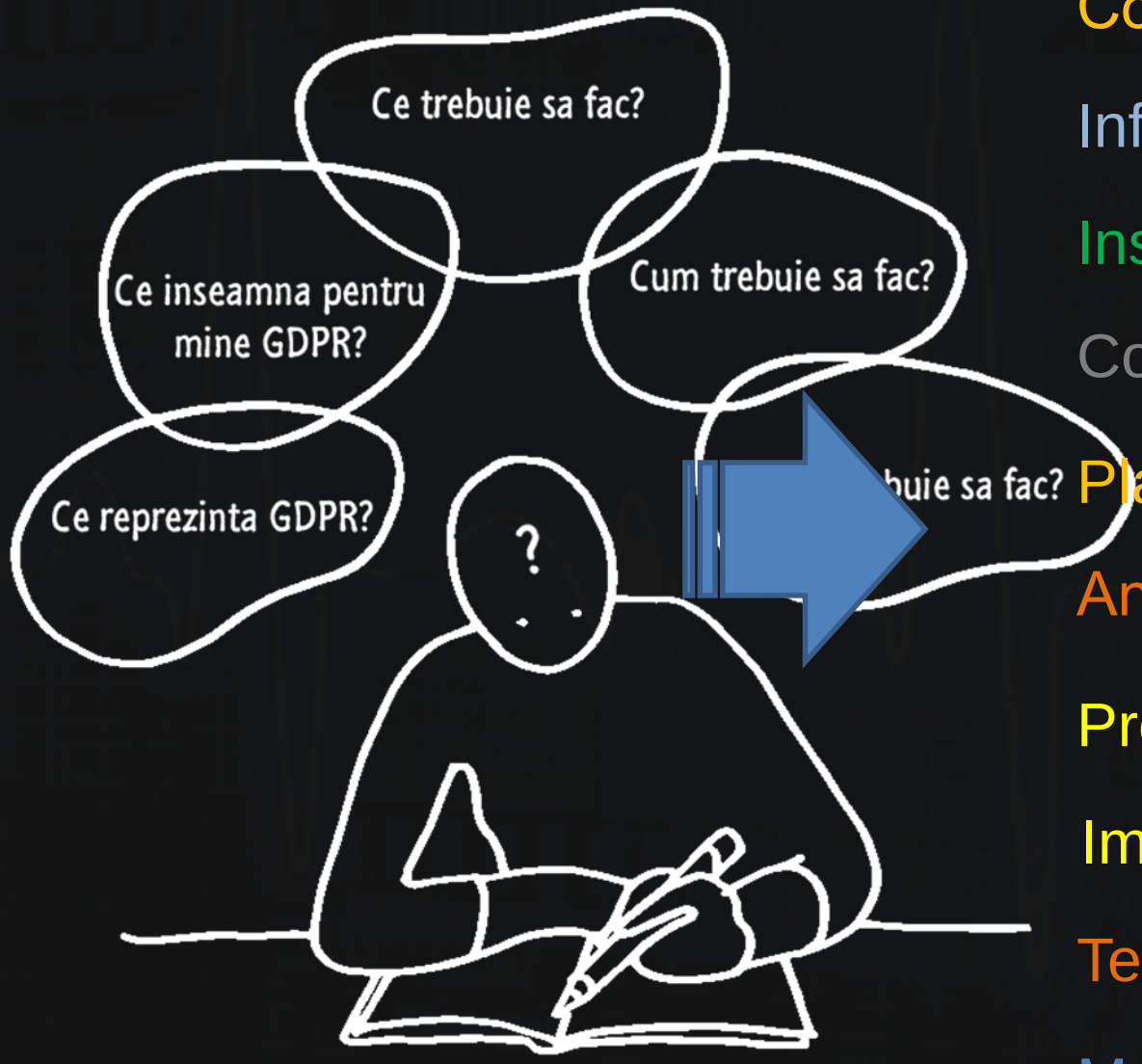
PHOENIX IT SOLUTIONS

Implementare GDPR





cerinte tehnice
libera circulatie
monitorizare
asumare
controlor
portabilitate
categorii
raspundere
procesator
ANSPDCP
rectificare
bresa de securitate
evidenta
prelucrare
stergere
cookie
transparenta
identificabil
IP uri
electronic
amenzi
justitie
GDPR
plangere
identificatori
proceduri
notificare
tert
securitate
parola
protectie
impact
DPO
certificare
riscuri
uitare
drept
conduita
operator
consiliere
DPIA
cerere acces
transfer
termen
auditare drepturi
persoana identificata
date biometrice
internet
masuri adecvate
acces
online
legalitate
evaluare
confidential
drept de acces
imputernicit
DataProtection
Legea 677
consimtamant
drepturi copii
20.000.000 euro
date speciale
date personale
localizare
incident
informatii
planuri
management
control
GPS
scop
legislatie



Conștientizare

Informare

Instruire

Consiliere

Planificare

Analiză

Proiectare

Implementare

Testare

Monitorizare

Comformitate cu GDPR

Analiza culturii organizaționale în contextul GDPR

- Date și categorii de date personale prelucrate
- Contextul prelucrărilor
- Fluxuri operaționale de activități de prelucrare date
- Legislația existentă. Contracte. Împuterniciri.

Activități procedurabile necesare

- Consimțământ
- Cereri de acces/ștergere/portabilitate
- Notificări
- Planuri de acțiune în caz de incident, evaluări periodice.

Măsuri tehnice necesare pentru securitatea datelor

- Securitate infrastructură IT&C
- Securitate fizică
- Instruire personal.

Securitatea prelucrărilor de date, pe scurt:

Art. 5

Datele cu caracter personal sunt prelucrate într-un mod care asigură **securitatea adecvată** a acestora, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("*integritate şi confidenţialitate*").

1111111111111111

Art. 24

Responsabilitatea operatorului

Operatorul pune în aplicare **măsuri tehnice şi organizatorice adecvate** pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar.

Securitatea prelucrărilor de date, pe scurt:

Secţiunea 2
<u>Securitatea</u> datelor cu caracter personal

Măsuri tehnice şi organizatorice adecvate:

- **pseudonimizarea** şi **criptarea** datelor cu caracter personal;
- capacitatea de a asigura **confidenţialitatea**, **integritatea**, **disponibilitatea** şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare;
- capacitatea de a **restabili** disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru **testarea**, **evaluarea** şi aprecierea periodice ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.

Securitatea prelucrărilor de date, pe scurt:

Art. 33: Notificarea autorităţii de supraveghere în cazul încălcării securităţii datelor cu caracter personal

Când are loc o încălcare a securităţii datelor cu caracter personal, operatorul notifică acest lucru autorităţii de supraveghere competente în termen de **cel mult 72 de ore** de la data la care a luat cunoştinţă de aceasta.

Notificarea conține cel puțin:

- categoriile şi numărul înregistrărilor de **date** și al persoanelor vizate în cauză;
- numele şi datele de **contact** ale responsabilului cu protecţia datelor sau un alt punct de contact al operatorului;
- **consecinţele** probabile ale încălcării securităţii datelor cu caracter personal;
- **măsurile** luate sau propuse spre a fi luate de operator pentru a remedia incidentul, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

Securitatea prelucrărilor de date, pe scurt:

Art. 34: <u>Informarea</u> persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal

- În cazul în care încălcarea securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul informează persoana vizată **fără întârzieri** nejustificate cu privire la această încălcare.

- Informarea conține o **descriere** într-un limbaj clar şi simplu a caracterului încălcării securităţii datelor cu caracter personal, precum şi cel puţin informaţiile şi măsurile menţionate la articolul 33 alineatul (3) literele (b), (c) şi (d), respectiv: date de contact, consecințe și măsuri de remediere.

Date privind sănătatea, date genetice, date biometrice

Potrivit art. 9, următoarele informații fac parte din categoriile speciale de date cu caracter personal:

- **date privind sănătatea** - date legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;

- **date genetice -** date referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective;

- **date biometrice** - date referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane.

Date privind sănătatea, date genetice, date biometrice

Prelucrarea date biometrice, genetice sau referitoare la sănătate **este interzisă**, cu excepțiile următoare:

- când persoana vizată şi-a dat **consimţământul explicit**;
- pentru **protejarea intereselor vitale** ale persoanei vizate (aflată în incapacitate fizică pentru a-și da consimțământul);
- în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacităţii de muncă a angajatului, de stabilirea unui **diagnostic medical**, de furnizarea de **asistenţă medicală** sau socială sau a unui **tratament medical** sau de gestionarea sistemelor şi serviciilor de sănătate sau de asistenţă socială (*de către un profesionist supus obligaţiei de păstrare a secretului profesional*);
- când prelucrarea este necesară din motive de interes public în domeniul **sănătăţii publice**.

Date privind sănătatea, date genetice, date biometrice

Alte aspecte specifice legate de prelucrarea datelor privind sănătatea, a datelor genetice sau a datelor biometrice:

- Desemnarea unui **responsabil cu protecţia datelor** (DPO);
- Realizarea evidenței activităților de prelucrare;
- Categoriile speciale de date cu caracter personal necesită ***un nivel mai ridicat de protecţie*;**
- Statele membre pot menţine sau introduce condiţii suplimentare, inclusiv restricţii, în ceea ce priveşte prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea.

Condiţii generale pentru impunerea amenzilor administrative (*proiect lege*)

Până la **100.000 lei** pentru încălcarea dispozițiilor referitoare la:

- Condiţiile aplicabile la **consimţământul** copiilor;
- Prelucrarea care nu necesită identificare;
- Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit;
- Obligațiile operatorului și ale persoanei împuternicite, art. 25-39 – ex. evidențele activităților de prelucrare, notificare breșă de securitate etc.
- **Securitatea** datelor cu caracter personal;
- Evaluarea **impactului** asupra protecţiei datelor şi consultarea prealabilă.

Până la **200.000 lei** pentru încălcarea dispozițiilor referitoare la:

- **Principii**le legate de prelucrarea datelor cu caracter personal ("legalitate, echitate şi transparenţă");
- Condiţii privind **consimţământul**;
- **Drepturile** persoanei vizate (transparență, informare, dreptul de acces, opoziție, portabilitate etc.);
- **Transferurile** de date cu caracter personal în străinătate.

Diverse considerații

GDPR poate presupune alocarea de noi resurse și investiții bănești. Dar, aduce și avantaje, cum ar fi:

- simplificarea și armonizarea la nivel juridic și administrativ a protecției datelor în Uniunea Europeană. Facilitează libera circulație a datelor personale în spațiul european;
- responsabilizarea operatorilor cu privire la prelucrările proprii de date și informații;
- stimularea inovației pentru tehnologiile care asigură stocarea și protecția datelor.

Statistic, se dezvoltă un milion de noi feluri de malware în fiecare zi. Astăzi, timpul mediu în care un malware stă nedetectat într-o organizație este de 201 zile (conform *Ponemon Institute*).

GDPR își propune să pregătească operatorii pentru un viitor în care informația devine critică pentru supraviețuirea noastră. Într-o societate marcată de atacuri cibernetice și teroriste, cu cât entitățile colectează și distribuie mai multe date despre oameni, cu atât expunerea potențială crește mai mult.

Rolul integratorului

Identificarea și implementarea măsurilor necesare pentru a proteja prelucrările de date personale împotriva:

- prelucrării neautorizate sau **ilegale**;
- pierderii, a **distrugerii** sau a deteriorării accidentale.

Identificarea și implementarea măsurilor adecvate pentru:

- a asigura **confidenţialitatea**, **integritatea**, **disponibilitatea** şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare;
- a **restabili** disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- **instruirea** personalului operatorului de date;
- **testarea**, evaluarea şi aprecierea **periodice** ale eficacităţii măsurilor neceare pentru securitatea prelucrării.

Securitatea prelucrărilor de date, pe scurt:

Cateva consideratii …
(Ref. Cyber security report publicat pe site-ul https://www.cnbc.com)

“There's no such thing as an impenetrable system, but often even a half-decent defense will deter many cybercriminals — they'll move on and look for an easier target”.

“Criminals are getting better, faster and nobody on the defensive is getting better fast enough”.

“Most hacks take minutes to do — and weeks to discover”.

“The study found that US companies took an average of 206 days to detect a data breach”.

“With the availability of personal details available on social media, phishing emails are better camouflaged than ever”.

“Even if your technology is tightly-controlled, people remain easy to fool”

“Once a phishing email is sent, it takes only about 1 minute and 40 seconds before the first user takes the bait”

Scurgeri de Informatii ...

RAPORT

cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2016

În 2016, CERT-RO a colectat și procesat **110.194.890** de alerte de securitate cibernetică, ***în creștere cu 61,55% față de anul 2015*** (68.206.856), dintre care:

- 38% (2,9 milioane) dintre adresele IP publice din România au înregistrat cel puțin o alertă;
- 81% (89 milioane) dintre alerte se referă la sisteme sau servicii vulnerabile;
- 13% (14 milioane) dintre alerte se referă la sisteme infectate cu malware de tip botnet;
- 639 de domenii web „.RO” au fost utilizate de site-uri web compromise.

Măsuri de prevenire a incidentelor de securitate:

- **Securizarea terminalelor** (stații de lucru, telefoane, tablete etc.) prin utilizarea unor soluții/tehnologii de tip antivirus/antimalware, sandbox și de criptare a datelor;
- **Securizarea infrastructurii de rețea** prin utilizarea unor soluții/tehnologii de protecție perimetrală (ex. firewall);
- **Monitorizarea continuă** a fluxurilor de date în cadrul infrastructurii IT prin utilizarea unor soluții/tehnologii specifice;
- Implementarea unor măsuri adecvate de **securitate fizică** în spațiile unde sunt procesate sau depozitate cantități mari de date;
- **Limitarea accesului** utilizatorilor la resurse și la date în baza atribuțiilor acestora (principiul "*nevoia de a cunoaște*");

Măsuri de prevenire a incidentelor de securitate:

- Implementarea unei proceduri adecvate de **backup** (copii de siguranță) care să includă și verificarea periodică a integrității datelor și a procesului de restaurare;
- Implementarea unei **politici de securitate** care să fie asumată și respectată de toți utilizatorii;
- Utilizarea unor **proceduri de răspuns** la incidentele de securitate și de gestionare a vulnerabilităților;
- Dispunerea de **personal adecvat** pentru securizarea infrastructurii IT și pentru a răspunde la incidentele de securitate;
- **Instruirea periodică** a personalului cu privire la riscurile, amenințările și vulnerabilitățile de securitate; fișa postului actualizată;
- Realizarea de **audituri/evaluări** periodice de securitate a infrastructurii IT, a personalului și a procedurilor.

Rolul integratorului

Viziunea integratorului asupra protecției datelor în context GDPR

- ❖ Impactul asupra aplicațiilor existente
- ❖ Impactul asupra infrastructurii hardware
- ❖ Impactul asupra infrastructurii de comunicație
- ❖ Impactul asupra sistemelor existente de securitate

Multumesc pentru atenție!

GENERAL DATA PROTECTION REGULATION

PHOENIX
IT SOLUTIONS