

Confidențialitatea și securitatea datelor

o abordare tehnică din perspectiva GDPR

drd. ing. Cătălin Mironeanu

IAȘI – 20 noiembrie 2019

Camera de Comerț și Industrie Iași

Caracteristicile de securitate a datelor

Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelilor și a sistemelor informatice în Uniune

<https://eur-lex.europa.eu/eli/dir/2016/1148/oj>

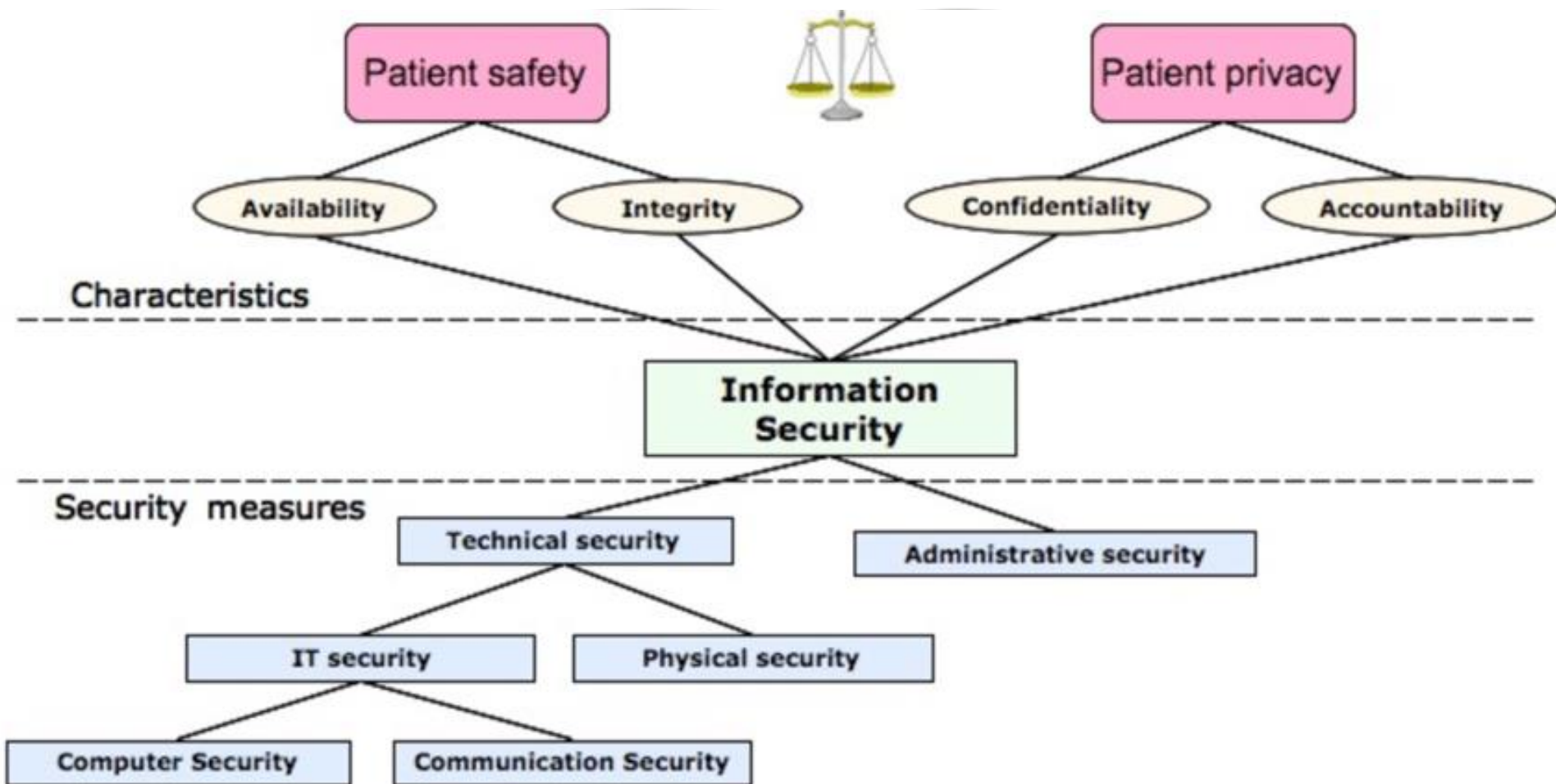
„Securitatea rețelilor și a sistemelor informatice” *capacitatea unei rețele și a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărei acțiuni care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate sau transmise sau prelucrate ori a serviciilor conexe oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;*

Managementul securității informației

INFOSEC - *ansamblul măsurilor și structurilor de protecție a informațiilor* ce sunt prelucrate, stocate sau transmise prin intermediul sistemelor informatice și de comunicații, precum și al altor sisteme electronice, împotriva amenințărilor și a oricăror acțiuni care pot aduce atingere confidențialității, integrității, disponibilității, autenticității și non-repudierii informațiilor precum și afectarea funcționării sistemelor informatice, indiferent dacă acestea apar accidental sau intenționat.

(HG 585/2002, art. 237)





Patient Safety and Patient Privacy in Information Security from the Patient's View: A Case Study

Åhlfeldt, Rose-Mharie, Söderström, Eva, *Journal of Information System Security (JISSEC)*

Confidențialitatea prelucrării

Al 6-lea principiu al prelucrării (GDPR - art. 5, alin. 1, lit. f): Datele cu caracter personal sunt prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("integritate și confidențialitate")



Confidențialitatea - asigurarea accesului la informații numai pe baza drepturilor de acces aprobate ale persoanei, în acord cu nivelul de clasificare a informației accesate și a permisiunii rezultate din aplicarea principiului nevoii de a cunoaște (need-to-know);

Integritatea - interdicția modificării - prin ștergere sau adăugare - ori a distrugerii în mod neautorizat a informațiilor;

Propunere Regulament ePrivacy

- revizuirea Directivei 2002/58/CE („Directiva asupra confidențialității și comunicațiilor electronice”) în vederea asigurării unui nivel ridicat de protecție a vieții private a utilizatorilor de servicii de comunicații electronice și a unor condiții de concurență echitabile pentru toți actorii de pe piață.

- propunerea revizuieste Directiva 2002/58/CE, luând în considerare obiectivele Strategiei privind piața unică digitală și asigurând **coerența cu GDPR**

- *„Punerea în aplicare a Directivei asupra confidențialității și comunicațiilor electronice nu a fost eficace din punctul de vedere al responsabilizării utilizatorilor finali. Prin urmare, pentru atingerea obiectivului este necesară punerea în aplicare a principiului prin **centralizarea consimțământului în cadrul unui software și informarea utilizatorilor cu privire la setările de confidențialitate.**”*

- *Art. 5 - Confidențialitatea datelor transmise în cadrul comunicațiilor electronice*
ro „Datele transmise în cadrul comunicațiilor electronice sunt confidențiale”
eng „Electronic communications data shall be confidential”

Confidențialitate vs Securitate

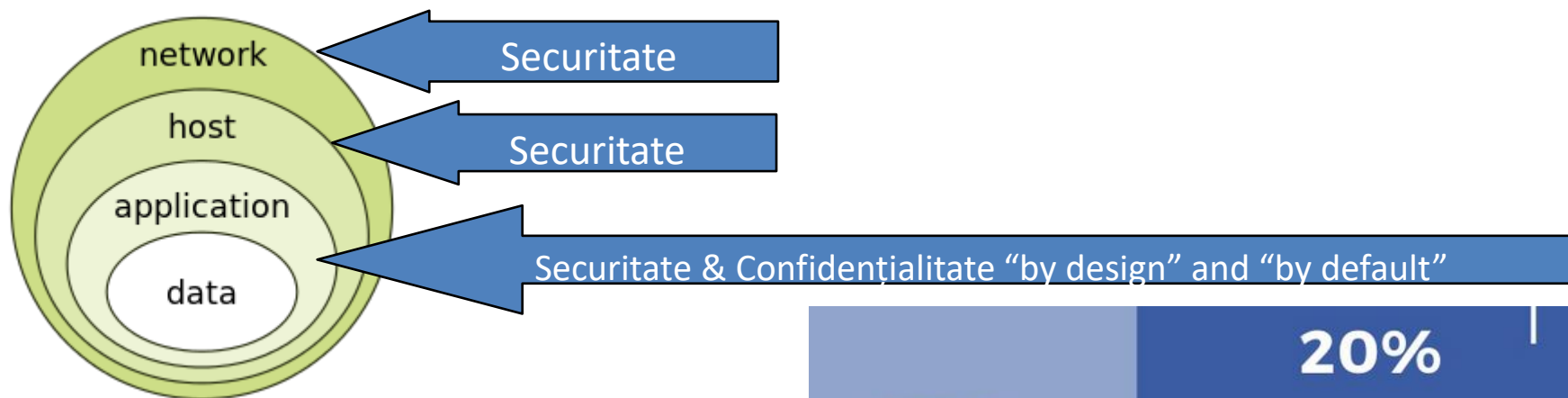


Data egress vs ingress

Adăugarea unei protecții suplimentare care să permită aceleași funcționalități pentru cei care privesc din interior => **securitate**

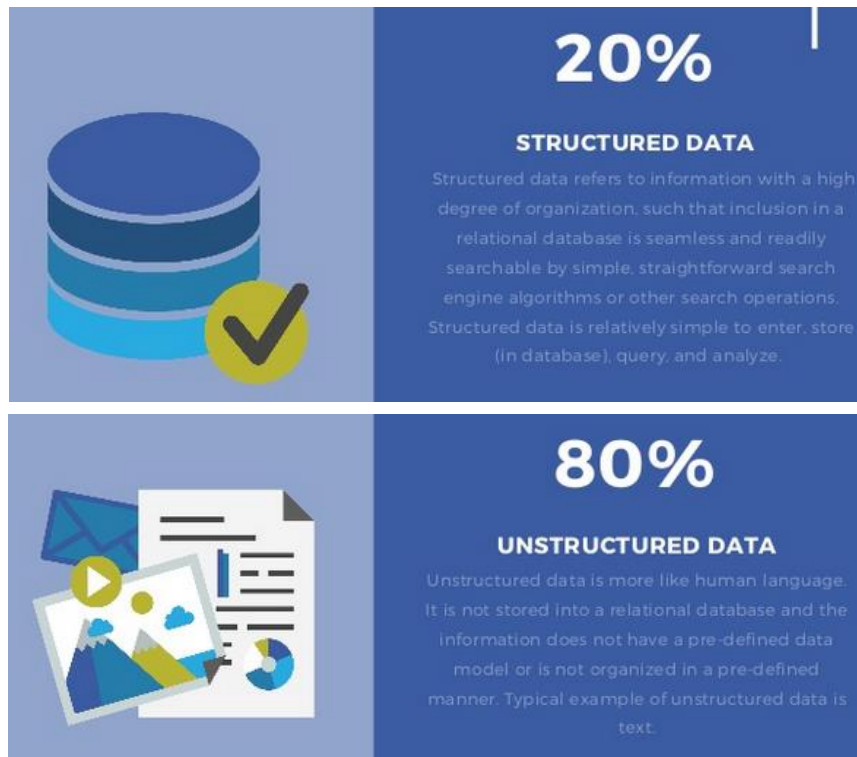
Adăugarea unui „filtru” pentru cei care privesc din afară => **confidențialitate**

Securitate -> Confidențialitate => Securitate



Date stocate în:

- baze de date relaționale
- baze de date NoSQL



Cerințe minime de securitate - stocare date

1. Crearea rolurilor și asocierea utilizatorilor

motiv 39 GDPR

2. Mascarea datelor „sensibile”

art. 32 și motiv 83 GDPR

3. Auditarea activităților

art. 24 GDPR

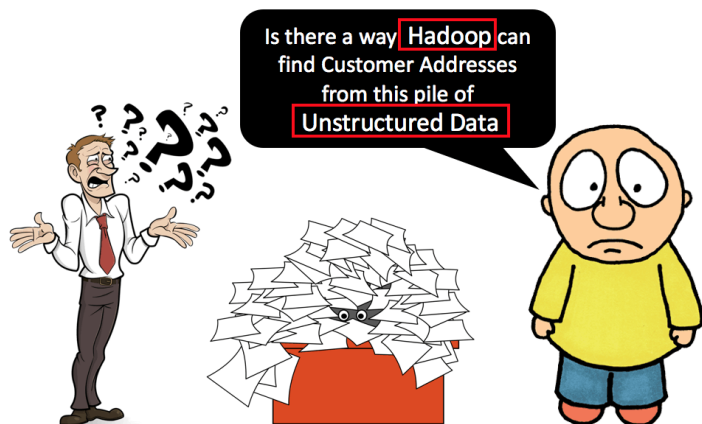
4. Crearea alertelor care să notifice încălcarea regulilor / semnalarea breșelor

motiv 39 GDPR

5. Prevenirea pierderii datelor

art. 32 (2) GDPR

GDPR în date nestructurate



© OvalEdge Inc.

```

{
  "Title": "The Cuckoo's Calling",
  "Author": "Robert Galbraith",
  "Genre": "classic crime novel",
  "Detail": {
    "Publisher": "Little Brown",
    "Publication_Year": 2013,
    "ISBN-13": 9781408704004,
    "Language": "English",
    "Pages": 494
  },
  "Price": [
    {
      "type": "Hardcover",
      "price": 16.65,
    },
    {
      "type": "Kindle Edition",
      "price": 7.03,
    }
  ]
}
  
```

Object Starts

Object Starts

Value string

Value number

Object ends

Array starts

Object Starts

Object ends

Object Starts

Object ends

Object ends

Array ends

Object ends

1. locația exactă a PII (Personal Identifiable Information)
2. Marcarea („tagging”) documentelor ce conțin date cu caracter personal
3. Aplicarea regulilor de securitate în funcție de tipurile de date cu caracter personal
4. Monitorizare și control

MongoDB fișiere de configurare

```
// Configure the mongo host details aka Config.js
"database": {
  "db_host": "mongodb://localhost:xxxxx/", // if cluster add host comma separated like
"mongodb://localhost1:xxxxx,localhost2:xxxxx,localhost3:xxxxx/"
  "db_name": "social",
  "db_auth": false, // if true supply the username and pw
  "db_username": "",
  "db_pw": "",
  "db_auth_type": "default", // default -> MongoDB auth, ldap -> ldap configured
//Mongo SSL configuration
  "ssl": false, // if true supply the certificate and key
  "sslValidate": false, //validate ssl certificate,
    // To validate (true)
    // MongoDB doesn't use the system's global trust store.
    // ***The sslCAFile must contains all intermediary certificates of the verification chain.
    // sslKey and sslCert is mandatory (can be given concatenated key file for both)
  "sslKey": "C:\\Certs\\key.pem", //path for key file
  "sslCert": "C:\\Certs\\key.pem", //path for cert file
  "sslCA": "C:\\Certs\\root_all.pem", // or .crt path for cert file
  "sslPass": "" //passphrase if any
}
// Set the log_level to DEBUG or INFO, required to make it to DEBUG when found errors otherwise INFO
Config.log_level
```

```
Transport Layer Security protocol
net:
  tls:
    mode: requireTLS
    certificateKeyFile: /etc/ssl/mongodb.pem
systemLog:
  destination: file
  path: "/var/log/mongodb/mongod.log"
  logAppend: true
storage:
  dbPath: "/var/lib/mongodb"
processManagement:
  fork: true
net:
  bindIp: localhost,mongodb0.example.net
  port: 27017
```

```
mongod --config <path/to/configuration/file>
```

Propunere Regulament ePrivacy

- Art. 5 - Confidențialitatea datelor transmise în cadrul comunicațiilor electronice
„Datele transmise în cadrul comunicațiilor electronice sunt confidențiale”

GDPR în date structurate

Schema Name	Table Name	Column Name	Column Comment	Sensitive Category	Sensitive Type
APP_A	APP_USER	PWD	--	PII – IT DATA	PASSWORD
APP_A	CUSTOMERS	CUST_EMAIL	--	PII	EMAIL
APP_A	CUSTOMERS	CUST_FIRST_NAME	--	PII	FIRST_NAME
APP_A	CUSTOMERS	CUST_STREET_ADDRESS	--	PII – ADDRESS	STREET
APP_A	CUSTOMERS	PHONE_NUMBER1	--	PII	PHONE

Candidate columns for Masking,
Pseudonymization, Audit Policies

Copyright Oracle

GDPR în date structurată

Schema	Table Name	Columns	Sensitive Columns	Rows	Sensitive Category
APP_A	APP_USER	3	1	496	PII – IT DATA
APP_A	CUSTOMERS	14	8	7	PII, PII – ADDRESS
APP_A	LINKED_DATA	6	4	500	PII-LINKED, PII-LINKED – BIRTH DETAILS
APP_A	PERSONAL_DATA	9	7	500	PII, PII – ADDRESS, PII – IDS
GENEVIS	EMP	24	4	14	JOB DATA
HR	JOBS	8	3	19	JOB DATA
HR	LOCATIONS	12	6	23	PII – ADDRESS, PII – IT DATA
HR	SUPPLEMENTAL_DATA	6	4	149	FINANCIAL DATA – PCI, JOB DATA, PII – IDS, PII – IT DATA

Candidate tables for Encryption /

Copyright Oracle

GDPR în date structurate

```
SQL> CREATE OR REPLACE TRIGGER secure_emp
 2 BEFORE INSERT ON emp
 3 BEGIN
 4   IF (TO_CHAR (sysdate, 'DY') IN ('SAT', 'SUN'))
 5     OR (TO_CHAR (sysdate, 'HH24') NOT BETWEEN
 6        '08' AND '18'
 7     THEN RAISE_APPLICATION_ERROR (-20500,
 8        'You may only insert into EMP during normal
 9        hours. ');
10 END IF;
11 END;
12 /
```

Nu pot introduce date în afara orelor de program
(L-V: 8-18)

```
SQL> CREATE OR REPLACE TRIGGER audit_emp_values
 2 AFTER DELETE OR INSERT OR UPDATE ON emp
 3 FOR EACH ROW
 4 BEGIN
 5   INSERT INTO audit_emp_values (user_name,
 6     timestamp, id, old_last_name, new_last_name,
 7     old_title, new_title, old_salary, new_salary)
 8   VALUES (USER, SYSDATE, :old.empno, :old.ename,
 9     :new.ename, :old.job, :new.job,
10     :old.sal, :new.sal);
11 END;
12 /
```

Orice activitate (introducere date, modificare sau ștergere) este înregistrată într-o tabelă de audit:

- cine a efectuat operația
- la ce dată (zi, oră, minut, secundă)
- ce valori au fost modificate
- cu ce valori au fost înlocuite



Copyright Oracle

GDPR în date structurate

User Audit Table

USER_NAME	TABlename	COLUMN_NAME	INS	UPD	DEL
SCOTT	EMP	SAL	1	1	1
SCOTT	EMP		0	1	0
JONES	EMP		0	0	0

Continuation

MAX_INS	MAX_UPD	MAX_DEL
5	5	5
5	0	0

```

SQL>CREATE OR REPLACE TRIGGER check_salary_count
2 AFTER UPDATE OF sal ON emp
3 DECLARE
4   v_salary_changes NUMBER;
5   v_max_changes    NUMBER;
6 BEGIN
7   SELECT upd, max_upd
8   INTO   v_salary_changes, v_max_changes
9   FROM   audit_table
10  WHERE  user_name = user
11  AND    table_name = 'EMP'
12  AND    column_name = 'SAL';
13  IF v_salary_changes > v_max_changes THEN
14    RAISE_APPLICATION_ERROR (-20501,
15      'You may only make a maximum of ' ||
16      TO_CHAR (v_max_changes) ||
17      ' changes to the SAL column');
18  END IF;
19 END;
20 /

```

Orice modificare pe o coloană „sensibilă” este oprită de regulile stabilite și stocate într-o tabelă de audit.

Copyright Oracle

GDPR în date structurate

JDK8 și 12.2.0.1 JDBC THIN DRIVER

```
java -Doracle.net.ssl_server_dn_match="true"  
-Doracle.net.tns_admin=./lib  
-Djavax.net.ssl.trustStore="truststore.jks"  
-Djavax.net.ssl.trustStorePassword="welcome1"  
-Djavax.net.ssl.trustStoreType="JKS"  
-Djavax.net.ssl.keyStore="/client_credentials/keystore.jks"  
-Djavax.net.ssl.keyStoreType="JKS"  
-Djavax.net.ssl.keyStorePassword="welcome1" DataSourceSample
```

Propunere Regulament ePrivacy

- *Art. 5 - Confidențialitatea datelor transmise în cadrul comunicațiilor electronice*
„Datele transmise în cadrul comunicațiilor electronice sunt confidențiale”

	Privacy	Security
Potrivirea în context	<i>"user's information"</i> <i>"Individual"</i>	<i>"confidentiality, integrity and availability"</i> <i>"Information"</i>
Încrederea	Privacy is the ability to decide what information of an individual goes where	Security offers the ability to be confident that decisions are respected
Cine este protejat	The issue of privacy is one that often applies to a consumer's right to safeguard their information from any other parties	Security may provide for confidentiality. The overall goal of most security system is to protect an enterprise or agency <i>"Agreement"</i>
Ordinea firească a implementării	It is possible to have poor privacy and good security practices	However, it is difficult to have good privacy practices without a good data security program
Legalitatea prelucrării & Obligativitatea	For example, if user make a purchase from XYZ Company and provide them payment and address information in order for them to ship the product, they cannot then sell user's information to a third party without prior consent to user <i>"It is the personal choice of an individual"</i>	The company XYZ uses various techniques (Encryption, Firewall) in order to prevent data compromise from technology or vulnerabilities in the network <i>"Yes, when the information is professional and legal"</i>

Concluzii

Politica de securitate

- construită corect
- implementată la toate nivelurile
 - date
 - aplicație
 - sistem informatic
 - rețea



permite implementarea cerințelor GDPR și ePR <= **Responsabilitate**

Vă mulțumesc pentru atenție !