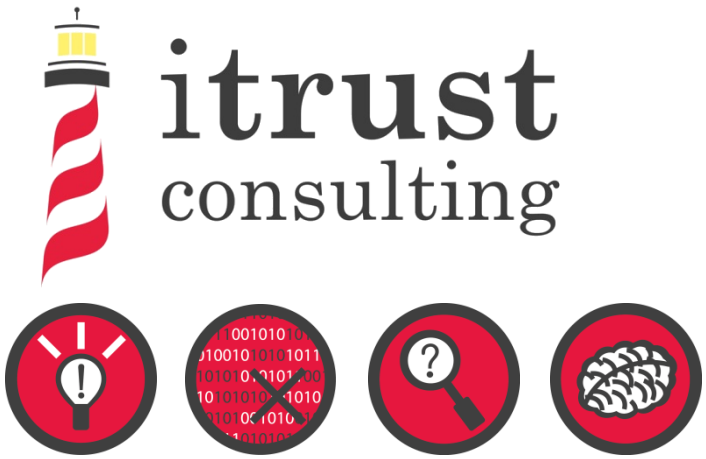


Tailoring information security to business requirements

# Certification framework for Data Protection

21/04/2016

**M. Aubigny**

**itrust consulting s.à r.l.**
6 Z.I. Bombicht
L-6947 Niederanven

Tel: +352 26 176 212
Fax: +352 26 710 978
Web: www.itrust.lu

## Overview of the presentation

- Context : Why a Certification is needed to ensure data protection ?
- General presentation of EuroPriSe
- EuroPriSe certification framework
- Classical EuroPriSe certification roadmap
- Magnify the Certification requirements
- New framework: Website certification


## Context: Data Protection Problematic



The problematic of our connected world:

**Data use vs Data misuse**

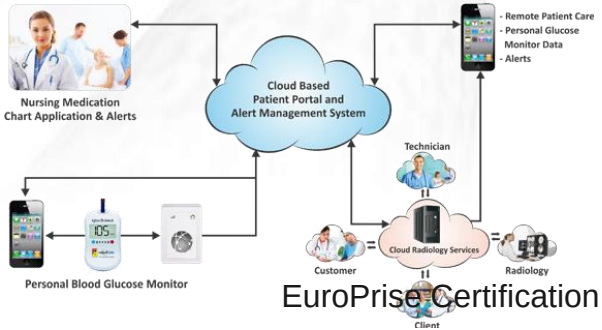
**Objective starting point:**

- We produce more and more personal data
- Personal data are more and more proceeded

**Subjective starting point:**

- We are great fans of connected services based on personal data.
- We want to keep our life secret.




**EVALUATE**

## Context : Regulation and Trust

To solve the problem: Data Protection Regulations as in Europe

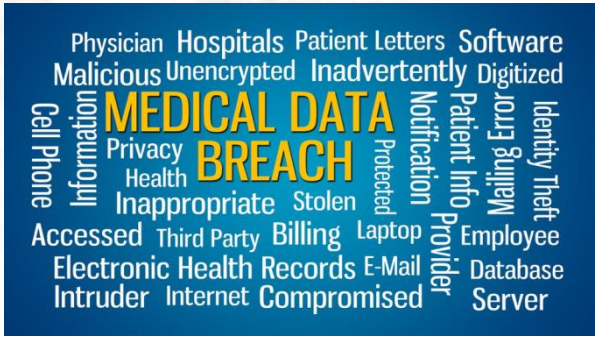
- Directive 95/46 EC
- Directive 2002/21/EC
- GDPR Directive 2016/… *(repealing Dir 95/46)*

**But the fear of personal data misuse still remains:**

61% of French people are ready to sell their personal data

**81%** of French people are afraid that personal data will be used for marketing goals

*"The Internet of Things and the Smart Homes" study for Intel Security*



## Context: Ensure confidence in Data Protection.

We need to restore and ensure the confidence of users that personal data are securely proceeded during the entire information treatment.

One solution promoted by the European Regulation : **CERTIFICATION**

*Article 42*

*Certification*

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

- CF. Directive 2016/… which include a long article 42 on certification framework (8 points against 3 points for the 2012/011 COD version) *and include 73 reference to the word certification*

**Which CERTIFICATION ?**

## Context: which certification ?

The international standard ISO 27001 on Information Security Management includes among objectives and controls (normative annexe derived from ISO 27002) one to ensure compliance of an information system to the Data Protection regulation. The ISO 27002 specifies this control especially in providing a link to another ISO standard ISO 29100.

| | | |
|---|---|---|
| A.18.1.4 | Privacy and protection of personally identifiable information | *Control*<br><br>Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable. |

Other information

ISO/IEC 29100[25] provides a high-level framework for the protection of personally identifiable information within information and communication technology systems. A number of countries have

Only ISO 27001 provides a certification approach.

However it has not for objective to clarify and guarantee the privacy issues of the information treatment.

## Context: dedicated certification framework.

Some certification framework exists on the market to ensure the level of skills required for data protection officers or to label website (especially eCommerce site): the best known is TRUSTe which is endorsed by big manufacturers as Apple or Microsoft.



**BUT** only EuroPriSe provides a certification framework of IT products or IT services fully focused and fully compatible with the European regulation and the European Members regulations with the guaranty of impartiality such as developed in ISO 27006/7.

## General presentation : A European story

The EuroPriSe certification framework has been set up during a European research project (eTen program):

- Funding by Europe Commission for 1.3 Mio€
- 9 partners from 8 European countries

- 18 uses cases during the project
- 6 successfully certified products or services during the project
- 65 granted experts during the project

Since 2008, EuroPriSe organisation has been led by ULD (*Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein)* and has:

- Performed 55 successful certifications or recertification of products or services (in Europe but also in USA)
- Granted 97 Experts in 19 countries
- Effective co-operation as expert organisation in European DPA training.

## General presentation : Endorsement and implementation

The EuroPriSe certification framework has been endorsed by:

- EDPS (European Data Protection Supervisor)
- Gartner (06/2008)
- French Senat Chamber (06/2009)
- Spanish Senat Chamber (04/2010)

★ EUROPEAN DATA PROTECTION SUPERVISOR
The European guardian of personal data protection

★ LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES
Le gardien européen de la protection des données personnelles

★ DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE
Der europäische Hüter des Schutzes personenbezogener Daten

- The European Parliament through the dedicated Commission for the Protection of Consumers and Internal Market (08/2010 and 04/2011)

**Certified products or services :**

SSP EUROPE

CARGLASS

ADMIRAL
ADMIRAL Casinos & Entertainment AG (ACE)

amv networks
security & privacy by design

RISER
RISER ID Services GmbH

quentry

KiwiSecurity
AUTOMATING VIDEO SURVEILLANCE

ixquick

## General presentation : Main benefits

Why choose the EuroPriSe certification framework ? The EuroPriSe certification allows to reach business goals by promoting:

- **Confidence** through:
  - Transparency : the certification criteria and process are public
  - Verifiability : main results (report) are public available on EuroPriSe website
  - Credibility: independent Body of certification and experts
- **Conformity** with the regulation based on the European most binding regulations (including specific European Member States' laws) and on Art 29.
- **Exhaustiveness** of analysis thanks to legal and technical experts collaboration
- **Marketing advantage**
- **EuroPriSe expert advice** during the entire process.


## Certification framework: Organisation

The organisation of the EuroPriSe framework is based on several pillars:

**Certification Authority**:
EuroPriSe Certification Authority
Address: Joseph-Schumpeter-Allee 25
53227 Bonn
Germany
E-Mail: contact@european-privacy-seal.eu

# Certification framework: Procedure overview

An IT product manufacturer or an IT service provider endorse expert *(generally a team of two experts [legal and technical])* which will be in charge of the certification dossier.

In relationship with certification authority the expert(s) will

- Define the target of evaluation(TOE)
- Determine the applicable criteria according to the EuroPriSe catalogue
- Write the evaluation report and the public report to be published.

The certification authority (body of certification) will

- Assess the evaluation report *(consistency, correctness)*
- Control the additional documentation *(ex: security policy, audit reports etc.)*
- Require (if necessary) clarification
- Check the public report *(correctness according to the evaluation report)*

The certification authority will

- Award of European Privacy Seal for 2 years
- Publish the public report on EuroPriSe website
- Ensure regular monitoring
- Provide recertification

## Certification roadmap: evaluation steps

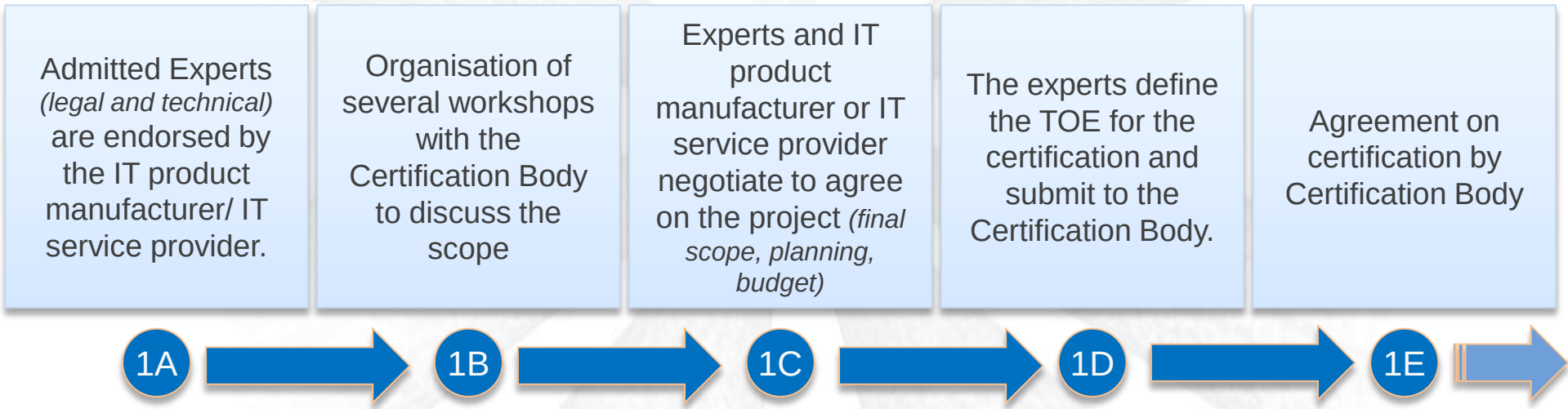
The evaluation of European Privacy Regulation Compliance for an IT products or an IT services is performed in 3 steps:

**Pre-evaluation**
Set up the certification process as project
*(choice of experts, scoping etc.)*

**Expert evaluation**
- TOE Definition
- Criteria selection
- Evaluation
- Reporting
*(understandable by external parties)*

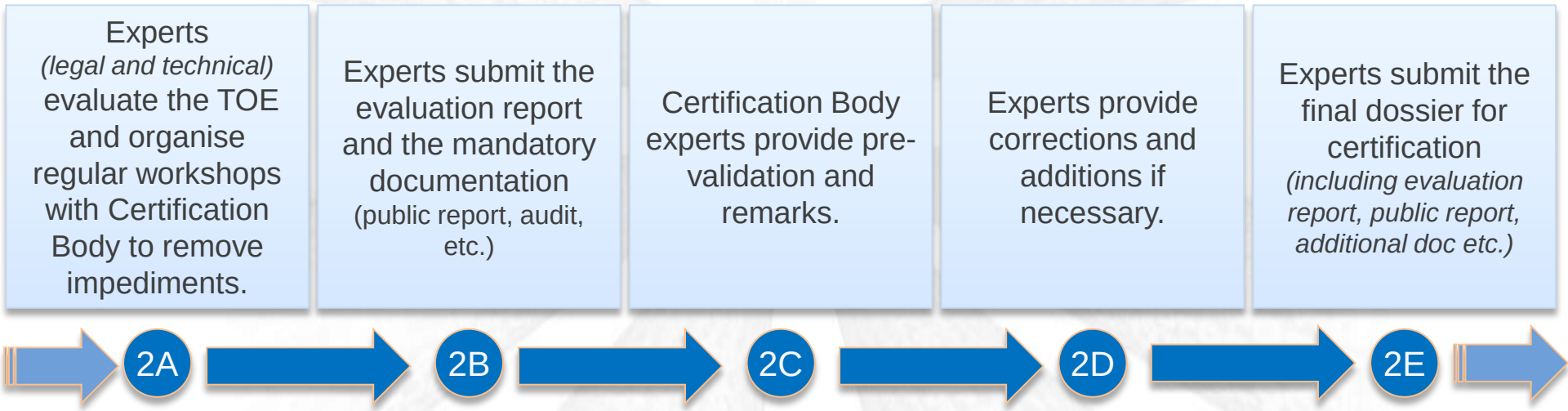
**Validation and Seal Award**
Certification body verify
- Exhaustiveness
- Consistency
- Conformity to regulation

# Certification roadmap: step 1 - pre-evaluation



## Certification roadmap: step 2 - evaluation

During this entire step, the experts will closely work with the Certification Body to avoid misunderstanding or legal/technical dead end.



# Certification roadmap: step 2 - evaluation

Certification Body Experts *(legal and technical)* assess the certification dossier.

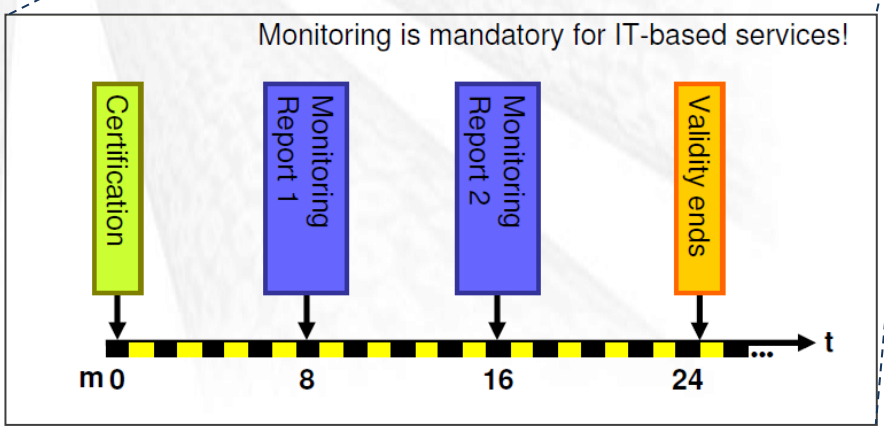
**IF** the dossier provides for the TOE
- ✓ **Exhaustiveness**
- ✓ **Consistency**
- ✓ **Conformity**

**IF NOT :** go back to 1B or 2A

Grant Certification EuroPrise Seal Award

For the IT based services, Certification Body provide regular monitoring

3A → 3B → 3C



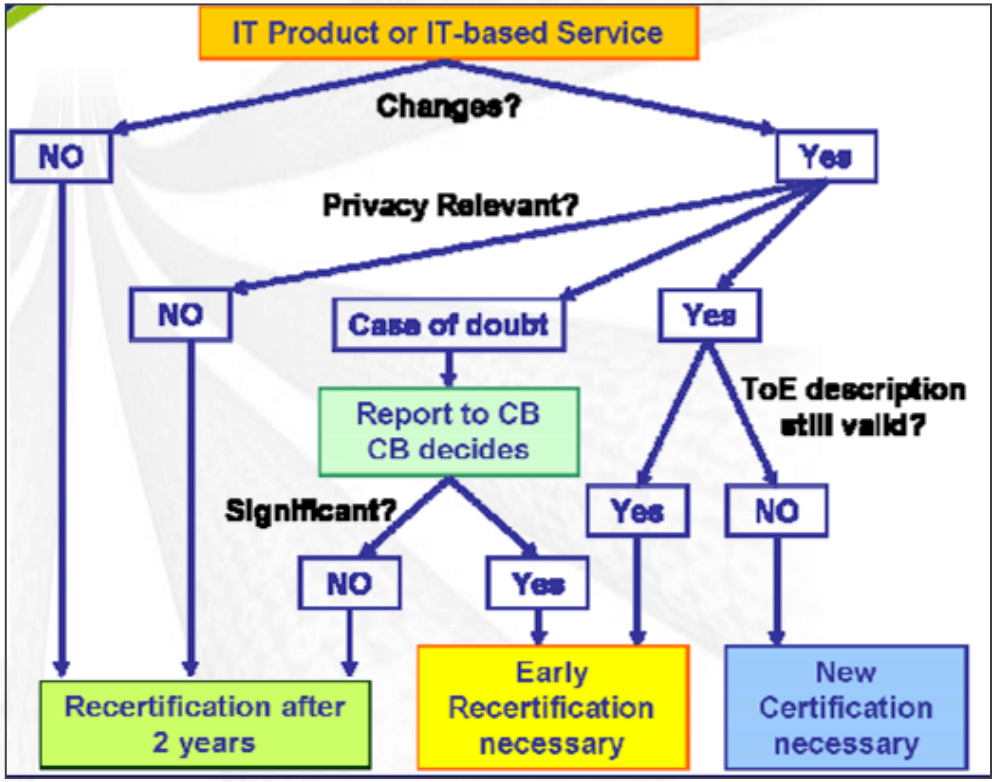

## IT-based Service:

*Services suitable for certification are IT-Based services such as web-based services (e.g. online banking or search engine services) and processing of data by a processor (e.g. data centre hosting mail servers).*

## Certification roadmap: Maintain Certification

The process of certification will mainly depend on the TOE validity and will lead either to a recertification process or to a new certification process at least after two years.

| Re-certification | Case 1 | Case 2 | Case 3 | Case 4 |
|---|---|---|---|---|
| Changes to Product or Service | No changes | Minor changes without impact on privacy evaluation | Privacy relevant changes | Privacy relevant changes |
| ToE description | Valid | Valid | Valid | Change required |
| Validity of original certificate | 2 years | 2 years | Ends | Ends |
| Recertification possible | Yes | Yes | Yes | No |
| Time of Recertification | After 2 years | After 2 years; reporting of privacy related changes to CB | Early Recertification | New Certification, validity ends |



## Certification roadmap: Cost of Certification or Recertification

The table below gives a rough estimation of the cost which essentially depends on the scope:

| | Certification | | | | Re-certification* | | | |
|---|---|---|---|---|---|---|---|---|
| Efforts | Tiny | Small | Medium | Large | Tiny | Small | Medium | Large |
| ToE fee | 200 € | 400 € | 600 € | 1.000 € | 0* | 0* | 0* | 0* |
| Efforts in h | <30 | 30-50 | 51-100 | >100 | <15 | 15-30 | 31-50 | >50 |
| Certification fee | 2.400 € | 4.800 € | 9.000 € | 18.000 € | 1.200 € | 2.400 € | 4.800 € | 9.600 € |
| Seal use monitoring fee for 2 years | 200 € | 200 € | 200 € | 200 € | 200 € | 200 € | 200 € | 200 € |
| Total | 2.800 € | 5.400 € | 9.800 € | 19.200 € | 1.400 € | 2.600 € | 5.000 € | 9.800 € |

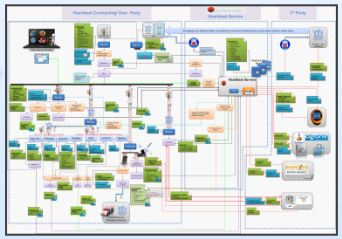
*if ToE remains unchanged

# Scrutinise the evaluation : what experts have to do ?

Definition and analysis of the TOE and its environment

Identification of the Data :
- Primary Data *(provide by the user)*
- Secondary Data *(produced by the processor)*

Precise description of the data flows



Analyse the relevant EU regulation for the data proceed:
*Ex. Dir. on Privacy, Telco, Health etc.*

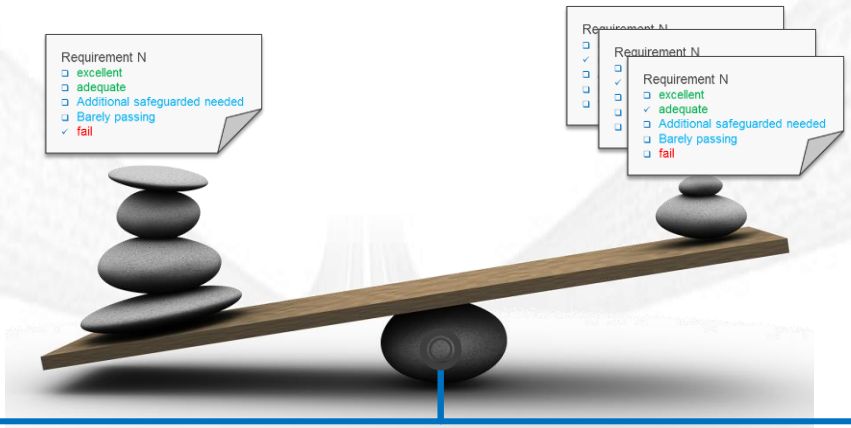
Determine the relevant EuroPrise criteria for the data *(primary and secondary)*

Evaluation according to requirements profiles *(agreement with CB required)*

Experts take a decision for each requirement:
- excellent
- adequate
- Additional safeguarded needed
- Barely passing
- fail

Redaction of the final report

# Scrutinise the evaluation : certification success criteria




**"passed" if**

- All requirements are fulfilled "excellent" or "adequate"
- Healthy mixture of "excellent", "adequate", "barely passing" and "additional safeguards needed"

**"failed if"**

- One requirement is evaluated as "fail"
- Majority of requirements are evaluated as "barely passing" and "additional safeguards needed"

# Scrutinise the evaluation : the EuroPriSe requirements.


Experts roles

**Set 1: Overview on Fundamental Issues**

**1.1 Fundamental Aspects of Processing**
- 1.1.1 Processing Operations; Purpose(s)
- 1.1.2 Processed Personal Data
- 1.1.3 Controller
- 1.1.4 Transnational Operations

**1.2 Fundamental Technical Construction**
- 1.2.1 Data Avoidance and Minimisation
- 1.2.2 Transparency

**Set 2: Legitimacy of Data Processing**

**2.1 Legal Basis for the Processing of Personal Data**
- 2.1.1 Legal Basis for the Processing of Personal Data in General
- 2.1.2 Legal Basis for the Processing of Sensitive Personal Data
- 2.1.3 Requirements of Data Processing for Certain Special Purposes
- 2.1.3 Requirements of Data Processing for Certain Special Purposes

**2.2 Special Requirements to the Various Phases of the Processing**
- 2.2.1 Data Collection (Information Duties)
- 2.2.2 Internal Data Disclosure
- 2.2.3 Disclosure of Data to Third Parties
- 2.2.4 Erasure of Data after Cessation of Requirement

**2.3 Compliance with General Data Protection Principles and –duties**
- 2.3.1 Purpose-specification and –limitation
- 2.3.2 Proportionality
- 2.3.3 Quality of Data

**2.4 Special Types of Processing Operations**
- 2.4.1 Processing of Data by a Processor
- 2.4.2 Transfer to Third Countries
- 2.4.3 Automated Individual Decisions

**2.5 Formalities**
- 2.5.1 Notification
- 2.5.2 Prior Checking

# Scrutinise the evaluation : the EuroPriSe requirements.

Experts roles

**Set 3: Technical-Organisational Measures: Accompanying Measures for Protection [illegible]e Data Subject** .

**3.1 General Duties**

- 3.1.1 Preventing Unauthorised Access to Data, Programs, Premises and Devices
- 3.1.2 Logging of Processing Personal Data
- 3.1.3 Network and Transport Security
- 3.1.4 Mechanisms to Prevent Accidental Loss of Data; Back-up Mechanisms and Recovery
- 3.1.5 Data Protection and Security Management
- 3.1.6 Disposal and Erasure of Data
- 3.1.7 Temporary Files
- 3.1.8 Documentation of Products and Services from a Customer's Perspective

**3.2 Technology-specific and Service-specific Require**ments

- 3.2.1 Encryption
- 3.2.2 Pseudonymisation and Anonymisation
- 3.2.3 Technical Data Protection Functionalities Required by Directive 2002/58/EC
- 3.2.4 Ensuring Transparency of Automated Individual Decisions

**Set 4: Data Subjects' Rights**

**4.1 Rights under the Directive 95/46/EC**

- 4.1.1 Right to Be Informed
- 4.1.2 Right of Access
- 4.1.3 Right of Correction
- 4.1.4 Right of Erasure
- 4.1.5 Right of Blocking *
- 4.1.6 Right of Objection to Processing

**4.2 Rights under the Directive 2002/58/EC**

- 4.2.1 The Right to be Informed of Personal Data Breaches
- 4.2.2 The Right to Be Informed of Security Risks
- 4.2.3 The Right to Confidentiality of
- 4.2.4 The Right to Receive Non-itemised Bills
- 4.2.5 The Right to Prevent Calling Line and/or Connected Line Identification and Call Forwarding
- 4.2.6 Special Rights Regarding Directories of Subscribers to Electronic Communications

## New Certification framework

EuroPrise is going to introduce a new framework to perform website certification through

**EuroPriSe Online Evaluation Tool for Website Certification**. This tool is provided to the experts as a software as a service solution (SaaS).

Legal and technical expert will be specifically endorsed to provide this type of certification.

## Conclusion

EuroPrise Certification framework is obviously a solid certification framework, perfectly in line with the expectancies of the new regulation.

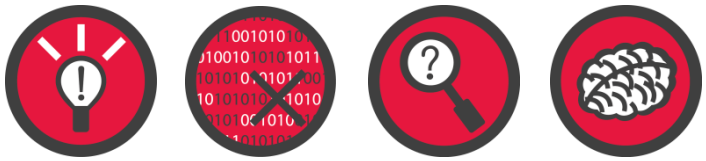
**BUT it needs to be used to be known and improve security of European citizens**

EuroPriSe Certification framework, even if it is presently managed by ULD, aims to be spread all around the European Countries to produce a kind of Privacy Protection Enforcement Grid able to protect European citizen and avoid economic dumping strategies based on Private Data processing :

*The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union.*

*Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law.* ***Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC****. Dir 2016/… (9)*

itrust
consulting




# Thank you for your attention