Information sessions

The General Data Protection Regulation

Codes of conduct and certifications

19th October 2017

Esch-sur-Alzette (Belval)

Alain Herrmann

IT Department

Definitions

Certification

- the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements (ISO).

Code of conduct

- A company code of conduct is a document written up voluntarily by a company in which sets out a set of principles that it commits itself to follow. In some cases, codes of conduct reach suppliers, subcontractors and third parties.

To demonstrate compliance with the obligations of the controller

To demonstrate compliance with the requirements of data protection by design / by default

Certifications / Codes of conduct

Processors:

To demonstrate sufficient guarantees with the GDPR requirements to the controller

To demonstrate compliance with the security of processing requirements

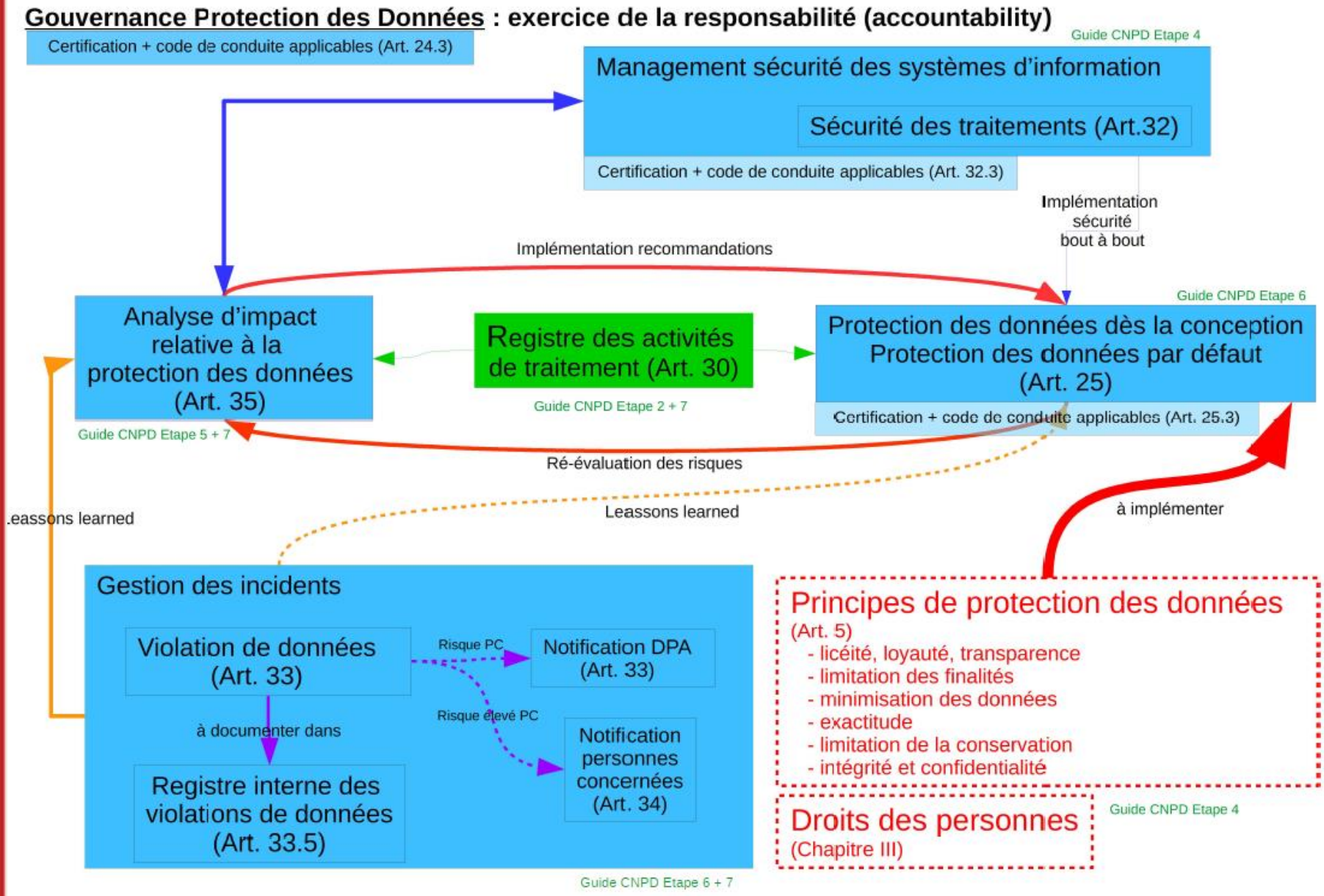
Transfer of data to third countries

What can be certified?

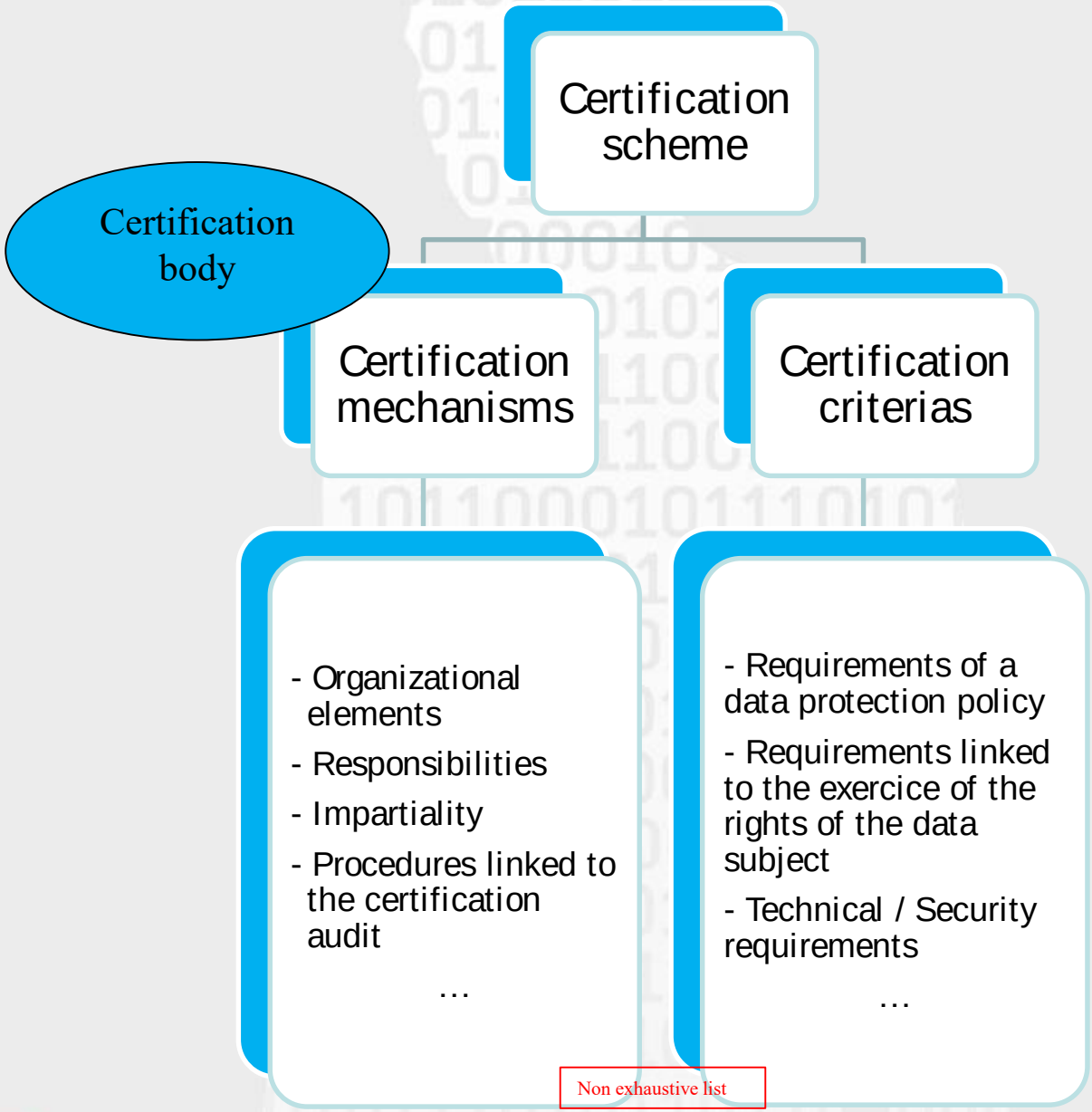
Processing operations from a controller or a processor.

A data protection governance programm from a controller or a processor.

Products and services.


Gouvernance Protection des Données : exercice de la responsabilité (accountability)
Certification + code de conduite applicables (Art. 24.3)
Guide CNPD Etape 4
Management sécurité des systèmes d'information
Sécurité des traitements (Art.32)
Certification + code de conduite applicables (Art. 32.3)
Implémentation sécurité bout à bout
Implémentation recommandations
Guide CNPD Etape 6
Analyse d'impact relative à la protection des données (Art. 35)
Guide CNPD Etape 5 + 7
Registre des activités de traitement (Art. 30)
Guide CNPD Etape 2 + 7
Protection des données dès la conception
Protection des données par défaut
(Art. 25)
Certification + code de conduite applicables (Art. 25.3)
Ré-évaluation des risques
.eassons learned
Leassons learned
à implémenter
Gestion des incidents
Violation de données (Art. 33)
Risque PC
Notification DPA (Art. 33)
Risque élevé PC
à documenter dans
Notification personnes concernées (Art. 34)
Registre interne des violations de données (Art. 33.5)
Guide CNPD Etape 6 + 7
Principes de protection des données
(Art. 5)
- licéité, loyauté, transparence
- limitation des finalités
- minimisation des données
- exactitude
- limitation de la conservation
- intégrité et confidentialité
Droits des personnes
(Chapitre III)
Guide CNPD Etape 4

Certification schemes



Certifications market history & analysis

(Source: CRISP workshop – Madrid – 30 September 2016)

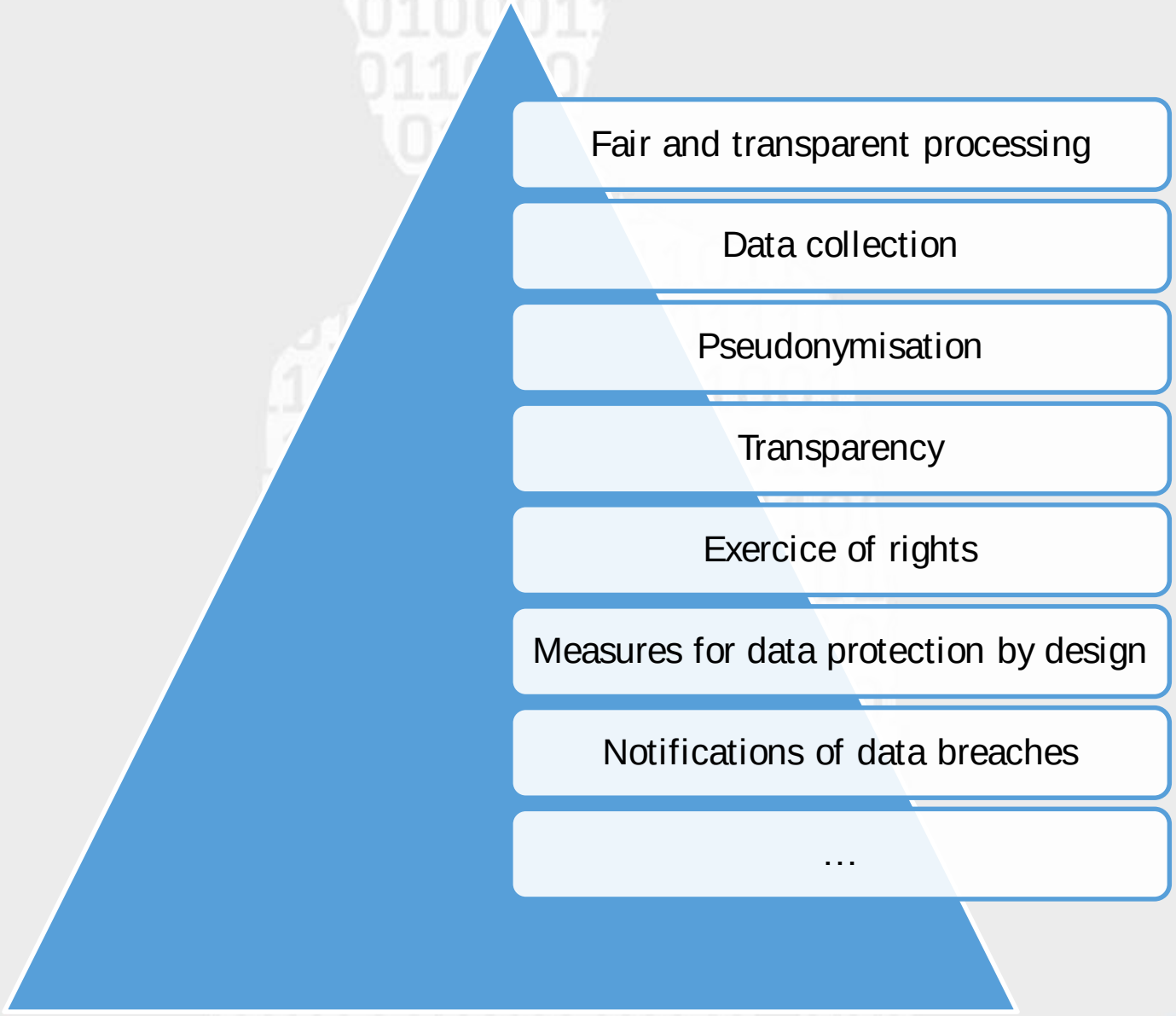
Codes of conduct

To contribute to the effective implementation of the GDPR

To take into account the particularities of the sector in which the processing takes place

To take into account particularities of micro, small and average companies

Content of a code of conduct (Non exhaustive list)



Who can certify?

Organizations that receive an agreement from the CNPD (GDPR + new national law)

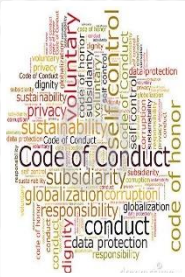
Accreditation	CNPD requirements
('standard' requirements) ISO 17065 ISO 17021 ISAE …	Data protection linked requirements

Additional information

Maximum period of 3 years (renewable)

Withdrawal of the certification

Periodical review from the CNPD



Codes of conduct: advised, approved, registered and published by CNPD

Penalties: aggravating or mitigating factor

DO NOT WAIT for certifications to comply with the GDPR!