# Certification RGPD
# GDPR-CARPA

Luxembourg

28 juin, 2022

CNPD - Alain Herrmann
Commissaire

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

# Qu’est-ce que la certification RGPD?

# Contexte juridique

## Article 42 RGPD – Certification

- Adoption des critères de certification (APD ou EDPB pour les seal EU)
- Exigences sur la certification propres au contexte RGPD
- Transparence + mise à disposition du public
- Particularité pour les certifications comme outils de transfert

## Article 43 RGPD – Organismes de certification

- Exigences liées à l'agrément des organismes de certification
- Art. 43.1(a) = article 15 de la loi du 1er août 2018 portant organisation de la CNPD et la mise en oeuvre du RGPD

# Quelques définitions

## Organisme d'accréditation

- APD ou Organisme national d'accréditation

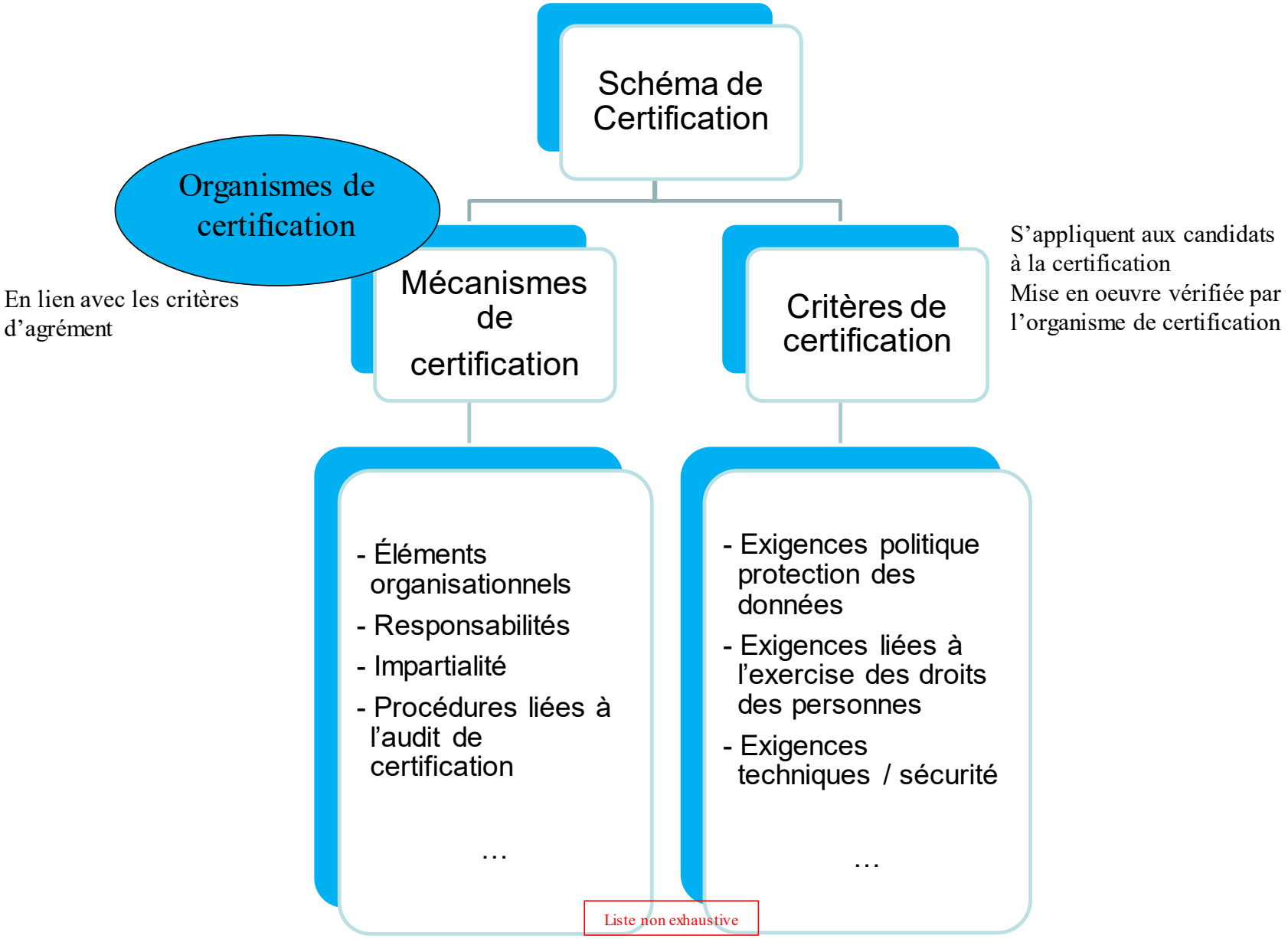
## Organisme de certification

- Un organisme de certification a pour activité de **délivrer, d'examiner, de renouveler et de retirer les certifications** sur la base d'un mécanisme de certification et de critères de certification approuvés.

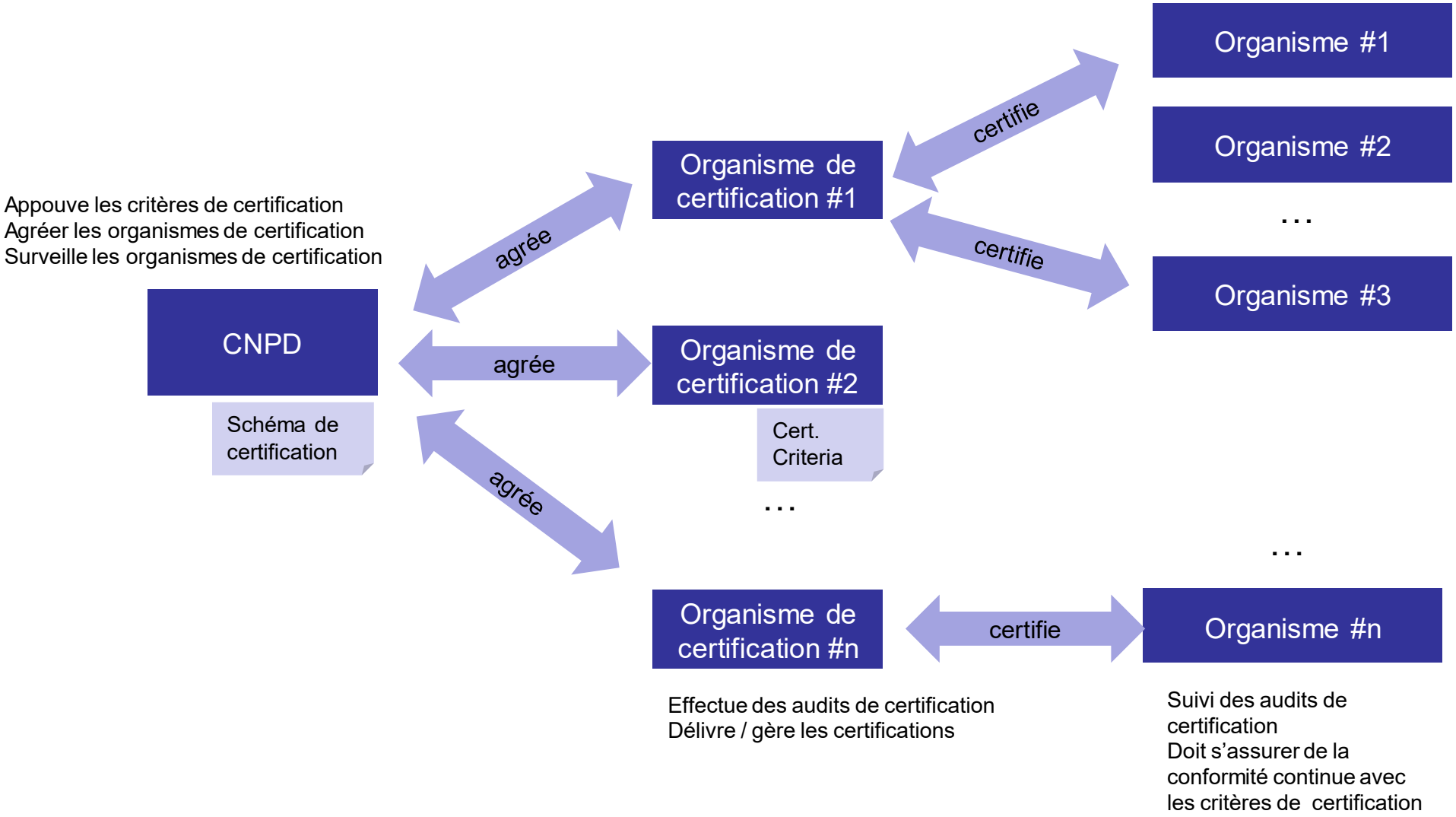
## Critères de certification

- Exigences auxquelles les organisations candidates à la certification doivent se conformer pour obtenir la certification

# Schémas de certification



# Les acteurs de la certification RGPD au Luxembourg



# Les critères d'agrément d'organismes de certification

ISO17065 (Evaluation de la conformité – Exigences pour les organismes certifiant les produits, les procédés et les services)

+

Exigences additionelles EDPB

+

Exigences liées au standard ISAE 3000

+

ISQC1

- ✓ Permet à la CNPD de se reposer sur des best practices / pratiques reconnues
- ✓ Méthode commune pour les activités d'évaluation effectuées par les organismes de certification

# Critères d'agréments organisme de certification

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

**Exigences générales** | **Exigences structurelles** | **Exigences pour les process** | **Exigences ressources** | **Exigences système de management**

1. Autorisation d'émettre des rapp
2. Preuve de ressources financières
3. Mise en place des mécanismes
4. …

Mise en place d'u
**général et fonctio**
de certification

Top management

Gestion des sous t
compétences, conf
indépendance)

**Le processus de certification mis en plac**
**critères :**

1. Méthodologie d'évaluation
2. Audit et émission du rapport ISAE 30
3. Revue du rapport ISAE3000
4. Décision de certification – mise en pl
5. Gestion des certifications
6. Monitoring permanent de l'indépendance

**Le candidat doit prouver :**

- Un nombre de ressources compét
- Des compétences & qualification (contrôle des CV, interview avec l
- Une bonne plannification et cont et techniques (revue du programm
-L'indépendance (revue du processus de contrôle de l'independance)

Prouver la mise en place d'un cadre de contrôle interne de l'activité de certification (audit interne, documentation)

- *Procédures et processus*

# Qu’est-ce qui peut être certifié?

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

**Les opérations de traitements mises en oeuvre par les responsables de traitements et les sous-traitants.**

| | |
|---|---|
| Gestion RH | **OUI** |
| Process AML / KYC | OUI |
| Software as Service | [OUI] |
| Logiciel en ‘boite’ | NON |

# Certification
# GDPR CARPA

## EDPB adopts first opinion on certification criteria

*2 February 2022* EDPB

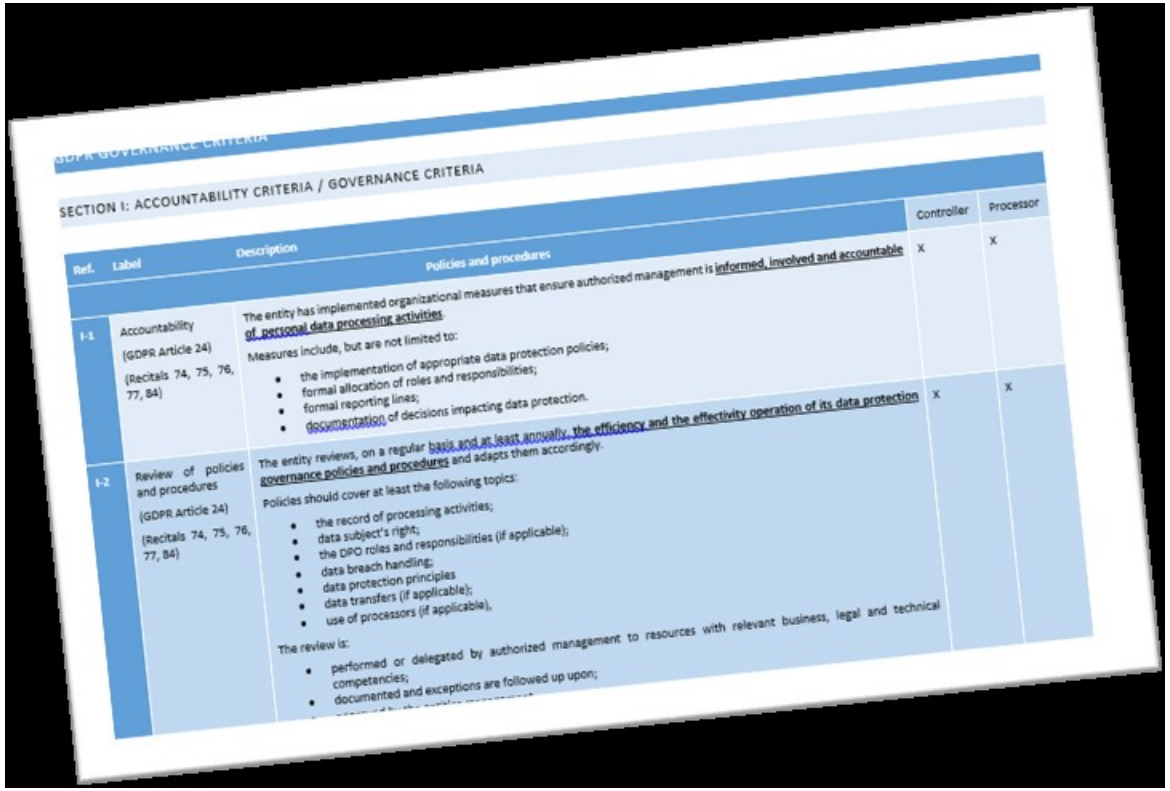
The EDPB adopted its opinion on the GDPR-CARPA certification scheme submitted to the Board by the Luxembourg Supervisory Authority (SA). This is the first time that the EDPB adopts a consistency opinion on criteria for a nationwide certification scheme. The GDPR-CARPA certification scheme is a general scheme, which does not focus on a specific sector or type of processing. It includes requirements on data protection governance in the organisation surrounding the processing activities.

EDPB Chair, Andrea Jelinek, said: "This opinion is an important step towards greater GDPR compliance. The main aim of certification mechanisms is to help controllers and processors demonstrate compliance with the GDPR. Controllers and processors adhering to a certification mechanism also gain greater visibility and credibility, as it allows individuals to quickly assess the level of protection of the processing operations."
The EDPB opinion aims to ensure the consistency and correct application of certification criteria among SAs in the European Economic Area. To this end, the EDPB considers that a number of changes need to be made to the draft certification criteria.

After approval by the SA, the certification mechanism will also be added to the register of certification mechanisms and data protection seals in accordance with Art. 42 (8) GDPR.

Note to editors:
*The present certification is not a certification according to article 46(2)(f) of the GDPR meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations.*

*All documents adopted during the EDPB Plenary are subject to the necessary legal, linguistic and formatting checks and will be made available on the EDPB website once these have been completed.*



SECTION 1: ACCOUNTABILITY CRITERIA / GOVERNANCE CRITERIA

| Ref. | Label | Description | Policies and procedures | Controller | Processor |
|---|---|---|---|---|---|
| I-1 | Accountability (GDPR Article 24) (Recitals 74, 75, 76, 77, 84) | The entity has implemented organizational measures that ensure authorized management is informed, involved and accountable of personal data processing activities. | Measures include, but are not limited to: • the implementation of appropriate data protection policies; • formal allocation of roles and responsibilities; • formal reporting lines; • documentation of decisions impacting data protection. | X | X |
| I-2 | Review of policies and procedures (GDPR Article 24) (Recitals 74, 75, 76, 77, 84) | The entity reviews, on a regular basis and at least annually, the efficiency and the effectivity operation of its data protection governance policies and procedures and adapts them accordingly. | Policies should cover at least the following topics: • the record of processing activities; • data subject's right; • the DPO roles and responsibilities (if applicable); • data breach handling; • data protection principles • data transfers (if applicable); • use of processors (if applicable), The review is: • performed or delegated by authorized management to resources with relevant business, legal and technical competencies; • documented and exceptions are followed up upon; | X | X |

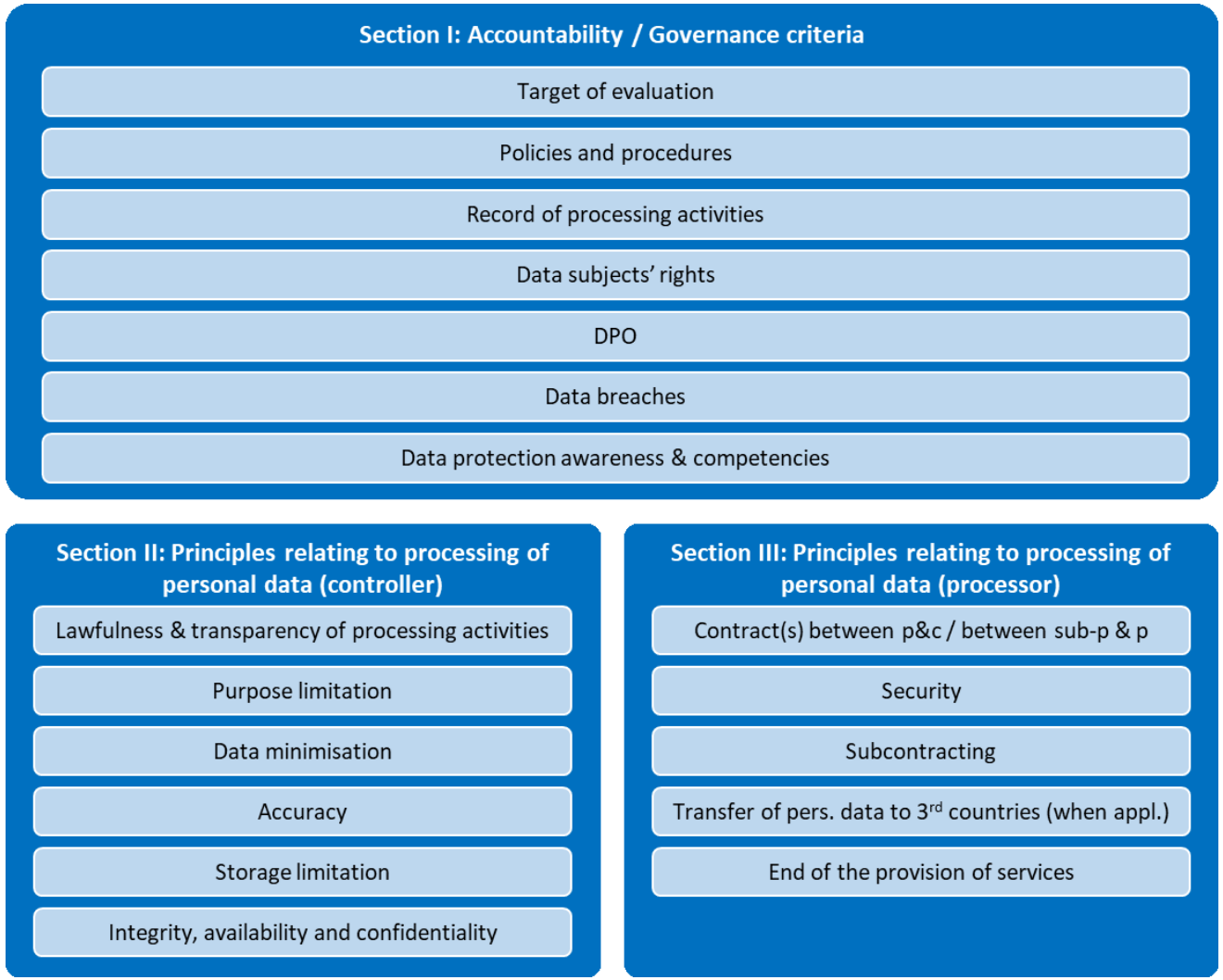
# La certification GDPR CARPA

La certification GDPR-CARPA est conçue pour fournir aux responsables du traitement et aux sous-traitants:

- un haut niveau de conformité au RGPD et
- une assurance qu'ils appliquent des mesures techniques et organisationnelles pour se conformer à leurs obligations RGPD pour leurs opérations de traitements faisant l'objet de la certification.

Il constitue un élément qui permet aux responsables du traitement et aux sous-traitants de démontrer la conformité de ces opérations de traitement certifiées avec le RGPD.

# GDPR CARPA: la structure des critères de certification




Les critères sont organisées en 3 sections :

- ✓ Section I:
  - ✓ S'applique aux responsables de traitement et sous-traitants;
  - ✓ Contient des critères relatifs à la gouvernance;
- ✓ Section II:
  - ✓ S'applique aux responsables de traitement
  - ✓ Couvre les principes de protection des données, droits des personnes, gouvernance de la sécurité;
- ✓ Section III:
  - ✓ S'applique aux sous-traitants
  - ✓ Contient des critères sur les obligations contractuelles (avec le RT), gouvernance de la sécurité, sous sous-traitance, l'arrêt du service de sous-traitance;

# La certification GDPR CARPA

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Critères non sectoriels:

Les critères de certification GDPR-CARPA sont conçus pour être suffisamment flexibles pour être pertinents pour une panoplie d'opérations de traitement dans plusieurs secteurs. Chaque entité peut définir et mettre en œuvre les mesures qui conviennent le mieux à sa situation et à son secteur spécifiques pour se conformer aux critères.

Limitation du champ d'application de la certification GDPR-CARPA:

Sécurité des traitements: uniquement éléments de gouvernance gestion des risques / sécurité

Seuls les responsables du traitement et les sous-traitants établis au Luxembourg, sous la supervision de la CNPD, peuvent demander une certification GDPR-CARPA.

# Exclusions du champ d'application de la certification GDPR CARPA

## GDPR-CARPA ne convient pas:

- pour certifier le traitement des données à caractère personnel ciblant spécifiquement les mineurs de moins de 16 ans;
- pour les certifications des activités de traitement dans le cadre d'un contrôle conjoint;
- pour les activités de traitement dans le cadre de l'article 10 du RGPD;
- pour les entités qui n'ont pas désigné un DPD (article 37 du RGPD). Il convient de noter que les entités sont libres de désigner un DPD, même dans le cas où elles ne sont pas obligées de le faire.

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

# Une certification RGPD

# NE DE-RESPONSABILISE PAS

# les organisations

# GDPR CARPA Procédure Certification

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

**Candidature**

- Applicabilité (ToE)
- Application process
- Engagement letter
- Contrat de certification

**Certification audit**

- Activités d'évaluation
- Non-conformités
- Assurance report (type II)

**Certification décision**

- Evaluation basée sur le rapport d'assurance

**Délivrance du certificat**

- Documentation formelle
- Registre Publique

**Certification Validité**

- Validité de la certification : 3 ans
- Validity d'un rapport ISAE: maximum 1 an
- Minimum 3 rapports ISAE requis pour 1 cycle

**Management certification**

- Changement pouvant affecté la certification
- Utilisation du seal GDPR-CARPA

GDPR CARPA
CERTIFIED
CNPD
#ref

# La certification GDPR CARPA

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

- ✓ Les responsables de traitement et sous-traitants ayant obtenu une certification GDPR-CARPA vont pouvoir démontrer l'exercise d'un haut niveau de responsabilité pour les operations de traitements certifiés

- ✓ Prise en compte du système de gouvernance de la protection des données: impact positif sur tous les traitements même hors scope de la certification

- ✓ Permet d'obtenir la confiance des clients / utilisateurs / personnes concernés dans les traitements certifiés

# La certification GDPR CARPA

- ✓ Approche totalement intégrée avec les exigences d'agrément - UNIQUE
- ✓ La CNPD a une maîtrise de l'entièreté du processus, y compris la propriété d'un schéma de certification – UNIQUE

- ➢ Minimisation des risques d'abus de la certification
- ➢ Minimisation des risques d'un audit de certification de faible qualité
- ➢ Possibilité de réaction rapide en cas de problème n'importe où dans la chaîne de certification

# Plus d'information sur notre site web

GDPR GOVERNANCE CRITERIA

SECTION I: ACCOUNTABILITY CRITERIA / GOVERNANCE CRITERIA

| Ref. | Label | Description | Policies and procedures | Controller | Processor |
|---|---|---|---|---|---|
| I-1 | Accountability (GDPR Article 24) (Recitals 74, 75, 76, 77, 84) | The entity has implemented organizational measures that ensure authorized management is informed, involved and accountable of personal data processing activities. Measures include, but are not limited to: • the implementation of appropriate data protection policies; • formal allocation of roles and responsibilities; • formal reporting lines; • documentation of decisions impacting data protection. | | x | x |
| I-2 | Review of policies and procedures (GDPR Article 24) (Recitals 74, 75, 76, 77, 84) | The entity reviews, on a regular basis and at least annually, the efficiency and the effectivity operation of its data protection governance policies and procedures and adapts them accordingly. Policies should cover at least the following topics: • the record of processing activities; • data subject's right; • the DPO roles and responsibilities (if applicable); • data breach handling; • data protection principles • data transfers (if applicable); • use of processors (if applicable), The review is: • performed or delegated by authorized management to resources with relevant business, legal and technical competencies; • documented and exceptions are followed up upon; | | x | x |

https://cnpd.public.lu/fr/professionnels/Certification.html

Email de contact: certification@cnpd.lu

**Questions?**