GDPR-CARPA

Certification Candidate

Shariq Arif

Senior Manager, Advisory

Grant Thornton

Agenda

- Introduction: the need for certification
- Evidencing accountability
- Ongoing assurance exercise
- The advantages of the GDPR-CARPA certification
- Unique attributes of the GDPR-CARPA certification
- Eligible institutions and companies
- ISAE 3000 certification
- Questions & feedback

Introduction: the need for certification

- In short: Article 42 of the GDPR encourages the establishment of certification mechanisms.

1. GDPR compliance is difficult to evidence

- Articles to comply with are not always detailed
- EDPB guidelines are numerous and difficult to reconcile

2. Not all processing activities warrant the same degree of scrutiny

- Firms typically want to have assurance that critical personal data processing activities are being administered to a heightened degree

3. Transparency and compliance with the GDPR can be enhanced

- Several certifications on the market are available, but the GDPR-CARPA is the only one to have been issued by a data protection authority

Evidencing accountability

- Internal tracker files can be reconciled to GDPR-CARPA criteria to evidence accountability

Simplified GDPR action plan

Main GDPR compliance criteria for Client	Main GDPR requirements	Required/Strongly Recommended activities
Governance	CLIENT shall have a data protection strategy	Prepare a Data Protection Policy (strongly recommended)
	CLIENT shall ensure that data protection is taken into account at the Board of Directors level	Have Data Protection Policy validated by the Board of Directors
	CLIENT shall ensure personal data is protected from by design and default	Have a Privacy by Design and Default Policy (strongly recommended)
Person in charge of data protection	Client shall nominate either: - an official Data Protection Officer (DPO) (*), or - a Data Protection Responsible (DPR) (*) Where a DPO is nominated this party should be communicated to the Local Supervisory Authority	Include a detailed description of the DPO/DPR duties in the Data Protection Policy (strongly recommended)
	Client shall ensure involvement of the DPO/DPR in all data protection-related matters	Include a detailed description of the DPO/DPR duties in the Data Protection Policy (strongly recommended)
Awareness on data protection	Client shall ensure an ongoing high level of awareness on data protection among employees	Hold training sessions to staff (regular)
Role of controller and processor – Related responsibilities	Client shall identify its roles of controller or processor in all personal data processing activities	Establish a Records of Processing Activities (RPA)(Art. 30) (strongly recommended and often a requirement)
GDPR compliance of Client as controller	Client as controller shall commit to GDPR compliance	Insert a data protection clause into Engagement Letters (EL) and, where applicable, General Terms and Conditions (GTC) outlining compliance of Client as per GDPR Art.24
		Ensure processing by a processor is governed by a contract or other legal act as per GDPR Art.28 ("Data Processing Agreement")
GDPR compliance of Client as processor	CLIENT as processor/sub-processor shall commit to GDPR compliance to their clients	Insert a data protection clause into Engagement Letters (EL) and General Terms and Conditions (GTC) outlining compliance of CLIENT as per GDPR Art.28
Subcontracting	CLIENT (as controller or processor) shall ensure that service providers (as processors/sub-processors) that process personal data on its behalf comply with GDPR obligations	Request data protection addendum for contracts signed before 25 May 2018
		Ensure that contracts signed after 25 May 2018 contain a data protection clause outlining compliance of service providers as per GDPR Art. 28
Legitimacy of data processing activities	CLIENT shall have a legal basis associated to each data processing activity	Ensure reflected in in RPA and Privacy Statement (where applicable)
Consent	CLIENT (as controller) shall analyse whether GDPR consent is required as part of its processing activities	Ensure reflected in in RPA and Privacy Statement (where applicable)
	Client (as controller) shall analyse whether cookies are used on its website. In this case, a GDPR compliant cookie notice ("cookies banner") is required.	Ensure the "cookies banner" allow users to express a valid consent as per GDPR Art.4 and EDPB Guidelines on valid consent (where applicable)
Personal data retention periods	CLIENT (as controller) shall not process personal data for longer than required	Identify data retention periods applicable to each processing activity. Integrate within the RPA (strongly recommended)
		Have a Data Retention Policy in place (strongly
		Analyse the possibility to erase personal data within CLIENT applications and filing systems holding personal data

✓ **Controllers: Demonstrate controller / processor obligations**

Governance | Awareness of Data Protection | Compliance requirements where acting as a Controller | Compliance requirements where acting as a Processor | ...

Main GDPR compliance priorities for B******	Section from GDPR-CARPA Criteria	Main GDPR requirements
Governance	Section 1.1 Accountability Section 2.a. 8: Processing of special categories of personal data Section 2.a.14/15: Right of Access and Portability Section 2.c.1/2: Data Minimisation Section 2.d.1/2: Accuracy of the data source / Data up-to-date Section 2.d.3/4: Right of rectification / Right of restriction Section 2.e.1/2: Retention periods and right of erasure	Where proportionate in relation to processing activities the controller shall include the implementation of appropriate data protection policies.
Governance	Section 1.1 Accountability	B****** shall ensure that data protection is taken into account at the Board of Directors level
Governance	Section 1.1 Accountability	Where proportionate in relation to processing activities the controller shall include the implementation of appropriate data protection policies.
	Section 1.2 Review of policies and procedures	Where proportionate in relation to processing activities the controller shall include the implementation of appropriate data protection policies.
Governance	Section 1.2 Review of policies and procedures	B****** reviews, on a regular basis and at least annually, the operational effectiveness of its data protection governance policies and procedures and adapts them accordingly.
Awareness on data protection	Section 1.12: Data Breach Section 1.13: Data Breach Notification Section 1.8: DPO Designation Section 1.11: DPO Tasks	B****** shall raise awareness on data protection among B****** employees
Awareness on data protection	Section 1.12: Data Breach Section 1.13: Data Breach Notification Section 1.8: DPO Designation Section 1.11: DPO Tasks	B****** shall ensure an ongoing high level of awareness on data protection among B****** employees
Role of controller and processor – Related responsibilities	Section 1.3: Management of the record of processing activiites Section 1.4: Management of the record of processing activiites Section 1.5: Content (RoPA) Section 1.6: Content (RoPA) Section 2..a.1: Identification of a valid legal basis	B****** shall identify its roles of controller or processor in all personal data processing activities

Grant Thornton

Evidencing accountability: determining the scope

- GDPR-CARPA assesses compliance per processing activity

Across the whole personal data lifecycle

Step 1: Assess which processing activities warrant certification

Step 2: Categorise the processing activity

Step 3: Determine the applicability of GDPR-CARPA criteria

Step 4: Apply the applicable evaluation criteria to the processing activity

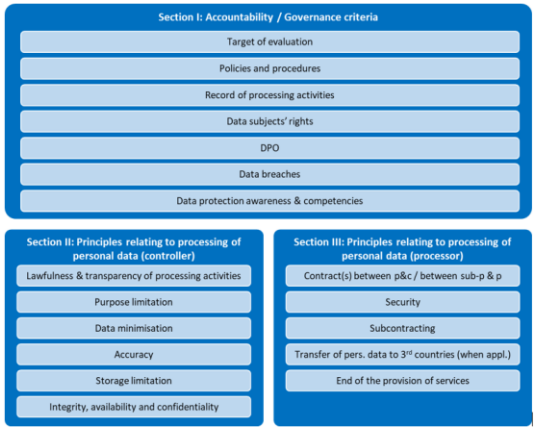
Business decision

Processing activities critical for going concern

Mature (optimized) processing activities that satisfy the GDPR-CARPA criteria

Processing activity (as per the register)	Role	Level 1 Organisation	Level 2 Circumstances / purpose	Level 3 functional application	Level 4 IT infrastructure
Recruitment	Controller	Financial institution	HR department	SAP-HR	Windows server farm, Oracle DB
Newsletter	Controller	Financial institution	Marketing	CRM	Cloud solution-SAAS
AML/KYC	Controller	Financial institution	Compliance Client relationship Managers	World Check Avaloq	Cloud solution-SAAS Unix servers – Oracle DB

Source: CNPD, 2018



Source: CNPD, 2022

Overview of Section I: Accountability criteria / Governance criteria

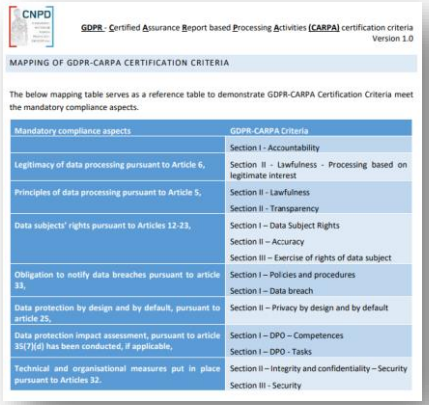
Subject	Criteria for controllers			Criteria for processors		
	Ref.	Page	Title	Ref.	Page	Title
Target of Evaluation	I-0	9	Definition of the target of evaluation	I-0	9	Definition of the target of evaluation
Policies and procedures	I-1	9	Accountability	I-1	9	Accountability
	I-2	10	Policies and procedures	I-2	10	Policies and procedures
	I-3	10	Review and update of policies and procedures	I-3	10	Review and update of policies and procedures
Record of processing activities	I-4	11	Record of processing activities	I-5	11	Record of processing activities
	I-6	12	Management of the record of processing activities	I-7	12	Management of the record of processing activities
Data Subjects' Rights	I-8	13	Facilitate the exercise of data subjects' rights	I-9	14	Facilitate the exercise of data subjects' rights

Source: CNPD, 2022

Grant Thornton

Evidencing accountability: preparatory steps

- Management reporting metrics can convey level of compliance <u>per processing activity</u>



CNPD

GDPR - Certified Assurance Report based Processing Activities (CARPA) certification criteria
Version 1.0

MAPPING OF GDPR-CARPA CERTIFICATION CRITERIA

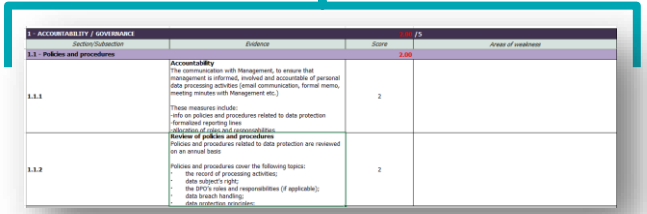
The below mapping table serves as a reference table to demonstrate GDPR-CARPA Certification Criteria meet the mandatory compliance aspects.

Mandatory compliance aspects	GDPR-CARPA Criteria
	Section I - Accountability
Legitimacy of data processing pursuant to Article 6,	Section II - Lawfulness - Processing based on legitimate interest
Principles of data processing pursuant to Article 5,	Section II - Lawfulness
	Section II - Transparency
Data subjects' rights pursuant to Articles 12-23,	Section I – Data Subject Rights
	Section II – Accuracy
	Section III – Exercise of rights of data subject
Obligation to notify data breaches pursuant to article 33,	Section I – Policies and procedures
	Section I – Data breach
Data protection by design and by default, pursuant to article 25,	Section II – Privacy by design and by default
Data protection impact assessment, pursuant to article 35(7)(d) has been conducted, if applicable,	Section I – DPO – Competences
	Section I – DPO - Tasks
Technical and organisational measures put in place pursuant to Articles 32.	Section II – Integrity and confidentiality – Security
	Section III - Security

Source: CNPD, 2022

✓ **Demonstrate compliance with data protection requirements**

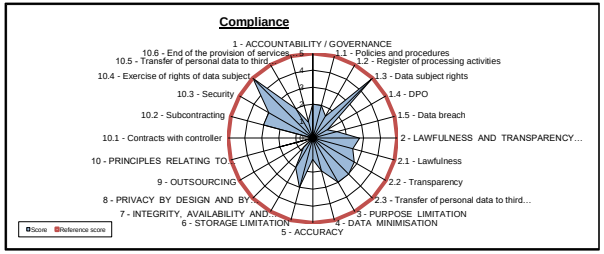
Section/Subsection	Reference score
Section I: ACCOUNTABILITY CRITERIA	5.00
ACCOUNTABILITY / GOVERNANCE	
Policies and procedures	5.00
Accountability	
Review of policies and procedures	
Register of processing activities	5.00
Management of the record	
Management of the record (Processor)	
Content	
Content (Processor)	
Data subject rights	5.00
Data subjects rights	
DPO	5.00
Designation	
Competences	
Position	
Tasks	
Data breach	5.00
Data breach	
Notification towards the controller (Processor)	

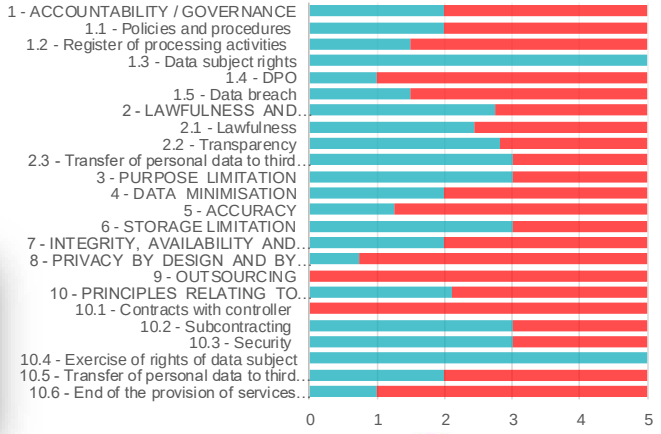


1 - ACCOUNTABILITY / GOVERNANCE — 2.60 /5

Section/Subsection	Evidence	Score	Areas of weakness
1.1 - Policies and procedures		2.00	
1.1.1	**Accountability** The communication with Management, to ensure that management is informed, involved and accountable of personal data processing activities (email communication, formal memo, meeting minutes with Management etc.) These measures include: - info on policies and procedures related to data protection - formalized reporting lines - allocation of roles and responsibilities	2	
1.1.2	**Review of policies and procedures** Policies and procedures related to data protection are reviewed on an annual basis Policies and procedures cover the following topics: - the record of processing activities; - data subject's right; - the DPO's roles and responsibilities (if applicable); - data breach handling; - data protection principles;	2	

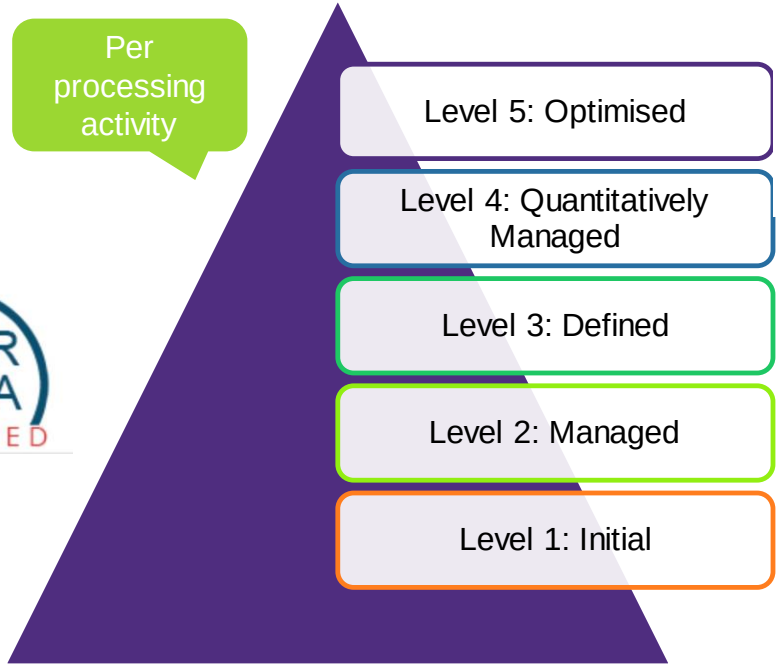
Source: Luxgap sàrl, 2021



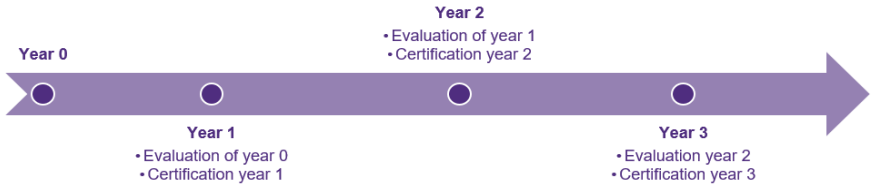


Grant Thornton

Ongoing assurance exercise



Source: Capability Maturity Model Integration



A **GDPR-CARPA certificate could be renewed for up to 3 years**, subject to:

- ✓ Annual ISAE 3000 engagements
- ✓ An unqualified audit opinion (clean report) in each instance

Note: GDPR certificate could be suspended, reduced, terminated or withdrawn.

The advantages of the GDPR-CARPA certification

	Common to other personal data protection certifications	Unique to GDPR-CARPA
Fully covers the GDPR	☑	☑
Distinguishes between Processor and Controller	☑	☑
Proportionate – high risk / robust controls	☑	☑
Allows certification for specific processing activities (focused scope)	☒	☑
Provides controls for parts of the GDPR where limited guidelines exist	☒	☑
Scalable (tailored)	☒	☑

Grant Thornton

Unique attributes of the GDPR-CARPA certification

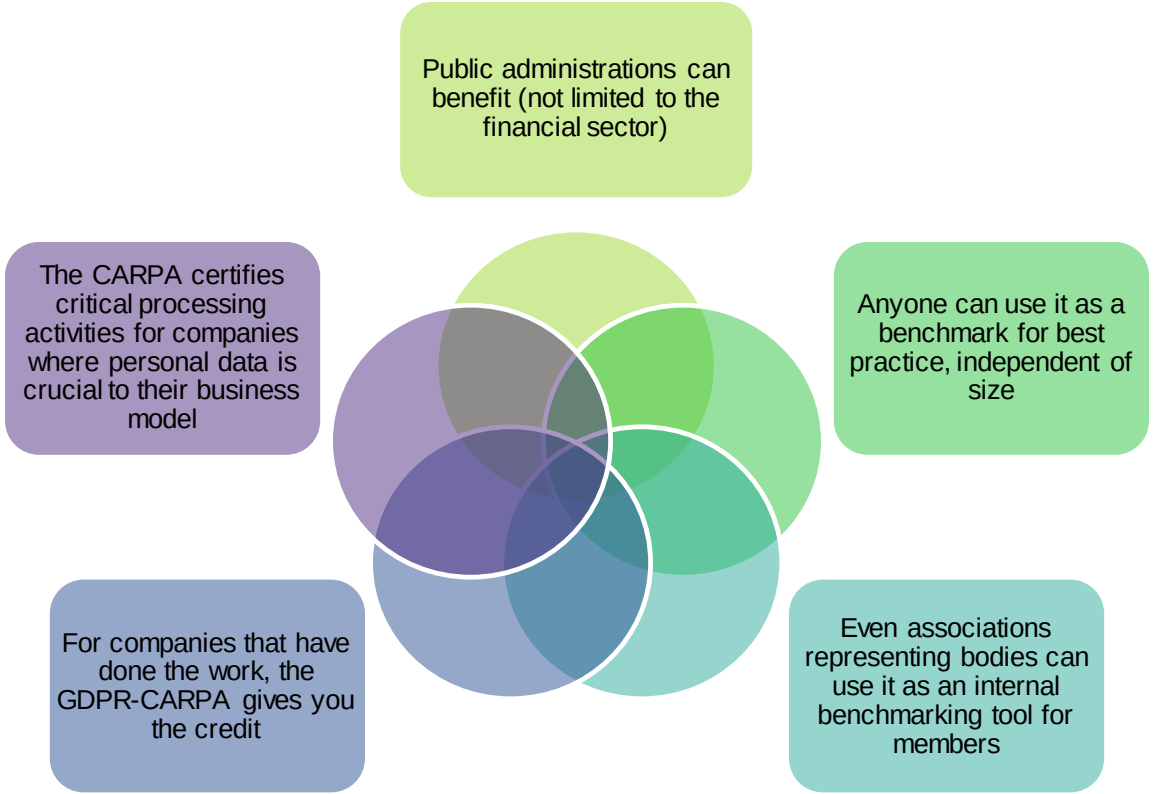
Certification created by a competent authority (CNPD) and assessed by CNPD-approved certification bodies subject to onsite inspections

Based on the GDPR, from the ground up

Considers how specific “processing activities” are governed and administered

Grant Thornton

Eligible institutions and companies



Grant Thornton

The ISAE 3000 certification

1st line

- The Business

"Doer"

2nd line

- DPO
- Control functions

"Reviewer" (*)

External assurance by a Réviseur d'Entreprises

3rd line

- Assurance Mandates

ISAE 3000 report paired to GDPR-CARPA

(*) Can be internal to the firm or outsourced to a third party

Aligning with GDPR-CARPA

Certification with GDPR-CARPA

Grant Thornton

Questions & feedback

Contact

Grant Thornton Luxembourg

13, rue de Bitbourg
L-1273 Luxembourg

T +352 45 38 78 1
F +352 45 38 29

W www.grantthornton.lu

Grant Thornton Luxembourg

Grant Thornton