



Towards GDPR-CARPA Certification

Michael Hofmann

28 June 2022



Building a better
working world



Contents

- 1 Why: GDPR-CARPA Certification
- 2 What: GDPR-CARPA Certification
- 3 How: Our services towards GDPR-CARPA Certification and use cases





1 Why: GDPR-CARPA Certification

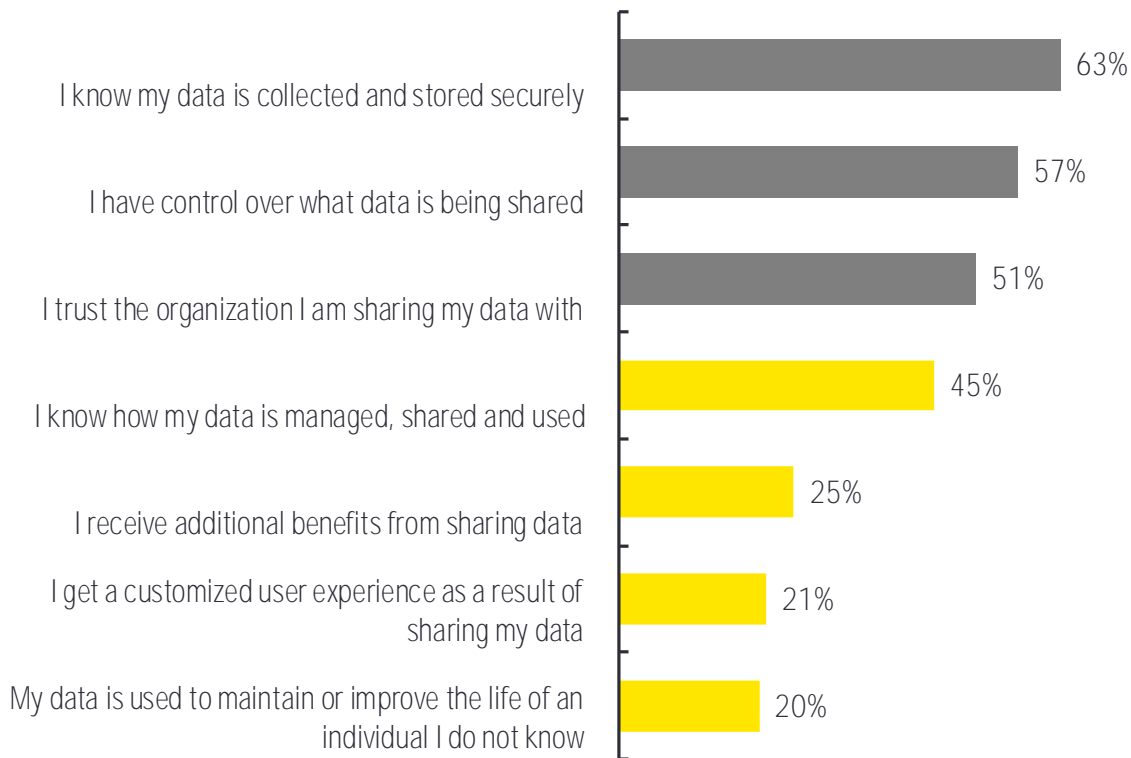


GDPR compliance programs will need to keep pace to address business and privacy risks as the industries continue to digitalize

Digital transformation/ emerging technologies	Complex IT environments	Technology implementations and upgrades (CIA principles)	Data breaches	Data governance	Insider threat (Awareness and training)	Third-party risk management (data controller vs data processor)
<ul style="list-style-type: none">Whether digitalization is used to transform in-store experiences or completely redesign the consumer journey, digital adoption will create vulnerabilities and increase the need for cybersecurity expertise and controls to protect customer data and their profiling.	<ul style="list-style-type: none">Legacy systems and proprietary systems are often based on older standards. The complexities of operational data and protocol conversion taken together with network communications and security, make it a daunting task without a structured approach for implementing GDPR.	<ul style="list-style-type: none">Failure to implement new information technology systems or needed upgrades to systems, including operational and financial systems, could expose companies to external and internal threats and adversely affect GDPR implementation.	<ul style="list-style-type: none">The breach of systems containing personal information could subject companies to adverse publicity, costly government enforcement actions or private litigation, and expenses.Failure to protect intellectual property rights and high-value assets could diminish the value of brands.	<ul style="list-style-type: none">Failure to comply with the various laws and regulations as well as changes in laws and regulations could have an adverse impact on reputation, financial condition, or results of operations. The increased handling of customer data will require a data governance strategy.	<ul style="list-style-type: none">Failure to monitor and act upon indicators that reveal insiders at work could result in the exposure of critical and physical assets. Insiders — whether employees, contractors or third parties — could use access to compromise the confidentiality, integrity or availability of network systems, data or premises, whether or not out of malicious intent.	<ul style="list-style-type: none">Companies have limited control over vendors. Maintaining strong due diligence, continuous monitoring, oversight and limiting vendor connectivity are key to minimizing the vendor risk landscape.



When sharing personal data with an organization, security, control and trust are rated as the most important



- COVID-19 has ushered in significant changes that may have **altered consumers' attitudes** toward data privacy, but they are unwavering about the importance of security.
- Consumers are more willing to share their personal data, but when doing so, the following factors are rated as most important:
 - Secure collection and storage processes (63%)
 - Control over what data is being shared (57%) and;
 - Trust (51%)

Q: Proportion of consumers that rate the factors outlined above as most important when choosing to share their personal data with an organization (respondents were asked to select their top three responses)

Source: EY global consumer privacy survey 2020 — https://www.Ey.Com/en_in/consulting/ey-global-consumer-privacy-survey

2 What: GDPR-CARPA Certification





CNPD established criteria for the GDPR Certified Assurance Report based Processing Activities ([GDPR-CARPA](#)).

- European Data Protection Board: 2.2.2022
- CNPD: 13.5.2022



What is CARPA?

- ▶ A certification which demonstrates GDPR data protection and privacy safeguards are in place for selected processing activities via independent, third-party attestation
- ▶ CARPA can help minimize compliance and reputation risks associated with GDPR

Who should consider it?

- ▶ Companies which handle significant amounts of PII and operate in Luxembourg and Europe*
- ▶ Companies which want to provide transparency for data subjects and B2B relations like between controllers and processors

How does it work?

- ▶ Certification is granted by a certification body which is authorized by the CNPD. EY to become certification body by 2022
- ▶ To become certified, the certification body **evaluates a company's ISAE 3000 attestation** report over specific processing activities

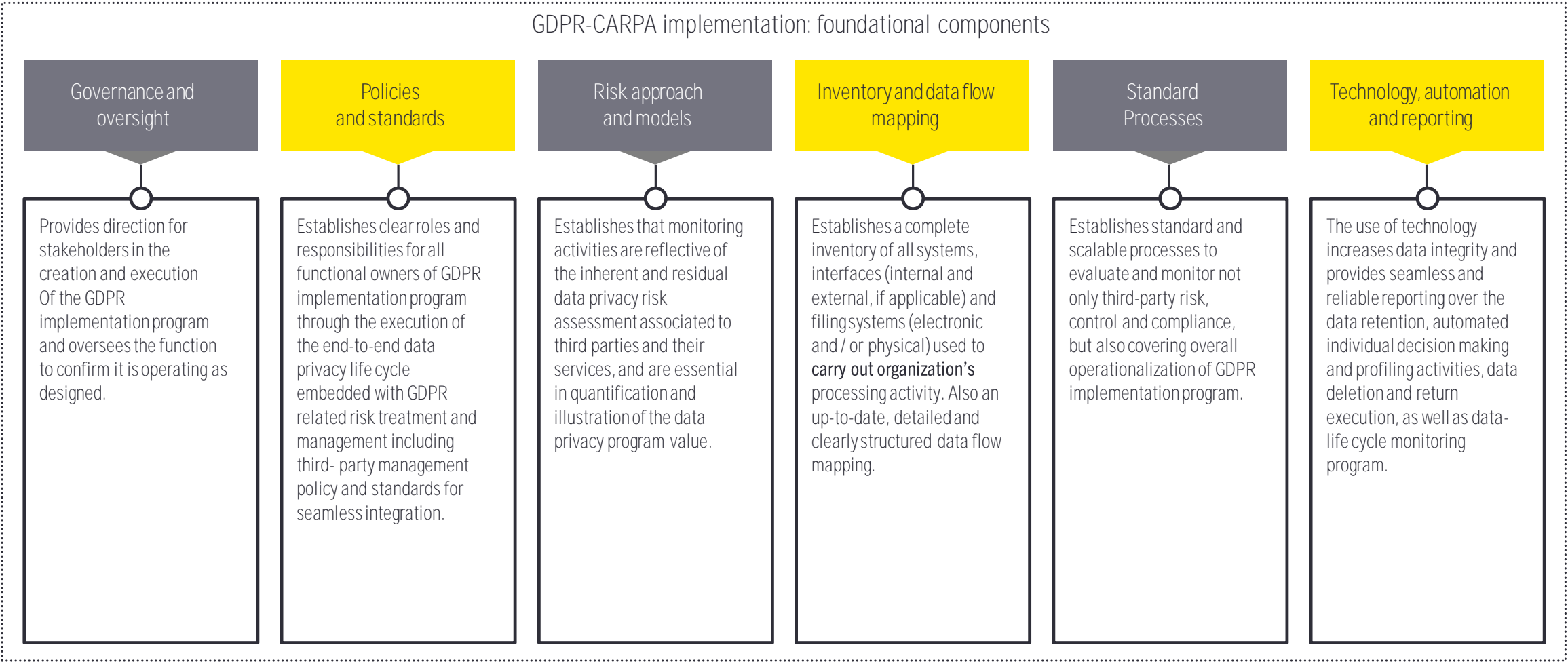
✓ Controllers: Demonstrate controller obligations

✓ Demonstrate compliance with **data protection req's by design** / default

✓ Publish the CARPA logo and reference certification bodies

✓ Demonstrate compliance with security of processing requirements

The following six areas are critical to establishing and operating an effective and efficient GDPR-CARPA implementation program:



Entities need to ensure that their internal measures be designed, implemented and controls operate effectively to allow them to reach the requirements set out in these certification criteria. When performing the certification audit, certification bodies will check whether the design, implementation and operation of these measures comply with the requirements defined by the certification criteria.



Accountability / Governance criteria	Principles Relating to Processing of Personal Data (Controller)	Principles Relating to Processing of Personal Data (Processor)
<ul style="list-style-type: none">- Policies and procedures- Record of processing activities- Data subject's rights- DPO- Data breaches- Data protection awareness & competencies	<ul style="list-style-type: none">- Lawfulness and transparency of processing activities- Purpose limitation- Data minimisation- Accuracy- Storage limitation- Integrity, availability and confidentiality	<ul style="list-style-type: none">- Contract(s) between processor & controller- Security- Subcontracting- Exercise of data subject's rights- Transfer of personal data to 3rd countries (if applicable)- End of the provision of services relating to processing

While Articles 42 and 43 of GDPR address fundamental requirements for certification procedures, the basis for certification criteria must be derived from the principles and rules set out by the GDPR in such a manner as to provide assurance that those principles and rules are complied with.

The certification procedure is guided by ISO/IEC 17065:20121 requirements which have been combined with the ISAE 3000 and other relevant standards in order to form the GDPR-CARPA accreditation requirements.

Typical 6 steps for
GDPR-CARPA
Certification
procedure

How we can help?

1. Application

- Applicability and application
- Engagement letter - ISAE 3000 (IRE general T&C)
- Engagement letter - certification

GDPR-CARPA
Maturity assessment



2. Certification audit

- ISAE 3000 Attestation engagement based on GDPR-CARPA certification criteria
- ISAE 3000 Attestation Report (type II)
- Classification of nonconformities

Providing ISAE
3000 Type 2
report



3 & 4. Certification decision & Issuing the Certification

- Assessment based on CNPD evaluation criteria
- Adaptation of the scope - if applicable
- Communication of the certification decision to the CNPD
- Granting of the certificate

Issuing the
GDPR-CARPA
certification



5 & 6. Monitoring & management of certificate

- Changes affecting certification (termination, scope reduction, suspension or withdrawal)
- Usage of the GDPR-CARPA seal

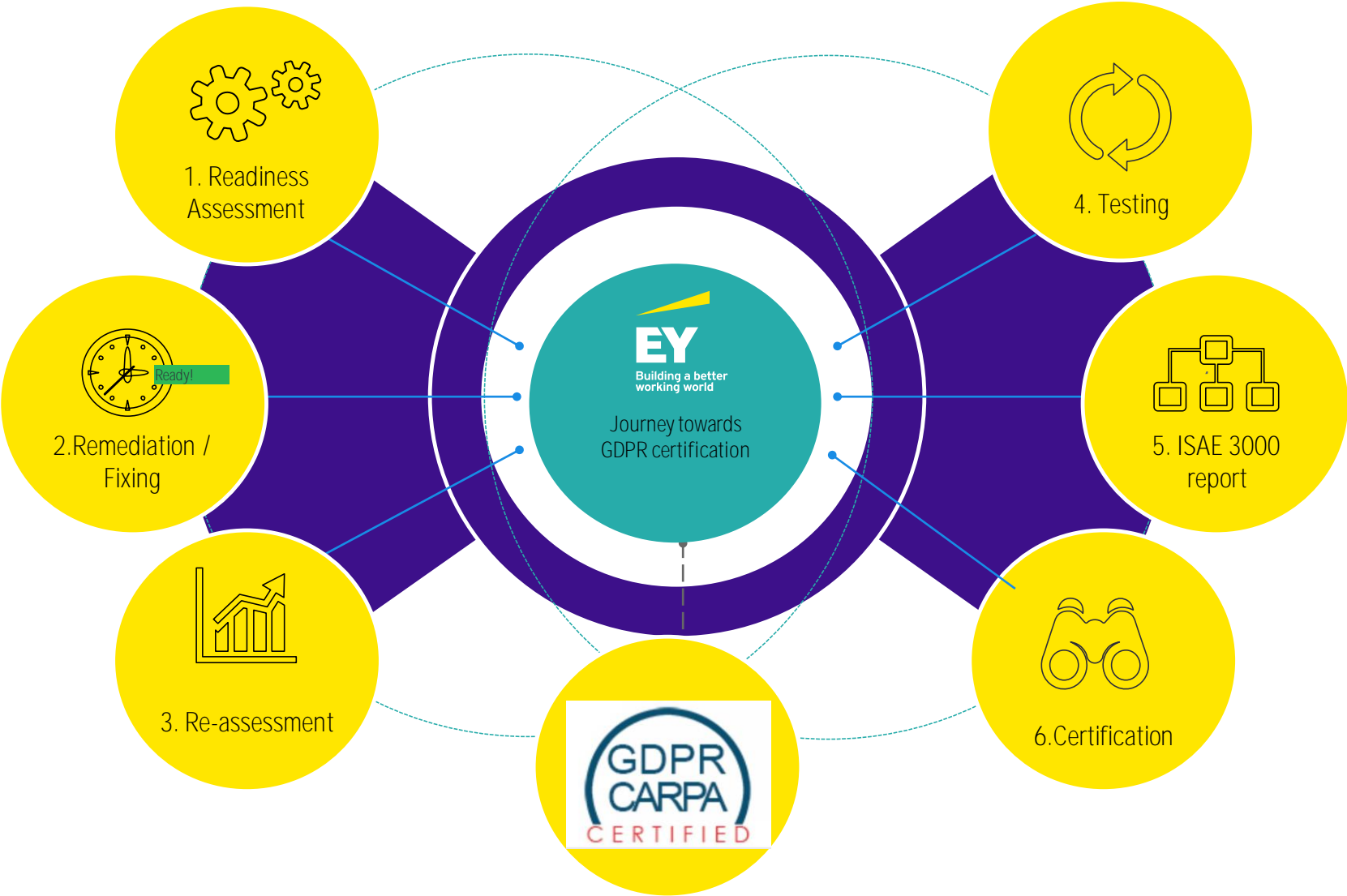
Monitoring and
Management of the certificate

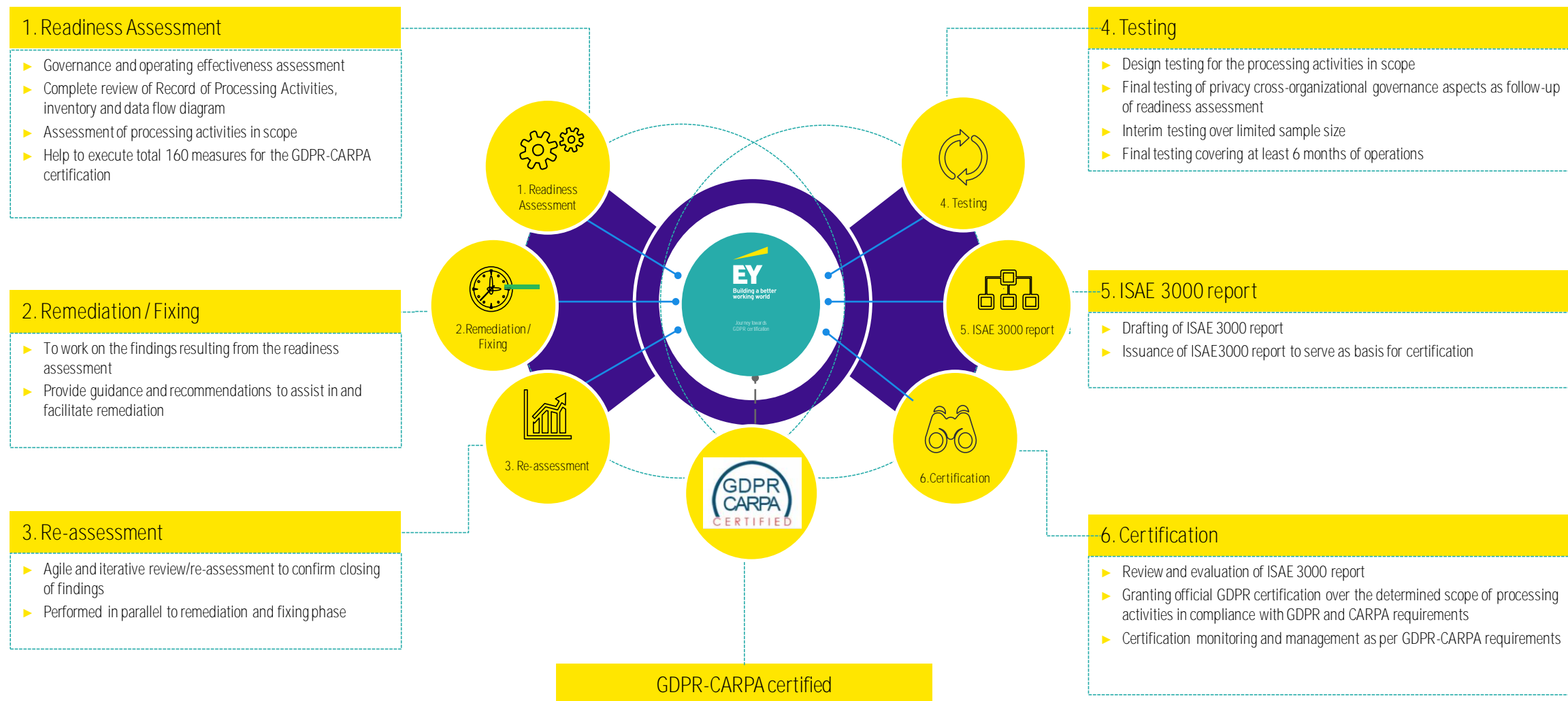


3

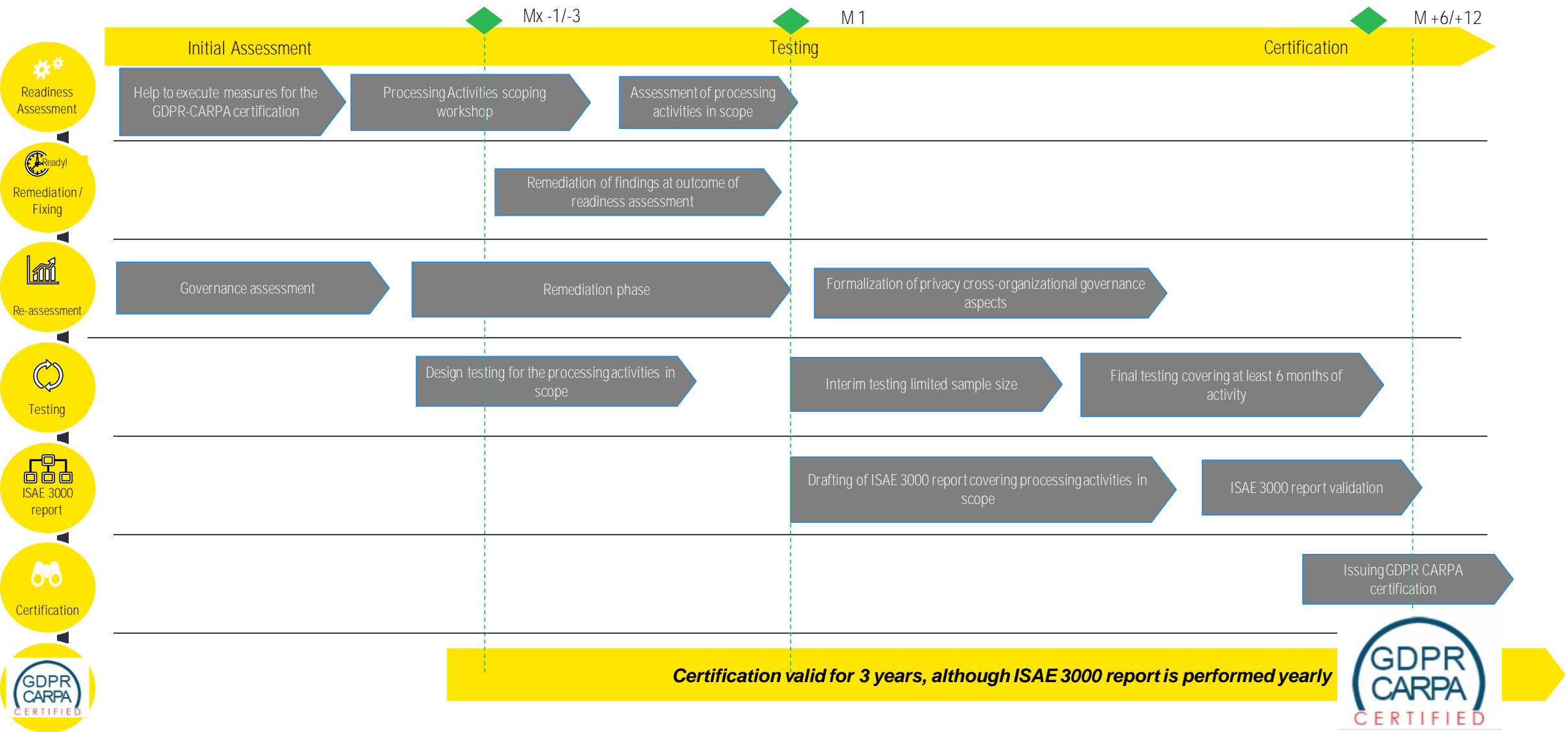
How:

Our services towards
GDPR-CARPA
Certification and use
cases





Journey towards GDPR-CARPA certification - Planning





1 Management in control

- EY data protection and privacy team helps the client to take control of the processing activities.
- We can oversee any items that demand follow up and management can easily check the overall status of data privacy compliance.
- Enables adoption of structured approach instead of unstructured processes.

2 Reduced risk and regulatory exposure

- We supports the client in identifying and reducing privacy risks within their practice.
- With support for multi-regulation compliance, we help them to reduce regulatory exposure and meet the different compliance requirements.

3 Improved efficiency and avoidance of costs

- Having a clear picture of the GDPR compliance activities and knowing where the high risks sit, we can lead to avoidance of costs.
- The costs could be fines (e.g., 4% of global annual revenue), audit costs and other expenditures.

4 Constant multidisciplinary support

- We provides clients with constant support of a global organization such as EY on GDPR-related activities and challenges.
- The operating model allows multidisciplinary support from advisory, law, fids.

5 End to end one-stop shop

- Our team provides the one of the most complete GDPR-specific solutions in the market, covering all the requirements of the regulation for GDPR-CARPA certification.
- We can help client to implement an end-to-end record of the processing activities and audit trail of data breaches and good governance monitoring including the remediation actions taken to the board and data protection authority.

6 Integrated and integrable solution

- All the modules (and related services) of our solution are integrated, providing consistency.
- We can help integrate all processing activities and their corresponding data-flow diagrams and inventories.

7 Scalability and up-to-date

- The client can start small, and acquire new modules and services only when required for achieving GDPR-CARPA certification.
- Updates are provided both from a process and content perspective (e.g., Regulatory updates).

8 Recognized industry practice

- Our team leverages the recognized industry practices developed by EY at a global level, allowing clients to increase their maturity posture in an efficient manner.



Assessment domain	Risks	Expected controls	Testing details	EU 2016/679 Reference	Activity in scope
SECTION I: DATA PROTECTION POLICIES AND PROCEDURES					
Subsection A: Accountability					
1 Existence and content of policies and procedures review	Lack of proper privacy governance model may lead entity to have no control while handling personal data.	Entity has implemented data protection governance policies and procedures that set organizational measures to ensure accountability of authorized management and effective personal data handling and management through all processing activities.	<p>Inspection of set of data protection policies and procedures and verify whether they properly cover the following topics:</p> <ul style="list-style-type: none"> • 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). <p>Verification that policies and procedures define formal allocation of roles and responsibilities, formal reporting lines and documentation of decisions impacting data protection.</p>	Art 24	<p>Policies and procedures over GDPR and data protection</p> <p>Privacy principles, policies and procedures</p>
2 Review, update and approval of policies and procedures	Obsolete policies and procedures may result in data protection breaches and ineffective data protection governance.	Entity management formally reviews and approves on a regular basis and at least annually the operational effectiveness of its data protection governance policies and procedures, including the register of processing operations.	<p>Inspection of documentation where review and approval of policies and procedures, including register of processing operations, are formalized by Entity authorized management.</p> <p>Where review and approval have been delegated by the authorized management, IA will ensure that delegated resources have relevant business, legal and technical competencies.</p>	Art 24	<p>Policies and procedures over GDPR and data protection</p> <p>Privacy principles, policies and procedures</p>
Subsection B: Data Subject Rights					
3 Data subjects rights	Lack of Data subjects rights principle may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage;	Entity has to implement procedure that explains the rights given to a data subject and sets out the mechanisms by which data subjects can exercise them, and how Entity will respond.	<p>Inquiries with management and inspection of data subjects rights policies and procedures to ensure the following measures have been implemented:</p> <ul style="list-style-type: none"> • a contact point has been appointed for receiving data subject's request for exercising their rights, that is easily reachable; • requests are recorded and their timely conducted execution documented; • for rejected requests, the justification of the reject is documented and communicated to the controller. 	Art 12	<p>Policies and procedures over GDPR and data protection</p> <p>Compliance with GDPR and related local regulation</p>

▶ Sample

Questions?
Reach out to:



Thank you!



Michael Hofmann
EY Luxembourg Partner
Executive Member of the Board
EY PFS Solutions
+352 621 632 053
michael.hofmann@lu.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2022 EYPFS Solutions S.à.r.l.
All Rights Reserved.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

