Demonstrate your GDPR compliance with the CARPA certification

Four years after the enforcement of the General Data Protection Regulation ("GDPR"), data protection and compliance remain a challenge – as recent colossal fines amounting up to 764 million euros showed recently.

With the GDPR-CARPA certification, companies can now label their compliance on the market.

Bringing assurance to companies regarding their GDPR compliance: this is the aim of the newly released GDPR-CARPA certification framework[1], an initiative of the National Commission for Data Protection (CNPD) and the first one approved on European level.

What is the GDPR-CARPA certification?

The implementation of data protection certification mechanisms has been first introduced by the GDPR. Finally, while a per se data protection certification remains voluntary, it constitutes a valuable asset for companies.

*Source: Luxembourg Times, April 27, 2022, <Demonstrate your GDPR compliance with the CARPA certification (luxtimes.lu)>
The CNPD, considering the challenge companies face to provide assurance regarding GDPR compliance, encourages companies to obtain the data protection certification, CARPA, which enjoys recognition and approval also by the European Data Protection Board. Being certified represents a transparency and trust driver for companies and contributes to their competitiveness in a more and more demanding market.

The advantage of CNPD’s certification framework is that it is designed to be general and transversal, hence suitable to all sectors. In fact, the certification focuses on specifically selected processing activities, for example client facing. Specifically, the framework is structured on three parts: a first part on data protection governance, while a second and third part on the principles applicable relates to the data controller and the data processor roles respectively.

The GDPR-CARPA certification aims to guarantee an effective GDPR control framework. First, the company to be certified should prove that it has sufficient measures in place regarding data governance, such as data protection policies and procedures, and mechanisms for managing data breaches. If the company acts as a controller in the course of the activities to be certified, it should be proven, among others, that data minimization, data retention, privacy risk management and data protection impact assessments are in place and working effectively. If, on the other hand, the company acts as a processor, it should mainly demonstrate that sufficient security measures are in place to protect personal data.

Using a well-known assurance reporting standard for greater transparency – ISAE 3000

A key step of the GDPR-CARPA certification process is the issuance of an ISAE 3000 Assurance report by an audit firm, based on the GDPR-CARPA certification criteria. Such reporting, well-known by the market for providing reasonable assurance on defined matters, is a strong demonstration of accountability and compliance with GDPR by companies.

How can we assist you in this journey?

“Independent of the current maturity level regarding data protection, EY assists companies in this journey through readiness assessments, advice in the implementation of GDPR compliance and the potential delivery of the GDPR-CARPA certification”, says Michael Hofmann, Partner, GDPR Leader at EY Luxembourg.

“As auditors, we have long experience in issuing ISAE 3000 Reports for companies seeking to provide greater transparency on compliance matters, with a dedicated team using proven methodology and project management tools”, adds Pierre-Marie Boul, Associate Partner, Asset Servicing Leader at EY Luxembourg.

[1] GDPR-Certified Assurance Report Based Processing Activities Certification Criteria

*Source: Luxembourg Times, April 27, 2022, <Demonstrate your GDPR compliance with the CARPA certification (luxtimes.lu)>