The merits of data protection certification under the GDPR

by **Sebastian Meissner**
Head of the EuroPriSe Certification Authority, EuroPriSe GmbH

EuroPriSe GmbH[1] is a company that developed a certification program whose seals certify compliance of IT products, IT-based services and websites with European Union (*EU*) data protection law and is awarded to companies.

Data protection seals of high quality are an important mean to increase the overall level of legal compliance, consumer trust and confidence in B2B[2] relationships. This is acknowledged by the EU's **General Data Protection Regulation (GDPR)**[3] which will apply in all Member States of the Union from May 25, 2018.

Art. 42(1) GDPR calls on Member States, supervisory authorities and the European Commission to encourage the establishment of data protection certification mechanisms, seals and marks that enable controllers and processors to demonstrate compliance of processing operations. The article stresses that the establishment of such mechanisms shall be encouraged, particularly at Union level.

Strong arguments suggest that a truly European approach is of the utmost importance for the success of data protection certification under the GDPR. Without such an approach, there is a high risk of the emergence of a multitude of seals of different quality, particularly on the Member State level. At worst, fragmentation might even lead to a race to the bottom in terms of cost and quality as well as to "forum shopping". Such a development would have the potential to damage the reputation of data protection certification mechanisms in general. This is why **a common EU GDPR baseline certification** is indispensable.

Art. 43, 1. GDPR stipulates that **certification bodies**, which have an appropriate level of expertise in relation to data protection, shall issue and renew certification. Pursuant to Art. 43, 2. GDPR, these certification bodies will be accredited by the competent supervisory authority and/or the national accreditation body. Art. 43, 3. GDPR determines that accreditation shall take place on the basis of criteria approved by the competent supervisory authority or by the European Data Protection Board (cf. Art. 68 ff. GDPR). Among others, prospective certification bodies have to demonstrate their independence and expertise and that their tasks and duties do not result in a conflict of interests (Art. 43, 2., (a) and (e) GDPR). They are also required to establish procedures for the issuing, periodic review and withdrawal of seals (Art. 43, 2., (c) GDPR).

We deem a harmonised European approach to be of particular importance in this context, as it is capable of ensuring a high level of independence and expertise of all future certification bodies. It is worth noting that certification bodies can only be accredited once the GDPR is applicable.

According to Art. 42, 5. GDPR, certifications shall be issued based on criteria approved by the competent supervisory authority or by the European Data Protection Board. Where the criteria are approved by the Board, this may result in a common certification, **the European Data Protection Seal**. Approved criteria may relate to the certification of products and services. This allows data subjects to quickly assess the level of data protection of relevant products and services (Recital (100) GDPR).

The GDPR further establishes several benefits of the law, which will tremendously increase the value of approved certification mechanisms: they may be used as an element to demonstrate **compliance** (cf. Art. 24, 3., 25, 3., 28, 5. and 32, 3. GDPR) and might have a **positive effect in an administrative fine context** (cf. Art. 83, 2., (j) GDPR). In addition, manufacturers and service providers may benefit from a seal that addresses the concepts of **privacy by design and by default** in the context of public tenders (cf. Recital (78) GDPR). Finally, approved certification mechanisms can even provide a **legal ground for the transfer of personal data to third countries** outside of the EU (cf. Art. 46, 2., (f) GDPR).

Last but not least, the value of approved certification mechanisms, seals and marks will be very high, since supervisory authorities must be provided with the reasons for **granting or withdrawing the requested certification** (Art. 43, 5. GDPR) and they even have the power to order the certification body to withdraw or not to issue a certification if the requirements for the certification are not or no longer met (Art. 58, 2., (h) GDPR).

1 https://www.european-privacy-seal.eu/
2 *Business to business.*
3 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *O.J.*, L 119.