EuroPriSe‘s GDPR Ready Certification Criteria

EuroPriSe CA

2017

All Updates at a Glance

What's new?

- Additional requirements due to GDPR §§ introducing new rights and duties (e.g., portability and DPIA)
- Amended requirements due to modification of existing rights and duties by GDPR §§ (e.g., content of controller-processor agreement)
- Deleted requirements due to abolishment of duties by GDPR §§ (e.g., notification & prior checking)

NOTE: The „GDPR ready" criteria catalogue has not been approved pursuant to Article 42(5) GDPR and EuroPriSe GmbH has not been accredited as a certification body pursuant to Article 43 GDPR yet.

Significant Changes due to GDPR

- Incorporation of GDPR requirements. The most relevant changes – in terms of new subsets / requirements - are as follows:
  - New title for requirement 1.2.1:
    - Previous title: “Data Avoidance and Minimisation”
    - New title: “Data Protection by Design and by Default”
  - Requirement 1.2.1 is divided into two sub-requirements:
    - 1.2.1.1 Data Protection by Design (Art. 5(1)(c) + 25(1) GDPR)
    - 1.2.1.2 Data Protection by Default (Art. 5(1)(c) + 25(2) GDPR)

Significant Changes due to GDPR

- New/updated requirements in subset 2.1 (“Legal Basis”):
  - 2.1.2.2 Added Social Security & Social Protection Law to Req. that previously only focused on “Processing of Sensitive Data in the Field of Employment” (Art. 9(2)(b) GDPR)
  - 2.1.2.9 Processing of Sensitive Data For Public Health Reasons (Art. 9(2)(i) GDPR)
  - 2.1.2.10 Processing of Sensitive Data for Archiving, Research or Statistical Purposes (Art. 9(2)(j) GDPR)
  - 2.1.2.11 Processing of Genetic Data, Biometric Data or Data Concerning Health (Art. 9(4) GDPR)
  - 2.1.4.2 Processing and Public Access to Official Documents (Art. 86 GDPR)
  - 2.1.4.4 Processing in the Context of Employment (Art. 88 GDPR)
  - 2.1.4.5 Processing for Archiving Purposes in the Public Interest, Scientific or Historical Research Purposes or Statistical Purposes (Art. 89 GDPR)

Significant Changes due to GDPR

- New subset “2.2 General Requirements”:
  - 2.2.1 Record of Processing Activities (Art. 30 GDPR)
  - 2.2.2 Designation of a Data Protection Officer (Art. 37 ff. GDPR)
  - 2.2.3 Designation of a Representative in the EU (Art. 27 GDPR)
  - 2.2.4 Data Protection Impact Assessment (Art. 35 GDPR)
  - 2.2.5 Prior Consultation (Art. 36 GDPR)
  - 2.2.6 Notification of a Personal Data Breach (Art. 33 f. GDPR)
  - 2.2.7 Processing under the Authority of the Controller or Processor (Art. 29, 32(4) GDPR)

No general evaluation of compliance with requirements 2.2.4 and 2.2.5, but only a “ToE-driven” one.

Significant Changes due to GDPR

- New requirement
  "2.4.5 Processing of Personal Data Relating to Children":
  - 2.4.5.1 Conditions Applicable to Child's Consent in Relation to Information Society Services (Art. 8 GDPR)
  - 2.4.5.2 Consideration of the Need for Specific Protection of Children when Performing a Balancing of Interest Test (Art. 6(1)(f) GDPR)
  - 2.4.5.3 Understandability of Information and Communication where Processing is Addressed to a Child (Art. 12(1)(1) GDPR)
  - 2.4.5.4 Inadmissibility of Automated Individual Decisions, including Profiling that are Addressed to a Child (Art. 22 in connection with recital 71 GDPR)
  - 2.4.5.5 Consideration of the Need for Specific Protection of Children when Assessing the Risks of the Processing (Art. 24(1), 32(1) and 35 in connection with recital 75 GDPR)

Significant Changes due to GDPR

- Amendment of subset “2.5 Compliance with General Data Protection Principles”:
  - 2.5.1 Lawfulness, Fairness and Transparency
  - 2.5.2 Purpose Limitation
  - 2.5.3 Data Minimisation
  - 2.5.4 Accuracy
  - 2.5.5 Storage Limitation
  - 2.5.6 Integrity and Confidentiality
  - 2.5.7 Accountability

The subset was moved to the end of set 2. This requires legal experts to provide a final assessment of compliance which focuses on the general data protection principles at the end of the legal part of an evaluation report. CA deems this to be useful.

Significant Changes due to GDPR

- Set 3: Technical-Organisational Measures (TOM)
  - Only minor changes have been made to set 3 in response to the GDPR, since the previous criteria are still relevant under the new legal circumstances.
- New sub-requirements in Set 4 (data subjects' rights):
  - 4.1.6 Right to Data Portability (Art. 20 GDPR)
  - 4.1.9 Right to be Informed of Personal Data Breaches (Art. 34 GDPR)
  - 4.1.10 Processing Which Does Not Require Identification (Art. 11 GDPR)