Comments on the document

Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

Authors:

Alessandro Simonetta
ISO/IEC JTC 1 SC 7/WG 6 and ISO/IEC JTC 1 SC 27 member
UNINFO UNI/CT 504 - Software engineering - Vice President
UNINFO UNI/CT 510 – Security - member
Contract professor at the Universities of Rome "Tor Vergata" and "Guglielmo Marconi"
alessandro.simonetta@gmail.com

Maria Cristina Paoletti
ISO/IEC JTC 1 SC 7/WG 6 member
UNINFO UNI/CT 504 - Software engineering – Member
mariacristina.paoletti@gmail.com

Date: 14 January 2020

Introduction:

The current writing of Article 25 in paragraph 2 provides that:

"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons".

In order to demonstrate that all countermeasures have been taken to ensure that personal data are **accurate** (page 21), it is necessary to measure their distance from reality through a quality system. For this purpose the international standard **ISO/IEC 25012:2008** is already adopted since 2013 for database of national interest of Italian public administrations (Agency for Digital Italy: 2019-2021 Three-Year Plan for IT in the Public Administration, Determination n. 68/2013 for database of national interest).

Indeed, the data quality model defined in **ISO/IEC 25012:2008** outlines 15 quality characteristics: Accuracy, Completeness, Consistency, Credibility, Currentness, Accessibility, Compliance, Confidentiality, Efficiency, Precision, Traceability, Understandability, Availability, Portability and Recoverability.

Furthermore, in addressing effectiveness (page 7 – 16) *"... the controller may determine appropriate key performance indicators to demonstrate compliance. Key performance indicators may include metrics to demonstrate the effectiveness of the measures in question. Metrics may be quantitative, such as level of risk, reduction of complaints, reduction of response time when data subjects exercise their rights; or qualitative, such as evaluations of performance, use of grading scales, or expert assessments."*

In the **ISO/IEC 25024:2015** (Measurement of data quality) standard are defined 63 data quality characteristics measures related to the ISO/IEC 25012, although it cannot be considered to be an exhaustive set. Generally, the measurement function normalizes the value within a range from 0 to 1. These standards are part of new series of International Standards named SQuaRE - Systems and software Quality Requirements and Evaluation (ISO/IEC 250xx) whose peculiarity is the definition of product quality models (software, data, services, quality in use).

The relevance of the product quality models is also confirmed by Whereas n. 100 of GDPR which set forth that: *"In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services".* Furthermore, Section 43 GDPR, specify that these certification mechanisms must be compliant with EN ISO/IEC 17065:2012. The mentioned standard represents the necessary requirements for bodies certifying products, processes and services.

This methodology will permit to define a measurement system. Indeed, if the core obligation is the effective implementation of the data protection principles and data subjects' rights and freedoms by design and by default, it's crucial put in place a measurement system since the design phase to achieve by default the core obligation.

After that, could be useful investigate about the «robustness» of the measurement system calculating for example the number of quality measures and their distribution, the quantity and type of algorithms used, the quantity and type of physical objects analyzed by the algorithms, the distribution of measures in the various phases of the data life cycle. This is a real meta-quality system.

Conclusion:

In our opinion, the **ISO/IEC 25012:2008** (Data quality model) and **ISO/IEC 25024:2015** (Measurement of data quality) **should be mentioned** inside the guideline to give an example how demonstrate that personal data are accurate, up to date, credible, complete, consistency, accessibile, compliance, confidence, efficiency, precise, traceable, understandable, available, portable and recoverable.

References:

The Italian reference standards above mentioned.

Agency for Digital Italy (AgID) - 2019 - 2021 Three-Year Plan for IT in the Public Administration

https://www.agid.gov.it/sites/default/files/repository_files/three_year_plan_for_it_in_public_administration_2019-2021.pdf

Databases of national interest - promote the use of international data quality standards UNI CEI ISO/IEC 25012:2014 applying, in particular, the technical rules defined by AgID with its Determination no. 68/ 2013 for critical databases, also fostering the process of measuring the quality of data, on the basis of standard UNI CEI ISO/IEC 25024:2016.

Agency for Digital Italy (AgID) - Determination n. 68/2013 for database of national interest

https://www.agid.gov.it/sites/default/files/repository_files/circolari/dt_cs_n.68_-_2013dig_-_regole_tecniche_basi_dati_critiche_art_2bis_dl_179-2012_sito.pdf

In order to guarantee the quality of the data present in the critical databases, for the updating methods, the reference administrations follow the indications of the ISO/IEC 25012:2008 Data quality model standard.