New GDPR certification for hosting and analysing confidential microdata : a concrete example of implementation

Keywords: personal data protection, GDPR compliance, confidential data, ISO

1. INTRODUCTION

Citizens demand greater transparency from public bodies and companies about the data they collect and manage. There is a growing concern about how they are retrieving, using (, transferring) and protecting this data. In response to public pressure, ambitious regulations are being implemented to guarantee privacy and security of personal information: The General Data Protection Regulation (GDPR) in the European Union, but also the General Data Protection Law (GDPL) in Brazil, the California Consumer Privacy Act (CCPA) in California, and the Australian and Canadian regulations. To help organisations manage personal data in compliance with citizen's expectations and legal and regulatory requirements, a new certification based on the ISO 27701 norm was issued in August 2019, taking into account the provisions of GDPR. ISO 27701 is an international standard that describes the governance and security measures to be set up for processing personal data, extending two well-known IT security standards (ISO 27001 and ISO 27002).

CASD is a research data center which provides secure access for research purposes to individual and personal microdata collected by several data producers mainly from the Official Statistical System. CASD has to provide guarantees to the data producers so that they can transmit microdata for providing access to researchers through CASD.

2. METHODS

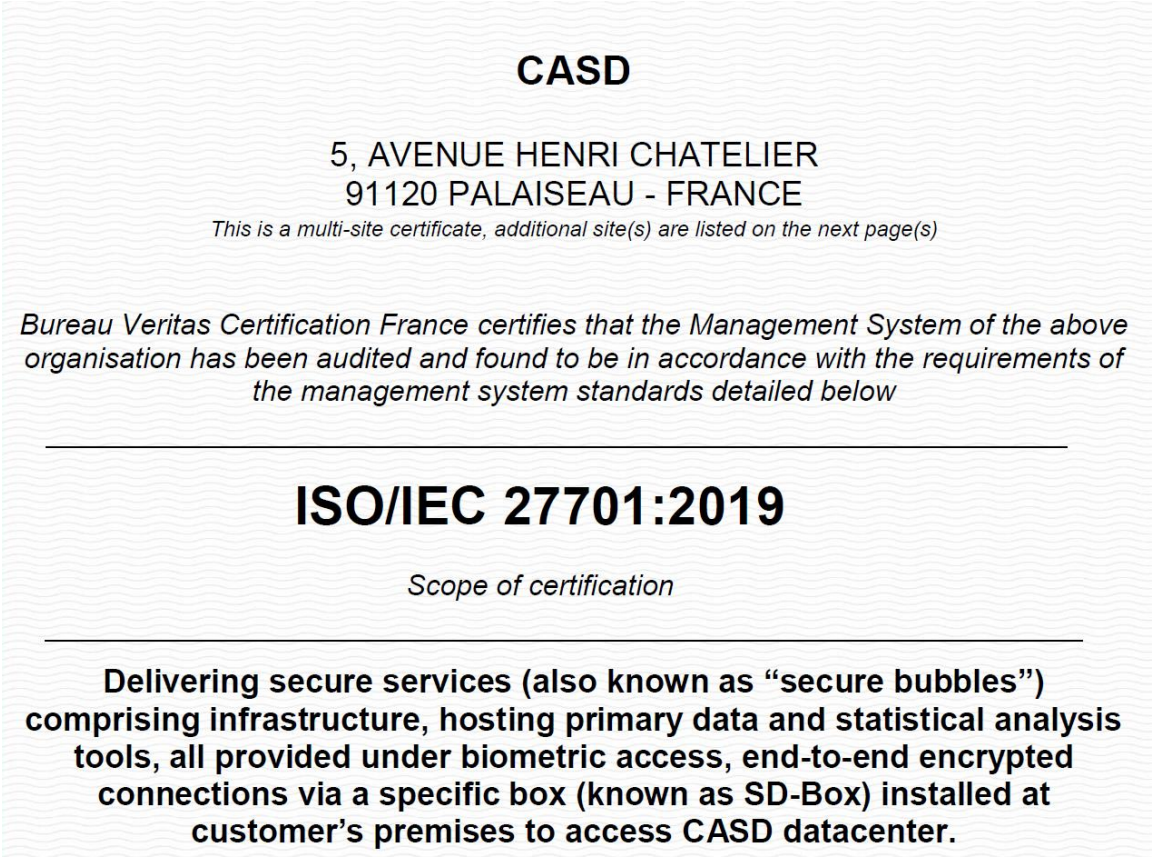
The approach taken by CASD aims at defining the governance structure needed for managing the protection of personal data that would involve all stakeholders, including the decision makers. Building up an end-to-end management of personal data protection entails four consecutive steps:

- First, CASD identified the level of protection and measures applying to all highly-detailed personal data managed. This includes the legal constraints stemming from GDPR and other regulations. This phase allowed defining the main objectives concerning personal data protection.
- Second, a data policy was elaborated in accordance with the data protection objectives. This required a strong involvement at senior management level: the personal data policy must validated to identify the resources needed to implement it.
- Third, an action plan was devised on the basis of an extensive risk analysis regarding the personal data handled and their protection.
- Once deployed at operational level, the performance of the implementation of the personal data policy must be constantly assessed to improve it continuously.

The presentation will extensively describe the approach needed to implement an auditable and certifiable personal data policy. It will also provide concrete examples of the virtuous outcomes of such an approach for organisations active in the field of official statistics production.

3. RESULTS

The main results of the definition of personal data policy and its implementation following the new ISO 27701 standard are that personal data protection must be handled at each stage of the data lifecycle; and that all members of the organisation must be involved in its implementation. After an audit in July 2020, CASD was one of the first organisations to get the ISO 27701 certification.



CASD

5, AVENUE HENRI CHATELIER
91120 PALAISEAU - FRANCE

This is a multi-site certificate, additional site(s) are listed on the next page(s)

Bureau Veritas Certification France certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27701:2019

Scope of certification

Delivering secure services (also known as "secure bubbles") comprising infrastructure, hosting primary data and statistical analysis tools, all provided under biometric access, end-to-end encrypted connections via a specific box (known as SD-Box) installed at customer's premises to access CASD datacenter.

4. CONCLUSIONS

The data protection certification, as prescribed by the ISO 27701 standard, gives an actual opportunity to formalize best practices in data protection management within an organisation and to reinforce its accountability in this respect. It is a key point in providing guarantees to all stakeholders (citizens, data protection authorities...) who are concerned about data protection. It also allows getting more opportunities to manage new data sources because data producers (especially legal departments) or citizens are more likely to entrust an organisation with a GDPR-compliance certification. Statistical institutes, who are obviously strongly involved in data protection, could also be interested in adopt this approach to strengthen their position toward e.g. public opinion.

REFERENCES

[1] ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, https://www.iso.org/standard/71670.html

[2] ISO 27701, an international standard addressing personal data protection, 02 April 2020, CNIL, https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection

[3] ISO/IEC 27701: Threats and Opportunities for GDPR Certification, January 2020, Eric Lachaud, Tilburg University