CHIOMENTI

Newsalert

Data Protection & Cybersecurity; Transactions Real Estate

Smart cities and artificial intelligence: the Italian Data Protection Authority sanctions the City of Trento

Introduction

With the decision of January 11, 2024[1] , the Italian Data Protection Authority (the "**Garante**") dealt with the issue of data processing in the context of the so-called "smart cities", sanctioning the City of Trento for having collected personal data through microphones and video surveillance cameras, positioned in public places, for purposes beyond those allowed by the urban security regulations. The sanctioned processing were, in fact, part of two smart urban security projects consisting of the training of an artificial intelligence technology for the detection of potential criminal events and, consequently, for the raising of the level of city security.

Net of the strictly technical-legal considerations, what emerges is the indirect admonition that can be drawn from the decision toward economic operators who intend to enter the service sector for smart cities in compliance with data protection regulations, including by making use of suitable data governance.

I Nodal points of the Measure

(1) Nature of personal data processed. The decision clarifies that the collection of audiovisual information through video surveillance systems may constitute the processing of personal data relating to crimes (see Article 10 GDPR[2]) by the mere fact that the activity is aimed at the detection and analysis of facts relevant to the protection of public safety, which may therefore constitute criminal offenses. The City of Trento's

[1]Register of Decisions No. 5, January 11, 2024, available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9977020.
[2] Regulation (EU) 2016/679.

argument to the contrary, based on the assumption that the use of the data collected in criminal proceedings would be only eventual and not immediate, was therefore rejected. What is more, the Garante declared that the processing in question also complied with Article 9 of the GDPR, since the purpose of the project included the research and analysis of special categories of personal data to allow, specifically, the training of artificial intelligence algorithms that would be able to recognize potential situations of risk to public safety.

(2) Legitimate basis for processing. Although the City of Trento had argued that the sanctioned processing could be justified and supported by the legal framework on urban security, the Garante clarified how the collection and analysis of personal data for smart urban security projects turns out to be an activity with purposes entirely incidental and eventual to the "*prevention and countering of widespread and predatory crime phenomena*."[3] . Likewise, contrary to the City of Trento's assertion, the processing could not have been made lawful by a general purpose of scientific research, since this purpose is not counted among its institutional competencies. Consequently, the City of Trento has not proven the existence of a legal framework capable of legitimizing the treatments put in place.

(3) Impact assessment. A third profile concerned the data protection impact assessment, aimed at adopting technical measures to minimize processing risks (see Articles 35 and 36 GDPR). In this regard, the Garante, premising that the City of Trento was "*certainly subject to the obligation to draw up the Data Protection Impact Assessment*", pointed out the defect of some fundamental elements for its proper execution, including:

I. the assessment of the proportionality of processing in relation to the purposes,

II. the assessment of the necessity of the processing, taking into account the possibility of conducting the scientific research projects in simulated urban environments or reducing or eliminating the processing of particular categories of data (*e.g.*, the content of conversations),

III. the identification and description of information systems and databases employed as a major premise within the risk mitigation process,

IV. the consideration of risks arising from the processing of the content of conversations,

V. the prior collection of citizens' opinions on the initiative.

(4) Anonymization techniques adopted. The incorrect use of anonymization techniques may be ineffective for GDPR compliance purposes. In fact, as for data related to recorded conversations, contrary to the City of Trento's claim, the Garante clarified that they cannot be considered anonymized by "*merely replacing the voice of the speaking subject.*" Similarly, with regard to video recordings, blurring the faces of people and vehicle license plates cannot be considered a suitable technique for anonymizing the personal data processed. In both cases, it is, in fact, possible to identify the data subjects by means of other information, including information that can be obtained from the same context of the filming or conversation. In conclusion, it seems relevant to point out that for each circumstance alleged to be suitable for proving risk mitigation techniques, it is the burden of the owner to attach the relevant documentation.

[3] As stipulated in Article 5(2)(a) of Decree Law No. 14 of February 20, 2017.

II Takeaways for business operators

II.I The necessary definition of a data governance plan

The development of digital services brings with it the necessary need to analyze a high volume of high-quality data (personal and otherwise). That is why the effective ability to process information in a compliant manner is a prodromal condition for the success of any innovative project based on data analysis.

Ensuring so-called data interoperability, allowing permeability between data sets stored by different private and public sector entities, may be the real turning point for the digital economy to flourish.

With this in mind, the EU Legislator has recently passed a number of regulations[4] that aim to incentivize the use (and reuse) of data for the development of digital services in both the public and private sectors, with a particular focus on microenterprises and SMEs, which find the toughest barrier to entry into the data economy.

In particular, the Data Governance Act ("**DGA**") offers important models for interoperability and data sharing (so-called "*data intermediaries*"), including the institution of data cooperatives ("**co-ops**"), which has already been adopted in several sectors, such as health, transportation or ride-sharing, and which can play a significant role in service development projects for the benefit of smart cities.

Co-ops are defined by the DGA as organizational structures included among brokerage services[5] that can be formed by data subjects, sole proprietorships and SMEs. The primary purpose of co-ops is the realization of democratic and mutualistic data governance, supporting the sharing of data among members so that they can collectively enjoy the benefits derived from its processing. Depending on the relevant business model, co-ops can be categorized as follows:

(i) *member-to-cooperative* co-op, where data are shared within the co-op for purposes internal to the organization, to be collected and processed for the purpose of providing a service,

(ii) *member-to-member* co-op, where data is shared among members by means of the channels established within the cooperative,

(iii) *federated* co-op, where data is shared among several entities that have common interests and similar "data governance" processes,

(iv) "*third party*" type co-op, where data are shared through traditional data sharing schemes with entities outside the cooperative and based on negotiated agreements and, where applicable, authorizations or expressions of consent from individual cooperative members,

(v) co-op of the "*open data*" type, where data is shared through a common space, available to all.

The creation and management of one of the co-op models outlined above, however, requires the adoption of specific contractual cautions and specialized assessments in order to build up an effectively exploitable data asset for all involved.

---

[4] We refer to Regulation (EU) 2022/868 (Data Governance Act), Regulation (EU) 2023/2854 (COD) (Data Act), Regulation (EU) 2022/1925 (Digital Markets Act) and Regulation (EU) 2022/2065 (Digital services act).
[5] In Article 10 of the Data Governance Act.

II.II Compliance with GDPR

The Garante's decision highlighted the following points with which economic operators are required to comply by making the appropriate preliminary assessments:

I. The nature of the data processed, in order to guide compliance according to the peculiar rules that the GDPR prescribes for different types of personal data, a mapping of the data that will be processed is essential. This is relevant not only for the purpose of choosing the legitimate basis but also for conducting an appropriate risk analysis and thus for taking the necessary security measures. For example, the processing of special categories of data under Article 9 of the GDPR is generally prohibited, unless there are specific exceptions expressly provided for in the GDPR.

II. The suitability of the lawful basis for processing, considering that for each purpose, and depending on the nature of the data processed, there should correspond a lawful basis suitable for licensing a specific processing of personal data.

III. Ensure that processing is transparent, in accordance with the principle of "*lawfulness, fairness and transparency*". The data controller must provide the data subjects with all the information required by the GDPR, especially taking into account the interpretations provided from time to time by the relevant authorities, even before starting the processing activities. For example, in the case where the processing is implemented by means of a video surveillance system, it is necessary to adopt a so-called first- and second-level information notice[6] describing it.

IV. The conduct and documentation of the data protection impact assessment prior to the start of processing, aimed at identifying risks to the rights and freedoms of data subjects arising from processing and minimizing them through the adoption of specific technical measures.

[6] The Garante has, in fact, ruled that if the data controller identifying itself as a public entity intends to carry out video surveillance activities, in addition to making a short version of the information notice by putting up warning signs near the area at stake, it must also prepare and make available for consultation by the data subjects an extended version of such notice, consisting of the elements indicated in Article 13 of Regulation (EU) 679/2016; see *ex multis* Decision No. 9920578 of July 18, 2023, available at the link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9920578.

Contact

Patrizia Liguti
Partner – Chiomenti
Transactions Real Estate
T. +39 02 72157 1
patrizia.liguti@chiomenti.net

Marilena Hyeraci
Of Counsel – Chiomenti
Data Protection & Cybersecurity
T. +39 02 72157 1
marilena.hyeraci@chiomenti.net

Pierluigi Perri
Of Counsel – Chiomenti
Data Protection & Cybersecurity
T. +39 02 72157 1
pierluigi.perri@chiomenti.net

Virginia Putortì
Associate – Chiomenti
Data Protection & Cybersecurity
T. +39 02 72157 1
virginia.putorti@chiomenti.net

Tommaso Bratina
Junior Associate – Chiomenti
Data Protection & Cybersecurity
T. +39 02 72157 1
tommaso.bratina@chiomenti.net