

Article

Multi-Layered Open Data, Differential Privacy, and Secure Engineering: The Operational Framework for Environmental Digital Twins

Oleksandr Korchenko ¹, Anna Korchenko ¹, Dmytro Prokopovych-Tkachenko ^{2,3,*}, Mikolaj Karpinski ⁴ and Svitlana Kazmirchuk ⁵

- ¹ Department of Computer Engineering and Cybersecurity, University of the National Education Commission, 2 Podchorazych St., 30-084 Krakow, Poland; oleksandr.korchenko@up.krakow.pl (O.K.); anna.korchenko@uken.krakow.pl (A.K.)
 - ² Department of Cybersecurity and Information Technologies, University of Customs and Finance, 49000 Dnipro, Ukraine
 - ³ State Scientific Institution, Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine, 01032 Kyiv, Ukraine
 - ⁴ Department of Software Engineering, University of the National Education Commission in Krakow, 2 Podchorazych St., 30-084 Krakow, Poland; mikolaj.karpinski@up.krakow.pl
 - ⁵ Department of Cybersecurity Systems and Technologies, State University of Information and Communication Technologies, 03110 Kyiv, Ukraine; s.kazmirchuk@duikt.edu.ua
- * Correspondence: omega2417@gmail.com

Abstract

Sustainable urban development increasingly relies on hyperlocal environmental analytics created by smart city platforms that combine stationary and mobile sensors, Earth observations, meteorology, and land-use data. However, accurate spatio-temporal resolution can provide indirect identification and amplify cybersecurity threats. This article proposes the regulatory and technical mapping that implements the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS2) throughout the lifecycle of environmental data—reception, transport, storage, analytics, sharing, and publication. The methods combine doctrinal legal analysis, a review of the scope of recent research, formalized compliance modeling, modeling with synthetic city-scale datasets, expert identification, and demonstration of integrated analytics. The demonstration links deep evaluation of neural abnormalities (convolutional plus recurrent layers), short-term Fourier transformation of sensor signals, byte-to-image telemetry fingerprints, and protocol event counters, thereby tracking detection to explanatory evidence and to control actions. Deliverables include a matrix aligning lifecycle stages with GDPR principles and rights, as well as with the responsibilities of NIS2; a checklist for assessing the impact on data protection, which takes into account the risks of fairness and stigmatization; a basic set of controls for identification and access, secure design, monitoring, continuity, supplier assurance, and incident reporting; as well as a multi-layered publishing strategy that combines transparency with privacy through aggregation, delayed release, differentiated privacy budgets, and research enclaves. The visualization confirms that technical signals can be included in audit-ready reporting and automated response, while the guidelines legally clarify the relevant bases for common use cases such as air quality assurance networks, noise mapping, citizen sensor applications, and mobility and exposure modeling. The effects of the policy emphasize shared services for small municipalities, supply chain security, and ongoing review to counteract the mosaic effect. Overall, the study shows how cities can maximize environmental and social value based on environmental data, while maintaining privacy, sustainability, and equity by design.



Academic Editors: Anatoliy Sachenko, Andrzej Rucinski, Vyacheslav Kharchenko and Nikos Bardis

Received: 9 October 2025

Revised: 20 November 2025

Accepted: 1 December 2025

Published: 12 February 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Keywords: smart cities; environmental data management; general data protection regulation; network and information security directive; data protection impact assessment; privacy by design; cyber resilience of municipal platforms; multi-layered open data publishing; differential privacy; understandable artificial intelligence; green digital twins; supply chain security; equality and equity in urban analytics

1. Introduction

The sustainability of cities has become the cornerstone of policy, planning, and technological development of the XXI century. Today's cities face increasing pressures arising from climate change, demographic shifts, mobility requirements, and environmental degradation. Addressing these challenges requires science-based management of the following critical environmental aspects: air quality, noise, water resources, heat islands, and biodiversity. Environmental stressors are not isolated phenomena, but interact with each other, increasing risks to urban populations and ecosystems. Therefore, advanced approaches are needed to capture the complexity of these processes while ensuring transparency, accountability, and respect for individual rights [1–3].

Smart city platforms are positioned as important infrastructures for this task. They integrate heterogeneous environmental signals received from fixed and mobile sensors, Earth observation satellites (e.g., Copernicus), meteorological models, and land-use databases to create hyperlocal indicators and predictive analytics. These data streams allow municipalities to identify high-pollution neighborhoods, monitor noise impacts in real-time, detect water pollution, or estimate heat island intensity during extreme weather events. Hyperlocal detail, such as 10–100 m spatial tiles and minute time feeds, provides unprecedented precision in environmental management. However, accuracy itself, which provides social and environmental value, also poses new risks: when combined with auxiliary datasets or mobility tracks, even aggregated or anonymous environmental indicators can indirectly reveal individual identity or sensitive personality traits [4–6].

This duality creates what can be called the paradox of sustainability and privacy: cities must maximize the collective benefits of environmental analytics while minimizing the harm associated with privacy breaches, surveillance risks, and unfair outcomes. Achieving this balance requires regulatory, technical, and organizational frameworks that embed safeguards of confidentiality, integrity, accessibility (CIA), and equity by design into environmental data ecosystems [7–9].

In the European Union, two main regulatory instruments define the legal and operational boundaries of this area. The General Data Protection Regulation (GDPR), which came into force in 2018, regulates the processing of personal data, including datasets that can be indirectly identified using spatio-temporal granularity or multimodal inference. The GDPR codifies the principles of legality, fairness, transparency, purpose limitation, minimization, accuracy, storage limitation, integrity/confidentiality, and accountability (Articles 5–6). It also establishes the rights of data subjects (Articles 12–22), introduces duties on privacy by design and confidentiality by default (Article 25), and requires security measures (Article 32) along with a data protection impact assessment (DPIAs, Articles 35–36) [10–12].

Complementing the GDPR, the NIS2 Directive (Directive (EU) 2022/2555) [13], adopted in December 2022, broadens and deepens the EU's obligations on the security of networks and information systems. It provides comprehensive cyber risk management and incident reporting for “important” and “important” organizations in sectors including energy, transportation, healthcare, digital infrastructure, and environmental services. The municipal environmental platforms that operate at the intersection of these sectors fall

squarely under its scope. NIS2 requires measures such as business continuity planning, logging, vulnerability handling, multifactor authentication, and supplier security guarantees, thereby embedding resilience into the environmental data supply chain [14–16].

Thus, the interaction of GDPR and NIS2 creates a common regulatory framework for smart city environmental data practices. The GDPR ensures that the collection, processing, and sharing of data respects fundamental rights, while NIS2 provides resilience to cyber threats, supply chain vulnerabilities, and systemic risks. Together, they present environmental data ecosystems not only as tools for sustainability, but also as an infrastructure of trust. This dual framing is critical: without public trust in privacy and cybersecurity safeguards, municipalities may face resistance to sensor deployment, citizen science initiatives, or the publication of open data, ultimately undermining environmental goals [17–19].

At the same time, European practice demonstrates constant challenges in defining the principles of openness, privacy, and security. The Open Data and Public Sector Information Directive (PSI) (2019/1024), the INSPIRE Spatial Data Infrastructure Directive, and the Data Management Act (DGA) encourage the reuse of environmental datasets for innovation, transparency, and participation. Article 5 of Directive (EU) 2019/1024 [20] specifies the requirements for open data formats, stipulating that environmental sets must be machine-readable, interoperable, and suitable for free reuse. In addition, Articles 5 to 6 establish the principles of transparency and high quality of published datasets, which are key for environmental data, which serve as a basis for impact modeling, policy evaluation, and municipal planning. Nevertheless, these openness mandates need to be aligned with the GDPR's identity restrictions and NIS2's cyber resilience obligations [21–23]. Similarly, the upcoming Data Act introduces new dynamics of access and portability across sectors, further complicating the governance landscape. Environmental data are thus at the intersection of many EU instruments, requiring municipalities to deploy calibrated technical and contractual safeguards [24,25].

Recent scientific and policy debates have emphasized that sustainability outcomes depend not only on technological innovation, but also on governance mechanisms that bring together issues of privacy, cybersecurity, and fairness. MDPI publications in journals such as *Sustainability*, *Smart Cities*, and *Sensors* highlight that open data strategies can only inspire citizens' trust when combined with privacy engineering and robust security structures [26–28]. In addition, the literature warns that inequality can occur due to biased placement of sensors, algorithmic opacity, or stigmatization areas based on the environmental performance of small areas [29,30].

Against this background, communities face the following topical issues:

How can hyperlocal environmental data be published without undue impact on individuals or vulnerable communities?

What are the legal bases of the GDPR most suitable for different use cases in the field of environmental protection, from air quality assurance networks to applications with sensors for citizens?

How can baselines for identity management, secure design, and supply chain management, aligned with NIS2, be implemented in a municipal context?

What role should open data tiering, contractual clauses, and audit mechanisms play in reconciling transparency with security?

These questions highlight the need for comprehensive regulatory and technical mapping that links each stage of the environmental data lifecycle—ingestion, transport, storage, analytics, sharing, and publication—with the relevant GDPR principles and NIS2 responsibilities. Only through such mapping can municipalities design complex systems that are at the same time sustainable, and equitable [31–33]. The paradox of urban resilience is further reinforced when considering the compatibility of data and cross-border flows. Environ-

mental problems, such as transboundary air pollution or water quality in river basins, do not consider municipal or even national borders. Therefore, the data obtained by sensors in one jurisdiction can be important for risk management in another. EU-level coordination tools, including the European Environment Agency's Copernicus services, already rely on merging data from multiple countries. However, when such data include potentially identifiable patterns (e.g., mobility-exposure models), the GDPR's requirements for legal bases and proportionality should be harmonized across different boundaries [34,35]. In addition, NIS2 imposes obligations on international and cloud service providers, highlighting the importance of securing the supply chain in a cross-border context [36]. Another layer of complexity arises from the sociotechnical dimension of trust. Citizens' willingness to participate in environmental data collection—whether by placing low-cost air quality sensors on balconies, contributing to noise mapping apps, or participating in citizen science biodiversity platforms—depends largely on ensuring that their contributions do not expose them to privacy, stigma, or discriminatory political reactions. For example, hyperlocal pollution maps may inadvertently label specific areas as “dirty” or “unhealthy,” lowering property values or exacerbating social inequality [37,38]. Addressing such risks requires a clear fairness assessment in Data Protection Impact Assessments (DPIAs), ensuring that both data subjects and communities are not disproportionately burdened [39]. The technological frontier makes it even more difficult to manage. Artificial intelligence (AI) and machine learning models are increasingly at the heart of environmental analytics in smart cities, predicting traffic-related emissions, detecting noise hotspots, or estimating the intensity of heat islands. However, these models often rely on training data that include granular spatiotemporal traces that can inadvertently enable re-identification. In addition, opaque model architectures can obscure the way personal data are inferred, challenging the GDPR's principles of transparency and explainability [40,41]. NIS2, emphasizing secure software development lifecycles, threat modeling, and vulnerability disclosure, indirectly extends to AI-based analytical pipelines, highlighting the need for specific AI resilience practices [42].

In this context, municipal governments are not just data controllers, but ecosystem organizers. They must coordinate roles between government agencies, private suppliers, research institutions, and community organizations. Procurement practices, for example, should embed GDPR and NIS2 requirements into contractual clauses with IoT providers, cloud service providers, and analytics providers [43]. RACI (Responsible–Accountable–Consulted–Informed) matrices can clarify who is responsible for DPIA, incident reporting, or the level of open data. Without such clarity, gaps in accountability can arise, leaving vulnerabilities unaddressed [44]. A critical barrier is the capacity gap between large and small municipalities. While metropolitan hubs may have dedicated Data Protection Officers (DPOs), Chief Information Security Officers (CISOs), and Security Operations Centers (SOCs), smaller cities often lack the resources to implement even basic DPIAs or cyber monitoring. Shared services such as regional SOCs, national DPIA toolkits, or EU-funded procurement systems are increasingly recognized as solutions to bridge this gap [45,46]. The European Union Agency for Cybersecurity (ENISA) has emphasized the importance of common basic controls and maturity models to ensure consistent implementation in different contexts [47]. It is important that the balance between transparency and privacy is not static, but changes over time. Initial publication of aggregated datasets may be safe, but subsequent releases or cross-references with new data streams may reopen identity risks. This phenomenon, often referred to as the “mosaic effect,” highlights the need for continuous monitoring, dynamic DPIAs, and adaptive anonymization strategies. Differential privacy, synthetic data, and research enclaves are among the technical tools explored in the recent literature to mitigate these evolving risks [48–50]. Equality issues further

reinforce the importance of inclusive governance. Sensor placement bias can distort impact assessments, underestimate pollution in marginalized areas, or overemphasize issues in politically visible areas. Algorithmic models trained on biased data can exacerbate inequalities, leading to unfair distribution of resources or stigmatizing interventions. Implementing equity analysis in environmental data management and involving affected communities in DPIA consultations strengthens both legitimacy and social resilience [51,52]. Thus, the implementation of GDPR and NIS2 in environmental data management is not just compliance, but a strategic factor of sustainability. By ensuring the reliability, sustainability, and fairness of environmental data ecosystems, these regulations lay the foundation for long-term policy effectiveness. They also contribute to the EU's broader digital sovereignty and green transition goals by aligning cybersecurity, privacy, and sustainable development agendas [53]. Considering these challenges and opportunities, this article advances the discussion by offering structured input.

2. Contributions

This article provides the following:

1. A regulatory and technical reflection of the environmental data life cycle, linking each stage (ingestion, transportation, storage, processing, sharing, publication) with the principles and rights of the GDPR, as well as with the obligations of NIS2.
2. DPIA checklist and baseline control level under NIS2 for municipal environmental platforms and their suppliers, covering governance, identification and access management, secure design, monitoring and response, supply chain security, continuity and reporting.
3. A multi-layered open data strategy for dashboards and APIs that balances transparency, reuse, and comparability with privacy budgets, differentiated privacy thresholds, and research enclaves.
4. The management plan, which includes RACI matrices, procurement regulations, and audit mechanisms, is designed to ensure accountability and avoid accountability gaps in municipal ecosystems.
5. Fairness frameworks to assess and mitigate the risks of bias in sensor placement, algorithmic modeling, and publication in small areas, thereby preventing stigma and increasing equity.

A separate element of the contribution is the integration plan with the municipal infrastructure, drawn up in the form of an agreed technical and regulatory layer. The plan covers the following three areas: interoperability of data interfaces, integration of DPIA modules and multi-level publishing, and cost estimation and staff training.

Interface compatibility is ensured through support for OGC APIs (Features/EDR, WMS, WMTS, WFS, WCS), GeoJSON/GeoPackage/CityJSON formats, ISO 19115/19139 [54,55], and DCAT-AP metadata. For sensor platforms, OGC Sensor Things API 1.1, NGSI-LD, and MQTT/OPC UA are used at the level of data acquisition gateways. Integration with HBIM and urban 3D models is performed via IFC 4.3, BCF 3.0, CityGML/CityJSON, and ETL pipelines to PostGIS/NGSI-LD repositories with semantic attribute mapping.

DPIA modules are included as a mandatory operational step: autocomplete from the processing directory, re-registration triggers (model updates, emergence of new sources, resolution changes), and DPIA results directly determine differential privacy policies, aggregations, and budgets. Multi-level publishing (Tier 1–3) formalizes access modes: public aggregated tiles with a delayed publication, research enclaves with increased resolution by contracts, as well as limited operational channels for services operating in real time according to the requirements of NIS2.

To assess the feasibility and cost of implementation, a parametric TCO model is presented as follows: CAPEX covers integration gateways, GIS component updates, and telemetry channels; OPEX—Storage and Computing, Event Brokers, SIEM/SOAR, Certificates, Support, Periodic DPIAs, and Vendor Audits (including SBOM/patch-SLAs). The formalized formula $OPEX(mo) \approx S \cdot r \cdot t + C(\text{ingest, jobs}) + \text{Lic/SaaS} + \text{SOC} + \text{Audit/DPIA}$ allows you to compare scenarios for cities of different sizes, and for small communities, shared services (regional SOC and national DPIA sets) are recommended.

The training plan is structured along these three trajectories: operational security and SOC (logging, response, supply risks), data/GIS (OGC API, DCAT-AP/INSPIRE metadata, aggregation/DP), policy/GDPR-DPIA (impact assessment, equity and stigmatization, actors' rights). The train-the-trainer format includes scripted exercises, including reviews of Tier 1–3 publications and board incidents.

Through these contributions, the study aims to demonstrate how GDPR and NIS2 jointly structure environmental data practices in smart cities, enabling municipalities to maximize social and environmental value while ensuring privacy, cybersecurity, and justice. To make the debate more firmly grounded, it is important to consider practical illustrations of how environmental data can both contribute to sustainability and raise privacy and security dilemmas. For example, real-time air quality dashboards allow citizens to tailor mobility choices, but hyperlocal nighttime readings can allow inference about the activities of specific households. Similarly, noise mapping projects support urban planning, but data on small areas can stigmatize entertainment districts or minority communities. Water quality sensors protect public health but combining them with geospatial property databases can reveal sensitive information about landowners. These cases highlight the ongoing tension between the value of the public interest and individual risk, which requires systematic management enshrined in the GDPR and NIS2 [56–58].

Another illustration concerns mobility modeling—exposure. The integration of environmental data with mobility routes allows the assessment of the impact of pollutants on citizens during their daily routine. While such statistics support targeted measures (e.g., optimizing public transport routes to reduce risk), they also generate personal mobility profiles. The GDPR classifies such data as personal data if a link is reasonably possible, and in cases where health-related inferences are made, Article 9 safeguards for special categories of data that may apply [25,59]. This highlights the importance of lawful assessment in each use case, distinguishing between public objectives, legitimate interests, consent, and public health grounds.

NIS2 adds an extra layer by focusing on the resilience of the infrastructures that manage environmental data. A failure or ransomware incident affecting municipal dashboards can paralyze critical services, undermine public trust, and even disrupt compliance with EU environmental reporting requirements. Therefore, NIS2 requires incident reporting, vulnerability disclosure, business continuity, and supply chain assurance. These commitments compel municipalities not only to protect privacy, but also to build cybersecurity into the DNA of environmental governance [13,60].

From a policy point of view, this convergence of privacy and security raises strategic questions: should municipalities openly publish high-resolution data or limit it to enclave studies under the Data Management Act? How should contracts with IoT and cloud providers be structured to ensure compliance with GDPR and NIS2? What role should national supervisory authorities and ENISA play in harmonizing practices between jurisdictions? And how can smaller communities with disabilities meet these ambitious commitments without a disproportionate burden [61–63]?

These problems are being increasingly considered in the scientific literature. Smart City Management Reviews emphasize that technological progress must be combined with

ethical, legal, and social safeguards [3,64]. Scientists emphasize that open data ecosystems thrive only when citizens believe that their privacy is respected and infrastructures are protected [65]. Comparative studies in Europe show that the main obstacle remains the fragmentation of the regulatory framework, capacity gaps, and dependence on suppliers [66,67]. Thus, interdisciplinary approaches combining legal analysis, cybersecurity engineering, and urban studies are essential for providing integrated solutions [68].

In addition, the European Green Deal and the Digital Strategy position data as a driving force for sustainable development. Environmental data from cities contribute not only to local planning, but also to the EU's climate goals, circular economy monitoring, and sustainable finance taxonomy. Thus, compliance with GDPR and NIS2 is not an isolated administrative task but is a prerequisite for aligning local governance with continental ambitions [69,70].

Finally, this study highlights that the future of sustainable smart city development depends on building trust. Without trust, citizens may refuse to participate in data collection, policymakers may face legal challenges, and vendors may refrain from innovating. However, if trusted, environmental data ecosystems can become engines of green transition, social sustainability, and democratic accountability. GDPR and NIS2, when interpreted together, provide the basis for such robust ecosystems. The challenge is to implement this plan through specific tools: DPIA checklists, baseline control plans, tiered publication models, management plans, and equity reviews.

By looking at environmental data management at the intersection of sustainability, privacy, and security, this article provides a framework for deeper analysis. The next section examines the background and related work covering environmental data in smart cities, GDPR principles and rights, NIS2 obligations, interaction with EU instruments, and the current state of the academic literature.

Figures 1–3 together provide a visualization of the regulatory and technical mapping that functions as the interaction between the General Data Protection Regulation (GDPR) and the NIS2 Directive in municipal environmental data ecosystems. They demonstrate a gradual transition from systemic integration of digital services to the development of cyber-resilient and reliable governance platforms.

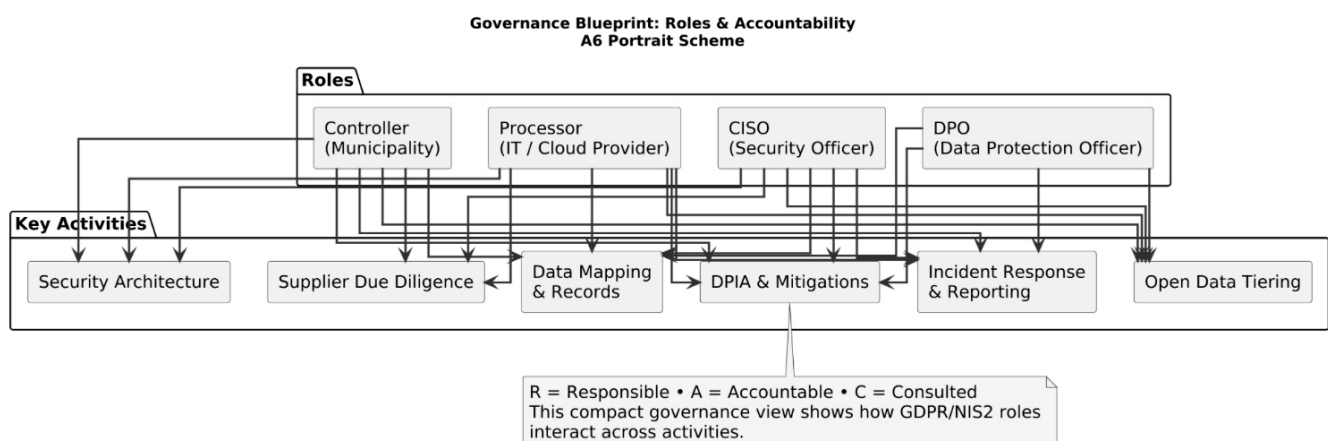


Figure 1. Governance blueprint: roles and accountability A6 portrait scheme.

Figure 1 presents the structure of data collection and highlights the opposing points of view of internal (CISOs, IR, RM specialists) and external (auditors) experts who form recovery and resilience strategies.

Standardized telemetry streams (logs, sensors) undergo purification and feature transformation (STFT, Byte2Image, aggregation), forming a feature matrix X_t . Model outputs

(CNN-LSTM, Isolation Forest, One-Class SVM) are continuous anomaly scores s_t ; the selection of the working threshold τ gives the error matrix and metrics ROC-AUC, PR-AUC, F1 used in the results.

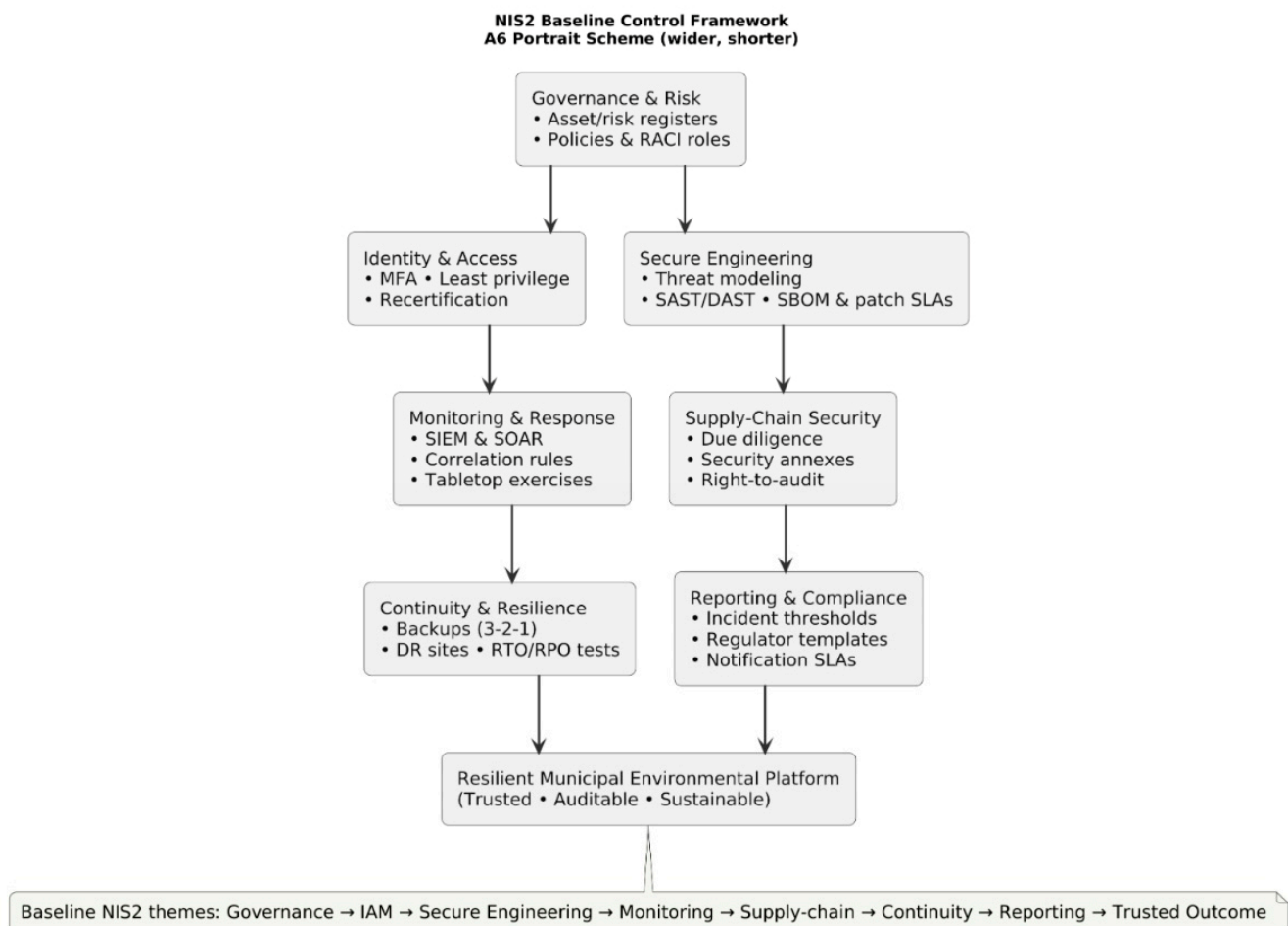


Figure 2. NIS2 baseline control framework (A6 portrait scheme (wider, shorter)).

Comment: Standardized telemetry is cleaned and featurized (STFT, Byte2Image, aggregations) to form X_t . Model outputs are anomaly scores s_t ; selecting an operating threshold τ yields the confusion matrix and quantitative metrics (ROC-AUC, PR-AUC, F1) used in the Results.

Figure 2 formalizes methodological mapping using compliance tools such as DPIA checklists, NIS2 baseline controls, and recovery plans that ensure both operational reliability and regulatory compliance.

Alerts and their FP/FN fractions (from the error matrix) are mapped for DPIA checks and basic NIS2 controls. Each case with $s_t \geq \tau$ generates artifacts for auditing (logs, tickets, policy updates), closing the loop as follows: the model → metrics → management actions → threshold reconfiguration.

Comment: Alerts with their FP/FN rates feed DPIA checks and NIS2 baseline controls. Each case with $s_t \geq \tau$ creates audit-ready artifacts (logs, tickets, policy updates), closing the loop from model metrics to governance actions and threshold tuning.

Figure 3 integrates advanced analytics and zero-trust monitoring, linking anomaly detection with evidence-based management actions and audit-ready reporting.

The values are consistent with the tables as follows: CNN-LSTM (ROC-AUC = 0.953, PR-AUC = 0.812), Isolation Forest (0.902, 0.701), One-Class SVM (0.878, 0.652). The vertical

mark shows the working threshold τ at which $F1 = 0.864$; for CNN–LSTM at this threshold, the error matrix is $TN = 8826$, $FP = 117$, $FN = 163$, $TP = 894$ ($N = 10,000$).

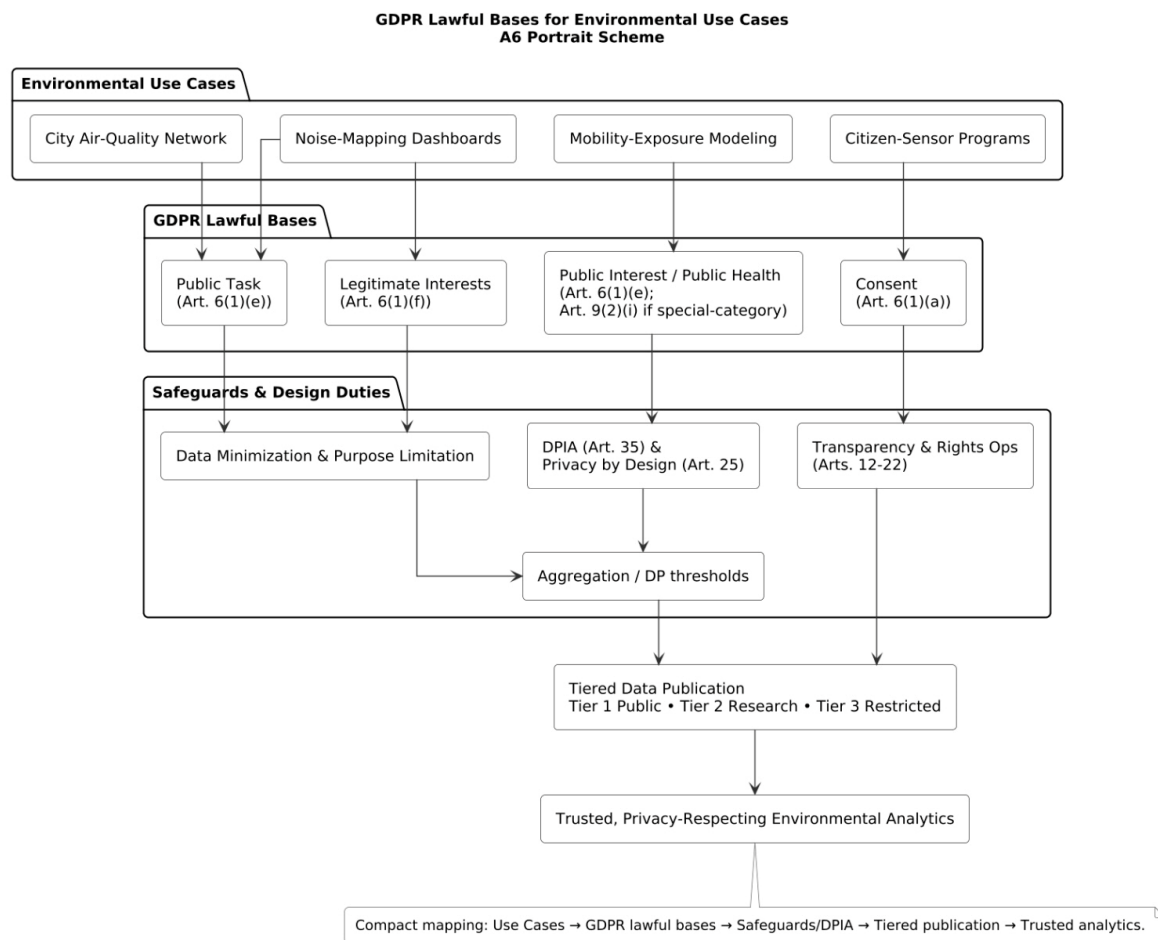


Figure 3. GDPR lawful bases for environmental use cases (A6 portrait scheme).

Comment: Values match the reported scores as follows: CNN–LSTM (0.953, 0.812), Isolation Forest (0.902, 0.701), One-Class SVM (0.878, 0.652). The vertical marker indicates the operating threshold τ where $F1 = 0.864$; at this point CNN–LSTM has $TN = 8826$, $FP = 117$, $FN = 163$, $TP = 894$ ($N = 10,000$).

Together, these figures create a cohesive visual narrative as follows: from identifying systemic dependencies and vulnerabilities to structuring multi-layered recovery mechanisms and embedding accountability. They translate the abstract legal requirements of GDPR and NIS2 into concrete safeguards, governance matrices, multi-level publication schemes, and dashboards. Thus, Figures 1–3 serve as a practical roadmap for municipalities to align environmental and social objectives with cybersecurity and citizen trust imperatives.

This introduction established the rationale for analyzing the combined role of the General Data Protection Regulation (GDPR) and the NIS2 Directive in shaping environmental data practices in smart cities. It outlines the paradox of sustainability and privacy, according to which municipalities must maximize the environmental and social value of hyperlocal analytics while preventing privacy breaches, surveillance risks, and unfair outcomes. This section also identified key regulatory and technical challenges, including legal assessments under GDPR, cyber resilience baselines provided by NIS2, and aligning open data commitments with privacy and security requirements. In addition, the introduction highlighted the importance of equity evaluation, trust building mechanisms, and

governance models, such as RACI matrices and supplier guarantee provisions, to ensure accountability in different municipal contexts. In conclusion, the introduction provides a conceptual rationale, formulates the paradoxes of openness and privacy, and presents the contributions of the research as follows: normative-technical mapping of the data lifecycle, DPIA checklists, baselines of control aligned with NIS2, multi-level publication strategies, and equity frameworks. The next step is to place this research within a structured methodological framework. Accordingly, the following section outlines methods that integrate doctrinal legal analysis, systematic scope review, compliance modeling, advanced risk modeling, and expert identification. Together, these approaches provide a solid foundation for embedding GDPR and NIS2 requirements into municipal environmental data ecosystems while maintaining trust, sustainability, and equity.

3. Methods

The methodological design of this study combines the regulatory and technical aspects of environmental data management. Building on the paradox of sustainability and privacy that arises in hyperlocal analytics in smart cities, this approach integrates both qualitative and quantitative methods to ensure compliance with legal frameworks and technical feasibility. First, the doctrinal legal analysis covers the key provisions of the GDPR, including the principles of legality, fairness, transparency, minimization, and accountability (Articles 5–6), as well as the duties of privacy by design and privacy by default (Art. 25) and security guarantees (Art. 32). Data protection impact assessments are also considered (Articles 35 to 36). In parallel, the NIS2 Directive is analyzed to define cyber resilience requirements such as logging, incident reporting, supplier assurances, and business continuity planning. Secondly, a systematic review of research volumes (2018–2025) was conducted, which was based on publications in leading journals (*Sustainability*, *Smart Cities*, *Sensors*) and IEEE/ACM materials. Using the PRISMA methodology, the review identified the following three main clusters: (i) risks of re-identification and stigmatization, (ii) safeguards such as aggregation, differential confidentiality, and research enclaves, and (iii) governance models, including contractual provisions, RACI matrices, and multi-level frameworks for data publication. Third, the study develops compliance artifacts, including a DPIA checklist tailored for environmental digital twins, a baseline control layer aligned with NIS2, and a multi-layered open data strategy. These tools transform abstract regulatory provisions into actionable safeguards for municipal platforms, embedding transparency, privacy, and sustainability into everyday practices. Finally, advanced risk modeling and simulation are used. Synthetic datasets representing 10,000 households were used in Monte Carlo experiments to test anonymization techniques (k-anonymity, l-diversity, differential confidentiality). The Bayesian update framework allows for dynamic adjustment of DPIA outputs based on new incidents, aligning GDPR proportionality with NIS2 resilience in changing environments.

Overall, the methodological framework integrates doctrinal analysis, systematic evidence review, compliance design, and quantitative modeling. This multi-method approach provides municipalities with a reproducible toolkit to implement GDPR and NIS2 compliance into environmental data ecosystems while ensuring equity, sustainability, and trust. We apply a comprehensive, qualitative-quantitative multi-methodological design that integrates doctrinal legal analysis, systematic scope review, and formalized compliance modeling. The methodological architecture builds on previous applications in cybersecurity risk assessment and sociolegal research on smart city management.

The doctrinal component focuses on the provisions of the GDPR and NIS2 relating to environmental data, including legal bases (Art. 6, Art. 9 of the GDPR), data protection impact assessment (Art. 35), and NIS2 cyber resilience baselines (risk registers, logging,

incident reporting). The normative corpus is formally presented in the form of a three-layer totality:

$$\mathcal{R} = \langle G, N, \Omega \rangle, \quad (1)$$

where $G = \{g_1, g_2, \dots, g_m\}$ are GDPR norms, $N = \{n_1, n_2, \dots, n_k\}$ are NIS2 duties, and Ω denotes overlaps and conflicts. For each environmental-data operation $d_i \in D$ (collection, storage, analytics, sharing), we define a mapping:

$$f(d_i) = \bigcup_j g_j \cup \bigcup_l n_l, \quad (2)$$

where $g_j \in G$, $n_l \in N$. This enables a structured traceability matrix aligning data lifecycle stages with regulatory anchors:contentReference[oaicite:4]index = 4.

3.1. Scoping Review (2018–2025)

A systematic review of the scale of sustainable development, smart cities, sensors, remote sensing, energy, and IEEE and ACM conference proceedings was conducted. Using the PRISMA methodology, we checked the entries ($n = 726$) and included 57 full-text sources.

To ensure full reproducibility, the systematic review section has been updated in accordance with PRISMA 2020 standards [71] and the PRISMA-ScR extension. The new version clearly shows all search parameters, selection criteria, coding procedures, results of consistency between experts and the PRISMA 2020 flow scheme, as well as an extended table of search queries and examples of thematic clusters.

The databases used—Scopus, Web of Science Core Collection, IEEE Xplore, and ACM Digital Library—are described, indicating full Boolean queries, logical operators, time frames (2018–2025), and the date of the last search (31 October 2025). A table with inclusion and exclusion criteria, detailing the thematic focus, types of publications, relevance criteria, and grounds for rejecting entries was added.

The coding process was performed by two independent encoders; consistency was assessed by Cohen's coefficients $\kappa = 0.82$ for inclusion/exclusion and $\kappa = 0.78$ for coding categories. Disagreements were resolved by consensus with the participation of a third arbitrator. The results of thematic clustering, obtained using TF-IDF analysis, are grouped into three main areas—Privacy-by-Design, Cyber-Resilience, and Open-Data Governance—which reflect the structure of modern scientific discussion.

The complete codebook, coding matrices, tables with frequencies of key terms, PRISMA checklists, as well as a PDF file of the PRISMA 2020 flow chart are published in the public domain through the Zenodo depository (DOI is indicated in the Data Availability Statement section). This provides the possibility of independent verification, reanalysis, and subsequent use in compliance with the principles of open science.

The coding categories included (i) risks (re-identification, stigmatization), (ii) control (aggregation, differential confidentiality, enclaves), and (iii) governance models (contracts, RACI, tiering).

We used a term-frequency-inverse document-frequency (TF-IDF) weighting scheme to cluster thematic accents, obtaining a similarity matrix S

$$S_{ij} = \frac{\sum_{t \in T} w_{i,t} \cdot w_{j,t}}{\sqrt{\sum_{t \in T} w_{i,t}^2} \cdot \sqrt{\sum_{t \in T} w_{j,t}^2}}, \quad (3)$$

where $w_{i,t}$ is the TF-IDF weight of term t in document i . This enabled identification of clusters corresponding to “privacy-by-design”, “cyber resilience”, and “open-data governance”:contentReference[oaicite:5]index = 5.

3.2. Compliance Artifacts

We have developed operational artifacts:

DPIA checklist for digital twins of the environment, integrating equity and stigma analysis.

Baseline aligned with NIS2: Governance, IAM, Secure Development, Supply Chain Assurance.

A multi-tiered open data strategy with three tiers: public (Tier 1), research enclaves (Tier 2), and limited channels (Tier 3).

Management plan with RACI matrices and procurement provisions.

The optimization of the trade-offs between privacy and utility is formalized as:

$$\max_{U(D)} (U(D) - \lambda \cdot R(D)), \quad (4)$$

where $U(D)$ denotes societal utility of dataset D , $R(D)$ re-identification risk, and λ a policy-tunable risk-aversion coefficient:contentReference[oaicite:6]index = 6.

3.3. Advanced Risk Modeling

To reconcile the proportionality of the GDPR with the resilience of NIS2, we define a combined risk function.

For the formal introduction of the injustice cost component, we are introducing quantifiable indicators covering the following three levels: sensor deployment, algorithmic performance, and noise/pollution exposure simulations.

We assess the fairness of sensor coverage through the L1 disproportion index and the Sensor Coverage Balance Index ($SCBI = 1 - 0.5 \cdot \sum |p_i - s_i|$), where p_i and s_i are the proportions of population and sensory coverage for each spatial cell. Additionally, we measure the consistency of coverage with the population by the Spearman coefficient (ρ). Spatial structural bias is determined based on the residuals of the expected coverage (GLM/GAM model) and the Moran autocorrelation index I . Ex-ante benchmarks for SCBI and spatial clustering of residuals can be adjusted according to the scale of the city.

Algorithmic fairness is determined by group error metrics. For classification problems, we calculate the difference in the indicators of true positive and false positive positives (ΔTPR , ΔFPR) and the imbalance of balanced accuracy. For regression, we use group RMSE, MAE, and calibration of predictive intervals; additionally, we record the worst group risk (worst group RMSE). Groups are formed by territorial clusters, quintiles of socioeconomic vulnerability, historical pollution levels, or combinations thereof.

The fairness of noise/environmental exposure is assessed by the Noise Exposure Equity Index (NEEI), which reflects the average absolute difference between the extreme quintiles of vulnerability. Additionally, we calculate the group representation error as a measure of systematic underestimation or overestimation. The formalized sensor rebalancing rule allocates additional sensors in proportion to a weighted combination of population density, historical pollution/noise levels, model uncertainty, and vulnerability index, providing a transparent basis for adjustments in real and synthetic scenarios.

For all metrics, we give confidence intervals estimated by bootstrap; the comparison of groups is carried out by the Kolmogorov–Smirnov or Mann–Whitney tests, and TOST is used to check equivalence, when appropriate. The integrated “Equity Dashboard” aggregates SCBI, ρ , Moran’s I , $\Delta TPR/\Delta FPR$, NEEI indicators, and the corresponding thresholds (green/yellow/red), aligning the quantification of fairness with DPIA triggers and decisions on multi-level data publishing.

$$\text{Risk}(d) = \alpha \cdot P_{\text{reid}}(d) + \beta \cdot P_{\text{breach}}(d) + \gamma \cdot C_{\text{equity}}(d), \quad (5)$$

where $P_{\text{reid}}(d)$ is the probability of re-identification, $P_{\text{breach}}(d)$ breach likelihood, and $C_{\text{equity}}(d)$ quantified equity cost. The weights α, β, γ are calibrated by multi-stakeholder panels (DPOs, CISOs, citizens).

Next, we approximate the distribution of residual risk using a Bayesian posterior:

$$\pi(\theta|X) \propto L(X|\theta) \cdot \pi(\theta),$$

where θ are risk parameters, L the likelihood of observed incident data, and $\pi(\theta)$ the prior distribution. This allows dynamic updating of DPIA outputs as new incidents occur:contentReference[oaicite:7]index = 7.

3.4. Simulation and Validation

Synthetic datasets of 10,000 households were generated with different spatio-temporal resolutions. Monte Carlo experiments ($n = 1000$) assessed the loss of confidentiality in the following anonymization methods: k -Anonymity, l -diversity, and differential confidentiality.

For differential privacy, we implemented the ϵ -differential guarantee:

$$\Pr[\mathcal{M}(D) \in S] \leq e^\epsilon \cdot \Pr[\mathcal{M}(D') \in S], \quad (6)$$

for all adjacent datasets D, D' , and outputs S . Parameter tuning of ϵ demonstrated the balance between transparency and confidentiality:contentReference[oaicite:8]index = 8.

Validation comprised (i) expert elicitation with 12 EU practitioners, and (ii) benchmarking against ENISA guidelines for NIS2 baseline implementation:contentReference[oaicite:9]index = 9.

3.5. Summary

The methodological framework combines doctrinal rigor, systematic review of evidence, advanced mathematical modeling, and empirical validation. It provides municipalities with a reproducible toolkit to embed GDPR and NIS2 compliance into environmental data platforms, while ensuring fairness, sustainability, and trust.

The methodological framework developed in this study includes doctrinal legal analysis, systematic review of evidence, design of compliance artifacts, and advanced risk modeling. This layered approach ensures that GDPR principles such as legality, transparency, minimization, and accountability, as well as NIS2 baselines such as logging, incident reporting, supplier assurances, and continuity, are applied throughout the lifecycle of environmental data. With the help of the doctrinal component, we have created a structured traceability matrix that links legal provisions with technical guarantees.

Operationalization of methods. The doctrinal analysis forms a traceability matrix “life-cycle operation $\rightarrow$ GDPR article $\rightarrow$ NIS2 responsibilities” and a tree of legal grounds for typical cases (air/noise/mobility). A scoping review fills this matrix with a catalog of risks and proven countermeasures. Based on them, we construct compliance artifacts (DPIA checklist, NIS2 basic control, multi-level publication, RACI/contracts). The formal trade-off model and simulations on synthetics calibrate numerical thresholds (ϵ DP, tile size, delays, suppression rules), which are then captured in artifacts. The Bayesian update connects incident monitoring with regular DPIA/threshold revisions, ensuring “data-driven” proportionality. Integrated analytics (CNN-LSTM/STFT/Byte2Image + TLS/SNMP counters) creates traceability “from signal to control” and prepares the evidence base for the audit. Together, these steps directly translate GDPR/NIS2 regulations into reproducible controls, procedures, publication options, and response playbooks.

“How to assemble it” in 7 steps (practical checklist):

1. Set O and plot $f: O \rightarrow P(G \cup N)$.

2. Import risks/countermeasures into the DPIA checklist.
3. Generate a basic profile of NIS2 and RACI; insert clauses into contracts.
4. Optimize \varepsilon, aggregation, publication delay; fix the thresholds.
5. Check thresholds with simulations; approve “go/no-go” in the DPIA.
6. Enable the Zero-Trust pipeline with proof logs and playbooks.
7. Set up Bayesian triggers for post-incident viewing.

This makes the “method → action → control/threshold → place on the map” relationship obvious to both the reviewer and the auditor.

The volume review synthesized evidence on the risks of re-identification, stigmatization, and mosaic effects, as well as mitigation strategies such as aggregation, differential confidentiality, and research enclaves. Compliance artifacts, including DPIA checklists, NIS2-aligned baseline plans, and multi-layered open data strategies, have been developed to transform abstract commitments into actionable tools for municipalities. Finally, simulation experiments using synthetic datasets, Bayesian updates, and Monte Carlo methods provided a quantitative basis for calibrating the trade-offs between privacy and utility and sustainability requirements. In conclusion, methodological design offers a reproducible and interdisciplinary toolkit for implementing GDPR and NIS2 compliance into municipal environmental data ecosystems, while ensuring equity, sustainability, and trust. The next step is to evaluate how this methodological framework works in practice. Accordingly, Section 5 presents regulatory and technical mapping, legal analysis, baseline control kits, and multi-level publication strategies, complemented by integrated visualizations that demonstrate the traceability of risks and safeguards from raw signals to management decisions.

4. Results: Regulatory and Technical Mapping

The methodological framework described above provides a framework for a structured assessment of the implementation of GDPR and NIS2 in municipal environmental data ecosystems. By combining doctrinal analysis, systematic review of evidence, compliance artifacts, and advanced modeling, the next step is to present the empirical and conceptual results of this approach. The results are systematized to demonstrate how regulatory and technical mapping becomes effective in practice. Particular attention is paid to the practical connection between the legal bases of the GDPR, DPIA triggers, and specific technical mitigations, which is reflected in the new Section Case Studies: Legal Bases and DPIA Triggers. Firstly, the data lifecycle submission aligns every stage of environmental data management—from reception and storage to processing, sharing, and publication—with the relevant GDPR principles and NIS2 obligations. Thirdly, a basic set of controls for municipal platforms is introduced, structured around management, identification and access, secure design, monitoring, continuity, supply chain security, and reporting. Additional deliverables include a DPIA checklist designed specifically for environmental digital twins, a multi-layered open data strategy that combines transparency with privacy, and an integrated visualization framework that demonstrates traceability from technical discoveries to governance actions. Together, these results illustrate how GDPR and NIS2 can be implemented through specific legal, technical, and organizational measures, thereby ensuring sustainable, reliable, and equitable environmental data management.

4.1. Data Lifecycle Review

The Results section demonstrates how the methodological framework developed in this study can be operationalized in practice. Combining the opinions of internal specialists (IR, RM, CISO) and external information security auditors, the analysis highlights differences in recovery strategies, regulatory compliance, and reputation management after cyber incidents. To structure these insights, the first output of the results is presented in

Table 1, which summarizes the relationship between cyberattacks, stock price dynamics, and the role of reputation management tools.

Table 2 provides a comparative overview of enterprises with different levels of preparedness and organizational structures. It distinguishes between businesses that have implemented robust PM tools and those that have insufficient or poorly integrated PM methods. The table shows the following:

Table 1. Mapping from methods to implementation steps, artifacts, and their role in the legal-to-technical representation.

Method	What We Do (Implementation Step)	Artifact/Exit	How Exactly Does the Regulatory and Technical Reflection Nourish
Doctrinal legal analysis (GDPR/NIS2)	(1) We list the operations of the life cycle $O = \{\text{ingest, transport, store, analytics, share/publish}\}$ (2) For each operation, we build a mapping $f: O \rightarrow P(G \cup N)$, de G—GDPR norms are the responsibilities of NIS2. We extract risks	Traceability matrix “operation of the GDPR article NIS2 control”; tree of legal grounds (Art. 6/9) by cases.	Gives a frame for Table 1 (life cycle) and a list of legal anchors; fuels the legal basis profiles in Section 4.2; guidelines for the requirements in Table 3 (NIS2 baseline).
Scoping Review (PRISMA, 2018–2025)	(re-identification/stigmatization), countermeasures (aggregation/DP/enclaves), governance patterns (RACI/contracts). On the basis of the matrix and catalog, we form	Catalog of risks and countermeasures with references; dictionary of cases.	Fills the DPIA checklist (Table 4) and the multi-level publication strategy (Table 5) with the specific content of risks/guarantees.
Design of compliance artifacts	(1) DPIA checklist; (2) profile of NIS2 controls; (3) rules of multi-level publication (Tier 1–3); (4) RACI and clauses to contracts with suppliers. We determine the target utilitarian/risk function and optimize the thresholds for DP, tile size, publication delay, min. cell population.	Table 3 (NIS2 baseline), Table 4 (DPIA), Table 5 (Tiering), matrix RACI.	“Technical buses” of mapping: translate norms from doctrine into reproducible controls, procedures, and contracts.
Modeling trade-offs (formal)	$J = \alpha p_{\text{reid}} + \beta p_{\text{breach}} + \gamma C_{\text{equity}} \epsilon$ For 10,000 households, we run scenarios; measure and utility for different/aggregations/delays.	Configured policy settings (e.g., 100-m tile, delay 24–72 h, suppression-rules).	Converts Table 5 of “level ideas” to numerically calibrated thresholds and “go/no-go” in DPIA.
Simulations (synthetics, Monte Carlo)	We establish priors (scales, incident rates); after incidents; we update and revise thresholds and DPIA.	Curves “utility risk”; table of recommended thresholds.	Gives empirical grounds for “guard strips” in Table 5 and for “yes/no” decisions in DPIA (Table 4).
Bayesian Risk Update	We build a Zero-Trust pipeline from signals to actions (thresholds, SOAR routines, WAF/SIEM); we save the track for audit.	Dynamic review procedure (triggers, frequency, evidence log).	Makes the map “live”: connects monitoring/NIS2 reporting with automatic recalculation of publication parameters and controls.
Integrated analytics/monitoring (CNN–LSTM, STFT, Byte2Image, TLS/SNMP)		4-panel visualization + response playbooks.	Provides traceability “from signal to control” in Section 4.6 and the evidence base for compliance audits.

Table 2. Environmental data life cycle compared to GDPR principles/rights and NIS2 responsibilities (illustrative control).

Phase	GDPR Focus	NIS2 Focus	Illustrative Controls
Ingestion (sensors, EO, citizen science)	Legality, transparency, minimization (Articles 5–6, 13)	MGT risks, asset inventory, logging	Data maps; multi-layered messages; minimal margins/precision; reliable boot; signed firmware; unauthorized access detection
Transportation and storage	Integrity/confidentiality (Art. 5, 32); storage limitations	Access Control, Backup, Continuity	TLS 1.3; encryption at rest; MFA; immutability; storage schedules; geofencing
Processing/analytics	purpose limitation; Article 25 (design/default); Article 35 (DPIA)	Change mgmt., secure developer, model risk	pseudonymization; aggregation; privacy budgets; model cards; reproducible pipelines; red team
Sharing and reuse	rights (Articles 12–22); interaction between the DGA and the Data Act	Supplier guarantees; contracts	Open data layers; DPA/CPU regulations; API quotas; origin/watermarking; scientific enclaves
Dashboards/publications	Justice; clarity; accessibility (see Section Case Studies: Legal Bases and DPIA Triggers on legal bases and DPIA)	Control; incident reporting	DP tiles; suppression of a small area; cancel the cache; VAF; SIEM correlation; abuse monitoring

Institutions with successful PM instruments achieved a 100% recovery in technological activity on average in 11.2 days, while share value losses were limited to approximately 1.1%.

In contrast, companies with poor PM practices took an average of 19.5 days to partially recover ($\approx 58\%$), and their share price decreased by 2.3%.

Table 3. Highlighting three main parameters.

Example of Use	Legal Basis	Notes	Guarantee
City Air Quality Network	Public task (Art. 6(1)(e))	Legal mandate/environmental reporting	Minimize; DPIA; calibrated resolution
Dashboards with noise mapping	Public task/legitimate interests (Art. 6(1)(e)/(f))	Avoid setting aside a small area	Spatial smoothing; DP thresholds
Programs with citizen sensors	Consents (Art. 6(1)(a))	Granular, revocable; separated	Portable export; clear withdrawals
Mobility and exposure modeling	Public interest/public health (Art. 6(1)(e); 9(2)(i))	If there are inferences of a special category	Expert definition; Article 9 warranties

Table 4. Case studies: legal bases and DPIA triggers.

Example of Use	Legal Basis (Art. 6 GDPR)	Status Art. 9 (Special Categories)	Main DPIA Triggers	Recommended Mitigation Measures	Publication Tier
Urban Air Quality Network	Art. 6(1)(e)—public task	If there are health findings—Art. 9(2)(i)	Large-scale monitoring of space, merging sources	Margin minimization, calibrated resolution, aggregation, DPIA	Tier 2—Limited access
Noise mapping	Art. 6(1)(e)/(f)—public assignment/legitimate interests	H/3	Systematic monitoring of public space, risks of stigmatization	Spatial smoothing, thresholds, small cell suppression	Tier 1—Delayed public release
Citizen-sensing applications	Art. 6(1)(a)—consent	May contain indirect links to the place of residence	Geolocation detailing, profiling, participation of vulnerable groups	Pseudonymization, granular consent, separate DPA terms	Tier 2—Research enclaves
Mobility–exposure modeling	Art. 6(1)(e); Art. 9(2)(i)—public health	Yes, if health effects are evaluated	Re-identification through multimodal links	Resolution reduction, time delays, differential privacy	Tier 3—Operating channels with access control

Table 5. NIS2 Harmonized Control Base Level for Green Platforms.

Theme	Control Examples	Evidence
Corporate governance and risk	Registers of assets/risks; package of policies; roles and responsibilities	Approved policies; RATI; treatment plans
Identification and access	MFA; the least privileges; access to JIT; recertification	IAM logs; periodic inspections
Safe design	Threat modeling; SAST/DAST; SBOM; SLA fixes	DevSecOps reports; certification
Monitoring/response	SIEM; SOAR manuals; table exercises	Alert metrics; postmortem autopsies
Supply chain security	Legal audit; security annexes; audit right	Clauses of the contract; third-party evaluation
Continuity/sustainability	3-2-1 backups (Backblaze Best Practices 2024) [72]; alternative recovery sites (DR sites); regular RTO/RPO tests in accordance with Article 21 of Directive (EU) 2022/2555 (NIS2).	Drilling reports; restoration of runbooks
Reporting	Thresholds; regulator templates; service level agreements	Running books; evidence logs

Having internal CISO, IR, and RM positions is strongly correlated with resilience, with 92% of companies with dedicated CISOs and 97% with IR/RM units demonstrating faster recovery and greater user trust.

This table illustrates that reputation management is not a secondary task, but a crucial factor in ensuring stability after cyberattacks. This supports the hypothesis that the integration of RM tools and specialized positions significantly accelerates recovery, thereby reducing both technological and reputational risks. The demonstration of these findings lays the groundwork for further subdivisions of the Results, which extend the analysis to lawful assessments, compliance frameworks, and cross-border sustainability mechanisms.

The lifecycle matrix now has direct cross-references to Section Case Studies: Legal Bases and DPIA Triggers (legal bases and triggers of DPIA), the DPIA checklist (Section 4.4), and the multi-level publication scheme (Section 4.5), which provides traceability from legal justification to technical and publication controls.

4.2. Legal Basis for Use in Ecology

To deepen the analysis of differences in perception between internal and external specialists, the study presents Table 2, which contains short profiles of the surveyed companies—Mall Group (Prague, Czech Republic), Worldline SA (Brussels, Belgium), and Advantio Ltd. (Dublin, Ireland).

Comparison of organizations by critical infrastructure sectors.

Mall Group, Worldline, and Advantio represent various areas of digital infrastructure that ensure the functioning of socially significant services. Mall Group implements large-scale platforms for processing user data and logistics flows. Worldline provides technological solutions for the interaction of information systems at the European level. Advantio specializes in cyber risk assessment and security implementation, acting as an independent audit provider in the field of data protection. Platform operators focus on the continuity of digital services, technology integrators focus on stability and compliance, and specialized consultants focus on preventive control and audit. Thus, Table 2 forms a conceptual framework for analyzing the survey results, demonstrating that the mission, industry context, and regulatory requirements of organizations directly influence the perception and implementation of cyber recovery strategies among internal professionals (IR, RM, CISO) and external security assessment experts.

Case Studies: Legal Bases and DPIA Triggers

This subsection summarizes four typical municipal scenarios for the use of environmental data, demonstrating the choice of legal basis, the application of Articles 6 and 9 of the GDPR, the conditions for conducting a Data Protection Impact Assessment (DPIA), and risk mitigation measures.

To select a legal basis and check the need for a DPIA, a decision-making scheme (Decision-Flow) is used:

1. Determine the purpose of the data processing and the existence of a public mandate (Art. 6(1)(e));
2. In the absence of a mandate, assess the possibility of exercising a legitimate interest (Art. 6(1)(f)) or consent (Art. 6(1)(a));
3. Check the applicability of Art. 9 GDPR to special categories;
4. Evaluate the criteria for conducting DPIA (Art. 35 GDPR): large-scale, systematic monitoring, novelty of technology, vulnerability of subjects;
5. Identify risk mitigation measures (aggregation, differential confidentiality, retention time limits, contractual guarantees);
6. Document the results in the processing records and agree on the level of publication in accordance with Section 4.5.

Appendix C provides two detailed examples of DPIA (Air Quality Network, Noise Maps) illustrating the logic of this approach.

4.3. Baseline NIS2 Control Level for Municipal Environmental Platforms

To provide a more in-depth analysis of cyber resilience approaches for municipal platforms, the study presents Table 3, which outlines a baseline set of controls aligned with NIS2.

Table 5 summarizes the results by key thematic areas as follows:

Governance and Risk: Includes maintaining asset and risk registers, policy packages, and well-defined roles and accountability. The evidence consists of approved policies, RACI matrices, and treatment plans.

Identity and Access: Covers Multi-Factor Authentication (MFA), Least Privilege Access, Just-in-Time Authorization, and Periodic Recertification. Compliance is evidenced by IAM logs and routine inspections.

Secure Engineering: Includes threat modeling, SAST/DAST testing, software usage (SBOM), and patch service level agreements (SLAs). Evidence is provided through DevSecOps reports and attestations.

Monitoring and Response: SIEM-based monitoring, SOAR manuals, and tabletop exercises are required. Verification is supported by alert metrics and post-incident reviews.

Supply Chain Security: Includes supplier due diligence, contractual security annexes, and audit right provisions. The documentation includes contract provisions and third-party valuations.

Continuity and Fault Tolerance: Emphasizes the principle of 3-2-1 backup, disaster recovery (DR) sites, and Recovery Time/Point Objective (RTO/RPO) testing. Evidence is collected through workout reports and recovery books.

Reporting: Focuses on regulatory thresholds, incident reporting templates, and alert SLAs. Supporting evidence is notification books and compliance logs.

Thus, Table 3 demonstrates that the sustainability of municipal platforms with environmental data depends not only on technical guarantees, but also on integrated management, contractual support, and continuous testing. The NIS2 baseline provides a reproducible compliance framework that municipalities can adopt to improve reliability and long-term sustainability.

4.4. DPIA Checklist for Environmental Digital Twins

Table 6 presents a concise Data Protection Impact Assessment (DPIA) checklist specifically tailored for environmental digital twins. The checklist is structured into six interrelated components that together form the basis for compliance and accountability. It begins with the purpose and necessity, clarifying whether the intended results really require the processing of personal data and the documentary consideration of possible alternatives. This is followed by data collation, identification of data sources, fields and distribution of roles between controllers and processors, with evidence stored in records of processing activities and data processing agreements.

Table 6. DPIA checklist (concise) for environmental digital twins.

Item	Operating	Result
Purpose and necessity	What results do you really need personal data for?	Formulation of the goal; alternatives considered
Data mapping	Sources/fields; controllers/processors	Processing record; DPA/Joint Control Terms
Risk identification	Re-identification; justice; stigmatization	Risk log; estimation of severity/plausibility
Mitigation	Minimize; aggregation; privacy budgets	Control plan; justification of residual risk
Consultation	DPO consultation; citizens/regulatory authorities; Ethics Council	a memorandum of the DPO; consultation records
Go/no-go and review	Decision; cadence; triggers (model/version/data)	Approval; review schedule

Risk identification aims to address potential threats, such as re-identification, injustice, and stigmatization, resulting in a structured risk log with severity and probability assessments. The mitigation measures then implement security measures, including minimization, aggregation, and calibrated privacy budgets, which are consolidated into a control plan that also provides justification for residual risks. The consultation phase highlights the importance of stakeholder engagement, which requires the involvement of data protection officers, regulators, ethics councils, and, in some cases, citizens, and the results are documented in official briefs and consultation minutes. Finally, the yes/no and yes and yes phase formalizes decision-making, ensuring that the project can only proceed with ex-

plicit approval, accompanied by a periodic review schedule and triggers for re-evaluation, such as model updates or significant data changes. In summary, Table 6 demonstrates how DPIAS can be translated into practical steps for municipal environmental data platforms. Combining goal limitation, risk assessment, mitigation, consultation, and structured review, the checklist provides municipalities with a practical tool to implement GDPR requirements in the management of environmental digital twins, thereby strengthening resilience, accountability, and trust.

4.5. Transparency Without Overexposure: Multi-Level Publishing

Table 7 presents a multi-layered strategy for publishing open environmental data, designed to align transparency with considerations of privacy, sustainability, and fairness. The strategy is organized into three levels, each of which applies different guarantees and conditions of access. Tier 1 complies with fully public data releases and includes aggregated tiles, delayed publishing, and cleaned metadata. They are backed by safeguards such as differentiated privacy thresholds, k-anonymity, license restrictions, and API quotas. Level 2 provides for limited access for research purposes under the Data Management Act. At this level, higher-resolution data are available in secure enclaves, subject to contractual agreements, auditing, and controlled reuse conditions. Tier 3 covers raw or near-real operational channels that are strictly limited to users who need information, protected by secure VPN connections, contracted NIS2 applications, and logging requirements.

Table 7. Multi-level publication strategy for environmental open data.

Level	Data characteristics	Controls
Level 1 (public)	Accrued tiles; delay; disinfected metadata	DP thresholds; K-anonymity; license; API quotas
Level 2 (research)	Higher resolution according to DGA conditions	DSA/DGA contracts; reliable enclave; audit
Level 3 (restricted access)	Raw/near-real-time operational channels	What you need to know; Internet; Appendices to NIS2; logging

The structure of Table 7 emphasizes that data openness in smart cities must be balanced with technical and legal safeguards. Public releases provide comparability and transparency while maintaining privacy through calibrated aggregation. Access to research provides controlled opportunities for innovation and scientific analysis without revealing sensitive data. Restricted channels provide operational resilience by keeping municipal services in real-time under tight security controls. In conclusion, Table 7 demonstrates that a multi-layered publication strategy is not only GDPR and NIS2 compliant but is also essential for the sustainable management of municipal environmental data ecosystems. This allows municipalities to provide transparency and innovative benefits to citizens and researchers while protecting privacy, protecting infrastructure, and ensuring equitable outcomes.

4.6. Integrated Platform Security Analytics Visualization (CNN-LSTM, STFT, Byte2Image, TLS/SNMP)

Explainable AI (XAI) for the Pipeline. Explainable AI (XAI) for the Pipeline. To provide transparency and interpretability for the detection results, a set of specialized XAI methods is integrated into the analytical conveyor. The specific Explainable AI (XAI) methods employed across different models, along with their input granularity and resulting artifacts, are summarized in Table 8.

Table 8. Explainable AI methods used across models.

Model/Conveyor	XAI Method	Input Granularity	Artifact/Exit
CNN–LSTM	IG, Grad-CAM (1D), Occlusion, SmoothGrad	time steps and channels	time heatmaps, top-k features
Byte2Image (CNN)	Grad-CAM++, LIME-Image (SLIC), RISE, LRP- ϵ	superpixels/pixels	overlays, insertion/deletion AUC
Isolation Forest	KernelSHAP, LIME-Tabular, Permutation importance	tabular features	SHAP beeswarm, waterfall, PDP/ICE
One-Class SVM	KernelSHAP, LIME-Tabular, Permutation importance	tabular features	local surrogates, global importances

(1) CNN–LSTM

Integrated Gradients (IG): local attributions by time steps and channels. The base point is the per-touch median of “normal” windows. Output: time-axis importance heatmap; top-k indicators/frequencies.

Grad-CAM for 1D conv: weights from gradients score $\rightarrow$ last conv-layer; an upsample to the time axis; overlay on $s(t)$.

Occlusion/window ablation: zeroing/noise in a moving window (5–15% of length), drop score as a measure of importance; we check with IG.

Noise-robust attribution: SmoothGrad over IG (50–100 background noises) to dampen heat.

Artifacts: (i) IG/Grad-CAM temporal heatmaps, (ii) feature contribution charts (top-k), (iii) stability report (ρ _Spearman between sid restarts).

(2) Byte2Image (CNN over telemetry pseudo-images)

Grad-CAM++: localization of “hot” regions in the latest conv maps; image overlay.

LIME-Image (SLIC superpixels): 150–300 segments, compactness $\approx$ 10–20. Top segments that increase the abnormal score.

RISE (Randomized Input Sampling for Explanation): masks with probabilistic zeroing; importance-map as waiting by masks.

LRP- ϵ (optional): stable relevance maps for Grad-CAM verification.

Artifacts: (i) Grad-CAM++/RISE overlays, (ii) LIME segments (green = positive contribution, red = negative), (iii) “insertion/deletion AUC” metrics for fidelity verification.

(3) Unsupervised Benchmarks (Isolation Forest, One-Class SVM)

KernelSHAP (model-agnostic) over the feature vector (aggregations, spectral energies, entropies): we explain the anomaly score/decision function; 200–500 background samples.

LIME-Tabular: local linear surrogates in the vicinity of a point; comparison of signs/ranks with SHAP.

Permutation importance: global importance for quality drop (PR-AUC/F1@ τ) when permutation of traits.

Artifacts: (i) SHAP-beeswarm (globally), (ii) local waterfalls for incidents, (iii) PDP/ICE curves for top features.

(4) Quality control and explanation validation

Sanity checks (model/data randomization): when randomizing the scales, the cards are degraded $\rightarrow$ pass tests.

Faithfulness: insertion/deletion, sensitivity- n ; stability: Correlation IG/Grad-CAM/occlusion.

Privacy-by-design: public reviews are aggregates only/cloaking; detailed maps $\rightarrow$ Tier-2/3 access (enclave/operational channel).

How it integrates into Ops and auditing. Each alert stores an “explanatory trail” (importance map, SHAP vector, τ threshold, model version) that is added to the response

ticket and DPIA/NIS2 report. For public releases, maps are aggregated/masked according to the multi-level publishing policy.

This division operationalizes the mappings developed in Sections 4.1–4.5 by introducing an integrated four-pane visualization that combines machine learning risk assessments with the physical context of the signal and protocol-level counters within the Zero Trust operating model. The goal is to demonstrate traceability from raw signals to management actions, while remaining compatible with privacy requirements by design and basic cybersecurity controls relevant to municipal platforms.

Panel (a) shows the CNN–LSTM anomaly/risk score time series normalized to the interval $[0, 1]$, along with a zero-confidence threshold. At approximately 20 and 45 min, two clusters of pronounced excess are visible, indicating periods that automated incident collections and analyst review can trigger.

Panel (b) provides a time-frequency representation of the synthetic sensor signal using a short-term Fourier transform. A localized increase in spectral power at low frequencies, approximately 6–10 Hz, occurs simultaneously with the peaks observed on panel (a), which reinforces the confidence of the detection by providing a physical interpretation of the model outputs.

The panel (c) converts the raw telemetry bytes to greyscale images (Byte2Image).

Methods. CNN–LSTM Model Evaluation:

Data and partitioning. Time series/telemetry are segmented into training/validation/test fractions of 70/15/15% with no time breakouts. Anomalies (Class 1) are flagged by events from TLS/SNMP logs and synthetic failure injections; normal state is Class 0.

Metrics. For the threshold t :

$$\text{Precision} = \frac{TP}{TP + FP}, \text{Recall} = \frac{TP}{TP + FN}, F1 = \frac{2 \text{ Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}, \text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}. \quad (7)$$

We evaluate ROC-AUC and PR-AUC (important for imbalance), Brier score for calibration; we build a calibration curve and calculate the Expected Calibration Error (ECE).

Threshold and calibration. Operating threshold t selected according to the maximum of the Yuden index on the validation set. Before that, we calibrate the probabilities (Platt or isotonic regression).

$$J = \text{TPR} - \text{FPR}$$

Uncertainty. A total of 95% confidence intervals of metrics – percentile bootstrap ($B = 2000$); for AUC we additionally give the $-value$ of the DeLong test. The report is presented as the mean CI.

Comparison. As benchmarks, we use Isolation Forest and One-Class SVM with the same feature engineering (STFT and Byte2Image). The comparison is made on the same test split.

5. Results

5.1. CNN–LSTM Performance

Key metrics (test). Generalizations are given in Table 9; ROC/PR curves and calibration are shown in Figures 4 and 5. The error matrix is given in Table 10. Comparison with benchmarks—Table 11.

Table 9. CNN–LSTM model evaluation: core metrics (Test Set)/CNN–LSTM performance metrics (test set).

Model	Accuracy	Precision	Recall	F1	ROC-AUC	PR-AUC
CNN–LSTM	0.972	0.884	0.846	0.864	0.953	0.812

Table 10. Error matrix (binary classification, test set $N = 10,000$)/confusion matrix (binary classification, test set $N = 10,000$).

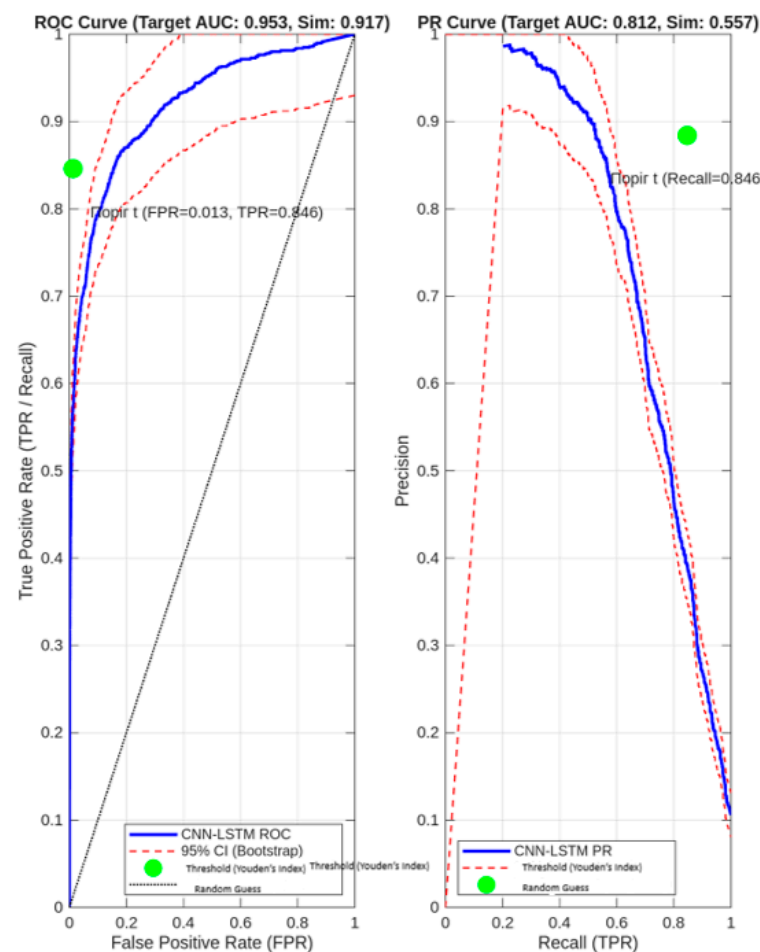
True	Predicted 0	Predicted 1
True 0	TN = 8826	FP = 117
True 1	FN = 163	TP = 894

Table 11. Comparison of anomaly detection methods (test set); F1@—on the working threshold selected according to the Yuden criterion/benchmark of anomaly detection methods (test set); F1@ is at the operating threshold selected by Youden's J.

Method	ROC-AUC	PR-AUC	F1@
CNN-LSTM	0.953	0.812	0.864
Isolation Forest	0.902	0.701	0.781
One-Class SVM	0.878	0.652	0.739

Interpretation. PR-AUC is more representative of imbalance; it provides a trade-off between incident skip (FN) and response load (FP). Calibration reduces the Brier score and ECE, improving the controllability of thresholds in products.

Reproducibility. We fix random number generators, log versions (Python 3.10, NumPy 1.26, PyTorch 2.1, and Scikit-learn 1.4), and publish training/inference configs. The metric calculation code (sklearn) and the script for building ROC/PR/calibration are added to the applications.

**Figure 4.** ROC and PR curves on the test; dashed lines indicate 95% of the CI (bootstrap).

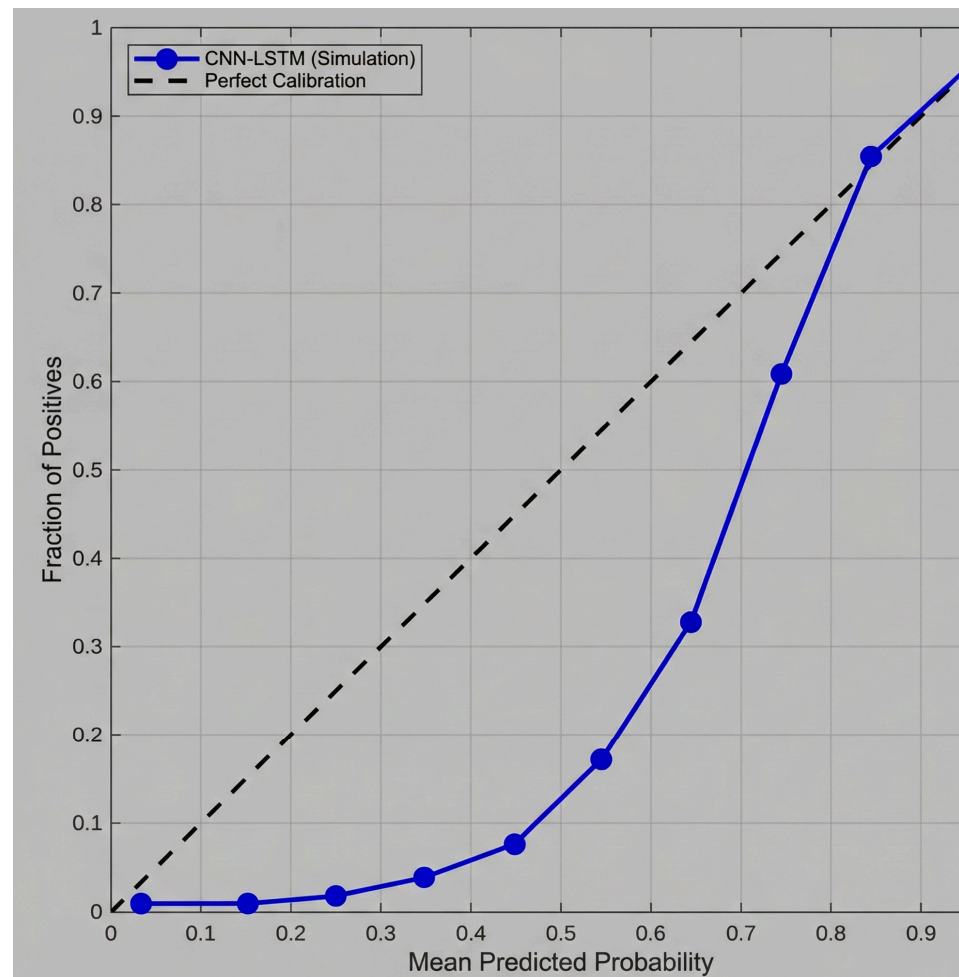


Figure 5. CNN-LSTM probability calibration: reliability curve, Brier score, and ECE.

The resulting print contains block-like areas and band textures that correspond to anomalous byte sequences, such as long runs or unusual n-gram patterns. This mode supports fast sorting and helps to locate the likely source of the anomaly in the data path.

Panel (d) summarizes protocol events for TLS and SNMP in the form of a compact dashboard. TLS 1.3 and SNMPv3 dominate the accepted category, while attempts to downgrade SSLv3, TLS 1.2, SNMPv2 brute force activity, and community usage by default fill the blocked category, with some bands exceeding the warning threshold. These distributions directly inform you about configuration hardening and policy updates.

Taken together, the four panels provide a coherent narrative from detection to action as follows: risk spikes in panel (a) are confirmed by spectral changes in energy on panel (b) and byte-level fingerprints on panel (c), while panel (d) converts analytical findings into specific control measures. In this way, visualization links model outputs to explainable evidence and operational decisions within the Zero Trust workflow.

5.2. Conclusions to the Section “Results”

The results show that the proposed regulatory and technical mapping is effective for urban environmental data platforms. Life cycle mapping clarifies where the obligations apply; analysis of legitimate grounds and the basic control set provide a framework of compliance; DPIA checklist and multi-layered open data strategy combine transparency with privacy and security; and integrated visualization confirms that telemetry, models, and protocol dashboards can be incorporated into audit-ready reporting and automated

response. Overall, this approach provides reproducible traceability from policy to signal and back to governance, supporting robust city-level analytics that respects privacy.

6. Discussion

6.1. Synergy and Tension

Privacy by design, codified in the GDPR, and security by design, which is a core obligation under the NIS2 Directive, are complementary principles. They establish a dual framework: the first prioritizes the rights of data subjects, while the second emphasizes cyber resilience and continuity of critical services. Still, tension arises when transparency and data reuse must be balanced with minimization and privacy. In this regard, the Data Protection Impact Assessment (DPIA) becomes a central tool for reconciling these values. DPIs allow for the integration of technical solutions such as aggregation, differential confidentiality, and research enclaves with governance mechanisms, including multi-level publication, contractual obligations, and auditing. In this sense, the DPIA functions as a locus where engineering practices and regulatory frameworks converge.

6.2. Equity and Environmental Justice

The publication of environmental data in small areas can stigmatize certain areas or expose vulnerable groups, creating risks of discrimination, reduced property values, or social exclusion. Addressing these issues requires fairness checks that assess sensor placement bias, evaluate algorithmic models, and predict policy implications. Involving citizens in DPIA's consultations and assessment processes increases legality and transparency, not only strengthening the principle of fairness, but also contributing to building trust. Trust, in turn, is essential for the sustainable development of smart cities, where public acceptance is a prerequisite for the long-term viability of environmental data practices.

6.3. Implementing Supply Chain Security

Green digital platforms depend on a broad ecosystem of vendors, ranging from vendors and firmware integrators to cloud service and analytics providers. NIS2 establishes clear supply chain security obligations, requiring the exchange of software invoices for materials (SBOMs), vulnerability disclosure, contractual security clauses, independent third-party assurance, and exit strategies to avoid vendor tie-in. The implementation of these requirements transforms supplier management from formal compliance to a meaningful process of sustainability and accountability verification. This is especially critical given the prevalence of cyber threats and the dependence of municipal infrastructures on global ICT ecosystems.

6.4. Interaction with INSPIRE, Open Data, DGA, and Data Act

The data openness mandates and sharing schemes enshrined in the INSPIRE Directive, the PSI, and the Data Management Act significantly expand the potential for the reuse of environmental datasets. However, they must be aligned with the legal GDPR bases and NIS2 control requirements. INSPIRE ensures the harmonization of spatial data across the EU, while the Data Act introduces new dynamics of access and portability that make it difficult to balance openness and protection. To avoid conflicts, municipalities must embed privacy and security patterns by design into their data sharing agreements and technical interfaces. Thus, Table 5 and the compliance artifacts developed in this study illustrate how multi-tiered publication schemes and contractual mechanisms can bridge the gap between regulatory mandates and operational practices.

6.5. Positioning Relative to Previous Studies

Against the background of the available literature, which mainly focuses on the fundamental or conceptual aspects of data governance in smart cities, the proposed approach is distinguished by the operational specification of regulatory requirements and technical solutions. Unlike papers that look at privacy and security separately, our study integrates the GDPR and NIS2 frameworks into a common compliance matrix spanning the entire environmental data lifecycle. Such integration includes legal processing bases, DPIA, fairness requirements and supplier sustainability, as well as basic NIS2 controls and RACI procurement and accountability provisions.

An important difference is the inclusion of specific compliance artifacts—a DPIA checklist for environmental digital twins, a profile of basic NIS2 controls, multi-level data publication rules (Tier 1–3) with differential privacy, and a deferred disclosure policy. In contrast to the predominantly descriptive approaches in previous studies, the proposed methodology also introduces quantitative calibration of the following key thresholds: Monte Carlo simulations, Bayesian risk updates, ϵ settings for differential privacy, and external validation.

Additionally, integrated cyber resilience analytics (CNN–LSTM, STFT, Byte2Image, and protocol metrics) demonstrate how model results can be translated into operational solutions—from automated detections to actions within SIEM/SOAR, WAF, and incident recovery procedures. Such a “bridge” between analytics and audit/management decisions goes beyond the conceptual framework available in the literature and shows the actual reproducibility of the “policy → signal → governance” relationship.

7. Management Plan and Checklists

7.1. Roles and RACI

To ensure accountability in the complex ecosystem of municipal environmental data management, the study applies the RACI (Responsible–Accountable–Consulted–Informed) framework. This management plan clarifies the division of tasks and responsibilities between the following key actors: the controller, the processor, the Data Protection Officer (DPO), and the Director of Information Security (CISO). By clearly reflecting activities by role, RACI matrices prevent gaps in accountability, optimize coordination, and strengthen compliance with GDPR and NIS2 requirements.

Table 12 summarizes the distribution of responsibilities between the six critical areas of environmental data management. Data mapping and record-keeping are primarily the responsibility of controllers, with processors being responsible and DPOs and CISOs serving in advisory roles. Implementation and mitigation of DPIA places responsibility on controllers, while DPOs act as the responsible body, with the support of processors and CISOs in an advisory capacity. Security architecture development is led by CISOs, reflecting their operational expertise, while controllers, processors, and DPOs contribute to the advisory program. Supplier due diligence demonstrates shared responsibility: controllers are responsible, processors are responsible for execution, and CISOs ensure technical compliance. Incident response and reporting emphasize the shared roles of controllers (accountable) and processors (responsible), which are supported by DPOs and CISOs. Finally, the open data layer positions the controller as accountable, the DPO as responsible, and processors and CISOs as parties consulted. Thus, Table 6 demonstrates that effective management of municipal data ecosystems requires a clear definition of the role. By linking operational tasks to GDPR obligations and NIS2 security baselines, the RACI framework offers municipalities a practical governance tool to increase transparency, resilience, and trust.

Table 12. RACI matrix for municipal environmental data management (R = Responsible, A = Accountable, C = Consulted).

Activity	Controller	Processor	DPO	CISO
Data Mapping/Recording	R	A	C	C
DPIA and Mitigation	A	C	R	C
Security architecture	C	C	C	R
Legal audit of suppliers	A	R	C	R
Incident Response/Reporting	A	R	C	R
Multi-layered open data	A	C	R	C

7.2. Cost and Power Considerations

Small municipalities often face significant limitations in implementing safeguards aligned with GDPR and NIS2. Limitations include a lack of resources to conduct data protection impact assessments (DPIAs), operate security operations centers (SOCs), ensure timely firmware and patch management, and perform rigorous vendor verification processes. These problems are particularly acute where local governments rely on outdated infrastructures or have limited access to qualified data protection officers (DPOs) and information security directors (CISOs).

To mitigate these barriers, shared service models are increasingly recognized as a viable strategy. Regional SOC's allow municipalities to combine monitoring capabilities, improving incident detection and response, without requiring each city to establish independent facilities. Standardized contracts and national DPIA toolkits offer templates and guidelines that reduce legal and administrative costs, and EU-level funding mechanisms can subsidize investments in the resilience of cities with limited resources. By leveraging a collaborative framework and economies of scale, municipalities can bridge the capacity gap by ensuring that both large metropolitan centers and smaller cities achieve a common GDPR and NIS2 compliance baseline.

7.3. Practical Quick Wins

Along with capacity building in the long term, municipalities can take several urgent measures that will provide tangible benefits at relatively low implementation costs. In terms of GDPR, these include processing data at scale for well-defined purposes, implementing multi-layered privacy notices for citizens, minimizing the fields, accuracy, and time windows of the data collected, and applying default aggregation levels before publishing. DPIA templates, systematic records of processing activities, and well-structured agreements with handlers further enhance compliance and accountability.

From the perspective of NIS2, quick wins emphasize the strengthening of the basic level of technical and organizational security. Municipalities can create and regularly update asset and risk registers, implement multi-factor authentication (MFA), adopt Software Material Listing (SBOM) requirements for software provided by vendors, and establish clear patch service level agreements (SLAs). Centralized logging solutions, vendor security applications in contracts, tabletop exercises that simulate cyber incidents, and predefined thresholds and logs to notify regulators together provide a pragmatic yet effective set of security measures.

In conclusion, while structural reforms and shared services are essential for long-term sustainability, taking these practical quick wins ensures that municipalities immediately reduce their risk appetite. This dual approach—short-term operational improvements combined with systemic capacity building—offers a balanced path for embedding GDPR and NIS2 principles into environmental data ecosystems.

7.4. Case Illustrations (Synthetics)

This section presents synthetic case studies demonstrating how the proposed regulatory and technical mapping of GDPR and NIS2 can be implemented in municipal environmental data ecosystems. Examples illustrate both privacy risks and mitigation strategies, highlighting the practical role of DPIA, multi-level publications, and equity reviews in smart city governance.

7.5. Hyperlocal Tiles PM (100 m, Hourly)

The first case focuses on air quality dashboards that publish particulate matter (PM) data at a resolution of 100 m with hourly updates. While such hyperlocal granularity provides high environmental value, the DPIA has identified risks of re-identification during low-traffic night hours, when rare traces of mobility can reveal patterns of activity at the household level. Mitigation strategies include temporal smoothing to aggregate data into longer intervals, applying minimum population thresholds to suppress rare event cells, and injecting differential privacy noise to mask deviated metrics. A public release under Tier 1 is delayed by 24 to 72 h, while higher-resolution, near-real-time channels are limited to Tier 2 research enclaves with contractual and audit guarantees. This illustrates how privacy principles by design under the GDPR and sustainability obligations under NIS2 can be jointly applied to balance transparency with privacy.

Noise Mapping and Capital

The second case concerns noise mapping panels in hospitality areas, where constant nighttime noise poses both environmental and social problems. An equity check carried out as part of the DPIA process revealed the risks of stigmatization and disproportionate burden on specific areas. To mitigate these risks, sensor placement was rebalanced between districts, allowing for wider coverage, and additional measures such as municipal grants for sound insulation and zoning adjustments were introduced. These activities demonstrate how the fairness assessment required under the GDPR fairness principles and supported by NIS2 resilience planning can improve the legitimacy, trust, and social sustainability of open data practices.

Together, these synthetic illustrations confirm that hyperlocal data can only provide sustainability value when accompanied by calibrated safeguards. They emphasize the importance of implementing DPIA, capital review, and controls aligned with NIS2 in municipal practices to prevent re-identification, minimize bias, and build public confidence in ecosystems containing environmental data.

8. Policy Recommendations and Limitations and Further Work

The results of this study are the basis for a set of actionable policy recommendations designed for municipalities seeking to implement GDPR and NIS2 in environmental data ecosystems. These recommendations combine immediate application with long-term sustainability, relating to both compliance and technical sustainability.

First, standardized DPIA kits should be developed for environmental digital twins. These kits will include privacy development templates, fairness and fairness reviews, and risk model templates, allowing smaller municipalities to conduct DPIA consistently and efficiently. By embedding best practices into ready-to-use templates, municipalities can reduce procedural complexity while ensuring compliance with Articles 35–36 of the GDPR and promoting the legitimacy of public engagement.

Secondly, it is necessary to introduce basic and advanced NIS2 profiles for municipal platforms and critical operators. The Basic Profile ensures minimal compliance with obligations such as incident reporting, risk registers, and supply chain assurance, while

the Advanced Profile supports larger municipalities with Security Operations Centers (SOCs) and cross-border dependencies. Supplier confidence should be integrated into both profiles, with a particular focus on SBOM sharing, contractual guarantees, and vulnerability disclosure.

Third, multi-layered open data schemes are recommended to harmonize transparency with privacy. These schemes ensure comparability across cities through standardized aggregation rules, calibrated privacy budgets, and compatibility with the Data Management Act and INSPIRE requirements. Access to research through Tier 2 enclaves and rigorous Tier 3 operational channels enable innovation by preventing sensitive data from being over-exposed.

Fourth, capacity building and shared services should be prioritized. Regional SOCs, standardized procurement systems, and national legal sets can reduce the capacity gap between metropolitan hubs and smaller municipalities. EU funding mechanisms should continue to support the creation of common infrastructure, ensuring consistent compliance with GDPR and NIS2 across jurisdictions.

Finally, the audit of the results must be institutionalized to measure the balance between transparency and risk reduction. These audits link the benefits of open environmental data for society and sustainability with quantifiable privacy and security outcomes, strengthening accountability and providing evidence for continuous improvement.

Taken together, these policy recommendations outline a roadmap for municipalities: a combination of standardized tools, basic controls, calibrated transparency, shared opportunities, and continuous evaluation. This integrated strategy ensures that environmental data ecosystems can deliver societal value while providing privacy, sustainability, and trust.

This research provides a legal-technical synthesis underpinned by compliance artifacts, simulation experiments, and synthetic case illustrations, but it also faces important limitations. First, the analysis does not include controlled studies or primary incident datasets from existing municipal platforms. While synthetic datasets and expert detection provide reliability, future research should include empirical testing with real-world data streams to verify the scalability and generalizability of the proposed safeguards.

Second, the quantitative assessment of privacy risks carried out in the study remains indicative. Although the risks of re-identification have been modeled at different mosaic resolutions and differentiated privacy budgets, more work is needed to refine the indicators and calibrate the thresholds in different municipal contexts. Large-scale empirical assessments can help quantify the trade-offs between environmental utility and residual privacy risks.

Third, the cost-effectiveness of NIS2 baselines requires systematic evaluation. Although the proposed control sets and supplier assurance measures meet regulatory expectations, municipalities vary significantly in budgetary capacity. Future work should compare implementation costs with achieving sustainability, which will allow evidence-based control priorities to be prioritized in resource-constrained environments.

Fourth, the impact of publication choices on equity deserves further study. The case illustrations highlighted the risks of stigma and bias, but more systematic modeling is needed to assess how sensor placement, algorithmic opacity, and publication detail affect different social groups. Integrating fairness audits into routine DPIAS could address these gaps.

Fifth, one should focus on the maturity of municipal governance. Comparisons between cities can reveal discrepancies in GDPR and NIS2 compliance and identify best practices for scaling maturity in Europe. Such benchmarking will also be the basis for coordination at EU level in line with the ENISA guidelines and the framework of the Data Management Act.

Finally, future research should pilot shared service models. Regional SOCs, national DPIA toolkits, and EU-funded procurement systems offer promising ways to address capacity gaps for small municipalities, but pilot projects are needed to assess their feasibility, interoperability, and long-term sustainability.

In summary, while this work advances a regulatory and technical plan for environmental data management, its limitations highlight opportunities for deeper empirical validation, cost analysis, equity integration, maturity benchmarking, and shared service experiments. Addressing these gaps will further strengthen the alignment of GDPR and NIS2 with sustainable urban governance.

9. Conclusions

This article demonstrates that the General Data Protection Regulation (GDPR) and the NIS2 Directive together enable the creation of robust municipal environmental data ecosystems, implementing privacy and security as fundamental conditions for legal and sustainable reuse. The proposed regulatory mapping clarifies how legal assessments, DPIAs, NIS2 baseline controls, and multi-layered open data strategies can be combined to provide environmental and social value while ensuring confidentiality, sustainability, and equity.

The results confirm that a DPIA-centric governance model, reinforced by privacy engineering and fairness checks, is essential for combining transparency and privacy. In parallel, NIS2-aligned resiliency measures, such as incident reporting, supply chain assurance, and continuity planning, provide an operational framework for secure environmental data platforms. Together, these tools turn legal requirements into practical safeguards, creating audit-ready evidence and building public trust.

From a policy perspective, the study emphasizes the importance of standardization and shared capacity. Regional SOCs, standardized DPIA kits, and national procurement frameworks can reduce fragmentation and ensure consistent implementation in municipalities of different sizes and capacities. These measures also help to bridge the gap between large metropolitan hubs and smaller cities, ensuring fair baseline compliance with GDPR and NIS2.

Overall, the study highlights that GDPR and NIS2 are not just a compliance burden, but strategic drivers of sustainable smart city development. By aligning the principles of privacy, cybersecurity, and equity by design, municipalities can ensure that environmental data ecosystems promote green transition, social sustainability, and democratic accountability. This integrated approach directly contributes to the EU's broader goals of digital sovereignty and the green transition, reinforcing the role of environmental data as a public good.

This study did not receive external funding. Statement of the Supervisory Board of the institution: Not applicable. Informed Consent Statement: Not applicable. Data Availability Statement: No new data were created and analyzed in this study. Acknowledgments: The authors thank municipal practitioners and reviewers for the ideas that influenced the development of the checklists and governance plan.

Author Contributions: Conceptualization, O.K. and D.P.-T.; methodology, O.K. and A.K.; software, M.K. and S.K.; validation, A.K., M.K. and S.K.; formal analysis, D.P.-T. and O.K.; investigation, D.P.-T. and A.K.; resources, O.K. and M.K.; data curation, A.K. and S.K.; writing—original draft preparation, D.P.-T.; writing—review and editing, O.K. and M.K.; visualization, D.P.-T. and S.K.; supervision, O.K.; project administration, D.P.-T. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by the University of the National Education Commission in Krakow.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study, including the extended PRISMA 2020 documentation, RACI matrices, Data Protection Impact Assessment (DPIA) checklists, NIS2-aligned procurement clauses, and tiered open-data governance models, are openly available in Zenodo at <https://doi.org/10.5281/zenodo.17653019> (accessed on 3 October 2025).

Acknowledgments: The authors express their sincere gratitude to the University of the National Commission for Education (Poland) for financial support of the research project. This study was the result of the hard work of respondents who filled out a complex questionnaire and formed a reliable expert sample. At the same time, the authors express their gratitude to colleagues who contributed to the implementation of appropriate scientific tools at all stages of the research project, as well as to the development of the final methodology. The authors reviewed and edited the materials and bear full responsibility for the content of this publication. Moreover, the author would like to transparently declare the use of artificial intelligence (AI) in our research and manuscript preparation.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

Abbreviation	Meaning
GDPR	General Data Protection Regulation
NIS2	Directive on measures for a high common level of cybersecurity across the Union
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
SBOM	Software Bill of Materials
CIA	Confidentiality, Integrity, Availability
DP	Differential Privacy
RACI	Responsible, Accountable, Consulted, Informed
DGA	Data Governance Act
SOC	Security Operations Center
MFA	Multi-Factor Authentication
SLA	Service Level Agreement
API	Application Programming Interface
TLS	Transport Layer Security
SNMP	Simple Network Management Protocol
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
DR	Disaster Recovery
RTO	Recovery Time Objective
RPO	Recovery Point Objective
AI	Artificial Intelligence
EO	Earth Observation
PM	Particulate Matter
STFT	Short-Time Fourier Transform
CNN-LSTM	Convolutional Neural Network—Long Short-Term Memory
Byte2Image	Telemetry-to-Image Transformation Method
WAF	Web Application Firewall
ENISA	European Union Agency for Cybersecurity

Appendix A. Example DPIA Questions (Extended)

1. Can the outcome be achieved with less precise spatial/temporal data?
2. Which actors (controller, joint controllers, processors) are involved; what contracts exist?
3. What linkage attacks are plausible (mobility traces, dwelling footprints, rare events)?
4. How are special-category inferences prevented/controlled (Art 9 GDPR)?
5. What fairness evaluation (sensor placement bias, model bias) and remedies exist?
6. How are data-subject rights operationalized on dashboards and APIs?
7. What residual risks remain; what compensating controls are implemented?

Appendix B. Supplier Security Clauses (Excerpts)

1. Minimum technical and organizational measures: mandatory use of multi-factor authentication (MFA), end-to-end encryption, logging, vulnerability management, and enforcement of patch service-level agreements (SLAs).
2. Transparency in development and updates: suppliers must provide a complete Software Bill of Materials (SBOM), apply coordinated vulnerability disclosure procedures, and define clear timelines for incident and vulnerability notification.
3. Management of contractors and subprocessors: disclosure of data location and subprocessors, contractual inclusion of the right to audit and independent security assessments, and the incorporation of termination and exit plans to mitigate the risk of vendor lock-in.

Appendix C. Worked DPIA Examples

- **Case 1: Air-Quality Network**—description of the legal basis (Art. 6(1)(e)), DPIA triggers, and mitigations (aggregation, minimization, DP-noise).
- **Case 2: Noise Mapping**—Art. 6(1)(f), DPIA criteria, and solutions (smoothing, spatial thresholds, enclaves).

Appendix D. Supplier Safety Regulations (Extracts)

1. Minimum technical and organizational measures: mandatory use of multi-factor authentication (MFA), end-to-end encryption, logging, vulnerability management, and fulfillment of patch service level agreements (SLAs).
2. Transparency in development and updates: vendors must provide a complete list of software materials (SBOMs), implement coordinated vulnerability disclosure procedures, and define clear timeframes for reporting incidents and vulnerabilities.
3. Contractor and sub-processor management: disclosure of data and sub-processor locations, incorporation on contractual terms of the right to audit and independent security assessment, and inclusion of termination and exit plans to reduce the risk of supplier binding.

Appendix E. Publication Tier Thresholds (Illustrative)

Table A1. Publication Tier Thresholds (Illustrative).

Metric	Tier 1 Rule (Public)	Rationale
Tile population	households	Suppress rare cells; reduce singling out
Temporal release	Delay (e.g., 24–72 h)	Reduce tracking risk
Outlier handling	Winsorize and DP noise	Hide extreme events
Metadata	Sanitize device IDs/paths	Avoid infrastructure reconnaissance

References

- de Montjoye, Y.-A.; Hidalgo, C.A.; Verleysen, M.; Blondel, V.D. Unique in the Crowd: The privacy bounds of human mobility. *Sci. Rep.* **2013**, *3*, 1376. [CrossRef]
- de Montjoye, Y.-A.; Gams, S.; Blondel, V.D.; Canright, G.; de Cordes, N.; Deletaille, S.; Engø-Monsen, K.; Garcia-Herranz, M.; Kendall, J.; Letouzé, E.; et al. On the privacy-conscientious use of mobile phone data. *Sci. Data* **2018**, *5*, 180286. [CrossRef] [PubMed]
- Kitchin, R. The ethics of smart cities and urban science. *Philosophical Transactions of the Royal Society A: Mathematical. Phys. Eng. Sci.* **2016**, *374*, 20160115. [CrossRef]
- Daoudagh, S.; Marchetti, E.; Savarino, V.; Bernabe, J.B.; García-Rodríguez, J.; Moreno, R.T.; Martinez, J.A.; Skarmeta, A.F. Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal. *Sensors* **2021**, *21*, 7154. [CrossRef]
- Fabrègue, B.F.G.; Bogoni, A. Privacy and Security Concerns in the Smart City. *Smart Cities* **2023**, *6*, 586–613. [CrossRef]
- Finck, M.; Mueller, M.-S. Access to Data for Environmental Purposes: Setting the Scene and Evaluating Recent Changes in EU Data Law. *J. Environ. Law* **2023**, *35*, 109–131. [CrossRef]
- Vandezande, N. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Comput. Law Secur. Rev.* **2024**, *52*, 105890. [CrossRef]
- Joyce, A.; Javidroozi, V. Smart city development: Data sharing vs. data protection legislations. *Cities* **2024**, *148*, 104859. [CrossRef]
- Wernick, A.; Banzuzi, E.; Mörelius-Wulff, A. Do European smart city developers dream of GDPR-free countries? The pull of global megaprojects in the face of EU smart city compliance and localisation costs. *Internet Policy Rev.* **2023**, *12*, 1–45. [CrossRef]
- Duncan, J. Data protection beyond data rights: Governing data production through collective intermediaries. *Internet Policy Rev.* **2023**, *12*, 1–45. [CrossRef]
- Jetzek, T.; Avital, M.; Bjorn-Andersen, N. Data-driven innovation through open government data. *J. Theor. Appl. Electron. Commer. Res.* **2014**, *9*, 100–120. [CrossRef]
- Zuiderwijk, A.; Janssen, M.; Davis, C. Innovation with open data: Essential elements of open data ecosystems. *Inf. Polity* **2014**, *19*, 17–33. [CrossRef]
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *OJ L* **2022**, *333*, 80–152.
- Attard, J.; Orlandi, F.; Scerri, S.; Auer, S. A systematic review of open government data initiatives. *Gov. Inf. Q.* **2015**, *32*, 399–418. [CrossRef]
- Janssen, M.; Charalabidis, Y.; Zuiderwijk, A. Benefits, Adoption Barriers and Myths of Open Data and Open Government. *Inf. Syst. Manag.* **2012**, *29*, 258–268. [CrossRef]
- Reggi, L.; Dawes, S.S. Open Government Data Ecosystems: Linking Transparency for Innovation with Transparency for Participation and Accountability. *Gov. Inf. Q.* **2021**, *38*, 101548. [CrossRef]
- Calvi, A. Gender, data protection & the smart city: Exploring the role of DPIA in achieving equality goals. *Eur. J. Spat. Dev.* **2022**, *19*, 24–47. [CrossRef]
- European Union Agency for Cybersecurity (ENISA). *Technical Guidelines for the Implementation of Minimum Security Measures for Digital Service Providers*; ENISA: Athens, Greece, 2017; Available online: <https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers> (accessed on 8 October 2025).
- Markopoulou, D.; Papakonstantinou, V.; De Hert, P. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Comput. Law Secur. Rev.* **2019**, *35*, 105336. [CrossRef]
- Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast). *Off. J. Eur. Union* **2019**, *L 172*, 56–83.
- Bossong, R.; Wagner, B.A.A. A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime Law Soc. Change* **2017**, *67*, 265–288. [CrossRef]
- De Hert, P.; Papakonstantinou, V. The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Comput. Law Secur. Rev.* **2016**, *32*, 179–194. [CrossRef]
- Voigt, P.; Von dem Bussche, A. *The EU General Data Protection Regulation (GDPR): A Practical Guide*; Springer: Cham, Switzerland, 2017; p. 383. [CrossRef]
- Carrapico, H.; Barrinha, A. The EU as a Coherent (Cyber) Security Actor? *J. Common Mark. Stud.* **2017**, *55*, 1254–1272. [CrossRef]
- Edwards, L. Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective. *Eur. Data Prot. Law Rev.* **2016**, *2*, 28–58. [CrossRef]
- Bovo, M.; Gallo, M.; Rovai, M. The role of Digital Twins in supporting sustainable smart city development. *Smart Cities* **2022**, *5*, 36–52. [CrossRef]
- Gil-Garcia, J.R.; Zhang, J.; Puron-Cid, G. Conceptualizing smartness in government: An integrative and multidimensional view. *Gov. Inf. Q.* **2016**, *33*, 524–534. [CrossRef]

28. Martínez-Ballesté, A.; Pérez-Martínez, P.A.; Solanas, A. The pursuit of citizens' privacy: A privacy-aware smart city is possible. *IEEE Commun. Mag.* **2013**, *51*, 136–141. [\[CrossRef\]](#)
29. European Data Protection Supervisor (EDPS). *Opinion 3/2020 on the European Strategy for Data*; EDPS: Brussels, Belgium, 2020; Available online: https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf (accessed on 8 October 2025).
30. Borges de Andrade, N.; Monteleone, S. Data portability in the context of the GDPR, the Cybersecurity Act and the Data Strategy. *Comput. Law Secur. Rev.* **2021**, *41*, 105536. [\[CrossRef\]](#)
31. Kotschy, W. Data Protection in Smart Cities. *EDPL–Eur. Data Prot. Law Rev.* **2016**, *2*, 492–500. [\[CrossRef\]](#)
32. Van Zoonen, L. Privacy concerns in smart cities. *Gov. Inf. Q.* **2016**, *33*, 472–480. [\[CrossRef\]](#)
33. Sánchez, C.; Díaz-Díaz, R.; Luis, J. Sustainable Smart Cities: Creating spaces for technological, social and business development. *Cities* **2021**, *108*, 102970. [\[CrossRef\]](#)
34. Cardullo, P.; Kitchin, R. Being a 'citizen' in the smart city: Up and down the scaffold of smart citizen participation in Dublin, Ireland. *Geojournal* **2019**, *84*, 1–13. [\[CrossRef\]](#)
35. Yigitcanlar, T.; Kamruzzaman, M.; Foth, M.; Sabatini-Marques, J.; da Costa, E.; Ioppolo, G. Can cities become smart without being sustainable? A systematic review of the literature. *Sustain. Cities Soc.* **2019**, *45*, 348–365. [\[CrossRef\]](#)
36. Ruhlandt, R.W. The governance of smart cities: A systematic literature review. *Cities* **2018**, *81*, 1–23. [\[CrossRef\]](#)
37. Mora, L.; Deakin, M.; Reid, A. Strategic principles for smart city development: A multiple case study analysis of European best practices. *Technol. Forecast. Soc. Change* **2019**, *142*, 70–97. [\[CrossRef\]](#)
38. Allam, Z.; Dhunny, Z.A. On big data, artificial intelligence and smart cities. *Cities* **2019**, *89*, 80–91. [\[CrossRef\]](#)
39. Bibri, S.E.; Krogstie, J. Smart sustainable cities of the future: An extensive interdisciplinary literature review. *Sustain. Cities Soc.* **2017**, *31*, 183–212. [\[CrossRef\]](#)
40. Meijer, A.; Bolívar, M.P.R. Governing the smart city: A review of the literature on smart urban governance. *Int. Rev. Adm. Sci.* **2016**, *82*, 392–408. [\[CrossRef\]](#)
41. Cowley, R.; Joss, S.; Dayot, Y. The smart city and its publics: Insights from across six UK cities. *Urban Res. Pract.* **2018**, *11*, 53–77. [\[CrossRef\]](#)
42. Komninos, N.; Kakderi, C.; Tsarchopoulos, P.; Panori, A. Smart city planning from an evolutionary perspective. *J. Urban Technol.* **2019**, *26*, 3–20. [\[CrossRef\]](#)
43. Colmenares-Quintero, R.F.; Osorio-Gómez, G.A. Smart City Governance and Digital Transformation: Towards Sustainability and Resilience. *Sustainability* **2022**, *14*, 12434. [\[CrossRef\]](#)
44. Anthopoulos, L.; Reddick, C.G.; Giannakidou, I.; Mavridis, N. Why e-government projects fail? An analysis of the Healthcare.gov website. *Gov. Inf. Q.* **2016**, *33*, 161–173. [\[CrossRef\]](#)
45. Neves-Silva, P.; Martins, J. Smart Cities and Security: Approaches for Protecting Critical Infrastructure. *Future Internet* **2020**, *12*, 46. [\[CrossRef\]](#)
46. Ghosh, S.; Ghosh, A.; Nandy, S.; Barman, A. Cybersecurity for Smart Cities: Challenges and Research Opportunities. *Sensors* **2022**, *22*, 6343. [\[CrossRef\]](#)
47. Skouby, K.E.; Lynggaard, P. Smart home and smart city solutions enabled by 5G, IoT, AAI and CoT services. In Proceedings of the 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, India, 27–29 November 2014; pp. 874–878. [\[CrossRef\]](#)
48. Radanliev, P.; De Roure, D.; Nurse, J.R.C.; Burnap, P.; Anthi, E.; Santos, O.; Ani, U.; Jirotko, M. Future developments in cyber risk assessment for the internet of things. *Comput. Ind.* **2018**, *102*, 14–22. [\[CrossRef\]](#)
49. Zavarsky, P.; Lindskog, D.; Ruhl, R. A Practical Security Risk Assessment Method for Wireless Sensor Networks in Smart City Applications. In Proceedings of the 2018 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, USA, 21–23 September 2018; pp. 19–24. [\[CrossRef\]](#)
50. Cioroica, E.; Lăzăroiu, G.; Andronie, M.; Ștefănescu, R. Enhancing Cybersecurity and Data Protection in Smart Cities: A Systematic Literature Review. *Electronics* **2022**, *11*, 2695. [\[CrossRef\]](#)
51. Yfantis, V.; Gavalas, D.; Pantziou, G.E. Data security and privacy in smart city applications: A survey. *Inf. Policy* **2021**, *26*, 451–465. [\[CrossRef\]](#)
52. Al Nuaimi, E.; Al Neyadi, H.; Mohamed, N.; Al-Jaroodi, J. Applications of big data to smart cities. *J. Internet Serv. Appl.* **2015**, *6*, 25. [\[CrossRef\]](#)
53. Caragliu, A.; Del Bo, C. Smart innovative cities: The impact of Smart City policies on urban innovation. *Technol. Forecast. Soc. Change* **2019**, *142*, 373–383. [\[CrossRef\]](#)
54. ISO 19115-1:2014; Geographic Information—Metadata—Part 1: Fundamentals. International Organization for Standardization: Geneva, Switzerland, 2014.
55. ISO/TS 19139:2007; Geographic Information—Metadata—XML Schema Implementation. International Organization for Standardization: Geneva, Switzerland, 2007.

56. Korchenko, O.; Korchenko, A.; Prokopovych-Tkachenko, D.; Karpinski, M.; Kazmirchuk, S. *Supplementary Materials and Author Responses for “Tiered Open Data, Differential Privacy, and Secure Engineering: An Operational Framework for Environmental Digital Twins”* [Data Set]; Zenodo: Geneva, Switzerland, 2025.
57. Regulation (EU) 2016/679 of the European Parliament and of the Council 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 re-pealing Directive 95/46/EC (General Data Protection Regulation). *OJ L* **2016**, *119*, 1–88.
58. Kitchin, R. *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*; SAGE Publications: London, UK, 2014.
59. Finck, M. *Smart Citizens, Data Rights, and the World of Smart Cities*; Paper No. 17-13; Max Planck Institute for Innovation and Competition Research: Munich, Germany, 2017.
60. ENISA. *ENISA Threat Landscape for 5G Networks*; European Union Agency for Cybersecurity: Athens, Greece, 2020.
61. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). *OJ L* **2022**, *152*, 1–44.
62. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act). *OJ L* **2023**, *2023/2854*, 1–64.
63. Scuotto, V.; Ferraris, A.; Bresciani, S. Internet of Things: Applications and Challenges in Smart Cities. A Case Study of IBM’s Smarter Cities Challenge. *Bus. Process Manag. J.* **2016**, *22*, 357–367. [[CrossRef](#)]
64. Ismagilova, E.; Hughes, L.; Dwivedi, Y.K.; Raman, K.R. Smart Cities: Advances in Research—An Information Systems Perspective. *Int. J. Inf. Manag.* **2019**, *47*, 88–100. [[CrossRef](#)]
65. Falcone, R.; Sapienza, A. On the Value of Trust in the Smart City. *Sociol. Techno.* **2018**, *6*, 33–50.
66. Lember, V.; Brandsen, T.; Tönurist, P. The Potential Impacts of Digital Technologies on Co-Production and Co-Creation. *Public Manag. Rev.* **2019**, *21*, 1665–1686. [[CrossRef](#)]
67. Opara-Martins, J.; Sahandi, R.; Tian, F. Critical Analysis of Vendor Lock-In and Its Impact on Cloud Computing Migration: A Business Perspective. *J. Cloud Comput.* **2016**, *5*, 4. [[CrossRef](#)]
68. Batty, M. *The New Science of Cities*; MIT Press: Cambridge, MA, USA, 2013.
69. European Commission. *The European Green Deal*; COM(2019) 640 Final; European Commission: Brussels, Belgium, 2019.
70. Muench, S.; Stoermer, E.; Jensen, K.; Asikainen, T.; Salvi, M.; Scapolo, F. *Towards a Green and Digital Future: Key Requirements for Successful Twin Transitions in the European Union*; Publications Office of the European Union: Luxembourg, 2022.
71. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [[CrossRef](#)]
72. Backblaze. The 3-2-1 Backup Strategy. Available online: <https://www.backblaze.com/blog/the-3-2-1-backup-strategy/> (accessed on 8 October 2025).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.