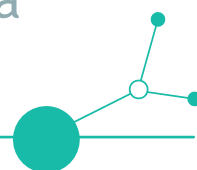


Public Data Opening Strategy

WP1 - Development and transfer of public data
opening and security strategy



Version 1.6
31 May 2026





Table of Content

LIST OF FIGURES	3
EXECUTIVE SUMMARY	4
1. INTRODUCTION	5
2. STRATEGIC OBJECTIVES AND STEP-BY-STEP GUIDE	9
2.1 VISION FOR A PUBLIC OPEN DATA ECOSYSTEM	9
2.2 OPEN DATA CULTURE WITHIN THE ADMINISTRATION	11
2.3 LOCAL STRATEGY AND POLICY	12
2.4 MODEL RESOLUTION FOR LOCAL OPEN DATA STRATEGIES	15
3. STEP-BY-STEP GUIDE	17
4. BETTER NOT'S	18
5. LEGAL AND REGULATORY FRAMEWORK	22
5.1 EUROPEAN LEVEL	22
<i>EU strategies and key EU legislation</i>	22
<i>Relevance of EU framework for local governments</i>	27
5.2 NATIONAL LEVEL	27
<i>National strategies and action plans</i>	27
6. OPEN DATA GOVERNANCE	34
6.1 ROLES AND RESPONSIBILITIES	34
<i>Main roles</i>	34
<i>Responsibilities</i>	35
<i>Other defined roles</i>	37
6.2 DATA COLLECTION	37
<i>Overview of data collection process</i>	38
<i>Data sources</i>	40
<i>Data collection methods</i>	43
7. DATA LICENSING	46
7.1 WHAT DOES AN OPEN DATA LICENCE COVER?	46
7.2 TYPES OF OPEN DATA LICENCES	47
<i>Public domain licences</i>	49
<i>Attribution licences</i>	49
<i>Share-Alike licences</i>	49
7.3 EXAMPLES OF OPEN DATA LICENSING	53
7.4 CHALLENGES IN OPEN DATA LICENSING	54
8. SECURITY STRATEGY	55
8.1 WHY IS DATA SECURITY IMPORTANT?	56
8.2 CORE PRINCIPLES OF PROACTIVE SECURITY IN OPEN DATA	57
8.3 BALANCING PRIVACY AND UTILITY IN OPEN DATA ANONYMISATION	58
9. DATA PUBLICATION AND MANAGEMENT	60
9.1 DATA AS A RESOURCE FOR DIVERSE RE-USE	60
9.2 HOW TO FIND DATA: THE IMPORTANCE OF METADATA	60
9.3 CLEANING DATA	61
9.4 CONTINUOUS DATA MANAGEMENT	62



GLOSSARY OF TERMS	63
SOURCES.....	68



List of Figures

FIGURE 1: WHAT IS OPEN DATA?	6
FIGURE 2: STEP-BY-STEP GUIDE TO OPENING DATA	17
FIGURE 3: EU STRATEGIES AND KEY EU LEGISLATION FOR OPEN DATA	22
FIGURE 4: HIGH-VALUE DATASETS	24
FIGURE 5: WHY GDPR REQUIRES DOWNSTREAM CONTROL OF PERSONAL DATA	26
FIGURE 6: HOW APIS ENABLE STRUCTURED DATA ACCESS	44
FIGURE 7: OPEN DATA LICENSES OVERVIEW	48
FIGURE 8: TYPES OF LICENSES, RIGHTS AND RESPONSIBILITIES	50
FIGURE 9: ANONYMISATION METHODS	59
FIGURE 10: WHY GOOD DATA NEEDS GOOD METADATA	61



Executive Summary

This Public Data Opening Strategy has been created within the Interreg Central Europe project DoorCE, focused on developing a data opening strategy for municipalities and public administrations. The strategy provides guidance on how to effectively collect, manage, and publish open data to foster innovation, transparency as well as public service improvement. By addressing key aspects such as open data governance, data collection, licensing or quality management, this strategy aims to support the integration of open data practices into everyday decision-making processes across Central Europe.

Open Data Governance Framework

The document emphasises the importance of creating a robust open data governance framework. Municipalities are encouraged to establish policies and structures that ensure data accessibility, compliance with legal standards and opportunities for internal training. Effective governance enables better data management and collaboration among various stakeholders, ensuring that open data serves the public interest.

Data Collection Methods and Sources

A vital component of the data opening strategy is the selection of appropriate data collection methods. The report outlines the need to identify relevant datasets and engage key stakeholders, including citizens, businesses, and government agencies. It stresses the importance of setting clear objectives for data collection, selecting the most effective methods (manual, automated, or crowdsourced), and ensuring the accuracy and relevance of the open data. Both static and dynamic data are covered, including real-time data from IoT devices and sensors.

Data Licensing and Legal Considerations

A key aspect of the strategy is the role of clear and transparent data licensing. DoorCE highlights the need for municipalities to adopt open data licences to avoid legal uncertainties and encourage data reuse. Proper licensing ensures that data is available for access and use while protecting both the rights of data creators and users. The report also addresses the complexities surrounding third-party data ownership and the need for clear consent in cases in which personal data is involved.

Data Quality Management and Validation

Ensuring data quality is critical to the success of an open data strategy. The report outlines methods for data validation and quality control, including cleaning, anomaly detection, and compliance with privacy regulations. It stresses the importance of using automated tools and manual review processes to ensure that the data is dependable and useful for decision-making.



1. Introduction

In an increasingly digital and interconnected world, open data has become a crucial tool for municipalities across Europe, driving transparency, efficiency, and innovation. Local administrations face growing demands for accountability and citizen engagement and need a sound basis for decision-making. The European Union is committed to the digital transformation and open government, reinforcing municipalities' roles as key actors in regional and national development. By embracing open data, municipalities not only comply with regulatory frameworks but also position themselves as leaders in smart, data-driven governance, unlocking new opportunities for collaboration, sustainability, and citizen-driven innovation. Open data can foster trust between public institutions and communities as it enables evidence-based policymaking, enhances public service delivery, and stimulates economic growth by empowering businesses, researchers, and civic tech initiatives.

Since the start of the open data movement, thousands of public datasets were opened across Europe enabling new applications and insights. Moreover, it started a switch of mindset about public data as a common good - like infrastructure - to enable a fair and thriving European economy. Open data became a vital part of the European digital agenda and Member States implemented their national strategies accordingly.

In 2020, the European Commission's „Economic Impact of Open Data study estimated that the re-use of open data had generated a market sized of €184 billion across the EU in 2019 and projected this to rise to €199.5 to €334.2 billion by 2025 (European Commission, 2020). In 2020, the EU's Open Data Maturity level had reached 86%, pointing to continued progress in the availability and strategic use of open data (data.europa.eu, 2025a). Beyond these quantitative indicators, the benefits of open data extend well beyond the economic sphere: open data helps reduce CO₂ emissions as it ultimately increases efficiency in the public sector, saves lives through improved emergency response systems, and contributes to the prevention of traffic accidents. These findings underscore the strategic value of open data as a driver of economic, social, and environmental impact (European Commission, 2020).

What is open data?

Open data is data in a digital format, which can be used, reused (e.g. for a different purpose than the data has initially been collected) and distributed freely by anyone at any time for any purpose.

data.europa.eu, 2025b

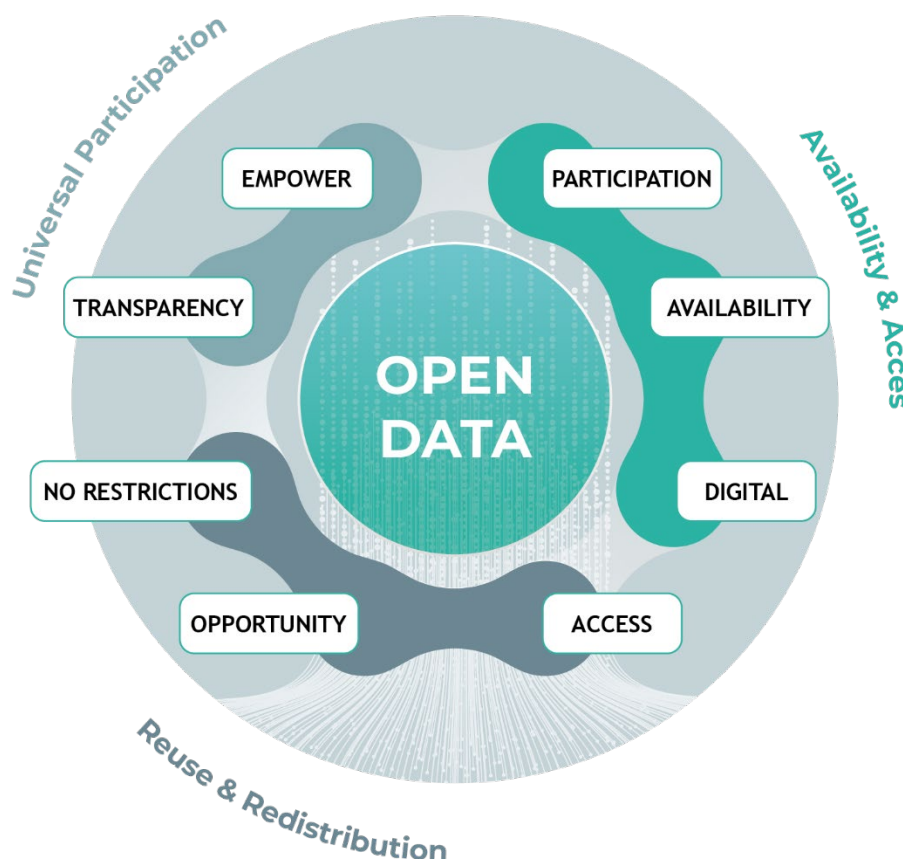


Figure 1: What is open data?

Source: The World Bank, 2015; own adaptation

However, opening data is not an end in itself, nor is it just about digitising and publishing information. Rather, it is a cultural shift within local government to make information available to the public in a standard format - like the way councils already provide information on a website. In the case of open data, the datasets

- have been collected through administrative processes,
- can be used for any purpose – and are licensed accordingly,
- are structured and machine-readable – and therefore usable for multiple applications,
- are described by metadata – to inform users about the content of the datasets.

This cultural shift requires both political support and motivation in the administration's leadership, as well as understanding among staff that providing information as open data may initially be perceived as 'extra work' – but also represents a meaningful contribution to transparency, innovation, efficiency public trust. At the heart of open government is the idea that providing data in an open format increases and promotes transparency in political and administrative decision-making and encourages citizen participation. This is a goal that all staff in public administrations should strive for in their daily work.

However, putting processes in place, promoting open data initiatives and providing sufficient resources – financial, human, and learning – is a key task for political and administrative



leadership. When both work side by side and share the same goal, open data can fulfil its potential.¹

The concept of open data can be traced back to the 1950s and 1960s, when it emerged in the fields of scientific research and education, especially in the context of data sharing among researchers. The term “open data” was first officially used in 1995 in a report by a U.S. agency on the dissemination of geophysical and environmental data. A key moment in the open data movement came in 2007, when around 30 Internet activists and open government advocates gathered in Sebastopol, California, to establish the Eight Principles of Open Government Data (Davies et al., 2019). These principles, inspired by the free and open source software movement, laid the foundation for how public sector data should be made accessible. The open data agenda gained strong political momentum in 2009, when U.S. President Barack Obama issued the Transparency and Open Government memorandum on his first day in office. This led to the launch of the first federal open data portal, data.gov, with over 310,000 datasets (Data.gov, 2026). European countries followed suit: in 2011, Italy launched its national portal dati.gov.it, and in 2012 the European Commission launched the EU Open Data Portal, now known as data.europa.eu, which currently hosts over 1.9 million datasets from across Member States (dati.gov.it, 2026; data.europa.eu, 2026a).

Since then, most European countries have created their own national open data portals, including countries from Central Europe:

- **Germany** - [GovData.de](https://govdata.de)
- **France** - data.gouv.fr
- **Spain** - datos.gob.es
- **Austria** - data.gv.at
- **Slovakia** - data.gov.sk
- **Poland** - dane.gov.pl
- **Croatia** - data.gov.hr
- **Slovenia** - podatki.gov.si

These portals serve as key infrastructure for implementing open data policies, providing machine-readable datasets under open licences, and enabling reuse by citizens, businesses, researchers, and developers. The portals often include data sets provided by municipalities. There are however few initiatives for the local administrative level and information and support services tailored to the needs of cities and regions could be further expanded.

This document is Deliverable 1 in the DoorCE project’s work in work package 1 - Development and transfer of public data opening and security strategy, finalised by May 2026. It offers a methodological review and strategic guidance for provisioning public open data with a focus on the local and regional level in a secure and impactful manner.

aconium GmbH together with TREXIMA Bratislava prepared this document as contractors for the contracting authority - the DoorCE project - Data Opener Central Europe - under project number CE0200647.

The purpose of this strategy is to ensure secure, efficient, and impactful provisioning of public open data (POD). It serves as a roadmap for public institutions and stakeholders, providing

¹ Note: For more detailed guidance on recommended formats and sector-specific standards, see the “Step 2: Define Open Data Standards and Formats” section of the data.europa.eu step-by-step guide.



actionable steps to manage and share open data while maintaining a high standard of security and usability.

Open data plays a critical role in digital transformation, fostering transparency, innovation, and collaboration across various sectors. It empowers stakeholders to make informed decisions, supports economic growth through innovation, and enhances public trust by enabling access to valuable information. As digital ecosystems expand, it is essential to address security challenges, ensuring data integrity and responsible usage.

This strategy is designed for a broad audience, providing guidance tailored to specific roles and expertise levels:

- **Public Institutions:** To support the design, implementation, and management of open data initiatives.
- **Small and Medium Enterprises (SMEs):** To leverage open data for innovation, business growth, and service development.
- **Policymakers:** To establish and refine policies that promote open data accessibility while ensuring compliance with legal and security frameworks.
- **Developers:** To create robust, user-friendly applications that utilise open data for public benefit.

This document is structured to cater to users with varying levels of familiarity with open data provisioning:

- **For Newcomers:** It provides a comprehensive introduction to the fundamental concepts, including the first steps required to design and implement open data strategies.
- **For Experts:** It outlines advanced methodologies, innovation pathways, and best practices to optimise data provisioning and security management.

To all readers, who are still a bit lost in open data terminologies and their meaning, please do not despair. This document provides a Glossary of Terms and will keep referencing real-life examples or best practices for illustration and summarise action points which are applicable in diverse settings.



2. Strategic objectives and step-by-step guide

„Public open data [or open government data] is useful only when it can be easily accessed through different digital services, like mobile apps. For instance, various open-data related applications should be as easy to access as weather forecasts on a mobile phone.“

Data Opener Central Europe (DoorCE) application

The DoorCE project, funded by Interreg Central Europe from 2024 to 2026, considers public open data or open government data, but has a special focus on the local level: cities and regions and considers the exchanges of experiences from the municipal partners who took part in the DoorCE project and established local Open Data Hubs.

2.1 Vision for a public open data ecosystem

An open data ecosystem at the local level is a dynamic network of people, organisations, policies, technologies, and data resources that work together to collect, share, and use data openly to benefit the local community. Along with the local government and administration the ecosystem consists of community organisations, civic technologists, academic institutions, private sector partners, and residents. Community members play a vital role not only as users but also as contributors, helping ensure data reflects lived realities. For the ecosystem to thrive, it needs open standards, strong data governance, active community engagement as well as a strategy to improve data literacy levels.

An effective **public open data strategy for a municipality** is essential for making data accessible, reusable, and valuable for various stakeholders, including government entities, businesses, researchers, and the public. However, **merely publishing data is not enough**—organisations must ensure data is structured, well-documented, secure, and continuously updated.

A well-structured open data strategy aims to:

- **Enhance transparency and accountability** - Open data promotes public trust by enabling citizens to access government and institutional data.
- **Boost economic growth and innovation** - Open datasets provide businesses, start-ups, and researchers with valuable insights for developing new applications, services, and research findings.
- **Facilitate interoperability and collaboration** - Standardised open data formats make it easier to integrate and combine datasets across industries and government sectors.
- **Ensure sustainability and governance** - Open data should not be a one-time initiative but a long-term commitment with defined governance and financial models.
- **Protect privacy and security** - Compliance with **GDPR, Open Data Directive (EU), PSI Directive**, and other regulations ensures that personal and sensitive data are not improperly disclosed.
- **Improve efficiency and reduce redundancy** - Open data helps organisations and governments avoid duplication of efforts by sharing datasets that can be reused for multiple purposes.
- **Increase civic participation and research impact** - Citizens, universities, and NGOs can use open data for evidence-based policymaking, public service improvements, and community projects.



The work on open data and establishing a public open data ecosystem starts within the municipality itself. In the following section, we have collected quick win advice.

Start small and make use of what you already have

Open data initiatives can start small, for example by opening a dataset, or by choosing a specific topic and selecting datasets accordingly. This is the DoorCE approach. The project partners have started with datasets on tourism and climate (see list of datasets in 6.2 Data collection).

Once a topic has been chosen, it is much easier to look for ideas within the organisation.

What data is already being collected? Where is it currently stored and in what format (tabular in rows and columns, XLS, CSV, PDF, text document, images)? In order to make use of what you already have, this data needs to be made available in a structured way and in a machine-readable format such as CSV, JSON, or XML. In addition, each record or/and dataset needs to be described. This metadata is necessary to make the data discoverable in a data portal or website - similar to the way a library catalogue provides certain information about a book so that library users can search for the book by title, author, publication date, publisher, and so on.

Think digital with legal certainty

This is a follow-up argument to "use what you already have". A lot of data is already collected and made available by municipalities, for example on the city website, social media accounts and information boards. The missing steps for publishing this as open data are to provide this information in a standard format so that the data can be used in different contexts and applications. By licensing a particular dataset under an open licence such as Creative Commons, both the provider and the user of that data can act with legal certainty. Strictly speaking, if the tourism office of a municipality provides the location and opening hours of public toilets as a PDF file on its website, it does not allow third parties to publish or redistribute this document without attribution - even though this may be perfectly fine and even in the interest of the municipality. Working on open data initiatives removes this legal uncertainty while making this data more usable. Choosing a digital and standard format also brings the benefit of interoperability. In simple terms, interoperability means that the format of the dataset can be used in different technical environments without any manual conversions.

View open data as public service: an advantage for the local administration and its citizens

Consider where open data comes from. Data is collected, stored, and used in the day-to-day work of local government and local administrations. Making this data available beyond the city hall leads to more transparency and more accountability of municipal actions. Furthermore, if the collection, storage, and use of this data is an integral part of the local administration's work - what is the argument for not publishing it? Initiatives such as the [Open Data Charter](#) (ODC, n.d.) are even promoting an „open by default“-approach, meaning that all datasets should be published unless there is a justified reason not to publish.

Consider the data demand side



Municipalities often receive inquiries from citizens or businesses to provide certain information. The inquiries which are made regularly should be taken as guidance for the decision what datasets should be made available (first). The choice, which datasets to open (first) can also be guided by best-practice examples of what data (sets) are the basis of certain services or applications. In the next section, we will present the journey from opening and publishing a specific data set to the creation of a service, which builds upon this open data.

2.2 Open data culture within the administration

Developing a local open data culture involves more than just publishing datasets. It requires a fundamental shift in how municipal administrations perceive and handle data. This transformation emphasises transparency, and the integration of data into everyday decision-making processes.

At the heart of this cultural shift is the recognition that data collected through routine administrative activities – such as budgeting, urban planning, and public service delivery – holds significant value beyond its initial purpose. When made openly available, this data can empower citizens and enhance public trust.

Internal processes and mindsets

For open data initiatives to succeed, it is essential that public servants and municipal staff view data sharing as an integral part of their roles rather than an additional burden. This requires embedding data literacy and openness into the organisational culture. Training programs, clear guidelines, and leadership support can help staff understand the benefits of open data, not only for the public but also for improving internal workflows.

Moreover, fostering a sense of ownership and pride in contributing to transparency can motivate staff. When public servants see their efforts leading to tangible community benefits, such as improved services or increased civic engagement, it reinforces the value of their work and encourages continued participation in open data practices.

Challenges and obstacles

Despite the potential benefits, several challenges can hinder the development of an open data culture within local administrations. One prominent example for an obstacle to open data culture are privacy and security concerns. Fear of data misuse and concerns about protecting personal information can lead to reluctance in making data openly available. Another example relates to internal resistance to change. In cases of resistance control over information is typically considered indispensable and can impede efforts to promote transparency and openness. Addressing these challenges requires a strategic approach that includes investing in infrastructure, developing clear policies, and fostering an environment that encourages experimentation and learning.

Finally, it can be concluded that developing a robust local open data culture is a gradual, neither top-down, nor bottom-up process, which requires commitment from all levels of the administration.



The role of NGO to open government data

Civil society's commitment to free and open data leads the public administration to publish data in the correct open formats and with the appropriate licences, making them accessible to all and improving the relationship with citizens. Several actions and campaigns are conducted using open source technologies to promote and enable digital citizenship, civic participation, and transparency in public administration. These actions create online and offline participatory processes for the promotion of data culture. Without an active community data remains silent.

As concrete examples, we highlight the actions promoted by Italian association on Data (Associazione onData, 2026) and the campaign #DatiBeneComune (datiBeneCommune, 2026) with the main results.

2.3 Local strategy and policy

Local open data strategies play a crucial role in enhancing transparency, innovation, and improved public services. Worldwide, local authorities are continually adopting open data approaches, which include aspects of citizen engagement, fostering economic growth, encouraging scientific work, and providing overall evidence-based policymaking. A well-constructed local open data strategy with political, legal, and technical harmonisation, complemented by semantic and structural harmonisation through common standards and shared data structures, needs to be ensured for effective implementation of open data activities and an open data culture within the administration and among staff.

This is particularly important when data is intended to be compared, combined or reused across local, national, European and global levels. Where common data structures exist, they facilitate the development of services, reporting tools and research activities. Well-known examples can be found in domains such as transport, where open standards like GTFS (General Transit Feed Specifications), e.g. GTFS-RT for Google Maps real-time services, support interoperability and broad reuse (GTFS.org, 2026).

More similar open standards:

- Mobility Domain
 - GTFS (General Transit Feed Specification): public transport stop locations
 - GTFS-RT (General Transit Feed Specification in realtime): live public transport updates, such as vehicle locations or service alerts
 - GBFS (General Bikeshare Feed Specification): real-time data on vehicle availability, locations and pricing
- Geospatial and Infrastructure
 - OpenStreetMap (OSM): representing physical infrastructure
 - GeoJSON/KML: used for mapping geospatial data, KML is often used for sharing location-based data, similar to how GTFS describes stop locations
 - IFC (Industry Foundation Classes): for Building Information Modeling (BIM) data, facilitating interoperability in the construction and architecture industry
- Meteorological and Environmental Data
 - NetCDF (Network Common Data Form): supports the creation, access and sharing of array-oriented scientific data, often used for weather and climate data



- GRIB (General Regularly-distributed Information in Binary): standard for storing and transmitting weather data, similar to GTFS in that it enables standardised consumption of specialised data

In other thematic areas, like local government contract registers, such common structures are often not yet sufficiently defined, which creates additional barriers for service developers and other re-users, even where datasets are otherwise well described. Local open data strategies should therefore promote the adoption of existing standards where available and encourage the identification of shared minimum attributes and good practices (UK Government, 2025). Therefore, this chapter addresses the importance of local open data strategies, key issues, and best practices in municipalities worldwide. Further, a model resolution is designed to support the start in the journey of opening data. This model can serve as a blueprint for cities looking to establish a robust local data strategy, enabling them to leverage their data while upholding public trust and legal obligations.

Successful Local Open Data Strategies: Case Studies

Barcelona

The city of Barcelona has integrated open data into its smart city vision, with emphasis on mobility, environment, and government. The city's open data strategy is built on principles of accessibility, interoperability, and sustainability. The "Open Data BCN" portal provides real-time live data on transport, air quality and urban planning, as well as historic datasets across various sectors, enabling businesses and researchers to develop solutions based on data. To go further, analytic informational stories, so called data stories, are provided by topic in various query formats, to make the data more accessible for citizens (Ajuntament de Barcelona, n.d.). In addition to the national data portal, the Spanish open data portal is also a user-friendly and well-structured data portal which, in addition to the provision of data, also offers sections with information compilations, events, interviews and news. Further, data request from interested parties can be forwarded to the administration via a channel to promote the open data initiatives. With this strategy, their citizen-centric approach and the overarching Spanish framework, Barcelona has positioned itself as a leader in digital sovereignty (Monge et al., 2022).

Open Data BCN: <https://opendata-ajuntament.barcelona.cat/en/>

Helsinki

Trust, innovation, cooperation and value. For Helsinki, the open data initiative is built on the principle that public data belongs to the people and should be freely accessible, usable and shareable. Therefore, the narrative of an open data ecosystem driven by multiple stakeholders is followed. Helsinki Region Infoshare (HRI), launched in 2011, was Finland's first open data portal, created through a joint effort by multiple cities, including Helsinki and Espoo. It remains a leading example of regional cooperation and has inspired national initiatives like the avoindata.fi portal. Today, the city's open data is also linked to the European Data Portal through automatic metadata sharing. Helsinki's open data platform includes detailed information on urban planning, energy consumption and sustainability projects. The city actively collaborates with universities and companies to foster innovation in climate action and public services. What sets Helsinki apart is its citizen-first approach, the city of Helsinki actively involves residents, start-ups and researchers in co-creating urban solutions (World Economic Forum, 2025). Overall, the city's data strategy



sets a bold vision: by 2025, Helsinki's data should be the most usable and used city data in the world (City of Helsinki, n.d.; Helsinki Region Infoshare, n.d.)

Helsinki Region Infoshare (HRI): https://hri.fi/en_gb/

Vienna

Vienna has long been recognised for its commitment to transparency and citizen engagement. In 2011, the city launched the Open Government (OGD) project with the aim of making city data freely available to the public to foster innovation, enhance public services and support economic development. The city's "Data Excellence Strategy" embodies the principles of "Open by Default" and "Open by Design," ensuring the accessibility, machine-readability, and free provision of open data. To follow this ambitious approach, city government established a dedicated team to oversee the initiative, ensuring data was regularly updated and maintained (City of Vienna, 2019).

Vienna's open data portal offers a wide variety of datasets, including public transport data, environmental data, urban planning data and cultural events data. The data is published in machine-readable formats with standardised metadata standards to facilitate ease of use. APIs are also published on the portal, making it simple for developers to integrate data into applications. Vienna's commitment to open data has already led to the development of over two hundred applications by third-party developers (City of Vienna, 2021).

Digitales Wien: <https://digitales.wien.gv.at/open-data/>

Ghent

As a blueprint for bottom-up initiative, the Open Data movement in Ghent started with the university of Ghent and students asking the mayor about Open Data, subsequently creating the hackathon "Apps for Ghent" together with the local community and the Open Knowledge Belgium in 2011. Now, going beyond just sharing data, the city of Ghent aims for a linked open data approach on a semantic website, to connect data and meaning, with data being available in RDF format and linked across Open Data available at regional and national level. The goal is to not only have access to the raw data, but to be able to jump from one data point to another. The city states, that by using the internet as a distribution platform of contextualised data, it will allow them to distribute content and filter datasets which are usually disconnected by design (Andrews, 2018). This not only allows for more extensive knowledge generation but also helped in developing a citywide semantic vocabulary, terminology and meaning, therefore facilitating easier data governance coordination. "Open Data is a dialogue, not a one-way street. Working together with others ensures that data can really make a difference" is the cities statement, reflecting the connected and bottom-up approach. To maximise the benefits of sharing data, the city advocates for the data usage in numerous applications. One highlight is the real-time live data embedded on the website, including data like rental bike and parking space availability, as well as live crowd-data, which provide a tangible real life feel for the data (Stad Gent, n.d.).

Ghent Open Data Portal: <https://data.stad.gent>



2.4 Model Resolution for Local Open Data Strategies

By adopting a formal open data strategy, municipalities can institutionalise these best practices for data governance, set clear goals for data accessibility, and overall promote more open and responsible data-sharing. To provide a structured approach and framework for local governments to develop and implement an open data strategy, a model city resolution is provided. This model resolution draws from international best practices, successful city models and principles of open governance to help local councils craft an approach that meets the specific communal needs. If a commitment to open data is formalised, more initiative-taking steps towards a more transparent, data-driven governance can be taken.

Resolution Supporting the Adoption of an open data strategy

Purpose

With this resolution, the City Council is issuing new regulations and proceedings on open data and brings them into force on [add date]. This sets the long-term vision, principles and objective for the use and governance of open data.

- Whereas open data promotes transparency, accountability and local engagement by making public information structured, standardised and easily accessible and therefore becomes a strategic asset for modern urban governances*
- Whereas open data aid in enhancing innovation, economic development, and efficiency in and of governmental services, research, businesses and public alike, to create new insights*
- Whereas it is necessary to establish clear regulations and governance structure for managing, publishing, and securing open data*

This city council resolution stipulates:

Implementation of an Open Data Strategy

- 1. The Council supports the development of an open data strategy that aligns with best practices and local needs.*
- 2. The Council confirms the selection of open datasets and potential for provision on an open data portal. The administration shall implement an open data regulation, ensuring that non-sensitive government data is made publicly available. The data is to be prepared and made available by the supplying units in a structured and machine-readable format so that they can be retrieved in automated procedures. When updates are made, old data should not be overwritten, but instead the new data should also be published to enable an evaluation over time.*

Governance

- 3. The Council directs the relevant department [e.g., IT, Smart City, data, economic development] or an appointed representative to oversee the activities as described in [2] and to prepare corresponding measures and requirements for the expansion of open data in an open data implementation plan including guidance for all departments.*
- 4. The departments and municipal bodies that have not yet provided data are instructed to identify relevant data to be made accessible by the end of quarter X. If necessary, this*



should be done in orientation to the open data portals of the largest European cities or other municipal portals.

5. *The city will collaborate with local businesses, academic institutions, and civic organisations to maximise the value of open data.*

Data Protection and Ethical Considerations

6. *The data publication shall adhere to national and regional data protection regulations, ensuring no violation of privacy or confidentiality.*
7. *The city shall adhere to ethical standards for data usage, including non-discrimination and accountability issues. If necessary, a guideline for data anonymisation and aggregation to minimise risks while maximising public value will be followed.*

Monitoring and Improvement

8. *The status of open data will be presented during an annual report to the City Council. In addition, the overseeing department or representative is commissioned to ask all municipal departments once every quarter whether new open data records can be made available.*
9. *Feedback mechanisms, including public consultations, will be integrated into the open data governance process.*

Based on resolutions by the City of Munich (City of Munich, 2022) and the City of Zurich (City of Zurich, 2021).



3. Step-by-step guide



Figure 2: Step-by-step guide to opening data
Source: Own adaptation



4. Better not's

Sometimes it is not only knowing about how to do things and where to start, but also equally important to know what NOT to do. In the often complex and evolving landscape of open data projects, mistakes and missteps are not only inevitable but also instructive. This is where this collection of experience-based insight of “Better Nots” spotlights the common pitfalls, dead ends and avoidable missteps faced in the everyday practice with opening data and data opening projects.

Rather than offering abstract or unsolicited advice, the aim is to ground each “Better Not” in the realities of practice. These entries emerge from concrete experiences and distil from lessons learned, by practitioners who navigated these challenges first hand.

Each “Better Not” is accompanied by contextual reflections that trace the journey of how the insight came to be to better equip anyone to recognise similar patterns and tensions in their own work with opening data and sidestep the same traps completely. However, this collection should not be misunderstood as a checklist of errors, nor a manual to success, it is a pool of practical guidance build on the common goal of open sharing, critical reflection, and mutual support.

To make these “Better Nots” more actionable, they are grouped into two levels: the project and the organisational level. This aims to help in distinguishing whether these pitfalls tend to occur in the day-to-day work of opening data or in the broader structures and policies that support a data opening strategy.

Organisational level

Better Not #1: Talk About Open Data as an Abstract Topic

What happened?

A small city wanted to build an app to share useful information with citizens. Early on, departments were asked to suggest datasets – but the call was ignored. Only after a prototype of the app was shown did departments begin contributing dataset ideas.

What changed?

Once a working prototype made the potential of the app visible, staff from different departments were more engaged and started suggesting relevant data for inclusion.

Why did this happen?

Terms like “open data” and “datasets” were too abstract. Staff perceived the request as extra, technical work led by the IT department – disconnected from their daily roles.

Lesson learned.

Do not expect engagement without a tangible example. Show a prototype or working tool early on. Concrete results make the value of open data visible – and motivate others to contribute.

Better Not #2: Launch without Internal Buy-In

What happened?

Open Data efforts initially faced low engagement. Departments worked in silos, saw Open Data as a purely technical task, and did not perceive it as relevant. There was little collaboration or motivation to share data.



What changed?

Internal meetings were held to open dialogue about Open Data's value. Most importantly, senior leadership – including the mayor and department heads – publicly endorsed the initiative, helping shift the perception of its importance.

Why did this happen?

There was cultural resistance to collaboration and change. Without leadership visibility or cross-departmental communication, Open Data felt disconnected from everyday work.

Lesson learned.

Cultural change starts from the top. Ensure visible support from leadership and create space for open, cross-departmental conversations. Open Data needs both relevance and legitimacy to take root.

Better Not #3: Ignore Open Data just because it is not mandatory.

What happened?

Privacy and cybersecurity often get initial attention in data projects because they are backed by strict regulations. Open data on the other hand is rarely treated with the same priority, which can result in unstructured, incomplete, or neglected datasets.

What changed?

Starting a project directly aimed at opening data helped shift the conversation. Participants started recognising open data as asset and not just an optional add-on. By starting an open data initiative, the opportunity is created to begin exploring the value of data for everyone and how to treat it with the same care and intent as other critical data areas.

Why did this happen?

Legal pressure and political focus drives action. Without it, open data can fall into oblivion in the day-to-day municipal business, even when it holds significant value for communities, services and the municipal alike.

Lesson learned.

Do not wait for a law to tell you open data matters. Build the mindset early, structure your ideas, manage it, and make it accessible. That is where the real value starts.

Better Not #4: Treat Data like a by-product

What happened?

Previous projects have brought teams and individuals who constantly work with data together, but had never considered it is potential as open data. This initiated a shared discussion about how data could be reused beyond the immediate needs.

What changed?

Cross-functional collaboration during a project created momentum. It sparked conversations and laid early groundwork for a cultural shift: from working in silos to seeing data as a strategic asset.

Why did this happen?

Data was often only seen as a technical output and managed in isolation. Without shared vision and opportunities for reuse, transparency, and collaboration potential, between teams, departments and even in citizen participation were missed.

Lesson learned.

Do not let data sit in silos. Create spaces for people to talk, question, and align. Seeing data as an asset is not just technical, it is cultural.



Project level

Better Not #5: Wait for Perfection

What happened?

A city's tree cadastre was not published because planting dates were missing or incomplete. Some entries had exact dates, some only years, and some none at all. The data was deemed "not ready."

What changed?

An employee suggested applying a "fit for use" approach instead of waiting for completeness. By removing the planting date column and publishing the rest, the data became usable – leading to a citizen-led "Water the trees in your neighbourhood" campaign.

Why did this happen?

There was a rigid definition of "complete data." A single missing field prevented publication, despite the dataset being useful for many purposes.

Lesson learned.

Do not let perfection delay progress. Ask if your data is *fit for use* – even partially. Be bold: remove non-essential columns if needed and release what is helpful now.

Better Not #6: Wait for Clean Data before getting Started.

What happened?

Data quality was a known issue, but improving it seemed too time-consuming to tackle. Open data was therefore viewed as an extra administrative burden that could not compete with daily priorities.

What changed?

Opening up first data sets triggered a shift. The act of preparing data for publication highlighted flaws and inconsistencies, making the opening data process complicated at first. However, it also created new motivation to clean things up. It became clear that open data is not just a goal, it is also the beginning of better data overall.

Why did this happen?

The realisation set in, that there is no quick fix for data quality. But making data public added urgency and purpose to the "cleaning" process and overall helped building a better working foundation for everyone.

Lesson learned.

Do not wait for flawless data. Start opening what you can. The process itself will surface gaps and drive future improvements, therefore strengthening the overall data landscape.

Better Not #7: Connect Live to Core Databases without Safeguards

What happened?

A domain database was directly integrated with the open data platform to enable real-time data sharing. As usage increased, response times slowed significantly, affecting the entire platform.

What changed?

To solve the performance issues, the direct connection was removed. Instead, data is now periodically exported from the database and published separately via the open data platform.

Why did this happen?

The direct connection created a heavy load on the system. Without caching or throttling, the popularity of the resource impacted the entire platform's performance.

Lesson learned.



Avoid direct connections to core systems without proper load management. Use caching or scheduled exports to protect system performance and ensure reliability – and improve data security in the process.

Better Not #8: Stick to Old Habits in new Collaborations.

What happened?

Teams with little experience in cross-border, multi-organisation or intercommunal projects often stick to their usual ways of working. However, for topics like opening data these collaborations are helpful and needed. A project like DoorCE required everyone to step out of that comfort zone and collaborate from day one.

What changed?

A shared, agile methodology helped everyone align quickly. Teams can adapt and support each other, so that even those not directly involved can pick up new practices.

Why did this happen?

A clear project structure and proceeding, including milestones, goals and a timeline makes it easier to start working. Further, flexibility and openness are key.

Lesson learned.

Do not cling to what is familiar. New types of projects may require new types of collaboration and therefore need new ways of working. Adopt strong frameworks early on to bring the topic of open data, your team, and future projects forward.



5. Legal and Regulatory Framework

Understanding the European and national regulatory framework is essential for effectively navigating and implementing open data strategies within municipalities and other public sector bodies.

At the European level, the chapter explores the key strategies and legislative instruments, such as the Open Data Directive, Data Governance Act or GDPR - that provide the overarching principles and legal structures guiding open data use across Member States. These frameworks not only set the direction but also define obligations and opportunities for local governments.

At the national level, we provide an overview of country-specific strategies, action plans, and legislation related to open data. These national frameworks interpret and implement EU-level requirements, often tailoring them to fit specific administrative and political contexts.

By examining both levels, this chapter aims to clarify the multi-level governance context of open data, highlighting how local administrations are influenced - and supported - by higher-level policy and legal instruments.

5.1 European level

EU strategies and key EU legislation

The following chapter explores European legislative frameworks aimed at enhancing access to and re-use of government-held data. It highlights the Open Data Directive, which came into force in 2019, replacing the previous Public Sector Information Directive (PSI Directive) (European Commission, 2019). Additionally, the chapter examines the European Data Strategy, introduced in 2020, which sets the foundation for Europe's data economy and defines further legislative actions, including the Data Governance Act and the Data Act. To sum up, it is explained how these frameworks are relevant for the local level (European Commission, 2020b).

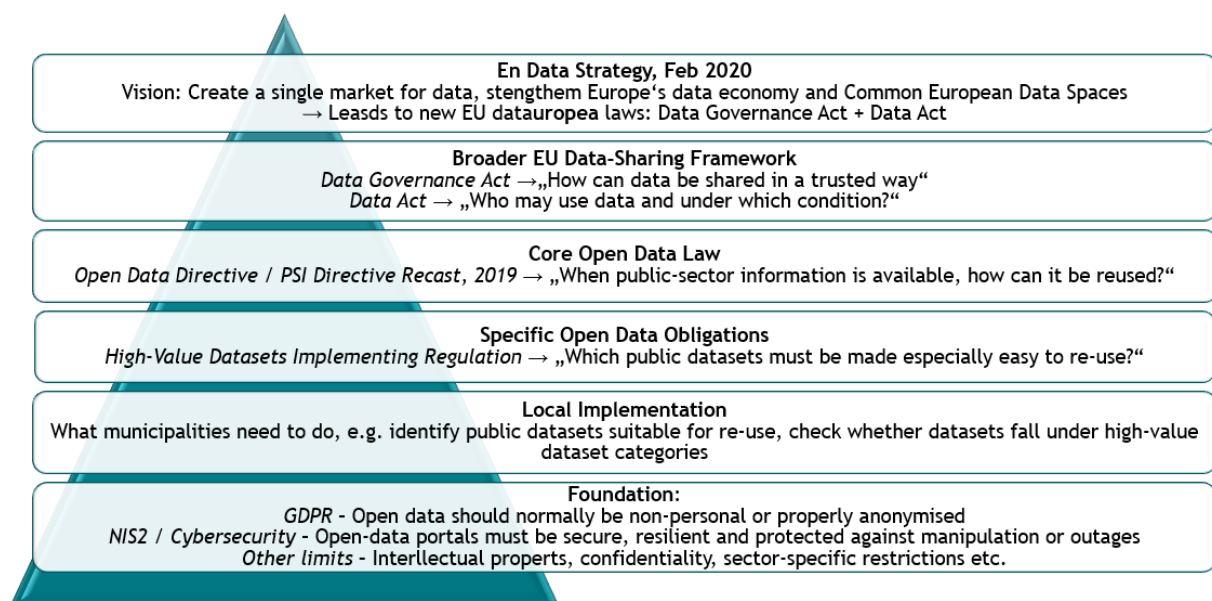


Figure 3: EU Strategies and key EU legislation for Open Data
Source: data.europa.eu, n.d.a; own adaptation



Open Data Directive

The review process of the Public Sector Information Directive (PSI Directive) was launched in 2017. One year later, in 2018, a proposal for a revision of the Directive was adopted by the European Commission. The European parliament, the Council of the EU and the Commission agreed on a revision of the Directive in 2019, and it was renamed [the Open Data and Public Sector Information Directive](#). The Directive's purpose is to make public sector and publicly funded data re-usable. Member states had to transpose the Directive 2019/1024 by 17 July 2021 (European Union, 2019). The Open Data Directive directs the intention to reuse public information, not on citizens' access to information. The Directive also encourages member states of the EU to make as much information as possible available for reuse. This covers data held by public sector bodies (including ministries), state agencies, municipalities, but also publicly funded organisations, for instance meteorological institutes. The Directive covers documents available in any existing format or language and where appropriate, by electronic means formats that are open, machine-readable, searchable, and reusable. Transparency and fair competition are two key strands of the internal market that the Directive is built on (data.europa.eu, n.d.b; European Union, 2003).

When the Directive is fully implemented, the new rules will:

- encourage the publication of dynamic data and promote the use of Application Programming Interfaces (APIs),
- restrict the exceptions that currently allow public bodies to charge fees above marginal dissemination costs for data reuse,
- expand the Directive's scope to include:
 - data held by public undertakings, subject to specific rules. In general, the Directive will apply only to data made available for reuse, with charges potentially exceeding marginal dissemination costs.
 - research data funded by public resources - member states will be required to establish open access policies for publicly funded research data, with new provisions making research data in open repositories more easily reusable.
- and enhance transparency requirements for public-private agreements involving public sector information, preventing exclusive arrangements.

One of the statements in the Directive mandates that the Commission adopt a **list of high-value datasets** provided to be provided free of charge. These datasets, identified within the thematic areas outlined in the Directive's Annex, possess significant commercial potential and can accelerate the creation of value-added information products across the EU.

The thematic categories of these datasets are:

- geospatial,
- earth observation and environment,
- meteorological,
- statistics,
- companies and company ownership,
- mobility.



HIGH-VALUE DATASETS

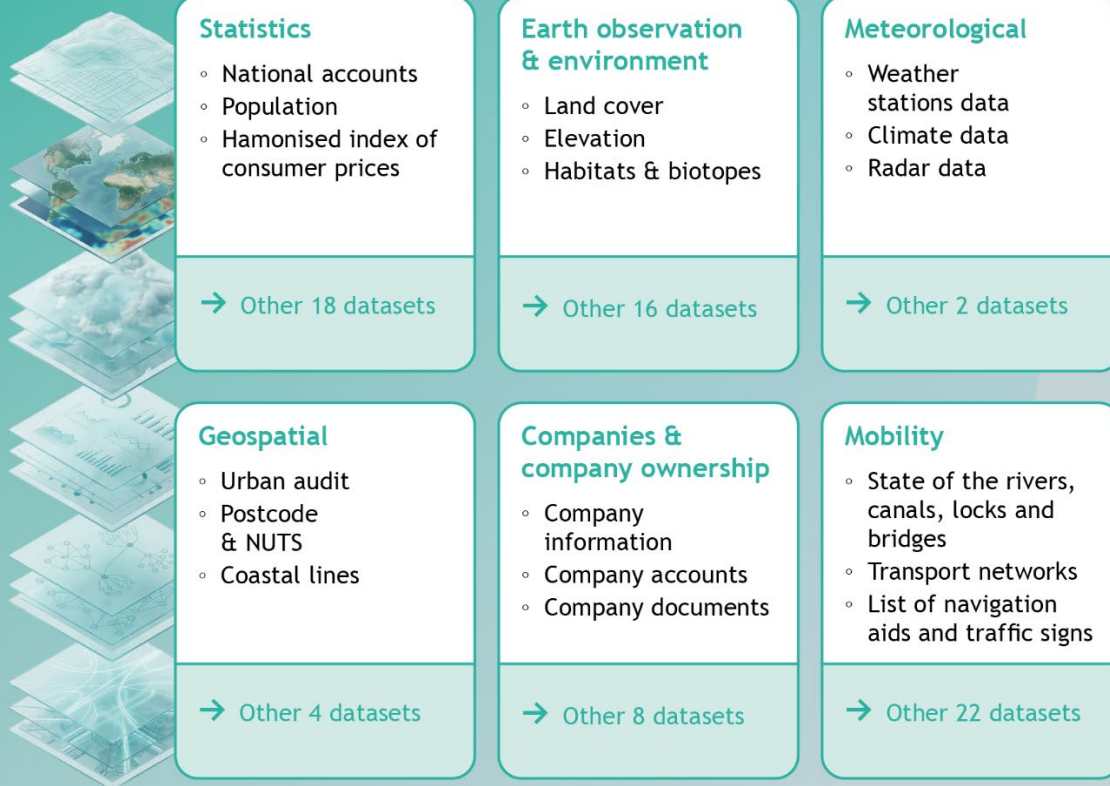


Figure 4: High-Value Datasets
Source: data.europa.eu, 2022; own adaptation

The list of designated high-value datasets was established through an implementing regulation by Commission in 2022. This action was taken within the established framework and with the support of a committee on open data and the reuse of public sector information, consisting of representatives from EU member states. (European Union, 2021; EUR-Lex, 2023; European Commission, 2024c)

European Strategy for Data

The European Strategy for Data tries to create a single market for data, maintaining Europe's competitiveness on the global stage and data sovereignty. It seeks to increase the availability of data while keeping those who generate (e.g.: companies, individuals) the data in control. A key initiative is the creation of Common European Data Spaces, facilitating the secure and fair use of data across sectors (European Commission, 2020).

Two critical legislative acts stem from this strategy:

1. The Data Governance Act (DGA)
2. The Data Act

Together, these initiatives support innovation, economic growth, and societal progress while protecting European values and rights in the digital world (European Commission, 2024.)



Data Governance Act (DGA)

The European Commission also published [the Data Governance Act](#) in response to the public consultation on the European Strategy for Data (European Union, 2022). The public consultation was held on 25 November 2020, and its intention was to gauge stakeholders' opinion on open data, data sharing and data spaces. The DGA entered into force in September 2023.

The regulation is designed to give individuals and organisations more control over how their data is used. One of the most important aims is to facilitate greater data flows, especially by promoting the reuse of public sector data that cannot be released as open data. It also opens the door for new types of data intermediaries. Data intermediaries service providers must follow certain conditions to be seen as trusted within EU's data spaces. Upon compliance with the established requirements, providers may adopt the designation "recognised data intermediation services provider in the Union" and are authorised to display the common EU logo designed for this purpose. This visual identifier facilitates the clear distinction of trusted and officially recognised services.

The DGA covers key elements of data handling—such as access, sharing, and commercial use—while maintaining a strong focus on data protection and security (European Union, 2022)

Data Act

[The Data Act](#) presents a complex initiative designed to address challenges and unlock opportunities related to data in the European Union, focusing on fair access, user rights, and the protection of personal data. The regulation, which entered into force on 11 January 2024, is one of the key components of the European Strategy for Data. The Data Act complements the Data Governance Act mentioned above. While the Data Governance Act regulates data-sharing processes and structures, the Data Act clarifies who can benefit from data and under which conditions (European Parliament and Council of the European Union, 2023).

One of the primary goals of the Data Act is to ensure a fair distribution of the value of data by establishing clear rules for accessing and using data, especially in sectors like the Internet of Things (IoT). The regulation mandates that connected products be designed in a way that allows users - businesses or consumers - to easily and securely access, use, and share the data generated by these devices.

In practice, the Data Act empowers individuals and businesses to access data generated by connected devices, allowing users to share this data with third parties. This can lead to greater competition in service markets, such as repair and maintenance services, and potentially lower costs for consumers. It also supports precision agriculture by providing farmers with real-time data to optimise crop yield and resource allocation, contributing to the Green Deal objectives. (European Commission, 2024b)

GDPR (General Data Protection Regulation)

[The General Data Protection Regulation \(GDPR\)](#) is the European Union's key legislation governing the collection, processing, and storage of personal data. The regulation was implemented on May 25, 2018. It establishes strict requirements for organisations operating within the EU, as well as for non-EU businesses that process the personal data of individuals residing in the EU. The regulation ensures data protection, transparency, and accountability while granting individuals control over their personal information (European Parliament and Council of the European Union, 2016).

The GDPR establishes the core rights of individuals in the digital era, ensuring their personal data is protected. It outlines the responsibilities of entities managing personal data, setting clear guidelines for lawful processing. Additionally, the regulation defines mechanisms to enforce compliance and introduces penalties for non-compliance to safeguard data privacy (European Council, 2024).

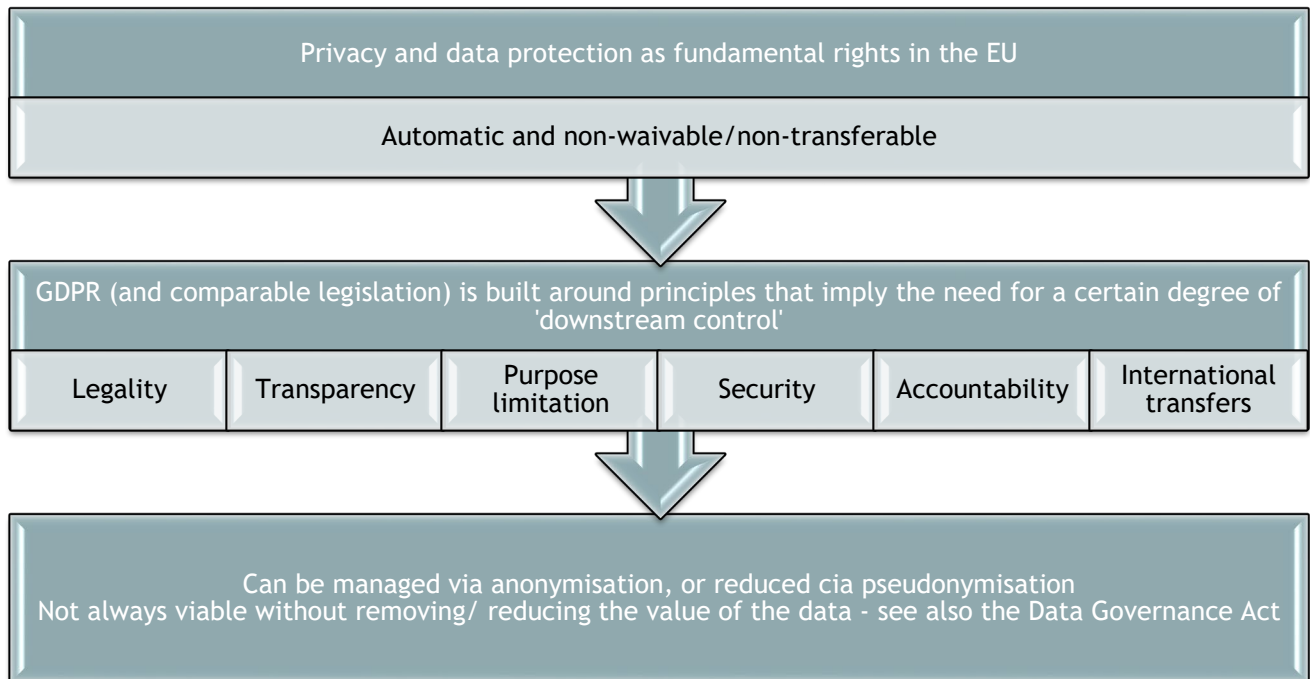


Figure 5: Why GDPR Requires Downstream Control of Personal Data
Source: data.europe.eu, n.d.b; own adaptation

NIS2

The [NIS2 Directive](#) (Directive (EU) 2022/2555) is the European Union's new cybersecurity framework for critical infrastructure and digital services, effective from October 2024. It applies to medium and large public and private entities across different sectors like transport, energy and public administration (European Commission, 2026).

For municipalities, this means that smart city platforms or data portals may fall under NIS2 if they support essential public services. Therefore, municipal IT teams must ensure risk management, incident response and security by design.

In general, open data as such is not the main object of NIS2, but the public-sector systems. Portals or infrastructure used to publish or operate data services may fall within cybersecurity obligations depending on national implementation and criticality. Practices like the prevention of unauthorised changes to published datasets and ensuring resilience against outages and cyber threats are still relevant in this context.

Open Data remains safe and encouraged, as long as it is technically secured and not directly tied to critical operations (European Commission, 2026).



Relevance of EU framework for local governments

EU frameworks such as:

- [Open Data Directive](#) (European Union, 2019)
- [Data Governance Act](#) (European Union, 2022)
- [Data Act](#) (European Parliament and Council of the European Union, 2023)

directly support local governments in promoting open data and responsible data use. These regulations provide the necessary legal structures for municipalities to release non-personal data, enhance transparency, and foster innovation.

Additionally, the [General Data Protection Regulation](#) (GDPR) (European Parliament and Council of the European Union, 2016), ensures that local governments manage personal data responsibly, protecting citizens' rights while enabling the reuse of public sector information. By following these frameworks, local governments can improve public services, boost local economies, and engage more effectively with citizens and businesses.

5.2 National level

Open data is a key tool for promoting transparency, innovation, and efficient public administration. However, for this data to be made available and used in accordance with the principles of law and the protection of the public interest, its publication and reuse must be also regulated by a clear legal system at the national level. In this chapter we will describe each of the member states represented in DoorCE project regarding their own open data policies. There are seven nation states participating in the DoorCE project: Austria, Croatia, Germany, Italy, Poland, Slovakia, Slovenia.

National strategies and action plans

Austria

The Freedom of Information Act (*Informationsfreiheitsgesetz*) was published in the Austrian Federal Law Gazette in February 2024 and is scheduled to enter into force in September 2025. Its primary objective is to enhance the transparency of governmental actions and the operations of state-owned enterprises. The act represents a legislative response to the legal tension arising from the conflict between the constitutional obligation to maintain official secrecy and the obligation to provide information, both of enshrined in the Austrian Federal Constitution. (Oesterreich.gv.at, 2024)

On the other hand, there are existing legal provisions governing access to information mentioned in [Article 20 of the Federal Constitutional Act](#). The key points include:

- **Article 20, paragraph 3 B-VG** defines official secrecy, which may be used as grounds to refuse access to information, but only in narrowly defined circumstances.
- **Article 20, paragraph 4 B-VG** establishes the obligation to provide information. The obligation is reflected in state-level information disclosure, as well as, in federal.
- **Article 20, paragraph 5 B-VG** requires the publication of studies, expert reports, and surveys commissioned by external administrative bodies, including their costs (JUSLINE Österreich 2026).

In addition, there are publication requirements set out in other legal domains, covering areas such as transportation data, geodata, environmental data, procurement data, and financial data.



Since Austria is one of the EU Member States, the Open Data Directive 2019/1024 has been transposed into national law through [the Federal Act on the Reuse of Information from Public Bodies, Public Companies, and Research Data \(Informationsweiterverwendungsgesetz\)](#) (Krabina, 2020).

[The Data Strategy for Austria](#) is another useful tool in the field of transparency and open data. Its objective is to ensure better, more efficient, and more transparent use of data, particularly within public administration. The strategy focuses on promoting data-driven decision-making, fostering innovation, and improving services for citizens. The strategy was developed in alignment with the European Data Strategy and the Data Governance Act. In Austria, a Data Access Act (*Datenzugangsgesetz*) is currently being drafted to support the practical implementation of Data Governance Act provisions at the national level (Data.gv.at., 2024).

Austria also has a strong legal framework for the protection of personal data and the assurance of cybersecurity.

- [Federal Act on the Protection of Natural Persons with regard to the Processing of Personal Data \(*Datenschutzgesetz - DSGVO*\)](#) (RIS, 2026a)
- [Federal Act enacting a Telecommunications Act 2021 \(*Telekommunikationsgesetz 2021 - TKG 2021*\)](#) (RIS, 2026b)
- [Regulation of the Data Protection Authority on Processing Operations for which a Data Protection Impact Assessment Must Be Carried Out \(Federal Law Collection II No. 278/2018\)](#) (RIS, 2018a)
- [Regulation of the Austrian Data Protection Authority on exemptions from the data protection impact assessment \(Federal Collection of Laws II No. 108/2018\)](#) (RIS, 2018b)

Croatia

The foundations for access to public information in Croatia are enshrined in the Constitution of the Republic of Croatia, which, since the 2010 amendments, guarantees the right to access public information as part of the right to freedom of expression. The main legal act in this area is the [Law on the Right of Access to Information](#), adopted in 2013 (Hrvatski sabor, 2013). This law is aligned with EU Directive 2003/98 on the re-use of public sector information, which was replaced by EU Directive 2019/1024. The law stipulates that public institutions and private entities performing public functions are considered holders of public information. It emphasises principles such as publicity and free access, timeliness, completeness and accuracy of information, equality, and the right of recipients to publicly disclose information. Public authorities are obligated to proactively publish relevant information, including laws, regulations, decisions, financial reports, and public procurement data.

Croatia has also established a legal framework to ensure the protection of personal data.

- The right to personal data protection is constitutionally guaranteed in the Constitution of the Republic of Croatia.
- [The Act on the Implementation of the General Data Protection Regulation](#), adopted in 2018, complements the GDPR by setting out specific provisions applicable in the Croatian context (Zakon.hr, 2018).

Germany

The foundation for creating a legal framework for open administrative data in Germany was laid by the [E-Government Act \(*E-Government-Gesetz - EGovG*\)](#), specifically [§12a "Open Data of the](#)



Federal Government - Authorization to Issue Regulations" (Bundesministerium der Justiz and Bundesamt für Justiz, n.d.a). This paragraph came into effect in 2017, and since then, federal administrative bodies have been obliged to publish raw data (with some exceptions). It specifies key criteria for open data and considers data protection and other legally regulated reasons that may prevent disclosure. The criteria include free provision of data, open access to data, and machine readability. The next step was the E-Government Act and introducing the Act on the Use of Public Sector Data, which came into effect in 2021. It creates an initial regulatory framework aimed at improving data provision as well as increasing standardisation and interoperability. Among other things, the draft law also serves to implement the revised EU Directive 2019/1024 (Open Data Directive, 2019).

In 2021, the federal cabinet adopted an Open Data Strategy of the Federal Government to improve the open data ecosystem of the federal government. The above-mentioned strategy includes three areas of activity with a total of sixty-eight implementation measures from various federal ministries and agencies and is planned to span five years.

In addition, in 2013, the national data portal for Germany GovData was established, providing a unified central access point to administrative data from federal, state, and local governments, as well as from public service providers, universities, researchers, research institutions, and research funding organisations. Its purpose is to enable easy access and search for open data in one place. (GovData, n.d.a)

Germany has a comprehensive legal framework for data protection, which includes federal and regional laws, as well as sector-specific regulations.

- Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG) (Bundesministerium der Justiz and Bundesamt für Justiz, 2017)
- Ninth Book of the Code of Social Law - Rehabilitation and Participation of People with Disabilities (Sozialgesetzbuch IX - SGB IX) (Bundesministerium der Justiz and Bundesamt für Justiz, 2016)
- Telemedia Act of 2007 (Telemediengesetz - TMG) (dejure.org, n.d.)
- Telecommunications Act (Telekommunikationsgesetz - TKG) (Bundesministerium der Justiz und Bundesamt für Justiz, 2021)

Italy

In Italy, open data legislation promotes transparency and access to government data. Italy also participates in the European Union's open data initiatives, aligning its efforts with broader EU policies aimed at promoting data sharing and transparency among member states. Open data initiatives in Italy have had a positive impact on transparency and civic engagement, as they allow citizens, businesses, and researchers to access valuable information.

The foundation of key legislation was laid by Law No. 241 of August 7, 1990, which introduced new rules on administrative procedures and granted citizens the right to access administrative documents (Normattiva, 1990). This law is a crucial instrument in promoting transparency in public administration, as it provides citizens with the right to access such documents. Following this legislation, Decree Law No. 179/2012 encourages public administrations to publish datasets in open formats in order to foster innovation and economic growth (Normattiva, 2012). Another important document is Legislative Decree No. 82/2005, known as the Digital Administration Code (CAD), which contains specific provisions for public sector data and defines terms such as "open format" and "open data," with Chapter V specifically dedicated to these topics (Normattiva, 2005). A further significant legal measure is Legislative Decree No. 36/2006, which implements the European Directive 2019/1024 on open data (Normattiva, 2006). Decree Law No. 76/2020



introduces a strategy for managing public sector information assets for institutional purposes (Normattiva, 2020). [Legislative Decree No. 97/2016](#) revised the measures concerning transparency and accountability in public administration, building on earlier legal frameworks (Normattiva, 2016). Lastly, [Legislative Decree No. 33/2013](#) reorganises the legal regulations regarding the obligations of disclosure, transparency, and dissemination of information by public authorities (Normattiva, 2013).

The National Plan for Open Data outlines specific strategies aimed at improving the availability and usability of data, while also encouraging active public engagement in the open data ecosystem. Another key document is the [Three-Year Plan for Information Technology in Public Administration](#), which provides a strategic framework for digital transformation. This plan emphasises the need for collaboration among public institutions, citizens, the business sector, and the academic community. Its most recent edition, covering the period 2022-2024, reflects the priorities of the National Recovery and Resilience Plan and focuses on enhancing the implementation of IT solutions in public services (Agenzia per l'Italia Digitale (AgID), 2022).

Italy's data security legislation is robust and designed to protect individual privacy and personal data while also supporting cybersecurity. At its core is the GDPR, with a legal framework that emphasises accountability, transparency, and resilience against data breaches, in line with broader EU objectives.

- [Legislative Decree No. 196/2003](#) regulates the processing of personal data in Italy and was amended to align with the GDPR. It includes provisions on data subject rights, responsibilities of data controllers and processors, and enforcement mechanisms (Normattiva, 2003).
- [The National Cybersecurity Strategy](#) outlines Italy's approach to cybersecurity, focusing on the protection of critical infrastructure, public administration, and private sector data (Agenzia per la Cybersicurezza Nazionale (ACN), n.d.).
- [Legislative Decree No. 65/2018](#) established the National Cybersecurity Agency (ACN) and defined its responsibilities in safeguarding national security in the digital domain. It also includes measures for incident response and data breach notification (Normattiva, 2018).
- [AgID adopted and published](#) "Guidelines containing technical rules for the opening of data and the reuse of public sector information" (Determination n° 183/2023) pursuant to Art. 12 Legislative Decree n° 36/2006 and subsequent amendments, Italian implementation of Directive 2019/1024, the Open Data Directive (Agenzia per l'Italia Digitale (AgID), 2023; European Union, 2019).
- Sector-specific regulations: Various industries—such as finance, healthcare, and telecommunications—have their own regulatory frameworks. For instance, the Bank of Italy provides guidelines for the financial sector, while the Ministry of Health enforces rules for the protection of health data.

Poland

Legislation concerning open data in Poland is primarily shaped by European Union regulations, national laws, and local government initiatives. Among the key legal acts and policies supporting open data in Poland is the [Act on Access to Public Information](#) from 2001 (Wolters Kluwer Polska, n.d.a). Every person (regardless of nationality) has the right to access public information without the need to demonstrate a legal interest or provide a reason for the request. The act sets out the rules for making documents, records, and data accessible by public institutions. While it promotes transparency and enables the public to access public information, its focus is more on access to data itself rather than on its reuse. Another significant piece of legislation is [the Act on Open Data and the Reuse of Public Sector Information](#), which came into force in December 2021 (Wolters Kluwer Polska, n.d.a). This law transposes EU Directive 2019/1024 into Polish law and goes beyond



the directive's minimum requirements. It broadens the types of available data, including high-value datasets, dynamic data, and research data. It encourages cooperation between the public and private sectors. It introduces the role of Open Data Officers and formally establishes the Open Data Program, ensuring a coordinated approach to transparency, innovation, and economic growth.

In addition to the above, Poland is also working on implementing the EU Data Act into national law.

Poland also has several laws and regulations forming a comprehensive framework for data protection and cybersecurity, especially in the context of open data.

- [Personal Data Protection Act \(Ustawa o Ochronie Danych Osobowych\)](#) - A national law aligned with the GDPR, establishing the Personal Data Protection Office and procedures for data protection enforcement (Wolters Kluwer Polska, n.d.b).
- [Cybersecurity Act \(Ustawa o Krajowym Systemie Cyberbezpieczeństwa\)](#) - Aimed at strengthening national cybersecurity, this law requires providers of essential services to implement security measures and report serious incidents (Wolters Kluwer Polska, n.d.c).
- [Act on Providing Services by Electronic Means \(Ustawa o Świadczeniu Usług Droga Elektroniczną\)](#) - Regulates electronic services, requiring transparency in data collection, user consent, and secure data transmission (Wolters Kluwer Polska, n.d.d).
- [Act on Combating Unfair Competition \(Ustawa o Zwalczaniu Nieuczciwej Konkurencji\)](#) - Protects trade secrets and confidential information, considering unauthorized data disclosure as unfair competition (Wolters Kluwer Polska, n.d.e).
- [Telecommunications Law \(Ustawa Prawo Telekomunikacyjne\)](#) - Regulates telecommunications, ensures user data confidentiality, and sets rules for data retention and consent collection (Wolters Kluwer Polska, n.d.f).

Slovakia

The legal framework governing data regulation and free access to information in Slovakia is currently fragmented across multiple legislative acts and subordinate regulations. The key legal instrument is [Act No. 211/2000 Coll. on Free Access to Information and on Amendments to Certain Acts \(commonly referred to as the “Freedom of Information Act”\)](#) (Národná rada Slovenskej republiky, 2000). This act underwent a significant amendment in 2022, which ensured the transposition of EU Directive 2019/1024 on open data and the re-use of public sector information.

Other relevant legal regulations that indirectly address to open data include:

- [Act No. 305/2013 Coll. on the Electronic Form of the Exercise of Public Authority \(commonly known as the e-Government Act\)](#) (Národná rada Slovenskej republiky, 2013)
- [Act No. 95/2019 Coll. on Information Technologies in Public Administration](#) (Národná rada Slovenskej republiky, 2019)
- [Decree No. 78/2020 Coll. of the Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatisation, establishing standards for information technologies in public administration](#) (Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, 2020a)
- [Decree No. 85/2020 Coll. of the Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatisation on Project Management](#) (Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, 2020b)

One of the objectives of the legal regulation in the area of data is to reduce bureaucracy and administrative burden for citizens and the business sector. Therefore, the above-mentioned legislative framework is complemented by [Act No. 310/2021 Coll., which amends Act No. 177/2018](#)



Coll. on Certain Measures to Reduce the Administrative Burden through the Use of Public Administration Information Systems (Národná rada Slovenskej republiky, 2021). This law, known as the “Anti-Bureaucracy Act,” focuses on decreasing administrative burdens through the use of public administration information systems.

In addition to the legal framework consisting of laws and decrees, the Government of the Slovak Republic approved the Strategy and Action Plan for the Accessibility and Use of Open Public Sector Data in 2017 (Úrad vlády Slovenskej republiky, 2017). This strategy outlines a set of tasks that need to be fulfilled to achieve its stated objectives. One of the goals of the strategy was the proposal of a Data Act and the development of an open data methodology. Furthermore, under the Action Plan of the Open Government Initiative in the Slovak Republic for the Years 2022-2024 (Úrad splnomocnenca vlády Slovenskej republiky pre rozvoj občianskej spoločnosti, 2022), an initiative was carried out to assess the impact of open data on selected aspects of society. This assessment aimed to identify the influence of open data on politics, the economy, the environment, and the social sphere.

In addition to the above, Slovakia also has several legal regulations that together form a comprehensive system for the protection of personal data and cybersecurity, especially in the context of open data.

- Act No. 18/2018 Coll. on the Protection of Personal Data and on Amendments to Certain Acts (Národná rada Slovenskej republiky, 2018a)
- Act No. 69/2018 Coll. on Cybersecurity and on Amendments to Certain Acts (Národná rada Slovenskej republiky, 2018b)
- Act No. 351/2011 Coll. on Electronic Communications (Národná rada Slovenskej republiky, 2011)

Slovenia

In 2015, the Slovenian government adopted the Public Administration Development Strategy 2015-2020 (Ministry of Public Administration for the Government of the Republic of Slovenia, 2015). This strategic document includes a dedicated section focused on the transparent management of public information. Based on the strategy, a series of biennial action plans were developed, the most recent being the Action Plan for the Implementation of Public Administration Development Strategy 2015 - 2020 for 2018 and 2019 (Vlada Republike Slovenije, 2018), that included concrete measures to strengthen the mechanisms of transparent public administration and to support publication of public sector information and development of open data.

In addition, Slovenia adopted document Open public sector data - Strategic work plan 2020 - 2021 (Ministrstvo za javno upravo, 2020). This plan includes modernisation of national data portal, API Interface updates, creation of data lake and definition of high value datasets in the line of the Open Data Directive.

Currently, work is underway on a new document Digital Slovenia 2030 - The umbrella strategy for Slovenia's digital transformation by 2030 (Vlada Republike Slovenije, 2023), which includes sections dedicated to open data.

The Ministry of Public Administration is responsible for maintaining and operating the national open data portal. It also plays an active role in shaping the legislative framework, issuing recommendations for data providers, organising hackathons and data challenges, and launching consultations to ensure that public institutions make their data available for reuse. Open data activities in Slovenia are carried out collaboratively through a stakeholder network involving data providers from various ministries and public institutions, data users (e.g., citizens), and data



editors working within the Ministry of Public Administration. The Ministry also offers a range of data management training courses aimed at encouraging open data publication and educating public servants, for example, in creating data publication plans, making data-driven decisions based on surveys, applying basic statistical methods, and engaging with advanced data science topics such as text mining.

Beyond the aforementioned plans and legal framework, Slovenia has enacted several additional legal provisions that collectively establish a comprehensive framework for personal data protection and cybersecurity, particularly in relation to open data. These include:

- [The Personal Data Protection Act \(Zakon o varstvu osebnih podatkov - ZVOP - 2\)](#) (Državni zbor Republike Slovenije, 2022)
- [The Information Commissioner Act \(Zakon o Informacijskem pooblaščenču - ZInfP\)](#) (Državni zbor Republike Slovenije, 2005)
- [The Electronic Communication Act \(Zakon o elektronskih komunikacijah - ZEKom - 2\)](#) (Žrt and Šik Bukovnik, 2025)



6. Open data governance

Data governance is defined as the exercise of decision making and authority for data-released matters. It represents the system of decision rights and accountabilities of people in organisation for information-related processes (Kastouni, 2022). It is executed according to models which describe the roles, actions and responsibilities of employees under certain circumstances. The data governance is also defined as “the exercise of authority and control (planning, monitoring and enforcement) over the management of data assets.” (DAMA, 2017)

Before diving into the methodology, the first step is to define the roles and actors for data administration and modification. It is crucial to establish clear responsibilities and access controls to ensure data integrity, data security and data management.

6.1 Roles and responsibilities

Data governance roles are positions within an organisation that ensure data is managed and used effectively. Data management is similar to corporate governance. The roles used in companies as corporate governance to run the business and make the most of their assets are also critical for managing data as an asset and maximising its value (Anmut, 2024). Effective data governance improves data analytics, which in turn enables higher-quality decision-making and better operational support. To implement successful data governance program, having a plan is not enough; significant roles and duties are required. (CPO Magazine, 2022).

Main roles

Data owner (Manager): Data Owner role is significant for ensuring data governance within the organisation (municipality). He or she has a pivotal role in the process of providing organisation with data integrity. Data owners have senior leadership and executives in charge of managing data and information. The Data Owner must have the authority and resources to enforce data governance policies and collaborate with various stakeholders across the organisation. Typically, this role is assigned to someone in upper management, like a department head, who has the necessary oversight and influence but works closely with Data Steward. (CPO Magazine, 2022).

Data Administrator (Data Custodian): Data Custodian is an IT specialist or team of IT specialists responsible for managing and safeguarding data within a data environment. This role encompasses overseeing the security and storage systems of datasets while adhering to the organisation’s data governance guidelines. Key responsibilities include data governance, data security, data quality management, and data access control, ensuring that data is effectively protected and managed throughout its lifecycle (Dremio, 2024; DQOps, 2024; Herzberg, 2021; DataScientest, 2023; CPO Magazine, 2022).

Data Administrator (Data Steward): A Data Steward manages data based on the defined standards and specifications set in agreement with the Data Owner. Data Steward is a subject expert with a thorough understanding of a particular data set and plays a crucial part in ensuring that the data in their care is of high quality and is fit for use by all data stakeholders in the organisation who are concerned with that set of data. In addition, he or she must thoroughly understand how that data needs to be documented, stored, and protected. They create processes and procedures that monitor and enforce data governance policies and establish guidelines for data handling, quality



assessments, and data security. Data stewards ensure their organisation's data accuracy, consistency, and reliability. This includes proactive measures like setting up validation rules and reactive measures such as rectifying identified issues. Data stewards should regularly monitor and review data quality metrics to ensure they meet organisational standards. (Enterprise Warehousing Solutions, 2025; HubSpot, 2022; Attacama, 2021)

Responsibilities

According to Melissa Malec, "Organised data is one of the most valuable assets an organisation can have. To make that a reality, you need to set up data governance responsibilities in your organisation." (Malec, 2025)

Data Owner (Manager) responsibilities

Data Quality Control: Ensures that data within the organisation is accurate, consistent, and up to date and oversees activities related to maintaining data quality.

Standards and Consistency: Maintains and enforces data standards, ensuring that all data follows consistent formats and definitions.

Collaboration: Collaborates with Data Stewards, Data Administrators, and other stakeholders to maintain high data quality across the organisation.

Data Classification and Protection: Ensures proper classification of data based on its sensitivity and importance, including overseeing the protection of personal or sensitive data.

Escalation and Resolution: Establishes an escalation matrix for addressing data quality issues and ensures these are resolved within set time limits.

Compliance: Ensures data usage complies with organisational policies, data governance frameworks, and regulatory requirements (e.g., GDPR) (CPO Magazine, 2022).

Data Administrator (Data Custodian) responsibilities

Access control and security: Manages data access by granting and revoking user permissions, configuring security roles, and ensuring compliance with data access policies. Defines the database infrastructure to safeguard it against internal and external threats while ensuring data privacy and regulatory compliance (e.g., GDPR, CCPA).

Performance Monitoring and System Maintenance: Monitors system performance. Resolves bottlenecks and ensures efficient data availability and responsiveness. Performs regular maintenance tasks, such as applying software updates, managing backups, and maintaining data integrity.

Incident Response and Troubleshooting: Investigates and resolves data-related incidents, including security breaches, system outages, and data quality issues. Offers technical support, identifies and addresses user-reported data problems, and escalates complex cases to the appropriate teams for further resolution.

Data Storage, Management, and Movement: Oversees the secure storage, custody, and movement of data, including data transmission logic. Documents all rules and codes governing data storage, processing, and transport while optimising storage resources. Manages the data lifecycle by archiving or decommissioning outdated datasets and ensuring compliance with data retention policies.

Technical Implementation and Collaboration: Implements dataset-specific standards, policies, procedures, and requirements, including logic for assessing data conditions. Collaborates with data owners and users to understand requirements, ensure data availability, and propose



improvements for efficiency and reliability. Participates in technical and business design processes to approve and align on a unified data vision. (Dremio, 2024; DQOps, 2024; Herzberg, 2021; DataScientest, 2023; CPO Magazine, 2022).

Data Administrator (Data Steward) responsibilities

Data Collection and Use Case Management: Collects and collates use cases for the dataset.

Dataset Standards and Policy Development: Develops, maintains, and updates dataset-specific standards, policies, and procedures to appropriately govern the dataset, including its metadata.

Dataset Condition Assessment: Measurements and methods of dataset condition.

Data Accessibility and Security: Ensures data accessibility, usability, safety, and reliability.

Requirement Management for Dataset: Manages new requirements of the dataset based on existing standards, policies, and procedures. (Firican, n.d.; Enterprise Warehousing Solutions, 2025; HubSpot, 2021)

Data entry typist responsibilities

Data entry: Enters the data into system.

Data maintenance: Updates and maintains the data into the system.

Ensuring accuracy: Verifies data for accuracy and completeness before entering it into the system.

Ensuring consistency: Ensure that data is consistent with existing records and follows defined formats and standards.

Data protection officer

Ensuring compliance with GDPR: Oversees the organisation's adherence to GDPR regulations, ensuring that data protection practices meet legal requirements.

Ensuring compliance with data protection: Ensures all aspects of data protection laws (e.g., GDPR, local regulations) are applied to how data is collected, stored, processed, and shared within the organisation.

Provides guidelines and legal advice for the proper usage of data (handling storage of personal data - sensitive information)

Internet of Things administrator (IoT administrator)

Leadership and Vision for IoT Initiatives: Internet of Things communication administrator is responsible for leading the vision and direction of IoT initiatives within an organisation.

Onboarding and Device Integration: Ensures an easy, user-friendly, and intuitive onboarding process that enables IT admins to easily add new devices to their systems.

Stakeholder Collaboration: Collaborates with different stakeholders, such as business leaders, citizens, vendors, and engineers, to identify the needs, goals, and challenges of IoT projects.

Remote Troubleshooting and Support: Troubleshoots remotely to reduce manual efforts and resolve user issues quickly.

Team Supervision and Mentorship: Supervise and mentors the IoT team, ensuring they follow best practices, standards, and policies for IoT security, performance, and reliability.

Analytics and Reporting: Collects and analyses data from IoT devices to create reports for internal and external stakeholders.

Continuous Improvement and Feedback: Provides feedback and recommendations for improvement based on analysis and team performance. (Grady Andersen and MoldStud Research Team, 2024; Lu and Neng, 2010)



Collaboration in data governance

The role of collaboration in data governance is particularly important. Right collaboration ensures that individuals or teams work together to maintain the usability, security, and quality of data. On the one hand there is setting rules and determining roles in data governance, on the other hand there is synchronisation of technical, legal, and municipal priorities.

The data protection officer is responsible for ensuring that data protection practices meet legal requirements, providing guidelines and legal advice for the proper usage of data while for data entry typist manages entering the data into system and updating them.

A remarkably simple example of collaboration in data governance might be the implementation of a new system for managing IoT devices, which generates a lot of data. The data needs to be stored and managed correctly, especially in connection with the protection of personal data.

Firstly, there is Data Owner (Manager) who is responsible for setting rules for managing IoT data, what data is critical and what access rules should be implemented. There should be a collaboration between Data Owner and IoT administrator. It is important to identify what IoT devices will generate the data and how that data will be used. Subsequently, the role of Data Custodian is needed because Data Custodian is responsible for technical infrastructure, which manages data from IoT devices. He or she ensures saving and protection of the data on servers, their backup and availability. Another vital role is Data Protection Officer who is responsible for protection of personal data that might be part of IoT data (Milvus, 2026).

Other defined roles

Data entry typist: Data typist is a person who uses computers, keyboards, and software to enter data into various databases. The role includes activities such as transcribing audio recordings, encoding handwritten documents, and other general document processing.

Data protection officer (DPO): Data protection officer is responsible for ensuring that an organisation complies with data protection laws, most notably the General Data Protection Regulation (GDPR). The data protection officer is critical in ensuring that personal and sensitive data is handled securely and legally, especially in sectors such as small municipalities where personal data is often managed. This role acts as the main point of contact for data protection authorities and individuals whose data is being processed. Data protection officers create and maintain a data protection policy tailored to the specific needs of small municipalities. Additionally, the Data protection officer must review and approve data usage policies to ensure they meet GDPR compliance.

Internet of Things communication administrator (IoT administrator): The IoT refers to the interconnected network of physical devices embedded with sensors, software, and connectivity that enable them to exchange data and interact with each other. The IoT administrator must understand software application behaviour, in order to deploy, configure and troubleshoot computer systems, and is required to have current knowledge in modern technologies to ensure that systems operate efficiently. (Grady and MoldStud Research Team, 2024; Lu tan and Neng Wang, 2010)

6.2 Data collection

Efficient and structured data collection is fundamental to ensuring the availability, quality, and usability of public open data. A well-defined approach helps municipalities mitigate challenges related to data accuracy, security, privacy, and accessibility. Municipalities are increasingly



expected to manage and share data in a way that supports public services, transparency, and community development. Collecting good quality data is the first and most important step toward these goals. Whether it involves traffic patterns, public space management, or environmental indicators, data can help cities make better decisions and engage more effectively with citizens. This chapter outlines practical steps for municipalities to build up their local data collection processes in line with European standards and everyday needs, and provides guidance tailored to the DoorCE project.

Overview of data collection process

In the context of the DoorCE strategy, municipalities are central actors responsible for identifying, collecting, and managing datasets relevant to local governance, service delivery, tourism, climate adaptation, and citizen engagement. They are expected to develop local data strategies aligned with national policies and EU regulations (e.g., the Open Data Directive). Responsibilities include establishing governance structures, defining data use cases, coordinating across internal departments, and ensuring that collected data meets quality, interoperability, and legal standards.

To ensure a successful implementation, each data contributor—whether a department, agency, or external contractor—should have clearly assigned roles and be held accountable for their part in the data collection process. Municipalities should also collaborate with each other, exchanging knowledge, sharing good practices, and avoiding duplication of effort, particularly when it comes to the identification and structuring of relevant datasets.

This chapter outlines these responsibilities in more detail, including who is responsible for which tasks and how accountability is ensured across actors involved in the data collection process. It also presents a step-by-step guide to the collection process itself—illustrating how structured, efficient data collection helps address challenges related to data accuracy, privacy, and accessibility. When carried out effectively, this process results in datasets that support transparency, innovation, and better decision-making for public institutions and the communities they serve.

Steps to collect data:

1. **Identify Opportunities for Data Collection** - Before initiating any data collection process, it is essential to recognise areas where data can provide value. Identifying relevant data opportunities ensures that the collected information serves a clear purpose and addresses stakeholder needs.
 - *Engage with Key Stakeholders:* Consult with other municipalities, organisations, government agencies, citizens, businesses, and researchers to understand their data needs. Identify pain points where data could facilitate better decision-making or service delivery.
 - *Assess Existing Data Gaps:* Review currently available datasets to determine where new efforts are necessary. Identify outdated, incomplete, or missing datasets.
 - *Evaluate Data Use Cases:* Consider how the collected data will be used—for policy, applications, research, or services—and how different users will access it.
2. **Select opportunities and set goals** - Once relevant data collection opportunities are identified; it is crucial to refine the focus and set clear objectives.
 - *Prioritise Based on Impact and Feasibility:* Consider the potential benefits and relevance of the data in different contexts (e.g., urban planning, transportation, sustainability). Assess technical feasibility, including data sources, collection methods,



and available resources. Weigh the legal and ethical considerations, such as data protection and compliance with open data standards.

- **Define Clear Goals and Outcomes:** Establish specific goals for each data collection initiative. Examples include enhancing public service delivery by collecting traffic and mobility data. Increasing government transparency by publishing procurement and budgeting data. Supporting environmental sustainability through air quality and waste management data collection. Define key performance indicators (KPIs) to measure the success and impact of data collection efforts.
 - **Determine Sources and Platforms for Data Collection:** Leverage city datasets, municipal records, online portals, IoT sensors, and other automated systems to collect data efficiently. Establish guidelines for integrating third-party datasets or data contributions from the public and private sectors.
3. **Create a plan and set methods for data collection** - A structured plan ensures that data collection is conducted efficiently, securely, and in compliance with best practices.
- **Assign Roles and Responsibilities:** Designate teams responsible for data gathering, quality assurance, processing, and storage. Ensure collaboration between IT specialists, policymakers, analysts, and external stakeholders.
 - **Select Data Collection Methods:** Manual Data Collection: Surveys, interviews, reports, and direct input from field workers or officials. Automated Data Collection: IoT devices, sensors, and real-time data streams (e.g., traffic cameras, weather stations). APIs and Web Scraping: Automated retrieval of structured data from digital platforms. Public Contributions: Open platforms where citizens can contribute data, such as participatory mapping or crowd-sourced reporting.
 - **Establish a Data Collection Timeline:** Define collection frequency (real-time, daily, monthly) based on the nature of the data. Set milestones for data validation, publication, and updates.
4. **Validate the method of data collection** - Data validation is critical to ensuring that collected data is accurate, reliable, and useful.
- **Ensure Data Accuracy and Integrity:** Verify that collection methods provide consistent and precise data. Use test cases, sample datasets, and pilot projects before full-scale data collection.
 - **Compliance with Standards and Regulations:** Ensure adherence to GDPR (General Data Protection Regulation) and other relevant privacy laws. Maintain transparency in data collection processes, ensuring ethical use and secure handling.
 - **Data Quality Control Measures:** Implement measures such as automated validation scripts, anomaly detection, and manual review processes. Create metadata documentation detailing sources, collection methods, and data limitations.
5. **Collect data** - The execution phase involves actively gathering the data, ensuring proper logging, monitoring, and security.
- **Real-Time Data Collection:** Use IoT sensors, GPS tracking, and other automated methods to collect live data. Ensure system uptime and data synchronisation for seamless collection.
 - **Batch Data Collection:** Retrieve historical datasets from government agencies, research institutions, and other sources. Standardise formats and ensure interoperability with existing datasets.
 - **Monitoring and Adjustments:** Continuously evaluate data collection efficiency. Adjust if unexpected errors or inconsistencies arise.
6. **Analyse and publish data** - Once data is collected, it must be processed, analysed, and made available for use.



- **Data Cleaning and Processing:** Standardise formats and remove errors, duplicates, or inconsistencies. Anonymise personal data to comply with privacy regulations.
- **Data Analysis and Visualisation:** Apply analytical models, statistical tools, and machine learning techniques to derive insights. Create dashboards, visual reports, and summaries for policymakers, for businesses and the public.
- **Data Publication and Accessibility:** Store and publish datasets in open formats (CSV, JSON, XML) for easy access. Provide APIs and developer tools to facilitate data usage in applications and services.

Data sources

Access to reliable and relevant data is essential for municipalities and citizens to make informed decisions, plan sustainable development, and respond to emerging challenges. This chapter provides an overview of recommended data sources that can support both the public sector and authorities and users of DoorCE applications.

Many countries operate central open data platforms where public sector data is collected and shared. These are valuable starting points for municipalities and individuals looking for standardised, regularly updated datasets. These portals often include datasets on demographics, transport, tourism flows, environmental indicators, and more.

At more specific levels, there are city-levels open data portals. Many smart cities operate their own open data portals, providing information on transportation, urban services, cultural events, or waste collection. These can be integrated into mobile apps, public dashboards, or community planning tools.

When discussing concrete fields of open data sources relevant to the DoorCE project, several thematic areas can be highlighted. For example, tourism-specific open data sources are provided by [the World Tourism Organisation \(UNWTO\)](#), which grants access to selected datasets through partnerships (UN Tourism, n.d.). Climate- and environment-related open data is often made available through national meteorological institutes or global initiatives like the Copernicus programme. Aggregation platforms like [Opendatasoft](#) also play a significant role by collecting, standardising, and visualising datasets from multiple regions, making them more accessible and actionable (Huwise, 2026).

One of climate-specific open data sources is [the Climate Data Store](#), it is a free and open online platform that provides access to an extensive collection of climate datasets and tools for analysing past, present and future climate conditions (Climate Data Store, 2026).

An example of an open data source focused on the environmental field is [the European Environment Agency](#). The European Environment Agency (EEA) is an agency of the European Union that provides valuable knowledge about the state of the environment in Europe. It plays a crucial role in supporting environmental and climate policy by delivering reliable, verified, and policy-relevant data (European Environment Agency, 2026).

Tourism/climate

Data for tourism is important for several reasons that help with effective decision-making, planning and enhancing the overall experience for travellers. It helps with management for municipalities about inflow of tourists, number of visitors, optimisation of visitor's capacity, monitoring demand of tourists. Based on data, environmental impact can be assessed, as well as better resource allocation, budget planning, marketing campaigns and improving safety and



quality of experiences for tourists. For users, this data can help with trip planning, understanding seasonal variations, or evaluating the environmental footprint of travel choices.

Examples of good practices include various fields:

Tourist Attractions and Activities

- Information on landmarks,
 - museums,
 - parks,
 - natural attractions,
 - cultural events.
- Tourism paths, routes, viewpoints, and activity options (e.g., adventure tourism, guided tours).

Accommodation and Facilities

- Hotels, hostels, campsites, and other accommodation types.
- Accessibility features (wheelchair accessibility, budget-friendly options).
- Location and availability of public facilities like toilets, parking lots, and drinking water points.

Visitor Statistics and Demographics

- Number of domestic and foreign visitors.
- Visitor origin (countries and regions).
- Number of overnight stays, occupancy rates, and accommodation capacity.
- Types of accommodation preferred and average duration of stay.

Tourist Services and Experience

- Information on restaurants, cafes, and food services.
- Calendar of events (cultural, sports, festivals).
- Health facilities, emergency services, and safety advisories for tourists.

Weather and Atmospheric Conditions

- Temperature, humidity, wind, and precipitation data.
- Seasonal variations and weather forecasts for visitors.
- Air quality measurements (pollution levels such as PM, NO particles).

Environmental Quality Monitoring

- Noise levels and pollution data.
- Monitoring of green spaces, urban heat islands, and tropical night occurrences.
- Tree condition data and species distribution (urban greenery).

Water Data

- Water quality of rivers,
- Water quality of lakes
- Water quality of seas.
- Bathymetry and hydrographic data.
- Suitability of bathing areas, safety, and conditions for swimming.



Smart Cities

A smart city is an urban area that uses an array of digital technologies to enrich residents' lives, improve infrastructure, modernise government services, enhance accessibility, drive sustainability, and accelerate economic development.

Open data available in real time plays a vital role in smart cities, supporting urban management at various scales and enhancing attributes like adaptability, efficiency, interoperability, flexibility, transparency, and the ability to respond instantly. Using open data to drive smarter solutions benefits everyone in the process.

Municipalities

- The implementation of data portals enhances staff efficiency by reducing the administrative burden associated with responding to written requests and phone calls for information.
- Open data fosters greater municipal transparency by enabling the sharing of information on local services with the public.
- Through open governance, the provision of innovative services, and differentiation from competing municipalities, local governments can attract new residents and foster investment-friendly environments.
- Monitoring pollution levels, water, and air quality, and sharing this information as open data with national regulatory authorities supports sustainability efforts and ensures compliance with environmental regulations.

Citizens

- Open data facilitates seamless interaction between residents and local government.
- Real-time access to municipal information, such as available parking spaces, local weather conditions, or road closures enhances quality of life and civic satisfaction.

Stakeholders

- Open data contributes to economic development. For example, access to localised weather data or water reservoir levels can benefit agricultural planning, while traffic data can help retailers optimise business hours and logistics.

Examples of good practices include various fields:

Transportation and Mobility

- Real-time and static data on public transport (routes, schedules, availability)
- Bike sharing systems, e-scooters, and parking facilities
- Data on road networks, pedestrian paths, and infrastructure for cycling

Urban Infrastructure and Energy Use

- Waste management (locations of waste containers, fullness measurement)
- Public utilities, lighting, and energy consumption patterns
- Mapping of urban features like administrative units, bridges, and public facilities

Environmental Impact and Sustainability Initiatives

- Data on energy consumption and areas suitable for renewable energy projects
- Public initiatives for reducing carbon footprint, sustainable tourism, and environmental conservation
- Protected sites, natural monuments, and conservation areas (Opendatasoft, 2023; Lnenicka, 2022)



Data collection methods

Data collection methods are techniques and procedures for gathering information for research purposes. These methods are integral to the data collection process, ensuring that accurate and comprehensive data is acquired. The selection of appropriate data collection methods is crucial for obtaining reliable and valid results. Understanding these methods is essential for conducting high-quality research and obtaining meaningful insights from collected data. In the context of data collection method, we differentiate two types of data: static and dynamic data.

Static data refers to data that does not change over time or change infrequently. Usually, it is collected at specific times or at periodic intervals and stored in structured formats. It is extracted from various databases, archives or historical records and includes demographic data, historical economic data, or historical statistics.

Dynamic data refers to data that changes frequently, because it is continuously updated. To differ from static data, it is collected in unstructured or semi-structured formats, thanks to constant changes based on new events or added information. Dynamic data is extracted from numerous sources e.g.: IoT devices, website analytics or real-time market and includes weather data, real-time traffic information or social media interactions.

Open data refers to datasets that are freely available for use, sharing, and analysis by anyone. The collection of open data involves various methods that enable access to publicly available information from different sources. The most used data collection methods (in connection with open data) include *Application Programming Interfaces (APIs)*, *Data extraction* or *AI scanning*. (SkillApp, 2024)

Application Programming Interfaces (APIs)

Application Programming Interfaces (APIs) represents a set of protocols, tools, and definitions, which enable different programs to interact with each other. APIs offer a standardised method for applications to exchange and communicate data, simplifying the process of gathering information from external sources, platforms, and services. With APIs - driven data collection, real-time access to current data is possible, ensuring accuracy while minimising manual work.

APIs allow data sharing between apps, systems, and devices through a request-response cycle. The APIs process is divided into a few simple steps:

1. The APIs client starts by sending a request to the APIs server. This could be triggered out by a user action (like clicking a button) or an external event (like receiving a notification). The request contains several elements:
 - Endpoint: A URL where the specific data or resource can be accessed.
 - Method: The action to perform (e.g., GET to retrieve data, POST to create data).
 - Parameters: Variables that tell the API how to handle the request.
 - Headers: Provide extra details like authentication or content type.
 - Body: The main data, such as form data to create or update a resource.
2. The APIs server receives the request, handles tasks like authentication, data validation, and retrieves or updates the data as needed.
3. The server sends a response back to the client, including:
 - Status Code: Indicates success (200 OK) or failure (404 Not Found).
 - Headers: Provide more details about the response.
 - Body: Contains the requested data or an error message.



Based on access, functionality, and architecture, there are several types of APIs:

- Open APIs: APIs that are accessible to anyone without needing authentication.
- Internal APIs: APIs used privately within an organisation for internal systems or applications.
- RESTful APIs: APIs based on the Representational State Transfer (REST) architecture, designed for simplicity and scalability.

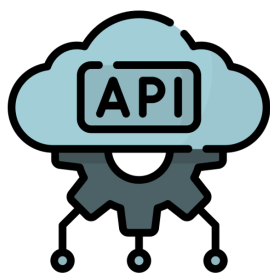
APIs link different software systems, applications, and devices, enabling them to interact with each other. This unlocks numerous advantages and disadvantages. Some of the key advantages and disadvantages of APIs are:

Advantages:

- Automation: APIs can automate repetitive works, which means productivity improving, especially for developers and testers.
- Innovation: Public APIs enable external engineering teams to use existing features, fostering innovation and speeding up development of new digital experiences.
- Security: APIs can add an extra layer of security by requiring authentication and authorisation for accessing sensitive data, helping to prevent unauthorised access.
- Cost efficiency: APIs offer access to valuable third-party tools and services, helping businesses save money by avoiding the need to develop complex systems internally.

Disadvantages:

- Access Control: APIs may require authentication and the use of API keys to control access.
- Usage Limits: APIs often have restrictions on usage, which can limit the amount of data that can be retrieved.
- Data Completeness: Some APIs might not offer all necessary data, requiring the combination of multiple APIs or other data collection techniques (Postman, 2025; GeekforGeeks, 2025; Carlos Pereira, 2023)



How APIs work

Clients sends a request to a server box
The request includes endpoint, method, parameters, headers and sometimes a body
The server processes the request and returns a response

What APIs enable

Standardise communication between systems
Real-time access to external data and services
Faster and more automated data exchange

Types and limit of APIs

APIs can be open, internal or RESTful
Access may still depend on authentication, API keys or usage limits
Some data may be incomplete or restricted by licensing or IPR conditions
(IPR= Intellectual Property Rights)

Figure 6: How APIs Enable Structured Data Access

Source: data.europa.eu, n.d.e; own adaptation

Data extraction

Data extraction represents a key step in the data lifecycle, allowing businesses to collect valuable information from various sources. It involves retrieving specific, usable information from larger, unrefined datasets. This process encompasses a range of techniques, from simple methods to more



sophisticated approaches. Once extracted, it can be stored in a destination such as a data warehouse, which is optimised for online analytical processing (OLAP).

The primary purpose of extracting data is to refine large, complex datasets into usable information. This process often involves handling batches of files, extensive tables that are too cumbersome for immediate use, or files that are formatted in a way that makes it challenging to extract actionable insights.

There are six main stages involved in data extraction:

1. To identify sources - Find where the data comes from (databases, files, APIs, etc.).
2. To set up connections - Connect to each source using the right tools.
3. To extract data - Pull the needed data from those sources.
4. To transform data - Clean, convert, merge, and format the data as needed.
5. To validate data - Check the data for accuracy and consistency.
6. To load data - Move the data into its final warehouse or database.

There are several methods to extract data:

- Web Scraping and Parsing
- Database Querying and Exports
- API Calls and Integrations
- Optical Character Recognition (OCR)
- File Parsing
- Email Extraction
- Log File Parsing
- Data Extraction from PDFs
- Data Capture from Sensors and IoT Devices
- Manual Data Extraction

Data extraction software, especially when automated, offers several advantages:

- **Improves Decision-Making:** By providing targeted data, it enables team to make informed decisions based on facts rather than assumptions.
- **Increases Accuracy:** Automation minimises human errors that can occur during manual data handling and formatting.
- **Saves Time:** Automated tools allow employees to concentrate on more valuable tasks, such as utilising the extracted data effectively (Kutz, 2025; Stich Data, n.d.)

AI scanning

AI scanning is revolutionising scanning, transforming it from a basic digitisation task into a powerful tool for data analysis, automation, and accuracy. This shift has the potential to simplify document management, strengthen data security, and boost efficiency across multiple sectors. In the past, scanning primarily involved converting paper documents into digital formats. However, with the integration of AI, this process goes beyond simple digitisation. AI-driven scanning systems can understand, interpret, and analyse the information within scanned documents, unlocking new opportunities in industries ranging from healthcare to finance and beyond (Alohi, 2024).



7. Data licensing

Effective data licensing ensures that data can be used responsibly while respecting intellectual property rights, data privacy regulations, and organisational goals. While open data is often associated with free access, this does not necessarily mean that it must be provided without cost. Activities such as data collection, processing, and distribution require financial and human resources. In some cases, open data can be offered under paid models.

Why is open data licensing important?

When making data available to citizens and businesses, it is essential to accompany it with a licence. Without a licence, the published data is not truly open, as users are uncertain about what they are permitted to do with it. In other words, the absence of a licence creates legal uncertainties and risks for citizens and businesses. This may discourage them from reusing the data, defeating the purpose of open data – namely, fostering innovation and generating value for society. For example, properly licenced open data can be used to develop a mobile app, which visualises urban heat intensity and helps citizens to avoid the hottest places in a city during days with elevated temperature. It should be noted that there are several e-learning modules on open data licensing such as the data.europa.eu Academy and its [course on the legal side of open data](#) (data.europa.eu, n.d.d). To facilitate data licensing, the [European Data Portal Licence Assistant](#) also provides guidance on selecting the appropriate licence for open data. Before exploring the most common and recommended types of licences for open data, it is important to first define what a licence is (data.europa.eu, n.d.c).

What is an Open Data Licence?

An **open data licence** is a legal agreement that allows data to be freely accessed, used, modified, and shared by anyone, typically requiring attribution to the original creator and ensuring that derivative works maintain the same freedoms. The most widely used open data licences are often general licences for creative works that have been adapted for data usage. It is recommended to publish open data under a licence with minimal restrictions, as this maximises potential reuse, innovation, and value creation while reducing legal barriers for users. Open data providers cannot think of all ways their data can be reused. It is therefore better to not impose any limitations (data.europa.eu, n.d.c).

7.1 What does an Open Data Licence cover?

When someone accesses and uses data under an open data licence, they implicitly agree to comply with its legally binding terms and conditions. In general, an open data licence defines the following rights and obligations for users, which may vary depending on the type of data and the goals of its creator.

Rights

- **Right to reproduce:** This grants permission to create copies of the data, such as by presenting it on another website.
- **Right to distribute:** If the licence includes this right, users are permitted to share the dataset with third parties. This includes distributing copies of the dataset and displaying it publicly, such as within an online service or application.



- **Right to modify:** This allows users to alter the data, create new datasets or derivative works, and distribute those new works to third parties.
- **Right to sublicense:** This enables users to grant third parties the right to use the dataset, such as by allowing them to distribute it or develop derivative works. Sublicensing allows the user to act as if they were the original data provider.
- **Right to use patent claims:** If included in the licence, this grants permission to use one or more patents held by the data provider. In the open data community, such patent grants are rare since raw data is not patentable. However, a licence may still include patent rights, usually to prevent legal restrictions on data use.
- **Right to use commercially:** This is a crucial right, and open data providers should be cautious when imposing limitations on the commercial use of their datasets. Restricting commercial use may prevent private entities from developing innovative solutions that benefit society. Some even argue that open data that cannot be commercially exploited is not truly open.
- **Right to use a trademark:** This grants permission to use a protected name or designation. In the context of open data, this right is generally less relevant, as trademarks rarely apply to datasets. Instead, open data providers typically prefer an attribution requirement to ensure proper credit.

Obligations

- **Obligation to provide notice:** Users must disclose the licence terms under which they are using the dataset. This ensures transparency.
- **Obligation to attribute:** Users must credit the original data source. This is the most common obligation in open data licences. The licence may specify how attribution should be given, whether by mentioning the name of the relevant public administration or providing the URL where the original dataset is available.
- **Obligation to apply the same licence to derivative works:** Also known as the "share-alike" requirement, this obliges users to apply the same licence as the original dataset to any modified datasets or derivative works.
- **Obligation to state changes:** Users must disclose any modifications made to the original dataset whenever they reproduce or distribute it. This typically includes noting the date of the latest update from the original source, as well as the date and description of any modifications made by the user.

In addition to rights and obligations most open data licences also include **disclaimers of warranty and liability**. This means the data is provided "as is," with no guarantees of accuracy or fitness for a specific purpose, and the data provider is not liable for any issues arising from its use such as loss, damage, or legal issues. These clauses protect the data publisher from being sued if, for instance, someone develops an app with the data and something goes wrong unintentionally. Hence, reusers also cannot blame the data provider if something in the data is outdated or incomplete. It is obvious that clauses on liability and warranty are an important part of open data licences (data.europa.eu, 2014).

7.2 Types of Open Data Licences

As outlined above, open data licences typically grant citizens and businesses permission to freely access, use, modify, and share data while imposing certain obligations. Over the years, the open data community has developed several internationally recognised licences that can be enforced in most authorities. At the same time, some countries and regions have created their own open



data licences, often based on existing international models but adapted to account for cultural, legal, or linguistic specificities.

When opening a dataset, local governments should first verify whether there is a legal requirement at the national level to use a specific licence, either in general or for particular categories of data. In some cases, local governments may be obligated to release data under a national licence, or practical considerations – such as integration with a national open data portal – may make using the national licence preferable. Examples for national open data licences are the [Datenlizenz Deutschland - Zero](#) in Germany or the [Étalab Licence Ouverte](#) in France (GovData, n.d.b; ALLiance, n.d.).

If there is no legal obligation to use the national licence, it is highly recommended to adopt one of the widely recognised international open data licences. For local governments committed to transparency and fostering innovative data reuse, developing a custom licence should be avoided. Creating a new licence can be time-consuming and may introduce uncertainties for users, who might struggle to determine what they are permitted to do with the data. Both national and independently developed licences can significantly restrict the usability of open data outside its country of origin.

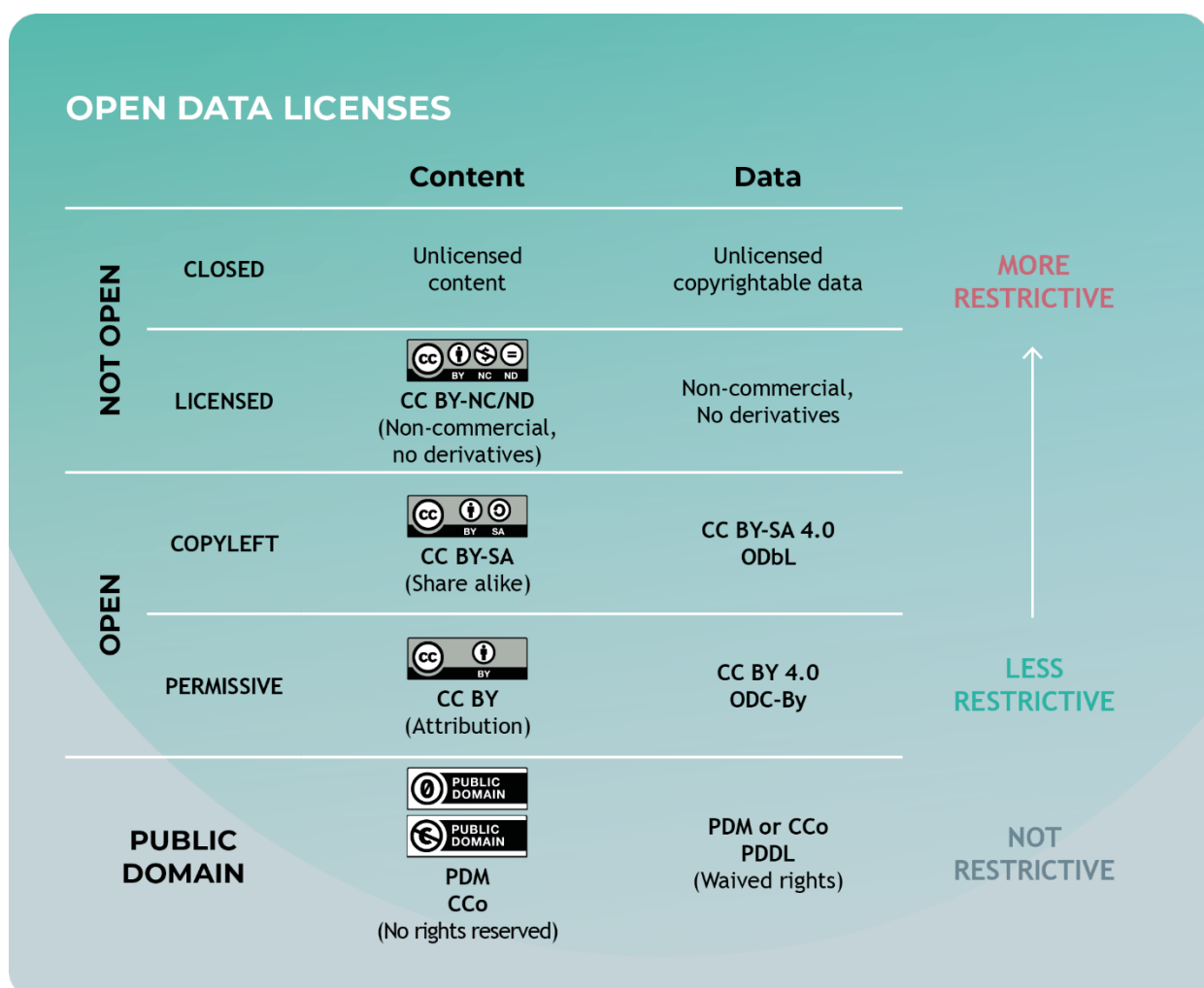


Figure 7: Open Data Licenses Overview
Source: Hall, 2021; own adaptation

Below are the most common international open data licences and their key features:



Public domain licences

The **Creative Commons Zero (CC0)** licence and the **Open Data Commons Public Domain Dedication and Licence (PDDL)** allow data creators to waive all copyright and database rights, effectively placing their work in the public domain. This means that anyone can freely use, modify, distribute, and build upon the data without attribution or restrictions.

Public domain licences are ideal for open data projects that prioritise maximum reuse and accessibility, such as government datasets and public knowledge resources. The primary distinction between **CC0** and **PDDL** lies in how they address database rights. Unlike **CC0**, **PDDL** explicitly covers the legal aspects of databases, providing a clear framework for data that includes both content and database structure.

Attribution licences

The **Creative Commons Attribution (CC-BY)** licence and the **Open Data Commons Attribution Licence (ODC-BY)** allow anyone to use, modify, and share open data for any purpose, including commercial use, provided that they properly attribute the original creator. These licences ensure maximum flexibility while maintaining credit for the data's source.

The difference between **CC-BY** and **ODC-BY** mirrors the distinction between the public domain licences mentioned earlier. **ODC-BY** specifically addresses database rights, ensuring that attribution applies to both the data content and its structure, whereas **CC-BY** was initially designed for general creative works.

Share-Alike licences

The **Creative Commons Attribution-ShareAlike (CC-BY-SA)** licence and the **Open Data Commons Open Database Licence (ODbL)** allow anyone to use, modify, and share open data, including for commercial purposes, as long as they provide attribution and licence any derivative works under the same terms. This ensures that all adaptations remain open and freely available, fostering a culture of shared knowledge and collaboration.

Unlike **CC-BY-SA**, which is designed for general creative works, **ODbL** applies specifically to databases and their structure, ensuring both the data and its organisation remain openly accessible. ODbL also distinguishes between derivative databases (which must be licensed under ODbL) and derivative works (which are not databases and do not necessarily require an ODbL licence).

Correct citation

Whereas **CC0** and **PDDL** do not contain any obligation to notice or attribute, attribution under the attribution licences, **CC-BY** and **ODC-by**, must follow the so called **TASL principle**, which includes:

- **Title** - Name of the dataset (if provided).
- **Author** - Name of the creator or organisation.
- **Source** - A link to the original dataset or its location.
- **Licence** - A mention of the licence with a link to its details.

Example: "Dataset Name" by [Creator/Organisation], available at [Source URL], licensed under [CC-BY 4.0](#) or [ODC-by](#) (Creative Commons, n.d.a; Open Data Commons, n.d.a).



The share-alike licences, **CC-BY-SA** and **ODbL**, should also follow the TASL principle, but should in addition contain a „share-alike“ notice, which is nothing more than a statement that any derivative work must be licensed under the respective licence.

Example: "Dataset Name" by [Creator/Organisation], available at [Source URL], licensed under [CC-BY-SA](#) or [ODbL](#) (Creative Commons, n.d.b; Open Data Commons, n.d.b). Derivative works must be shared under the same licence.

When comparing Creative Commons (CC) licences and Open Data Commons (ODC) licences, a logical question arises: Why use CC licences at all when ODC licences are specifically designed for databases? The primary reason is that CC licences have a longer history and are more widely recognised across various fields, including the arts, education, and research.

CC licences are well-suited for non-structured datasets, such as spreadsheets, tables, and documents, as well as mixed datasets that contain multimedia elements. In these cases, CC licences provide sufficient legal clarity and flexibility for data reuse while benefiting from their broad familiarity and adoption.

License type	Examples	Icon	Copy	Share	Modify	Commercial	Attribution
Public domain Maximum openness	CCO		Yes	Yes	Yes	Yes	No
	PDDL						
Attribution open, but credit required	CC BY		Yes	Yes	Yes	Yes	Yes
	ODC-BY						
Share-alike Open, but derivatives must stay open	CC BY-SA		Yes	Yes	Yes	Yes	Yes
	ODbL						
Restrictive CC Not fully open	CC B-NC		Partly	Partly	Partly	No or limited	Usually yes
	CC BY-ND						
	CC BY-NC-SA						
	CC BY-NC-ND						
Commercial/ Custom Not open by default	Paid API access, subscription, enterprise terms		Depends on contract	Depends on contract	Depends on contract	Usually yes, but under paid terms	Depends on contract

Figure 8: Types of Licenses, Rights and Responsibilities

Source: Creative Commons, n.d.c; own adaptation

It is important to note that there are also other Creative Commons (CC) licences for data, which are however not considered fully open. There are:

- CC BY-NC (Attribution-NonCommercial)
 - Allows data usage and sharing for non-commercial purposes only.
 - This restriction prevents companies from using the data for commercial gains.
- CC BY-NC-SA (Attribution-NonCommercial-ShareAlike)
 - Restricts commercial use and requires derivatives to be licenced under the same terms.
- CC BY-ND (Attribution-NoDerivatives)
 - Allows sharing but prohibits modifications to the original data.



- CC BY-NC-ND (Attribution-NonCommercial-NoDerivatives, version 4.0)
 - The most restrictive licence, allowing only non-commercial use without modifications.

Apart from that, licences can also be commercial. Commercial licences are used when data is provided under exclusive access or paid conditions. These licences allow:

- **Subscription-based API access** (e.g., companies pay for higher-tier data access).
- **Tiered pricing models** based on data volume or frequency of use.
- **Enterprise licensing agreements** for proprietary datasets.
- **Custom licences** tailored to specific business partnerships.

Commercial licensing is particularly relevant for organisations that wish to **monetise high-value datasets** while maintaining control over their distribution.

Local authorities should absolutely avoid using restrictive CC or commercial licences when publishing data unless there are sufficiently good reasons to do so. Otherwise, their datasets will not be open, which will eliminate the possibility of reasonable reuse by citizens and innovative businesses.

Where should the data provider display licence information?

Licence information, which defines the rights and obligations associated with a dataset, should be easily accessible and clearly readable for users. Ideally, open data should be shared via a website, where the licence details are prominently displayed.

While the full text of the licence does not necessarily need to appear on each dataset's page, it is recommended to provide a hyperlink to the complete licence description. To enhance visibility, the hyperlink can be formatted with a distinct header, colour, larger font size, and the official licence logo. This type of licence indication is commonly referred to as a "human-readable description."

If a single licence applies to all datasets within an open data portal, it can be referenced in the general terms of use, typically located in the website footer. However, for clarity and transparency, it is still advisable to include a reference to the applicable licence on each dataset's individual page.

In addition to a human-readable description, licence information should also be provided in a machine-readable format as metadata. Open data published online should always include machine-readable metadata that describes the dataset and specifies the applicable rights and conditions for reuse.

The appropriate metadata format for licence descriptions depends on the data format. If data is made available not only as raw files but also via a web API, the licence information should be included directly in API responses rather than being hidden in the API documentation.

The most common machine-readable metadata formats for open data include:

- DCAT (Data Catalog Vocabulary)
- Dublin Core
- Schema.org
- ISO 19115/19139
- DataCite Metadata Schema



- VIVO

How should the licensing process be structured in practice?

The following licensing process is particularly recommended for the initial data opening, which normally encompasses multiple datasets. When opening additional data later on, the process must not necessarily be followed or at least not all of the recommended steps must apply. It is possible to settle on a licence for most of your datasets and to only decide otherwise in truly specific cases. Thus, the proposed process should merely serve as a guidance whenever a dataset is opened.

Step 1: Initial analysis of data to be opened.

Begin by reviewing the datasets you plan to open and consider any additional datasets that may be made available in the future. Some elements of the data may originate from third-party sources and be subject to their own licensing conditions. Other elements may contain personal or confidential data, whose dissemination is limited or prohibited by law. Additionally, your datasets may vary in format and intended applications, potentially requiring different licensing approaches. Conducting this preliminary analysis will help shape your strategy for the following steps, including consultations with internal and external stakeholders.

Step 2: Research and consultation with target groups

With a clearer understanding of your data and long-term open data objectives, you can now identify appropriate licensing options. The selection of licences should be guided by the needs of potential data users and their intended applications. For example, datasets primarily used by citizens may benefit from minimal restrictions, while those likely to be commercially exploited may require attribution obligations.

To ensure alignment between your open data strategy and actual demand, conduct research and engage with potential data users: including businesses, researchers, non-profit organisations, and public authorities at local, regional, or national levels. This consultation will help verify that your open data supply corresponds to the needs of your community.

Step 3: Consultation with a legal expert

After gathering insights from external stakeholders, it is crucial to discuss your findings with a legal expert. This expert can identify potential legal challenges, assess the feasibility of licensing certain datasets, and recommend the most appropriate licences. They can also provide expert insights into copyright and intellectual property laws that non-specialists may not be familiar with.

Engaging a legal expert, whether from within the local administration or an external advisor, will equip you with solid arguments and a clearer understanding of licensing options, preparing you for discussions with internal stakeholders. Such internal stakeholders could be the mayor, the local council, senior public officials (department heads), the IT team, the different teams or agencies which collect data and others.

Step 4: Discussion with internal stakeholders and formal decision

This step is essential for two key reasons:

1. **Technical feasibility** - Internal stakeholders, particularly those involved in data collection and management, may identify technical constraints that impact licensing decisions. Their expertise is particularly valuable in assessing the applicability of licensing choices to future datasets.



2. **Institutional acceptance** - Ensuring broad support for the open data licensing strategy within your organisation is critical. Without internal consensus, conflicts may arise, leading to decreased motivation, inconsistent data collection practices, and potential misalignment with licensing goals. Additionally, licensing decisions often require formal approval from senior officials or local legislative bodies. Gaining buy-in from decision-makers is essential for successful implementation.

Step 5: Data governance and regular review of licensing decisions

Establishing an open data licence is not a one-time task, but part of an ongoing data governance process. Once licensing decisions have been implemented, it is important to develop mechanisms for monitoring compliance, managing updates, and incorporating user feedback. Over time, changes in legislation, data composition, or user needs may require updates to licensing terms or the addition of new licence types. Implement regular reviews of your licensing strategy to ensure that it remains legally sound and aligned with expectations of both internal and external stakeholders. Consider establishing a process through which data users can provide input or raise concerns related to licensing – this feedback can be invaluable in identifying issues and enhancing trust.

By following this structured, consultative approach, your organisation can develop a well-informed and widely accepted open data licensing strategy.

7.3 Examples of open data licensing

Population by District (CC0)

Your city plans to publish population data by district on its newly developed open data portal in both JSON and CSV formats. The dataset includes historical data and will be updated annually. Given that data collection requires minimal effort and there is a general expectation that such information should be publicly available, you decide that attribution is unnecessary. Additionally, you do not want to impose a formal citation requirement on citizens when they reference the data on social media or other platforms. To ensure maximum accessibility and ease of use, you opt for the **Creative Commons Zero (CC0)** licence, which places the data in the public domain.

Managed Individual Trees (CC-BY)

Your city aims to release detailed information on urban trees, including their location, species, maintenance status, and other attributes. This dataset will be available in JSON, CSV, and GIS formats, with updates every three months. Since the data collection process is complex and resource-intensive, you seek recognition for your efforts. Furthermore, you want to ensure that re-users provide a direct link to the dataset to enhance accessibility and visibility. Given that you do not anticipate frequent dataset integration or extensive commercial use, you choose the **Creative Commons Attribution (CC-BY)** licence, which requires users to credit your organisation when using the data.

Hiking Trail Network (ODbL)

Your municipality intends to publish geospatial data on eco-trails, hiking paths, and nature reserves in GIS format (WMS and WFS) with regular updates. The dataset includes route difficulty, trail length, GPS waypoints, points of interest, and trail conditions. Your primary goal is to promote outdoor recreation and tourism while ensuring that any improvements – such as updated trail maps or corrections – remain openly available. To prevent commercial applications from



modifying the data without sharing improvements back with the public, you opt for the **ODC Open Database Licence (ODbL)**. This share-alike licence ensures that any enhancements made to the dataset must also be shared under the same terms, keeping the data freely accessible while continuously improving.

7.4 Challenges in open data licensing

Third-party data ownership

In cases where datasets incorporate third-party data sources, licensing can become problematic, particularly when a share-alike obligation exists. If portions of the dataset are subject to a different licence, you may be unable to publish the full dataset under a less restrictive licence such as **CC0** or **CC-BY**. Before selecting a licence, carefully review data ownership and existing licensing agreements to ensure compliance.

Unclear publication consent

When datasets contain personal data – such as information collected in social or medical research, publication may require explicit consent from individuals. Even if the personal data represents only a small fraction of a larger dataset, failing to obtain clear consent can create legal and ethical challenges. In such cases, you may need to:

- Apply a more restrictive licence that limits reuse.
- Remove personal data with unclear legal status before publication.
- Delay publication until all consent issues are fully resolved.

Compatibility issues with share-alike licences

Licences that require derivative works to be shared under the same terms can create compatibility issues when integrating multiple datasets. This is particularly challenging with the **CC-BY-SA** licence, which applies to all derivative works, including reports, visualisations, and modified datasets. For instance, combining **CC-BY-SA** data with **CC0** or **ODbL** data in a new dataset may not be legally feasible, discouraging companies, researchers, and government agencies from using **CC-BY-SA** licensed datasets.

In contrast, **ODbL** presents fewer issues because it distinguishes between:

- Derivative databases (which must be shared under **ODbL**).
- Derivative works (such as visualisations or reports), which can be licensed more freely.

When selecting a share-alike licence, consider its impact on interoperability and ensure it aligns with your open data goals.

Compatibility issues with licensing metadata

Implementing licensing metadata across datasets is often challenging due to the decentralised nature of data management within local administrations. Different departments may use varying formats, structures, and standards, leading to inconsistencies or omissions in how licensing information is documented. This fragmentation can undermine the clarity and legal certainty of open data offerings. To address this, open data providers should establish internal guidelines and encourage the use of standardised metadata models, such as **DCAT-AP**, to ensure consistency and interoperability. Regular coordination between departments and support from a central data governance team can significantly improve metadata quality and reliability (Graux, 2025).



8. Security strategy

With the topic of open data, the line between transparency and privacy is increasingly hard to draw. As you embark on the journey of opening data, the dual challenge of making valuable datasets accessible while also safeguarding sensitive information will be faced sooner rather than later. Unlike traditional data environments, open data is designed to be widely shared, freely reused and integrated across systems and organisations. As highlighted before this openness is a strength, but can, if not managed appropriately, also be a risk. Once the data is put out, the control over what happens to it in use is significantly reduced. Even harmless appearing data can lead to unintended harm and privacy breaches. For example, mobility data might seem anonymised, yet when cross-referenced with further datasets, they can reveal personal behaviours and even trace back to individuals (data.europa.eu, 2024).

Example: The Netflix prize competition

What was supposed to be a USD 1-million prize competition with anonymised data for improving movie recommendation services, ended up in a lawsuit with the competition cancelled. In 2006 Netflix released a dataset containing several thousand movie ratings, created by over 400.000 Netflix subscribers. The user data was reduced to a numeric ID, to be able to track ratings belonging to the same user and the competition aimed to finding an algorithm for movie recommendations, which beat the Netflix accuracy at that time by a 10% gain. However, only a couple of weeks later, a PhD student was able to disclose private information by cross-referencing this supposedly anonymised data with another publicly available dataset, the movie ratings on IMDB. While one might argue this was “only” about movies, even just this unwanted publicised finding could expose more sensitive information, for example about political orientation. This incident became one of the most referenced examples of how “anonymised” data can be de-anonymised and potentially cause harm (Narayanan and Shmatikov, 2008).

Further, open data and open data platforms are susceptible to other forces: human error, targeted cyberattacks, misconfigurations and even the exploitation of seemingly harmless datasets for malicious purposes. Even just a single mishap, such as uploading the wrong version of a dataset or mislabelling permissions could potentially lead to exposure of sensitive information and legal consequences. Loss of public trust, legal actions, financial penalties and operational disruption are just a few consequences for such errors.

Proactive security strategies are therefore not just a technicality, they are essential components of ethical, reputable, and sustainable open data governance. Through data classification, risk assessments and privacy impact reviews, vulnerabilities can be anticipated and countered before they escalate into incidents. Therefore, a security strategy does not hinder transparency or the process of opening data, it enables it to be a protected system, build on a culture of openness and founded by trust (Kuttappa, n.d.).



8.1 Why is Data Security important?

- Meet compliance requirements and comply with global standards like GDPR and ISO 27001 (Stiftung Datenschutz, 2022).
- Build a culture of security awareness and responsibility by clearly outlining practices.
- Prevent data breaches and avoid loss of data and customer trust caused by security incidents, as well as legal and financial penalties.

Data security strategy is important because it is the practice of safeguarding and protecting the digital information from unauthorised access, as well as accidental loss, disclosure and modification, manipulation, or corruption throughout its entire lifecycle, from creation to destruction.

Data security strategies are influenced by:

- **Data Protection Laws and Regulations:** Ensure compliance with national and international data protection laws such as GDPR (EU), CCPA (California), or HIPAA (USA). This is especially relevant for sensitive or personally identifiable data. European legislation as well as legislation of other countries is more described in chapter 5.
- **Encryption and Secure Transfer:** Use encryption techniques (e.g., SSL/TLS) to secure data in transit, ensuring that data is protected when transferred between systems, particularly for sensitive or personal data.
 - TLS/SSL encryption is a very crucial security protocol for the internet. It provides a secure and private connection between servers and clients, which helps to protect sensitive data from prying eyes. The encryption process involves the use of cryptographic keys, which are used to encrypt and decrypt the data. The keys are unique to each session, ensuring that the data is protected from interception and tampering.
- **Access Control Mechanisms:** Implement role-based access controls (RBAC) to restrict access based on user roles and permissions. Only authorised users should be able to access sensitive data.
- **Data Anonymisation:** For public data containing personal or sensitive information, employ anonymisation or pseudonymisation techniques (e.g., removing or encrypting personally identifiable information) to safeguard individuals' privacy.
- **Security Audits and Monitoring:** Regularly perform security audits, vulnerability assessments, and continuous monitoring of systems that store or process public data to detect unauthorised access or security threats.
- **Data Integrity:** Use checksums or hash functions to ensure that data remains unaltered during transmission and storage, preventing corruption or tampering (IBM, n.d.)



8.2 Core principles of proactive security in Open Data

A set of core principles can aid in balancing transparency with protection. Key principles for a proactive security strategy include:

1. Privacy by Design

DO

- From the start, build anonymisation, data minimisation and aggregation into the data lifecycle.
- Use privacy-preserving techniques like aggregation or cryptographic technologies to protect personally identifiable information (PII)

DON'T

- Apply aggregation or de-identification only at the final stages before opening data.
- Assume removing IDs is sufficient to protect privacy.

2. Context-Aware Disclosure

DO

- Evaluate the dataset in context and consider what other datasets it might be combined with
- Assess the risk inference or re-identification before release

DON'T

- Forget to consider external linkability of your data.
- Forgo a real-world context analysis.

3. Continuous Risk Assessment

DO

- Regularly audit datasets and security threats
- Periodically update risk policies as technology and user behaviour evolves

DON'T

- Assume a one-time risk assessment is sufficient.
- Ignore emerging vulnerabilities or rely on existing methods.

4. Clear Governance and Accountability

DO

- Define roles and responsibilities for data stewardship, approval, and security oversight.
- Document decisions around data publishing, including decisions on data access and usage rules, data security and privacy guidelines, compliance with regulatory requirements (like GDPR), overall

data quality standards (Tip: Some universities publish their data governance documentation as templates)

DON'T

- Operate without transparency about roles and responsibilities, especially regarding approval and management of data releases.

5. Community Feedback and Transparency in Security Practices

DO

- Enable channels for reporting misuse or identified risks.
- Publish methodologies used for data protection and anonymisation methods

DON'T

- Obscure your data handling processes

(data.europa.eu, 2024; Kitchin, 2014)



8.3 Balancing privacy and utility in open data anonymisation

When opening data, two fundamental objectives must be considered: enabling public value through data reuse and protecting (individuals') fundamental rights. Under 26 GDPR, data is anonymous only if individuals are not identifiable “taking into account all the means reasonably likely to be used”. Where re-identification remains reasonably possible, the data remains personal data and subject to the GDPR (European Data Protection Board, 2025).

Not all Open Data requires anonymisation

Therefore, it is important to distinguish between;

- Non-personal data (e.g., weather data, traffic counts, air quality measurements, public procurement totals) → no anonymisation required
- Personal data (e.g., mobility traces, health records, detailed demographic microdata) → requiring protection
- Datasets that should not be published at all (e.g., small-population health registries with rare diseases) → anonymisation would either fail or destroy their value

Depending on the type of data, anonymisation is not a default obligation for all open data. However, where personal data is involved and publication serves a legitimate public interest anonymisation is crucial to consider (Alam et al., 2021; Gomede, 2023; Zigomitos et al., 2020).

When Publication Makes Sense Despite Anonymisation Needs

For certain datasets, anonymisation enables socially valuable publication:

- **Public health statistics** (e.g. infection rates by age group)
- **Mobility flow data** aggregated to city level
- **Education outcomes** by school district
- **Consumer complaint categories** without individual identifiers

In these cases, anonymisation reduces re-identification risk while preserving meaningful analytical value.

Methods and Practical Examples

Anonymisation should follow a structured, risk-based approach (Art. 5(2), 25 GDPR). The choice of method depends on the dataset and its intended analytical use.

Method	Example in Practice	Privacy Effect	Utility Impact
Removal of direct identifiers	Deleting names and ID numbers from a school dataset	Low alone (quasi-identifiers remain)	Minimal
Aggregation	Publishing unemployment rates per region instead of individual employment histories	High if groups sufficiently large	Loss of individual-level analysis
Pseudonymisation (Art. 4(5) GDPR)	Replacing names with unique codes for internal research	Risk reduction only; still personal data	High utility retained
k-anonymity	Generalising age (e.g. 34 -> 20–39) or postcode (5 digits -> 3 digits) so each combination appears at least k times	Protects against simple linkage	Reduces granularity
l-diversity/t-closeness	Ensuring that within each anonymised group multiple disease categories are present	Reduces attribute inference	Further distortion



Differential privacy	Adding calibrated noise to statistical outputs (e.g. census tables)	Strong protection against linkage attacks	Depends on ϵ ; affects accuracy
Synthetic data	Generating artificial patient records that preserve statistical distributions	Potentially high if model robust	May distort rare correlations

Figure 9: Anonymisation Methods

Source: Own compilation

Particularly in open data contexts, where datasets are publicly accessible and can be combined with external sources, the absence of contextual controls significantly increases linkage risk. Empirical research on k-anonymity shows that even compliant datasets may allow attribute inference when quasi-identifiers are linkable to external registers (Zigomitos et al., 2020)

Therefore, open data strategies should:

- Prefer aggregation or differential privacy for statistical releases.
- Explicitly consider evolving technological capabilities (Recital 26 GDPR).
- Avoid assuming anonymisation is “forever”; periodic reassessment is necessary
- Integrate anonymisation into data protection by design (Art. 25 GDPR). (AEPD-EDPS, 2021)

Ultimately, balancing privacy and utility in open data is not about achieving zero risk. It requires:

- 1) Identifying whether personal data is involved
- 2) Assessing whether publication is necessary and proportionate
- 3) Selecting suitable anonymisation techniques
- 4) Evaluating residual re-identification risk in light of public accessibility (Stiftung Datenschutz, 2022)
- 5) Documenting the assessment (accountability principle, Art. 5(2) GDPR)



9. Data publication and management

A quick recap and summary: Essentially, it takes four elements to publish open data:

1. Data in an open format,
2. A licence for this data,
3. Metadata, which provides information and describes characteristics of the data,
4. A place to publish the data.

In the following paragraphs, this section will take a dive into the necessary steps for the publication of open data and the continuous management.

9.1 Data as a resource for diverse re-use

This question might seem technical, but can be summarised in a few key points and examples:

A municipality might already publish a lot of information on their website. Formats may include web texts and information, which are provided in downloadable formats such as PDF documents or excel charts. As soon as a specific software is necessary to open a downloaded file, it is not considered to be an open format. Instead of using the quite common .xls (or similar) file format, CSV should be preferred as it is the simplest format and offers a broad potential for reuse. As for data published in PDF files, it must be noted that this format might seem very accessible to citizens. It does not, however, fulfil the requirement of machine-readability. Data published as PDF can therefore not be considered as open.

During initiatives to publish (more) open data and identifying possible datasets, an administration can already do a thorough check of what data is already published on its website - but in formats, which are not meeting the open data standards.

It might be helpful to think about the open data as the “raw” resource to be further interpreted, e.g. values separated by comma in CSV. To those, who are not yet familiar working with open data, this basic form itself can pose a challenge as this format seems not very practical and easy to read for many people. However, this basic format offers many more possibilities for re-use by both humans, who are interpreting the dataset and for applications, which are specifically built to re-use the dataset for a specific purpose. In a way, using the data to publish it with extra explanations in a PDF format can therefore be considered to be an interpretation of the raw data with a presentation for a specific target audience, e.g. citizens. The underlying data should be made available as open data as well.

9.2 How to find data: the importance of metadata

Publishing data only makes sense if the data is findable. It therefore needs to be accompanied by elements, which describe the published data. This is called metadata. Metadata is the information that explains what the data is about. It helps users understand how to use the data correctly. Municipal staff need to create simple, clear descriptions for each dataset. This includes the dataset title, a summary of what it contains, the time period it covers, who collected it, how often it is updated as well as any specific terms or codes used.



For those who are new to the topic of open data, think about a library catalogue. Here, each element which users can borrow is described with a set of categories: the title, the authors name, the publishing date, the publishing company, and edition. This helps to clearly identify the both the content as well as the organisation responsible for the work.

Providing good metadata makes the open data more useful and trustworthy, as is poignantly described in the following graphic:

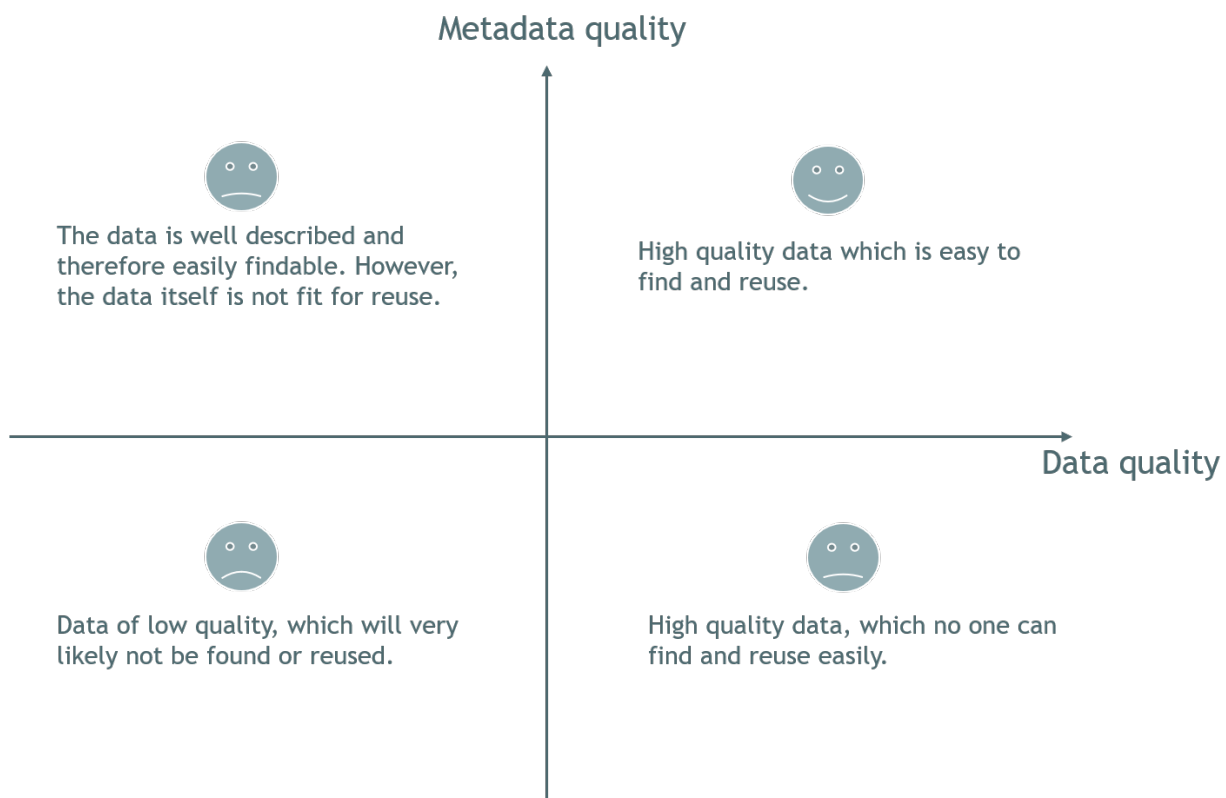


Figure 10: Why Good Data Needs Good Metadata
Source: Nielsen, 2025; own adaptation

9.3 Cleaning data

Before making data public, it needs to ensure that the data is accurate, consistent, and safe to share. This means checking for errors like typos or missing values, removing duplicate entries, and making sure private or sensitive information is not included. The data should also be formatted clearly, for example, using consistent date formats or categories.

Depending on the size of the dataset, this can be a time-consuming task. There are tools, which can help, such as the Open Data Editor created by the Open Knowledge Foundation (Open Knowledge Foundation, 2025). It can be accessed here: <https://opendataeditor.okfn.org/>.

The Open Data Editor is an open source and no-code software, which can help to validate datasets. It is installed locally as a desktop app. Uploaded files are therefore analysed locally on the user's computer.

Finding duplicates, however, can be a challenging task and not all duplicates will be found by supporting tools. Before publishing a dataset, it can be helpful to check what similar datasets published by other municipalities look like. The following resources can help to browse data published by other municipalities:



- the German [Musterdatenkatalog](#) (Bertelsmann Stiftung, n.d.)
- Open data portals of other cities, e.g. [City of Brussels](#) (City of Brussels, n.d.)
- Studies such as the [Use Case Observatory](#) can provide inspiration for what data was used for which services/reuse cases (Carsaniga et al., 2022)

9.4 Continuous data management

Publishing open data is only the first step—making it easy to find and access is just as important. If data is hidden deep within a website or spread across multiple locations, its usefulness drops significantly. Municipalities should aim to publish open data in a structured and user-friendly way. Linking your datasets to national or European portals can also help improve visibility beyond the local level. Additionally, clear responsibilities for the provision and management of open data should be established according to the roles explained in the chapter Data Governance - Roles and responsibilities.

Once published, open datasets must be actively managed and monitored to stay relevant and trustworthy. Data can become outdated, incomplete, or incorrect over time if it is not maintained. Municipalities should establish routines for regularly reviewing datasets – checking for broken links, updating information, and removing obsolete files. Clear update schedules and ownership responsibilities (e.g., “This dataset is updated quarterly by the Mobility Department”) can make an enormous difference in quality and user trust.

To manage this effectively, municipalities can set up a simple internal monitoring process. This might include assigning each department a data steward responsible for their datasets, creating a shared calendar of update deadlines, and using basic monitoring tools (like automated link checkers or Excel tracking sheets) to flag issues. Depending on the internal organisation, a central open data coordinator can oversee this process, offer support, and report on the overall status of the open data program. Regular internal reviews or open data “health checks” every 6 or 12 months can help to keep things running smoothly.

Proper data management also enables greater reuse of open data, which is where its real value lies. Well-maintained datasets can be used by app developers, local start-ups, researchers, journalists as well as other government bodies. These re-users rely on the data to be up to date and complete. For example, transport data might power a real-time transit app; environmental data could support citizen-led green projects. By ensuring datasets are updated, documented, and dependable, municipalities increase the chances that the community will use them in creative and impactful ways. Inviting feedback and highlighting successful reuse stories can further encourage engagement and innovation. The DoorCE project dives into this topic in the **Public Open Data Utilisation Strategy**.



Glossary of Terms

TERM	DESCRIPTION
Application programming interface (API)	Application programming interface (API) is a set of rules that allows two or more computer programs or components to communicate with each other.
App Builders	App Builders are design-to-code solutions that enable design and development teams to quickly and easily design and build real web applications.
Comprehensive knowledge archive network	Comprehensive knowledge archive network is an open-source data management system for powering data hubs and portals.
Data	Data are facts and statistics, collected to be examined and considered for reasoning, discussion, or calculation.
Data Acquisition	Data Acquisition (DAQ) refers to the process of converting real-world physical signals into digital data, enabling it to be displayed, analysed, and stored on a computer. For instance, capturing the temperature of a room using a thermocouple sensor and converting it into a digital format is a basic example. Contemporary DAQ systems often incorporate advanced features such as data analysis tools, reporting software, network integration, and options for remote control and monitoring.
Data Admin (Data custodian)	Data Admin (Data custodian) is responsible for the overall management of data resources in an organisation, including database planning, analysis, design, implementation, and maintenance.
Data Analytics	Data Analytics is the discipline focused on examining raw data to draw meaningful insights and conclusions. Many data analytics methods and processes have been automated through algorithms and mechanical systems, allowing for efficient processing of raw data for human interpretation. Various organisations, including businesses, use data analytics to enhance performance and boost profitability. This is achieved by leveraging specialised software and tools to collect, process, and analyse the raw data.
Data Archive	Data Archive is a storage solution for important data that does not require frequent access or modification. Businesses typically use data archives to store legacy information or to comply with regulatory requirements such as HIPAA, PCI-DSS, or GDPR. While the data remains accessible if needed, it is



	primarily kept for long-term preservation rather than regular use.
Data Attributes	Data Attributes refer to information used to describe or categorise an object or entity. Examples include characteristics such as color, gender, or yes/no responses. This type of data is often combined with other data types to provide deeper context and enhance analysis.
Data Check	Data Check is process used to confirm that the data entered has the correct data type.
Data Directory	Data Directory is a centralised repository that holds metadata critical for understanding and managing distributed databases and files. It offers a comprehensive view of the data overseen by various service units, encompassing master and replicated data, business data entities, as well as details on service unit responsibilities, data security protocols, and recovery procedures. This directory is essential for ensuring efficient data management and governance.
Data Metrics	Data Metrics are pieces of collected data that help measure against a stated goal. It is a quantitative measurement of data.
Data Protection	Data Protection is the practice of securing critical information from corruption, compromise, or loss, while also ensuring that it can be restored to a usable state if it becomes inaccessible or damaged. This process is vital for maintaining data integrity and availability in the event of an incident.
Data Quality	Data Quality assesses how effectively a dataset aligns with key criteria such as accuracy, completeness, validity, consistency, uniqueness, timeliness, and fitness for its intended purpose. Ensuring high data quality is essential for the success of data governance initiatives within an organisation.
Data Security	Data Security involves safeguarding digital information from unauthorised access, corruption, or theft throughout its entire lifecycle. This practice ensures the confidentiality, integrity, and availability of data, protecting it at every stage from creation to disposal.
Data Stamp	Data Stamp typically refers to a recorded marker that indicates when (and sometimes by whom) a piece of data was created, modified, or processed.
Data Structure	Data Structure is a method of organising and storing data within a computer to enable efficient access and utilisation. It encompasses both the logical or mathematical representation of data and its specific implementation within a computer program.



Data Usage	Data Usage is a handling, processing, and use of data for intended purposes, including data analysis, reporting, decision-making, research, and service delivery.
Data User	Data Users are a person involved in accessing and investigating integrated datasets for statistical and research purposes.
Data Validation	Data Validation is checking the accuracy and quality of source data before using, importing or otherwise processing data.
Data Validity Alert	Data Validity Alert ensures the accuracy, relevance, and format of that information within datasets.
Dataset	Dataset is a collection of data treated as a single unit.
Dataset Element	Dataset Element is a basic unit of information that has a unique meaning and subcategories of distinct value.
Extract, Transform, and Load (ETL)	Extract, Transform, and Load (ETL) is a process of combining data from multiple sources into a large, central repository called a data warehouse.
External user	External user is a particular product being used on the outside only and is not suitable for inside use.
GDPR (Legal) Officer	GDPR (Legal) Officer role is to ensure that the organisation processes the personal data of its staff, customers, providers or any other individuals in compliance with the applicable data protection rules.
Guided forms	Guided forms provide step-by-step experience to help your signers easily complete long or complex forms through questions that adapt based on previous answers.
Hackathon	Hackathon also known as a hack day, hackfest, datathon, or codefest. It is an event where participants engage in fast-paced, collaborative engineering over a short timeframe, typically 24 to 48 hours. During this intensive period, teams employ agile software development practices, such as sprint-based design, to work on various projects. Participants may include computer programmers, graphic designers, interface designers, product managers, project managers, domain experts, and others, all working together to create or improve software solutions.
Health Check System	The Health Check System is designed to help you identify areas of your system and internal processes that are working well for you, and areas that may need a little improvement.
HTTP	HTTP stands for Hypertext Transfer Protocol. It is an application protocol that defines a set of guidelines for transferring data, including text, images, and multimedia, over the World Wide Web (WWW).



	HTTP facilitates communication between web servers and clients by specifying how requests and responses should be formatted and transmitted.
Information seeker	An information seeker is an individual who actively seeks out information, either through sources such as libraries, databases, and other digital media, or through traditional methods such as books, magazines, and newspapers.
Internal user	Internal users are a person inside or an organisation that helps run its operations and uses the company's financial information to make decisions.
IoT device	IoT device is nonstandard computing hardware such as sensor, actuator or appliance, that connect wirelessly to a network and can transmit data.
JSON	JSON, or JavaScript Object Notation , is a lightweight, text-based format used for representing structured data. It is easy for humans to read and write and simple for machines to parse and generate. JSON is often used for data interchange between web applications and servers, and it is widely supported by programming languages for data storage and transmission.
Metadata	Metadata is data that provides information about other data, but not the content of the data itself, such as the text of a message or the image itself.
Metalanguage	Metalanguage helps in describing the concepts, grammar and objects associated with a particular programming language.
Open data	Open data is data that can be freely used, re-used and redistributed by anyone - subject only, at most, to the requirement to attribute and share alike.
Open Data Hubs	Open Data Hubs are the cross-border digital platform that helps start-ups, companies and research institutes to develop digital solutions based on real data.
Open Street Map	Open Street Map is the free and editable map of the world, created and maintained by huge international community.
Protocol MQTT	Protocol MQTT is a standards-based messaging protocol, or set of rules, used for machine-to-machine communication.
Quality controller (Data manager, Data steward)	Quality controller (Data manager, Data steward) is an expert who oversees product quality to guarantee it meets company, regulatory and consumer standards.
Real time data	Real time data refers to information that is made available for use as soon as it is generated.
Small and medium - sized enterprises (SME)	Small and medium-sized enterprises are businesses that maintain revenues, assets, or number of employees below a



	certain threshold. (Each country has its own definition of what constitutes a small and midsize enterprise.)
Spreadsheet	Spreadsheet is a file of rows and columns that helps sort, organise, and calculate data.
Time series	Time series is a series of data points indexed in time order.
TXT file	TXT file is a standard text document that contains plain text. It can be opened and edited in any text-editing or word-processing program.
Typist	Typists are people whose job is to type letters, reports, and other documents.
Universal data acquisition system	Universal data acquisition system is the method of sampling signals to measure real - world physical events
User Portal	User Portal , a private website companies use to provide clients with an easy, intuitive, and personalised entry point where information, documents, tools, links, and other services can be accessed anytime.
WordPress	WordPress is a free and open - source content management system that lets anyone create and manage websites easily.



Sources

- 1) AEPD-EDPS (2021) *10 misunderstandings related to anonymisation* [online]. Available at: https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf (Accessed: 16.04.2026).
- 2) Agenzia per l'Italia Digitale (2022) *Piano Triennale per l'Informatica nella Pubblica Amministrazione: Aggiornamento 2022-2024* [online]. Available at: https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pa_2022-2024.pdf (Accessed: 15.04.2026).
- 3) Agenzia per l'Italia Digitale (2023) *Open Data: AgID adotta le Linee Guida* [online, 03/08/2023]. Available at: <https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2023/08/03/open-data-agid-adotta-linee-guida> (Accessed: 15.04.2026).
- 4) Agenzia per la Cybersicurezza Nazionale (n.d.) *Strategia Nazionale di Cybersicurezza 2022-2026* [online]. Available at: <https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza> (Accessed: 15.04.2026).
- 5) AGID - Agenzia per l'Italia Digitale (2024) *Contesto normativo - dati.gov.it* [online]. Available at: <https://www.dati.gov.it/contesto-normativo> (Accessed: 23.03.2025).
- 6) AGID - Agenzia per l'Italia Digitale (2026) *dati.gov.it - Catalogo dei dati aperti della Pubblica Amministrazione* [online]. Available at: <https://www.dati.gov.it/> (Accessed: 23.03.2025).
- 7) Ajuntament de Barcelona (n.d.) *Mapa de data stories. Barcelona Dades* [online]. Available at: <https://portaldades.ajuntament.barcelona.cat/ca/map-datastories> (Accessed: 23.03.2026).
- 8) Ajuntament de Barcelona (n.d.) *Open Data BCN | Ajuntament de Barcelona's open data service* [online]. Available at: <https://opendata-ajuntament.barcelona.cat/en/> (Accessed: 23.03.2026).
- 9) ALLiance (n.d.) *Accueil IA dans l'État* [online]. Available at: <https://alliance.numerique.gouv.fr/> (Accessed: 15.04.2026).
- 10) Alohi Team (2024) *AI in Scanning: A Game-Changer in Digital Transformation* [online, 8 February]. Available at: <https://www.alohi.com/blog/ai-in-scanning-a-game-changer-in-digital-transformation> (Accessed: 10.04.2025).
- 11) Andrews, J. (2018) *Ghent: using the semantic web to connect data and meaning*, Cities Today [online]. Available at: <https://cities-today.com/how-ghent-is-using-the-semantic-web-to-connect-data-and-meaning> (Accessed: 23.03.2026).
- 12) Anmut (2024) *Data Governance Roles Explained: Data Owner, Steward & Custodian* [online]. Available at: <https://www.anmut.co.uk/data-governance-roles-and-responsibilities/> (Accessed: 31.03.2025).
- 13) Associazione on Data (2026) *Associazione onData, Substack* [online]. Available at: <https://ondata.substack.com/> (Accessed: 23.03.2026).
- 14) Ataccama (2021) *What is a Data Steward?* [online]. Available at: <https://www.ataccama.com/blog/what-is-a-data-steward/> (Accessed: 11.09.2024).
- 15) Becker, S., Altendeitering, M. (2024) *Interoperable Open Data Platforms: A Prototype for Sharing CKAN Data Sources*. In: International Conference on Data Science, Technology and Applications, 2024.
- 16) Bertelsmann Stiftung (n.d.) *Musterdaten katalog für Kommunen* [online]. Available at: <https://www.bertelsmann-stiftung.de/de/unsere-projekte/smart-country/musterdatenkatalog> (Accessed: 15.04.2026).



- 17) Bundeskanzleramt Österreich (n.d.) *data.gv.at: Open Data in Austria* [online]. Available at: <https://www.data.gv.at/> (Accessed: 23.03.2026).
- 18) Bundesministerium der Justiz, Bundesamt für Justiz (2016) *SGB IX - Sozialgesetzbuch Neuntes Buch - Rehabilitation und Teilhabe von Menschen mit Behinderungen* [online]. Available at: https://www.gesetze-im-internet.de/sgb_9_2018/BJNR323410016.html (Accessed: 15.04.2026).
- 19) Bundesministerium der Justiz, Bundesamt für Justiz (2017) *BDSG - Bundesdatenschutzgesetz* [online]. Available at: https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html (Accessed: 15.04.2026).
- 20) Bundesministerium der Justiz, Bundesamt für Justiz (2021) *TKG - Telekommunikationsgesetz* [online]. Available at: https://www.gesetze-im-internet.de/tkg_2021/ (Accessed: 15.04.2026).
- 21) Bundesministerium der Justiz, Bundesamt für Justiz (no date) *§ 12a EGovG - Offene Daten des Bundes, Verordnungsermächtigung. In: Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG)* [online]. Available at: https://www.gesetze-im-internet.de/egovg/_12a.html (Accessed: 15.04.2026).
- 22) Bundesministerium des Innern und für Heimat (BMI) (2025) *Open Data* [online]. Available at: <https://www.bmi.bund.de/DE/themen/moderne-verwaltung/open-government/open-data/open-data-node.html;jsessionid=B024ECF7492FBCF5E88CE79D01F38B09.live862#Start> (Accessed: 28.05.25).
- 23) Bundesministerium für Digitales und Verkehr (BMDV) (2021) *Federal Act enacting a Telecommunications Act (Telecommunications Act - TKG 2021)* [online]. Available at: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2021_1_190/ERV_2021_1_190.pdf (Accessed 28.05.2025).
- 24) Camera dei Deputati (2022) *Protezione dei dati personali* [online]. Available at: https://temi.camera.it/leg18/temi/la_protezione_dei_dati_personali.html (Accessed 28.03.2025).
- 25) Carsaniga, G., Dogger, J., Regeczi, D. (2022) *The Use Case Observatory: A 3-year monitoring of 30 reuse cases to understand the economic, governmental, social and environmental impact of open data. Volume I* [online]. Available at: https://data.europa.eu/sites/default/files/report/The_Use_Case_Observatory_Volume_I_0.pdf (Accessed: 15.04.2026).
- 26) Central State Office for the Development of the Digital Society (n.d.) *data.gov.hr: Open Data Portal* [online]. Available at: <https://data.gov.hr/> (Accessed: 23.03.2026).
- 27) City of Brussels (n.d.) *Open Data City of Brussels* [online]. Available at: <https://opendata.brussels.be/explore/> (Accessed: 15.04.2026).
- 28) City of Helsinki (n.d.) *Digital Helsinki* [online]. Available at: <https://www.hel.fi/en/decision-making/information-on-helsinki/design-and-digitalisation/digital-helsinki> (Accessed: 23.03.2026).
- 29) City of Munich (2022) *Öffentliche Sitzung der Vollversammlung vom 18. Mai 2022. Beschlussseite zu TOP B 21* [online]. Available at: <https://risi.muenchen.de/risi/dokument/v/7178007> (Accessed 31.05.2025).
- 30) City of Vienna (2019) *Data Excellence Strategy of the City of Vienna* [online]. Available at: <https://digitales.wien.gv.at/en/data-excellence-strategy-of-the-city-of-vienna/> (Accessed: 23.03.2026).
- 31) City of Vienna (2021) *Open Access to a wide range of municipal data* [online]. Available at: <https://smartcity.wien.gv.at/en/open-government-data-2> (Accessed: 23.03.2026).
- 32) City of Zurich (2021) *Statistik Stadt Zürich, Reglement über offene Verwaltungsdaten, Neuerlass; Strategie Open Government Data 2030 der Stadt Zürich, Genehmigung und*



- Verbindlichkeitserklärung* [online]. Available at: https://www.stadt-zuerich.ch/dam/web/de/politik-verwaltung/politik-recht/stadtratsbeschluesse/2021/Jul/StZH_STRB_2021_0743.pdf (Accessed 31.05.2025).
- 33) Climate Data Store (2026) *Climate Data Store* [online]. Available at: <https://cds.climate.copernicus.eu/#!/home> (Accessed: 15.04.2026).
- 34) CMS legal (2024) *Data protection and cybersecurity laws in Austria* [online]. Available at: <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/austria> (Accessed: 28.05.2025).
- 35) CMS legal (2024) *Data protection and cybersecurity laws in Germany* [online]. Available at: <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/germany> (Accessed: 28.05.2025).
- 36) CPO Magazine (2022) *Data Owners vs. Data Stewards vs. Data Custodians – The 3 Types of Data Masters and Why You Should Employ Them* [online]. Available at: <https://www.cpomagazine.com/cyber-security/data-owners-vs-data-stewards-vs-data-custodians-the-3-types-of-data-masters-and-why-you-should-employ-them/> (Accessed: 11.09.2024).
- 37) Creative Commons (n.d.a) *Attribution 4.0 International* [online]. Available at: <https://creativecommons.org/licenses/by/4.0/> (Accessed: 15.04.2026).
- 38) Creative Commons (n.d.b) *Attribution-ShareAlike 4.0 International* [online]. Available at: <https://creativecommons.org/licenses/by-sa/4.0/> (Accessed: 15.04.2026).
- 39) Creative Commons (n.d.c) *Sharing openly, sharing globally* [online]. Available at: <https://creativecommons.org/cc-licenses/> (Accessed: 15.04.2026).
- 40) DAMA International (2017) *DAMA-DMBOK: Data management body of knowledge*. 2nd edn. Basking Ridge, NJ: Technics Publications.
- 41) data.europa.eu (2014) *Data and metadata licensing* [online]. Available at: https://data.europa.eu/sites/default/files/d2.1.2_training_module_2.5_data_and_metadata_licensing_en_edp.pdf (Accessed: 15.04.2026).
- 42) data.europa.eu (2022) *High-value datasets - an overview through visualisation* [online, 23 November 2022]. Available at: <https://data.europa.eu/en/publications/datastories/high-value-datasets-overview-through-visualisation> (Accessed: 15.04.2026). The page credits the article to Davide Mancino and states that the website is managed by the Publications Office of the European Union.
- 43) data.europa.eu (2024) *Cybersecurity and open data: Balancing transparency and protection* [online, 11 October]. Available at: <https://data.europa.eu/en/news-events/news/cybersecurity-and-open-data-balancing-transparency-and-protection>. (Accessed 31.05.2025).
- 44) data.europa.eu (2025a) *Open Data Maturity Report 2025*. Available at: <https://data.europa.eu/en/open-data-maturity/2025> (Accessed: 23.03.2026).
- 45) data.europa.eu (2025b) *Introducing open data* [online]. Available at: <https://data.europa.eu/en/academy/introducing-open-data> (Accessed: 12.03.2025).
- 46) data.europa.eu (n.d.) *Licensing assistant: licences* [online]. Available at: <https://data.europa.eu/licensing-assistant/licences?locale=en> (Accessed: 15.04.2026).
- 47) data.europa.eu (n.d.) *Understanding the legal side of open data* [online]. Available at: <https://data.europa.eu/en/academy/understanding-legal-side-open-data> (Accessed: 15.04.2026).
- 48) data.europa.eu (n.d.) *Why do we need to license?* [online]. Available at: <https://data.europa.eu/academy/learn/mod/url/view.php?id=254&forceview=1> (Accessed: 15.04.2026).



- 49) data.europa.eu (n.d.a) *Data governance and introduction to the foundations of data spaces / Data spaces: Introducing the concept and the relevance in today's world* [online]. Available at: <https://data.europa.eu/academy/learn/mod/lesson/view.php?id=260&pageid=137> (Accessed: 15.04.2026).
- 50) data.europa.eu (n.d.b) *Data Sharing and licensing in the public sector / Understanding open data: Legal openness* [online]. Available at: <https://data.europa.eu/academy/learn/mod/lesson/view.php?id=253&pageid=130> (Accessed: 15.04.2026).
- 51) data.europa.eu (2026a) *The official portal for European data* [online]. Available at: <https://data.europa.eu/en> (Accessed: 23.03.2026).
- 52) data.europa.eu (2026b) *What is open data* [online]. Available at: <https://data.europa.eu/en/dataeuropa-academy/what-open-data> (Accessed: 23.03.2026).
- 53) DataGuidance (2024) *Poland: Ministry of Digitization launches public consultations on the implementation of the Digital Services Act* [online]. Available at: https://www.dataguidance.com/news/poland-ministry-digitization-launches-public_ (Accessed: 28.03.2025).
- 54) DataScientest (2023) *Data Custodian: Role, missions and skills* [online]. Available at: <https://datascientest.com/en/data-custodian-role-missions-and-skills#:~:text=What%20is%20a%20data%20custodian%3F%20Also%20known%20as,database%20to%20ensure%20it%20remains%20accessible%20and%20secure> (Accessed: 11.12.2024).
- 55) Dati.gov.it (2026) *Home Page* [online]. Available at: <https://www.dati.gov.it> (Accessed: 23.03.2026).
- 56) datiBeneCommune (2026) *Liberiamoli tutti!, Substack* [online]. Available at: <https://datibenecomune.substack.com/> (Accessed: 23.03.2026).
- 57) DatiOpen.it (2025) *Portale italiano di Open Data* [online]. Available at: <http://www.datiopen.it/> (Accessed: 28.03.2025).
- 58) Davies, T., Walker, S., Rubinstein, M., Perini, F. (eds.) (2019) *The State of Open Data: Histories and Horizons*. Cape Town and Ottawa.
- 59) dejure.org (no date) *Telemediengesetz (TMG)* [online]. Available at: <https://dejure.org/gesetze/TMG> (Accessed: 15.04.2026).
- 60) Direction interministérielle du numérique (DINUM) (n.d.) *data.gouv.fr* [online]. Available at: <https://www.data.gouv.fr/> (Accessed: 23.03.2026).
- 61) Dodds, L. (2013) *Publisher's Guide to Open Data Licensing* [online, 15 December 2013]. Available at: <https://theodi.org/insights/guides/publishers-guide-to-open-data-licensing/> (Accessed: 31.05.2025).
- 62) Dodds, L. (2013) *Reuser's Guide to Open Data Licensing* [online]. Available at: <https://theodi.org/insights/guides/reusers-guide-to-open-data-licensing/> (Accessed: 31.05.2025).
- 63) DQOps (2024) *Data Owner vs Data Steward vs Data Custodian, Role Definition and Responsibilities* [online]. Available at: <https://dqops.com/data-owner-data-steward-data-custodian-roles/> (Accessed: 31.03.2024).
- 64) Dremio (2024) *Data Custodian* [online]. Available at: <https://www.dremio.com/wiki/data-custodian/> (Accessed: 31.03.2025).
- 65) Državni zbor Republike Slovenije (2005) *Zakon o Informacijskem pooblaščenju (ZInfP)* [online, 16. 12. 2005]. Available at: <https://pisrs.si/pregledPredpisa?id=ZAKO4498> (Accessed: 15.04.2026).



- 66) Državni zbor Republike Slovenije (2022) *Zakon o varstvu osebnih podatkov (ZVOP-2)* [online, 27. 12. 2022]. Available at: <https://pisrs.si/pregledPredpisa?id=ZAKO7959> (Accessed: 15.04.2026).
- 67) Enterprise Warehousing Solutions (2025) *Data Steward Roles and Responsibilities: A complete Guide* [online]. Available at: <https://www.ewsolutions.com/data-stewardship-roles-a-complete-guide/> (Accessed: 28.03.2025).
- 68) EUR-Lex (2023) *Open data and the reuse of public-sector information* [online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4405374> (Accessed: 22.04.2025).
- 69) European Commission (2003) *Directive (EU) 2003/98/EC of the European Parliament and the Council of 17 November 2003 on the re-use of public sector information, Official Journal of the European Union* [online], L 345, pp. 90-96. Available at: <https://eur-lex.europa.eu/eli/dir/2003/98/oj/eng> (Accessed: 23.03.2026).
- 70) European Commission (2020) *A European strategy for data. COM(2020) 66 final* [online, 19 February 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066> (Accessed: 15.04.2026).
- 71) European Commission (2020a) *The Economic Impact of Open Data: Opportunities for value creation in Europe* [online]. Available at: <https://data.europa.eu/sites/default/files/the-economic-impact-of-open-data.pdf> (Accessed: 16.05.2025).
- 72) European Commission (2020b) *A European strategy for data, COM(2020) 66 final* [online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066> (Accessed: 23.03.2026).
- 73) European Commission (2022) *Open Data Best Practices in Europe: Estonia, Slovenia & Ukraine* [online]. Available at: https://data.europa.eu/sites/default/files/report/Open_Data_Best_Practices_in_Europe_Estonia_Slovenia_and_Ukraine.pdf (Accessed: 28.03.2025).
- 74) European Commission (2024a) *A European strategy for data* [online]. Available at: <https://digital-strategy.ec.europa.eu/en/policies/strategy-data> (Accessed: 28.03.2025).
- 75) European Commission (2024b) *Data Act* [online]. Available at: <https://digital-strategy.ec.europa.eu/en/policies/data-act#:~:text=The%20Data%20Act%20is%20a%20comprehensive%20initiative%20to,rights%2C%20while%20ensuring%20the%20protection%20of%20personal%20data> (Accessed: 28.03.2025).
- 76) European Commission (2024c) *European legislation on open data 2024* [online]. Available at: <https://digital-strategy.ec.europa.eu/en/policies/legislation-open-data> (Accessed: 28.05.2025).
- 77) European Commission (2026) *NIS2-Richtlinie: Sicherung von Netz- und Informationssystemen. Gestaltung der digitalen Zukunft Europas* [online, last updated 20 January 2026]. Available at: <https://digital-strategy.ec.europa.eu/de/policies/nis2-directive> (Accessed: 23.03.2026).
- 78) European Council (2024) *The general data protection regulation* [online, 13 June 2024]. Available at: <https://www.consilium.europa.eu/en/policies/data-protection-regulation/> (Accessed: 28.03.2025).
- 79) European Data Protection Board (2021) *Our Members* [online]. Available at: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en (Accessed: 28.03.2025).
- 80) European Data Protection Board (2025) *Guidelines 01/2025 on Pseudonymisation* [online]. Available at: https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf (Accessed: 16.04.2026).
- 81) European Environment Agency (2026) *European Environment Agency* [online]. Available at: <https://www.eea.europa.eu/en> (Accessed: 15.04.2026).



- 82) European Parliament and Council of the European Union (2016) *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 repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. *Official Journal of the European Union*, L 119, pp. 1-88 [online]. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (Accessed: 15.04.2026).
- 83) European Parliament and Council of the European Union (2023) *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 and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance)*. *Official Journal of the European Union*, L 2023/2854, 22 December [online]. Available at: <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng> (Accessed: 15.04.2026).
- 84) European Union (2016) *Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*. *Official Journal of the European Union* [online, 4 May 2016], L 119, pp. 89-131. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680> (Accessed: 28.05.2025).
- 85) European Union (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard of the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. *Official Journal of the European Union*, L 119, 4 May, pp. 1-88 [online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679> (Accessed: 28.05.2025).
- 86) European Union (2018) *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard of the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decisions No 1247/2002/EC*. *Official Journal of the European Union*, L 295, 21 November, pp. 39-98 [online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1725> (Accessed: 28.05.2025).
- 87) European Union (2018) *Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance)*. *Official Journal of the European Union*, L 303, 28 November, pp. 59-68 [online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1807> (Accessed: 28.05.2025).
- 88) European Union (2019) *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) "Open Data Directive"*. *Official Journal of the European Union* [online, 26 June 2019], L 172, pp. 56-83. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L1024> (Accessed: 28.05.2025).
- 89) European Union (2021) *The Data Governance Act & The Open Data Directive* [online]. Available at: <https://data.europa.eu/en/publications/datastories/data-governance-act-open-data-directive> (Accessed: 28.05.2025).
- 90) European Union (2022) *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)* [online], L 152, pp. 1-44. Available at: <https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng> (Accessed: 23.05.2026).



- 91) European Union (2023) *Data Governance Act became applicable on 24 September* [online]. Available at: <https://data.europa.eu/en/news-events/news/data-governance-act-became-applicable-24-september#:~:text=The%20regulation%20is%20to%20establish%20structures%20and%20processes,and%20organisations%20with%20greater%20control%20over%20their%20data> (Accessed: 22.04.2025).
- 92) European Union (2025) *Data protection under GDPR* [online]. Available at: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.html (Accessed: 28.03.2025).
- 93) Federalismi.it (eds.) (2022) *I dati aperti in Italia: un focus sull'openness digitale dei Comuni* [online]. Available at: <https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=48199> (Accessed 28.03.2025).
- 94) Firican, G. (2020) *The main responsibilities of a Data steward* [online]. Available at: <https://www.lightsondata.com/main-responsibilities-of-a-data-steward/> (Accessed: 28.03.2025).
- 95) FORUM PA (2020) *Open Data: cosa sono, come sfruttarli e stato dell'arte in Italia* [online]. Available at: <https://www.forumpa.it/pa-digitale/open-data-cosa-sono-come-sfruttarli-e-stato-dellarte-in-italia/> (Accessed: 28.03.2025).
- 96) Garante per la protezione dei dati personali (2016) *The Italian Data Protection Authority: who we are* [online], Roma: Garante per la protezione dei dati personali. Available at: <https://www.garanteprivacy.it/web/garante-privacy-en/the-italian-data-protection-authority-who-we-are> (Accessed: 28.03.2025).
- 97) GeeksforGeeks (2025) *What is an API* [online]. Available at: <https://www.geeksforgeeks.org/what-is-an-api/> (Accessed: 20.09.2024).
- 98) Gomedes, E. (2023) *Data anonymization: Balancing privacy and utility* [online]. The Modern Scientist. Available at: <https://medium.com/the-modern-scientist/data-anonymization-balancing-privacy-and-utility-6ae6ceb1ebf7> (Accessed: 15.04.2026).
- 99) Gov.pl (2021) *Nowa ustawa o otwartych danych* [online]. Available at: <https://www.gov.pl/web/ia/nowa-ustawa-o-otwartych-danych> (Accessed: 28 May 2025).
- 100) GovData (n.d.a) *GovData - Das Datenportal für Deutschland* [online]. Available at: <https://www.govdata.de/> (Accessed: 23.03.2026).
- 101) GovData (n.d.b) *Datenlizenz Deutschland - Zero - Version 2.0* [online]. Available at: <https://www.govdata.de/dl-de/zero-2-0> (Accessed: 15.04.2026).
- 102) Grady, A., MoldStud Research Team (2024) *The Impact of IoT on Network Administration* [online]. Available at: <https://moldstud.com/articles/p-the-impact-of-iot-on-network-administration> (Accessed: 11.09.2024).
- 103) Graux, H. (2025) *Report on licence usage on the data.europa.eu portal: An analysis of trends, practices, and recommendations for data providers* [online]. Available at: <https://data.europa.eu/sites/default/files/report/Report%20on%20licence%20usage%20on%20the%20data.europa.eu%20portal.pdf> (Accessed: 15.04.2026).
- 104) GTFS.org (2026): *General Transit Feed Specification* [online]. Available at: <https://gtfs.org/> (Accessed: 23.03.2026).
- 105) Hall, M. (2021) *Which open licence should I choose?* [online]. Agile. Available at: <https://agilescientific.com/blog/2021/2/17/which-open-licence-should-i-choose> (Accessed: 15.04.2026).
- 106) Helsinki Region Infoshare (n.d.) *Helsinki Region Infoshare - Open data service*. Available at: https://hri.fi/en_gb/ (Accessed: 23.03.2026).



- 107) Helsinki Region Infoshare (n.d.) *How to open data?* [online]. Available at: https://hri.fi/en_gb/support/how-to-open-data/ (Accessed: 23.03.2026).
- 108) Herzberg, B. (2021) *The Datamasters: Data Owners vs. Data Stewards vs. Data Custodians* [online]. Available at: <https://blog.satoricyber.com/the-datamasters-data-owners-vs-data-stewards-vs-data-custodians/> (Accessed: 10.09.2024).
- 109) Hrvatski sabor (2013) *Zakon o pravu na pristup informacijama* [online, 21 February 2013]. Available at: https://mfin.gov.hr/UserDocsImages/dokumenti/sluzbenik_za_informiranje/Zakon%20o%20pravu%20na%20pristup%20informacijama.pdf (Accessed: 15.04.2026).
- 110) Huwise (2026) *Homepage* [online]. Available at: <https://hub.huwise.com/pages/home/> (Accessed: 15.04.2026).
- 111) IBM (n.d.) *Data protection strategy: Key components and best practices*, IBM Think [online]. Available at: <https://www.ibm.com/think/insights/data-protection-strategy> (Accessed: 23.03.2026).
- 112) Information Commissioner of the Republic of Slovenia (2026) *Official website* [online]. Available at: <https://www.ip-rs.si/> (Accessed: 28.03.2025).
- 113) JUSLINE Österreich (2026) *Bundesverfassungsgesetz Österreich Art. 20 B-VG 2026* [online]. Available at: <https://www.jusline.at/gesetz/b-vg/paragraf/artikel20> (Accessed: 28.05.2025).
- 114) Kastouni, M. Z., Lahcen, A. A. (2022) *Big data analytics in telecommunications: Governance, architecture and use cases*. In: Journal of King Saud University-Computer and Information Sciences, 34(6), 2758-2770.
- 115) Kitchin, R. (2014) *The Data Revolution: Big data, open data, data infrastructures and their consequences*. Los Angeles.
- 116) Korn, N., Oppenheim, C. (2011) *Licensing Open Data, A Practical Guide* [online, May 2011]. Available at: https://www.e-education.psu.edu/geog585/sites/www.e-education.psu.edu/geog585/files/lesson9/Licensing_Open_Data_A_Practical_Guide.pdf (Accessed: 31.05.2025).
- 117) Krabina, B. (2023) *A Guideline for Open Data* [online]. Available at: https://www.data.gv.at/wp-content/uploads/2023/07/Open_Data_Guideline.pdf (Accessed: 23.04.2025).
- 118) Krabina, B. (2023) *Offene Daten der Zivilgesellschaft, Ein Leitfaden für die Praxis*. [online]. Available at: https://www.bertelsmann-stiftung.de/fileadmin/files/PicturePark/2023-12/Krabina_BST_Open_Data_Leitfaden_231204.pdf (Accessed: 31.05.2025).
- 119) Kuttappa, S. (n.d.) *Data security: Why a proactive stance is best* [online]. IBM. Available at: <https://www.ibm.com/think/insights/data-security-strategy> (Accessed: 15.04.2026).
- 120) Kutz, J. (2025) *What is Data Extraction? Data Extraction Techniques* [online]. Available at: <https://airbyte.com/data-engineering-resources/data-extraction> (Accessed: 10.04.2025).
- 121) Lancom Systems (2026) *Network security according to NIS2, Requirements and areas of the new NIS2 directive* [online]. Available at: <https://www.lancom-systems.com/solutions/network-security/network-security-according-to-nis2-directive> (Accessed: 23.03.2026).
- 122) LawyersSlovakia.com (2024) *GDPR Legislation in Slovakia* [online]. Available at: <https://lawyerslovakia.com/gdpr-legislation-in-slovakia/> (Accessed: 28.03.2025).
- 123) Lnenicka, M. (2022) *Transparency of open data ecosystems in smart cities: Definition and assessment of the maturity of transparency in 22 smart cities* [online]. Available at:



- <https://www.sciencedirect.com/science/article/abs/pii/S2210670722002281> (Accessed: 14.04.2025).
- 124) Lu, T., Neng, W. (2010) *Future Internet of Things* [online]. Available at: https://web.archive.org/web/20171013174223id_/http://metalab.uniten.edu.my:80/-azie/AllArt/Future%20Internet%20_%20The%20Internet%20of%20Things%20-%20Lu%20Tan.pdf (Accessed: 11.09.2024).
- 125) Malec, M. (2025) *Understanding data governance responsibilities: A comprehensive 2025 guide* [online]. Available at: https://hatchworks.com/blog/data-governance/data-governance-responsibilities/#:-:text=Core%20Responsibilities%20in%20Data%20Governance%201%20Ensuring%20Data,balance%20between%20accessibility%20and%20security%20is%20key.%20_ (Accessed: 31.03.2025).
- 126) Marzano, F. (2023) *Dati aperti. Che cosa sono e perché sono importanti nella PA?* [online, 20 novembre 2023]. Available at: https://www.repubblica.it/tecnologia/blog/open-government-2050/2023/11/20/news/dati_aperti_che_cosa_sono_e_perche_sono_importanti_nella_pa-420824018/ (Accessed: 28 March 2025).
- 127) Milvus (2026) *What is the role of collaboration in data governance?* [online]. Available at: <https://blog.milvus.io/ai-quick-reference/what-is-the-role-of-collaboration-in-data-governance> (Accessed: 01.04.2025).
- 128) Ministerstwo Cyfryzacji (2024) *Będziemy bezpieczniejsi w sieci - w życie wchodzi przepisy Aktu o usługach cyfrowych (DSA)* [online]. Available at: <https://www.gov.pl/web/cyfryzacja/bedziemy-bezpieczniejsi-w-sieci--w-zycie-wchodza-przepisy-aktu-o-uslugach-cyfrowych-dsa> (Accessed: 28.03.2025).
- 129) Ministrstvo za javno upravo (2020) *Odpri podatki javnega sektorja - strateški delovni načrt za 2020-2021* [online]. Available at: https://podatki.gov.si/sites/default/files/reports/Open%20Data_Strates%CC%8Cki%20delovni%20plan_julij2020.pdf (Accessed: 15.04.2026).
- 130) Ministry of Digital Affairs (n.d.) *Otwarte Dane / dane.gov.pl* [online]. Available at: <https://dane.gov.pl/> (Accessed: 23.03.2026).
- 131) Ministry of Investment, Regional Development and Informatization of the Slovak Republic (n.d.) *data.gov.sk* [online]. Available at: <https://data.slovensko.sk/> (Accessed: 23.03.2026).
- 132) Ministry of Public Administration for the Government of the Republic of Slovenia (2015) *Public Administration 2020: Public Administration Development Strategy 2015-2020* [online, 29 April 2015]. Available at: https://www.gov.si/assets/ministrstva/MJU/Kakovost-in-inovativnost-v-javni-upravi/Strategija/Strategija_razvoja_ANG_final_web.pdf (Accessed: 15.04.2026).
- 133) Ministry of Public Administration of the Republic of Slovenia (n.d.) *OPSI: Open Data Slovenia* [online]. Available at: <https://nio.gov.si/en/products/portal%20Bodprti%20podatki%20Slovenije-744> (Accessed: 23.03.2026).
- 134) Narayanan, A., Shmatikov, V. (2008) *Robust De-anonymization of Large Sparse Datasets* [online]. Available at: <https://pdfs.semanticscholar.org/2e8b/9a7a085a8bc18783e76b776c6e780116efd8.pdf> (Accessed: 15.04.2026).
- 135) Národná rada Slovenskej republiky (2000) *Zákon č. 211/2000 Z. z. zo 17. mája 2000 o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií)* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2000/211/?ucinnost=07.05.2025> (Accessed: 15.04.2026).



- 136) Národná rada Slovenskej republiky (2011) *Zákon o elektronických komunikáciách* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2011/351/20200909> (Accessed: 15.04.2026).
- 137) Národná rada Slovenskej republiky (2013) *Zákon č. 305/2013 Z. z. zo 4. septembra 2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2013/305/> (Accessed: 15.04.2026).
- 138) Národná rada Slovenskej republiky (2018a) *Zákon č. 18/2018 Z. z. z 29. novembra 2017 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov* [online]. Available at: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/18/vyhlasene_znenie.html (Accessed: 15.04.2026).
- 139) Národná rada Slovenskej republiky (2018b) *Zákon č. 69/2018 Z. z. z 30. januára 2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/20200701> (Accessed: 15.04.2026).
- 140) Národná rada Slovenskej republiky (2019) *Zákon č. 95/2019 Z. z. z 27. marca 2019 o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2019/95/20190501> (Accessed: 15.04.2026).
- 141) Národná rada Slovenskej republiky (2021) *Zákon č. 310/2021 Z. z. z 24. júla 2021, ktorým sa mení a dopĺňa zákon č. 177/2018 Z. z. o niektorých opatreniach na znižovanie administratívnej záťaže využívaním informačných systémov verejnej správy a o zmene a doplnení niektorých zákonov (zákon proti byrokracii) v znení zákona č. 221/2019 Z. z. a ktorým sa menia a dopĺňajú niektoré zákony* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2021/310/20240101> (Accessed: 15.04.2026).
- 142) Nielsen, C. (2025) *Metadata quality approach from Danish Agency for Digital Government*. In: *From Data to Metadata: enhancing quality across borders* [online]. Available on: <https://data.europa.eu/sites/default/files/course/Webinar%20%27From%20data%20to%20metadata%27%20-%20Slides.pdf> (Accessed: 28.05.2025).
- 143) Normattiva (1990) *Legge 7 agosto 1990, n. 241: Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi* [online]. Available at: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1990-08-07;241> (Accessed: 15.04.2026).
- 144) Normattiva (2003) *Decreto legislativo 30 giugno 2003, n. 196: Codice in materia di protezione dei dati personali* [online]. Available at: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196%21vig=> (Accessed: 15.04.2026).
- 145) Normattiva (2005) *Decreto legislativo 7 marzo 2005, n. 82: Codice dell'amministrazione digitale* [online]. Available at: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82!vig=> (Accessed: 15.04.2026).
- 146) Normattiva (2006) *Decreto legislativo 24 gennaio 2006, n. 36: Attuazione della direttiva 2003/98/CE relativa al riutilizzo di documenti nel settore pubblico* [online]. Available at: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2006-01-24;36!vig=> (Accessed: 15.04.2026).
- 147) Normattiva (2012) *Decreto-legge 18 ottobre 2012, n. 179: Ulteriori misure urgenti per la crescita del Paese* [online]. Available at: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2012;179> (Accessed: 15.04.2026).
- 148) Normattiva (2013) *Decreto legislativo 14 marzo 2013, n. 33: Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni* [online]. Available at:



<https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2013-03-14;33>
(Accessed: 15.04.2026).

- 149) Normattiva (2016) *Decreto legislativo 25 maggio 2016, n. 97: Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche* [online]. Available at: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2016;097> (Accessed: 15.04.2026).
- 150) Normattiva (2018) *Decreto legislativo 18 maggio 2018, n. 65: Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione* [online]. Available at: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2018;65> (Accessed: 15.04.2026).
- 151) Normattiva (2020) *Decreto-legge 16 luglio 2020, n. 76: Misure urgenti per la semplificazione e l'innovazione digitale* [online]. Available at: <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2020-07-16&atto.codiceRedazionale=20G00096&atto.articolo.numero=0&qId=&tabID=0.4407254915755261&title=lbl.dettaglioAtto> (Accessed: 15.04.2026).
- 152) Oesterreich.gv.at (2024) *Veröffentlichung im Bundesgesetzblatt: Informationsfreiheitsgesetz* [online]. Available at: <https://www.oesterreich.gv.at/.syndication?pagelId=ff158169-82bb-41c6-8389-6615a146c0c1> (Accessed: 28.05.2025).
- 153) Office for Personal Data Protection of the Slovak Republic (2023) *Rights of the Data Subjects* [online]. Available at: <https://dataprotection.gov.sk/en/rights-data-subjects/rights-data-subjects/> (Accessed: 28.03.2025).
- 154) Open Data Charter (n.d.) *ODC Principles* [online]. Available at: <https://opendatacharter.org/principles/> (Accessed: 23.03.2026).
- 155) Open Data Commons (2025) *Licenses FAQ* [online]. Available at: <https://opendatacommons.org/faq/licenses/> (Accessed: 31.05.2025).
- 156) Open Data Commons (n.d.a) *Open Data Commons Attribution License (ODC-By)* [online]. Available at: <https://opendatacommons.org/licenses/by/> (Accessed: 15.04.2026).
- 157) Open Data Commons (n.d.b) *Open Data Commons Open Database License (ODbL)* [online]. Available at: <https://opendatacommons.org/licenses/odbl/> (Accessed: 15.04.2026).
- 158) Open Data Institute (2013) *Publisher's Guide to the Open Data Rights Statement Vocabulary*. [online]. Available at: <https://theodi.org/insights/guides/publishers-guide-to-the-open-data-rights-statement-vocabulary/> (Accessed: 31.05.2025).
- 159) Open Data Institute (2015) *What are the impacts of non-open licences?* [online]. Available at: <https://theodi.org/insights/guides/what-are-the-impacts-of-non-open-licences/> (Accessed: 31.05.2025).
- 160) Open Data Watch (2022) *Slovakia Open Data Inventory Profile* [online]. Available at: <https://odin.opendatawatch.com/Report/countryProfileUpdated/SVK?year=2022> (Accessed: 28.03.2025).
- 161) Open Knowledge Foundation (2025) *Open Data Editor Docs* [online]. Available at: <https://opendataeditor.okfn.org/> (Accessed: 15.04.2026).
- 162) Opendatasoft (2023) *Harnessing open data to create smart communities* [online]. Available at: https://www.opendatasoft.com/wp-content/uploads/2023/12/Ebook_Harnessing_open_data_to_create_smart_communities.pdf (Accessed: 14.04.2025).



- 163) OPSI - Odprti podatki Slovenije (n.d.) *Kaj so odprti podatki?* [online]. Available at: <https://podatki.gov.si/posredovanje-podatkov/kaj-so-odprti-podatki> (Accessed: 28.03.2025).
- 164) Pereira, C. (2023) *Data Collection Techniques: Web Scraping, APIs, and Databases* [online]. Available at: <https://carlos-miguel-pereira.medium.com/data-collection-techniques-web-scraping-apis-and-databases-4feba2f9c649> (Accessed: 20.09.2024).
- 165) Polish Ministry of Digital Affairs (2026) *Dane.gov.pl - Poland's Data Portal* [online]. Available at: <https://dane.gov.pl/en> (Accessed: 28.03.2025).
- 166) Polska (2001) *Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej. Dz.U. 2001 nr 112 poz. 1198* [online]. Available at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/dostep-do-informacji-publicznej-16913107> (Accessed: 28.03.2025).
- 167) Polska (2002) *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. 2002 poz. 1513 Art. 18* [online]. Available at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/swiadczenie-uslug-droga-elektroniczna-16979921/art-18> (Accessed: 28.03.2025).
- 168) Polska (2002) *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. 2002 nr 144 poz. 1204* [online]. Available at: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20021441204/T/D20021204L.pdf> (Accessed: 28.03.2025).
- 169) Polska (2004) *Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz.U. 2004 nr 171 poz. 1800* [online]. Available at: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20041711800/T/D20041800L.pdf> (Accessed: 28.03.2025).
- 170) Polska (2018) *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2019 poz. 1781* [online]. Available at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-danych-osobowych-18722262> (Accessed: 28.03.2025).
- 171) Polska (2018) *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560* [online]. Available at: <https://www.dziennikustaw.gov.pl/DU/2018/1560/D2018000156001.pdf> (Accessed: 28.03.2025).
- 172) Polska (2021) *Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, Dziennik Ustaw 2021, poz. 1641* [online]. Available at: <https://cms.dane.gov.pl/documents/65/D2021000164101.pdf> (Accessed: 28.03.2025).
- 173) Polska (2021) *Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego* [online]. Available at: <https://dane.gov.pl/> (Accessed: 28.05.2025).
- 174) Postman (2025) *What is an API?* [online]. Available at: <https://www.postman.com/what-is-an-api/> (Accessed: 20.09.2024).
- 175) Ragioneria Generale dello Stato (n.d.) *Cosa sono gli Open Data* [online]. Available at: <https://bdap-opendata.rgs.mef.gov.it/content/cosa-sono-gli-open-data> (Accessed: 28.03.2025).
- 176) Regione Lazio (n.d.) *Leggi e direttive* [online]. Available at: <https://dati.lazio.it/leggi-e-direttive> (Accessed 28.03.2025).
- 177) RIS (2018a) *Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V)* [online, 9.11.2018]. Available at: https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_278/BGBLA_2018_II_278.html (Accessed: 15.04.2026).
- 178) RIS (2018b) *Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV)* [online, 25.05.2018]. Available at:



- https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_108/BGBLA_2018_II_108.html
(Accessed: 15.04.2026).
- 179) RIS (2026a) *Datenschutzgesetz - Bundesrecht konsolidiert, Fassung vom 14.04.2026* [online]. Available at: <https://ris.bka.gv.at/geltendefassung.wxe?abfrage=bundesnormen&gesetzesnummer=10001597&tid=121676594&ShowPrintPreview=True> (Accessed: 15.04.2026).
- 180) RIS (2026b) *Telekommunikationsgesetz 2021 - Bundesrecht konsolidiert, Fassung vom 15.04.2026* [online]. Available at: <https://www.ris.bka.gv.at/geltendefassung.wxe?abfrage=bundesnormen&gesetzesnummer=20011678&ShowPrintPreview=True> (Accessed: 15.04.2026).
- 181) Roddewig, S. (2022) *Data Stewards: Who They Are & Why Stewardship Matters* [online]. Available at: <https://blog.hubspot.com/marketing/data-steward> (Accessed: 11.09.2024).
- 182) Secretaría de Estado de Digitalización e Inteligencia Artificial and Red.es (n.d.) *data.gob.es* [online]. Available at: <https://datos.gob.es/es/> (Accessed: 23.03.2026).
- 183) SkillApp (2024) *Understanding the Key Differences - Static Data vs Dynamic Data Explained* [online]. Available at: <https://skillapp.co/blog/understanding-the-key-differences-static-data-vs-dynamic-data-explained/> (Accessed: 02 April 2025).
- 184) Slove-lex (2000) *Act No. 211/2000 Coll. on Free Access to Information and on amendments to certain laws (Freedom of Information Act)* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2000/211/> (Accessed: 28.05.2025).
- 185) Slove-lex (2013) *Act No. 305/2013 Coll. on the Electronic Form of the Activities of Public Authorities and Amendments to Certain Laws (e-Government Act)* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2013/305/20160501.html> (Accessed: 28.05.2025).
- 186) Slove-lex (2018) *Act No. 177/2018 Coll., on measures to reduce administrative burdens by using public administration information systems (Anti-Bureaucracy Act)* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/177/20180901> (Accessed: 28.05.2025).
- 187) Slove-lex (2019) *Act No. 95/2019 Coll. on Information Technologies in Public Administration and Amendments to Certain Laws* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2019/95/20190501> (Accessed: 28.05.2025).
- 188) Slove-lex (2020a) *Decree No. 78/2020 Coll. from the Office of the Deputy Prime Minister for Investments and Informatization, establishing standards for information technologies in public administration* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2020/78/> (Accessed: 28.05.2025).
- 189) Slove-lex (2020b) *Decree No. 85/2020 Coll. from the Office of the Deputy Prime Minister for Investments and Informatization, concerning project management* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2020/85/> (Accessed: 28.05.2025).
- 190) Služba Vlade Republike Slovenije za digitalno preobrazbo (2022) *Republika Slovenija pristopila k Mednarodni listini o odprtih podatkih* [online]. Available at: <https://www.gov.si/novice/2022-10-28-republika-slovenija-pristopila-k-mednarodni-listini-o-odprtih-podatkih/> (Accessed: 28.03.2025).
- 191) Stad Gent (n.d.) *Explore - Open Data Portaal - Stad Gent* [online]. Available at: <https://data.stad.gent> (Accessed: 23.03.2026).
- 192) Stich Data (n.d.) *What is Data Extraction? Data Extraction Tools & Techniques* [online]. Available at: <https://www.stichdata.com/resources/what-is-data-extraction/> (Accessed: 10.04.2025).



- 193) Stiftung Datenschutz (2022) *Practice Guide to Anonymising Personal Data* [online]. Available at: https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Anonymisierung_personenbezogener_Daten/SDS_Practice_Guide_to_Anonymising-Web-EN.pdf (Accessed 31.05.2025).
- 194) Stiftung Datenschutz (2022) *Praxisleitfaden zum Anonymisieren personenbezogener Daten* [online]. Available at: https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Anonymisierung_personenbezogener_Daten/SDS_Studie_Praxisleitfaden-Anonymisieren-Web_01.pdf (Accessed: 16.04.2026).
- 195) Svoboda, N., Vedder, L., Böhm, F., Möller, M., Rey-Mazón, E., Schmidt, M., Stahl, U. (2023) *The Data Steward Service Center (DSSC): FAIRagro RDM-Expertise Hub*. In: Proceedings of the Conference on Research Data Infrastructure (Vol. 1). DOI: 10.52825/cordi.v1i.367
- 196) UK Government (2025) *Local government transparency code 2015* [online]. Available at: <https://www.gov.uk/government/publications/local-government-transparency-code-2015> (Accessed: 23.03.2026).
- 197) UN Tourism (n.d.) *UN Tourism | Bringing the world closer* [online]. Available at: <https://www.untourism.int/> (Accessed: 15.04.2026).
- 198) Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (2020a) *Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o štandardoch pre informačné technológie verejnej správy* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2020/78/20200501> (Accessed: 15.04.2026).
- 199) Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (2020b) *Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu zo 14. apríla 2020 o riadení projektov* [online]. Available at: <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2020/85/20200501> (Accessed: 15.04.2026).
- 200) Úrad splnomocnenca vlády Slovenskej republiky pre rozvoj občianskej spoločnosti (2022) *Akčný plán Iniciatívy pre otvorené vládnutie v Slovenskej republike na roky 2022 - 2024* [online, 13. júla 2022]. Available at: https://www.minv.sk/swift_data/source/rozvoj_obcianskej_spolocnosti/otvorene_vladnutie/2022/APOGP2022-2024.pdf (Accessed: 15.04.2026).
- 201) Úrad vlády Slovenskej republiky (2017) *Stratégia a akčný plán sprístupnenia a používania otvorených údajov verejnej správy* [online, jún 2017]. Available at: https://www.slovensko.sk/_img/CMS4/strategia_otvorene_udaje.pdf (Accessed: 15.04.2026).
- 202) Vlada Republike Slovenije (2018) *Akcijski načrt izvedbe Strategije razvoja javne uprave 2015-2020 za leti 2018 in 2019* [online, 19. 4. 2018]. Available at: https://www.gov.si/assets/ministrstva/MJU/Kakovost-in-inovativnost-v-javni-upravi/Strategija/Dvoletni_akcijski_nacrt_SJU_2018-2019.pdf (Accessed: 15.04.2026).
- 203) Vlada Republike Slovenije (2023) *Digitalna Slovenija 2030 - Krovna strategija digitalne preobrazbe Slovenije do leta 2030* [online, marec 2023]. Available at: <https://www.gov.si/assets/ministrstva/MDP/Dokumenti/DSI2030-potrjena-na-Vladi-RS-marec-2023.pdf> (Accessed: 15.04.2026).
- 204) WentzWu (2020) *CISSP PRACTICE QUESTIONS - 20201118* [online]. Available at: <https://wentzwu.com/2020/11/17/cissp-practice-questions-20201118/> (Accessed: 11.09.2024).
- 205) Wolters Kluwer Polska (n.d.a) *Dostęp do informacji publicznej. Dz.U. 2022 poz. 902 (tekst jedn.)* [online]. Available at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/dostep-do-informacji-publicznej-16913107> (Accessed: 15.04.2026).



- 206) Wolters Kluwer Polska (n.d.b) *Ochrona danych osobowych. Dz.U. 2019 poz. 1781 (tekst jedn.)* [online]. Available at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-danych-osobowych-18722262> (Accessed: 15.04.2026).
- 207) Wolters Kluwer Polska (n.d.c) *Krajowy system cyberbezpieczeństwa. Dz.U. 2026 poz. 20 (tekst jedn.)* [online]. Available at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/krajowy-system-cyberbezpieczenstwa-18746756> (Accessed: 15.04.2026).
- 208) Wolters Kluwer Polska (n.d.d) *Świadczenie usług drogą elektroniczną. Dz.U. 2024 poz. 1513 (tekst jedn.)* [online]. Available at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/swiadczenie-uslug-droga-elektroniczna-16979921> (Accessed: 15.04.2026).
- 209) Wolters Kluwer Polska (n.d.e) *Zwalczanie nieuczciwej konkurencji. OpenLEX. Dz.U. 2026 poz. 85 (tekst jedn.)* [online]. Available at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/zwalczanie-nieuczciwej-konkurencji-16795259> (Accessed: 15.04.2026).
- 210) Wolters Kluwer Polska (n.d.f) *Prawo telekomunikacyjne. Dz.U. 2024 poz. 34 (tekst jedn.)* [online]. Available at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/prawo-telekomunikacyjne-17116702> (Accessed: 15.04.2026).
- 211) World Economic Forum (2025) *The power of data: how Helsinki is improving citizens' lives* [online]. Available at: <https://www.weforum.org/impact/power-of-data-helsinki> (Accessed: 23.03.2026).
- 212) Zakon.hr (2018) *Zakon o provedbi Opće uredbe o zaštiti podataka* [online]. Available at: <https://www.zakon.hr/z/1023/zakon-o-provedbi-opce-uredbe-o-zastiti-podataka> (Accessed: 15.04.2026).
- 213) Zigomitros, A., Casino, F., Solanas, A., Patsakis, C. (2020) *A Survey on Privacy Properties for Data Publishing of Relational Data* [online]. Available at: <https://doi.org/10.1109/ACCESS.2020.2980235> (Accessed: 16.04.2026).
- 214) Žrt, A., Šik Bukovnik, I. (2025) *Data protection and cybersecurity laws in Slovenia* [online, 8 October 2025]. Available at: <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/slovenia> (Accessed: 15.04.2026).



DoorCE Public Data Opening Strategy © 2026 by Jane Doe is licensed under CC BY-SA 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/4.0/>