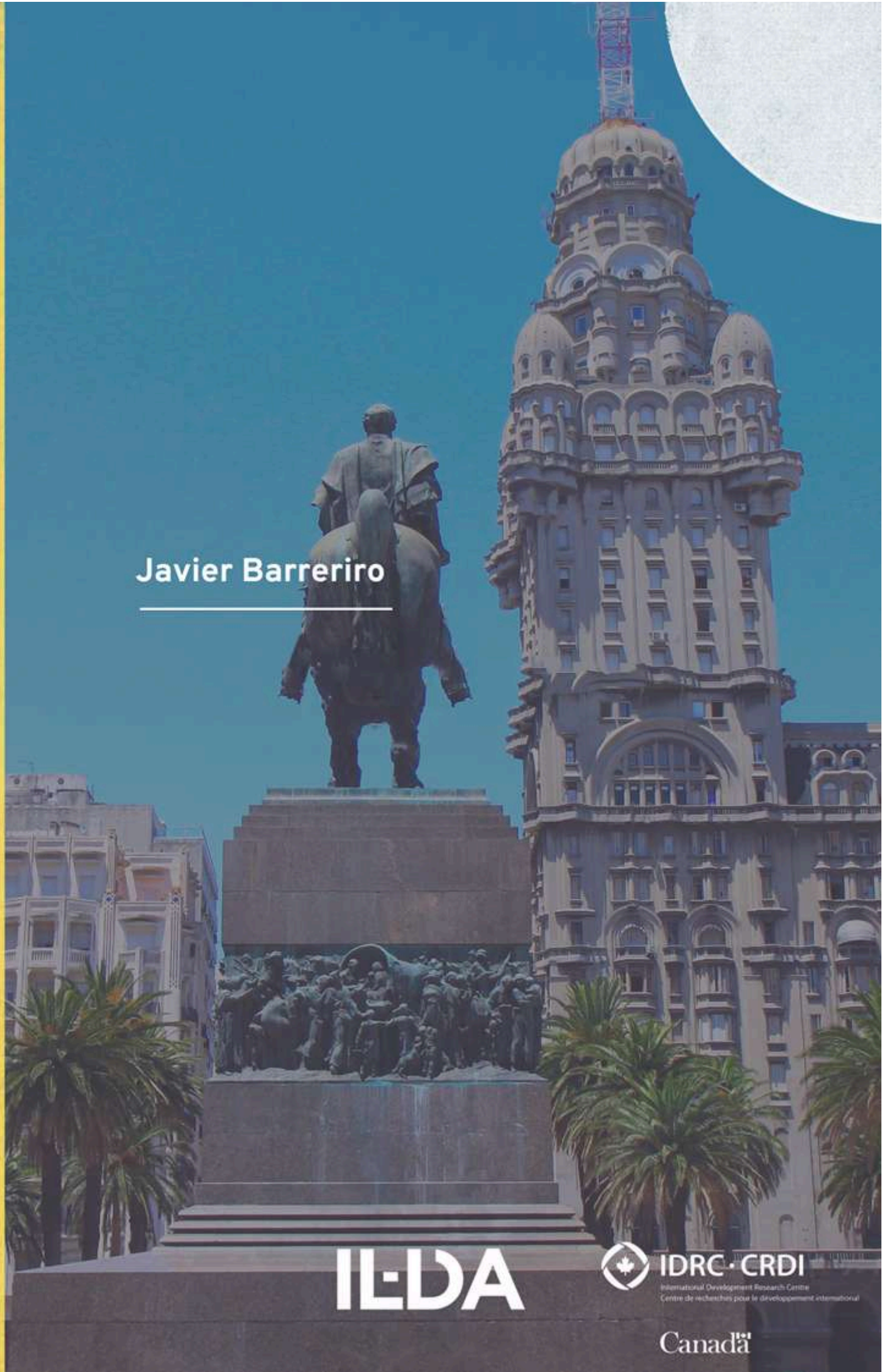


Javier Barreriro

IL-DA

IDRC · CRDI

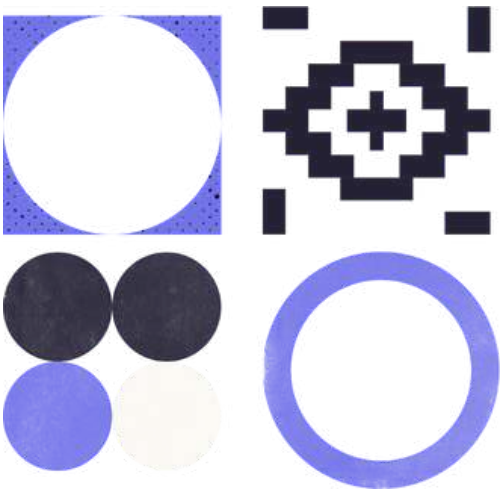
International Development Research Centre
Centre de recherches pour le développement international

Canada

We are especially grateful to **Javier Barreiro**, who carried out the research that underpins this report.

With more than 15 years of experience in the technology sector, Javier's professional career has enabled him to participate in high-impact projects both in the public sector and for various organisations. For more than 10 years he worked for AGESIC, Uruguay's Digital Government Agency, where as AGESIC's Director of Technology, he was responsible, for example, for designing and implementing the first Artificial Intelligence Strategy for Digital Government and the Public Data Policy for Digital Transformation, as well as various enterprise architecture and interoperability projects. He is a university lecturer in Software Engineering, a member of the Project Evaluation Committee of ANII's Public Services Innovation Programme, and he was part of the Honorary Scientific Advisory Group (GACH) during the pandemic. He is a founder and member of the Board of Directors of DaMa Uruguay, a non-profit association of professionals dedicated to promoting data management and governance practices. He is also a consultant for the IDB and RedGealc (Network of e-Government Leaders of Latin America and the Caribbean) on data, enterprise architecture and emerging technologies. He is currently part of Domus Global, a highly specialised, 360° visionary digital transformation accelerator organisation. At Domus, he heads IUGO, a specialised GovTech business unit.

This report was produced within the framework of the *Inter-American Programme for Data and Algorithms*, funded by the International Development Research Centre (IDRC).



Author:
Javier Barreiro

Legal overview:
Cecilia Amieva, Managing Partner; Diego Fernando Saralegui and Carolina Vega from ECIJA Uruguay's TMT Team, via the connection facilitated by TrustLaw, the global legal pro bono network of the Thomson Reuters Foundation, through a partnership with the Patrick J. McGovern Foundation.

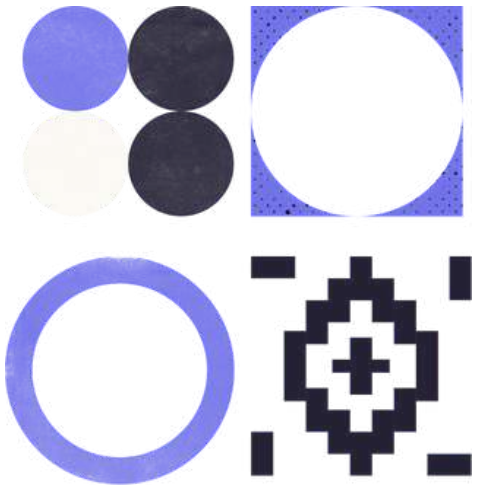
Coordination:
Gloria Guerrero

Design:
Violeta Belver

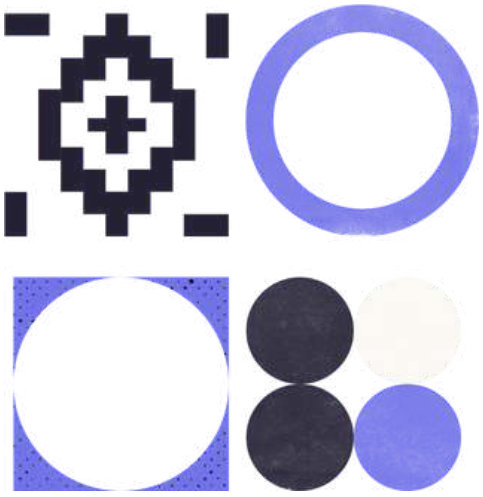
Style:
Aremí González

Translation:
Supported by the Thomson Reuters Foundation, through a partnership with the Patrick J. McGovern Foundation

Acknowledgements:
International Development Research Centre (IDRC)



Index



Foreword

By: Gloria Guerrero,
Executive Director of ILDA

In a deeply interconnected and increasingly digital world, data sharing and data governance are essential for meeting the challenges of the 21st century. In Latin America, these dynamics are influenced by unique contexts that combine promising developments and persistent challenges.

According to the first edition of the *Global Data Barometer*, Latin America faces fragmentation in its data policies: while some countries have made significant progress in openness and data protection, data sharing is still a work in progress.

For this project, data sharing is used in a broad sense, encompassing the regulatory frameworks that establish the technical and organisational guidelines for data sharing, institutional capacities and political willingness to allocate resources and processes to enable these policies to succeed. In this way, data sharing and interoperability processes have a technical component linked to the creation of internal skills and their implementation, but also a political component related to the decision to apply the policy and the cultural change within organisations that is needed. We therefore consider the processes, people and systems that ensure that these policies remain in place over time.

It is within this context that the Latin American Open Data Initiative (Iniciativa Latinoamericana por los Datos Abiertos, ILDA) has conducted the research entitled *Data Sharing Strategies in Latin America*, which consists of three national case studies. This project is part of the *Inter-American Programme for Data and Algorithms* supported by the International Development Research Centre (IDRC), which seeks to explore the topic in greater depth. The purpose of this research project is to analyse and understand how data sharing systems work at a national level in Brazil, Colombia and Uruguay. These three case studies have allowed us to identify a set of good practices that can be inspirational for other countries in the region and to pinpoint challenges and areas of opportunity for this field of study.

Each case study seeks to understand the regulatory frameworks, data infrastructure and its characteristics, processes and implementation, and the involvement of various actors (public, private and civil society) in these data sharing processes at a national/federal level. This research follows on from a series of Data Governance Reports carried out in Colombia, Mexico and Uruguay in 2022 and is complemented by a series of legal studies on data sharing conducted by specialised law firms in each country, which contributed on a pro bono basis through the connection facilitated by TrustLaw, the Thomson Reuters Foundation's legal pro bono network.

The project aims to provide a diagnosis and possible next steps on data governance, which could also be a useful input for future AI governance in the region. This work aims not only to understand the existing regulatory and technical structures, but also to lay the foundations for a sustainable, inclusive and democratic ecosystem that promotes interoperability and the ethical use of data-driven technologies.

The case of Uruguay is presented below, led by Dr Javier Barreiro and the law firm ECIJA Uruguay. Uruguay's coordinated and consistent digital strategy, supported by a robust regulatory framework and an advanced technological infrastructure, has positioned it as a regional benchmark in data governance and interoperability. This success is largely due to the institutional continuity of the governance and data sharing agenda, an aspect that distinguishes Uruguay from other countries in the region, which face challenges maintaining policies in the long term. The constant evolution of the legal framework, especially in key areas such as personal data protection, information security and interoperability, has allowed for a progressive improvement in data management and data sharing at a government level.

The case of Uruguay highlights the importance of having an integrated digital architecture, as demonstrated by the Interoperability Platform (PDI), which has enabled efficient and secure data sharing between multiple public authorities. This platform has been crucial in streamlining and improving the quality of public services, promoting seamless inter-institutional collaboration and more equitable access to services for citizens. At a regulatory level, Uruguay has aligned itself with international standards, creating a favourable environment for the protection of citizens' rights and fostering trust in the management of personal data. However, the country still faces challenges related to privacy protection, especially in the use of disruptive technologies such as artificial intelligence and facial recognition. These developments must be accompanied by a clear and transparent regulatory framework to avoid risks such as mass surveillance and abuse of technologies, which could erode public trust.

With this investigation by the Latin American Open Data Initiative (Iniciativa Latinoamericana por los Datos Abiertos, ILDA), we reaffirm our commitment to contribute to the development of the regional data ecosystem and generate evidence to strengthen the existing data governance capacities and models.

1. Introduction

Data sharing refers to the process of making data accessible to multiple users, applications or organisations. This can be done within the same organisation or between different entities, and its purpose is to improve collaboration, decision-making and operational efficiency. In this process, it is essential to ensure that data are shared securely, respecting privacy and legal regulations.

Data sharing also involves the use of technological platforms that facilitate controlled and secure access to data, as well as the implementation of policies and procedures to ensure that the information shared is of high quality and relevant to users.

Over the last 20 years, Uruguay has witnessed a profound transformation in data sharing and interoperability in the public sector, consolidating its position as a regional leader in this area. This process has been the result of a digital strategy coordinated and led mainly by the Agency for e-Government and the Information Society (AGESIC) created in 2007.

AGESIC's mission as well as several high-impact projects involving various public and private actors have been instrumental in fostering the modernisation of the state, the digitisation of public services, and the creation of an ecosystem of data sharing between different public and private sector entities.

The Organisation for Economic Co-operation and Development (OECD) defines **data sharing** as "the act of providing access data for use by others, subject to applicable technical, financial, legal or organisational use requirements" (OECD, 2021).

The European Union (EU), through Regulation 2022/868 of the European Parliament, defines it as "the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licences subject to a fee or free of charge" (2022, p. 19)[1].

Within the above framework and in order to establish a common vocabulary for this document, it has been necessary to establish some basic definitions of **interoperability**:

- ISO/IEC 2382:2015 states that it is the "capability to communicate, execute programs or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units"[2].

[1](2022, 3 June). 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). Available at https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

[2]International Standard. (2015, May). *Information technology – Vocabulary*. ISO / IEC 2382:2015. Available at https://www.iso.org/standard/63598.html

- The Institute of Electrical and Electronics Engineers (IEEE), from a technical point of view, states that it is "the ability of two or more systems or components to exchange information and to use the information that has been exchanged" [3].
- The European Commission, from a data governance strategy perspective, determines that it is "the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems" (Naser, 2011, p. 25)[4].

These definitions can be complemented by a four-level view of interoperability: legal, technical, semantic and organisational.

According to the *White Paper on e-Government Interoperability for Latin America and the Caribbean* (ECLAC) and the European Commission[5], there are different types of interoperability, as shown below:

- **Technical interoperability:** "entails addressing the technical issues (hardware, software, telecommunications) involved in interconnecting computer systems and services, including key elements such as open interfaces, interconnection services, integration of data and middleware, presentation and exchange of data, accessibility and security services" (UN. ECLAC and European Commission, 2007, p. 13).
- **Semantic interoperability:** "ensures that the precise meaning of information that is exchanged is unambiguously communicated in all of the applications involved in a given transaction, and that systems are able to combine information received from other information sources and process it properly" (UN. ECLAC and European Commission, 2007, p. 13).
- **Organisational interoperability:** "entails defining business objectives, modelling processes and facilitating collaboration among governments wishing to exchange information, even when their organisational structures and internal processes differ. In addition, it means addressing the requirements of the user community and defining the services that need to be made available and made easily identifiable, accessible and user-friendly" (UN. ECLAC and European Commission, 2007, p. 13).

In the European Interoperability Framework Implementation Strategy[6] in the *Annex to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, it is stated that:

---

[3] (1991, 18 January). *610 – 1990 – IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. IEEE. DOI: 10.1109/IEEESTD.1991.106963

[4]Naser, Alejandra. (Coord.). (2011). "Digital governance and government interoperability. A guide to implementation". *Project documents*. (LC / TS. 2021 / 8°), Santiago. Economic Commission for Latin America and the Caribbean (ECLAC). Available at https://repositorio.cepal.org/server/api/core/bitstreams/6a12e389-3dcb-4cba-830a-99f038835423/content

[5]UN. ECLAC and European Commission. (2007). *White book of e-government interoperability for Latin America and the Caribbean*. Available in: White book of e-government interoperability for Latin America and the Caribbean: version 3.0 (cepal.org)

[6]European Commission. (2007). *Annex to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Interoperability Framework – Implementation Strategy.* Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017DC0134

- **Legal interoperability:** "is about ensuring that organisations operating under different legal frameworks, policies and strategies are able to work together. This might require that legislation does not block the establishment of European public services within and between Member States and that there are clear agreements about how to deal with differences in legislation across borders, including the option of putting in place new legislation" (European Commission, 2007, p. 26–27).
- **Technical interoperability:** "covers the applications and infrastructures linking systems and services. Aspects of technical interoperability include interface specifications, interconnection services, data integration services, data presentation and exchange, and secure communication protocols. [...]. Technical interoperability should be ensured, whenever possible, via the use of formal technical specifications" (European Commission, 2007, p. 30–31).
- **Semantic interoperability:** "ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words 'what is sent is what is understood'. [...]. The semantic aspect refers to the meaning of data elements and the relationship between them. It includes developing vocabularies and schemata to describe data exchanges, and ensures that data elements are understood in the same way by all communicating parties; the syntactic aspect refers to describing the exact format of the information to be exchanged in terms of grammar and format" (European Commission, 2007, p. 29).
- **Organisational interoperability:** refers to the way in which public administrations align their business processes, responsibilities and expectations to achieve commonly agreed and mutually beneficial goals. In practice, organisational interoperability means documenting and integrating or aligning business processes and relevant information exchanged. Organisational interoperability also aims to meet the requirements of the user community by making services available, easily identifiable, accessible and user-focused" (European Commission, 2007, p. 28).

Having introduced these definitions and outlined the development of this report, it is now time to present how **data governance** can be defined. In this regard, according to *Dama – Dmbok: Data Management Body of Knowledge*, data governance refers to "the exercise of control over the management of data assets throughout their lifecycle", being the function that "governs all other data management activities and ensures that data are handled according to policies and best practices". It further defines **data management** as "the process of developing, implementing and monitoring plans, policies, programmes and practices that secure, protect and enhance the value of data and information assets throughout their lifecycle".

This document is structured considering and addressing the definitions presented. Chapter 2 sets out the main regulatory framework for data sharing in direct relation to legal interoperability, which the country sees as the basis for creating regulatory certainty and the foundation for the secure development of data sharing. It also summarises the different laws, regulations and decrees that have been developed in relation to data sharing.

Chapter 3 discusses the national data governance strategy and the involvement of different actors – public sector, private sector, academia, civil society – in its creation. It also presents aspects of the specific implementation of the regulations and data strategy, the existence of

the necessary resources and the existing data infrastructure in Uruguay as a tool that enables governance. In addition, the existence of public consultations, training, awareness-raising and induction processes within the public sector, coordination between national and local levels, as well as possible collaborations with civil society and international actors are analysed. Finally, aspects related to organisational and technical interoperability can be seen here.

Chapter 4 analyses some cases which, due to their characteristics, provide an overview of what has been presented in the previous chapters, identifying some particular opportunities for improvement.

Finally, chapter 5 brings together the main conclusions and some challenges and opportunities for consideration.

2. Regulatory framework

It can be affirmed that Uruguay has a solid legal framework in terms of exchange, personal data protection and information security, which, over time and under successive governments and administrations, has been continued, updated and improved, a factor that strongly distinguishes it in the region. This positive regulatory process has been progressive and has been aimed at strengthening privacy protection, ensuring transparency and promoting interoperability in the public and private spheres.

To illustrate this development, Law No. 18,331[7] was enacted in 2008, establishing the right to privacy of personal data and regulating its processing in the public and private sectors. This law created the Personal Data Regulatory and Control Unit (URCDP, in Spanish), which is responsible for supervising compliance with regulations, conducting censuses of databases and issuing opinions on administrative sanctions.

In the same year, Decree No. 664/008[8] was enacted, which regulates the law and established the Registry of Personal Databases under the responsibility of the URCDP. One year later, in 2009, Decree No. 414/009[9] defined general provisions on the rights of data subjects, the registration regime and the obligations of those who manage these databases.

In 2010, Law No. 18,719[10] made AGESIC responsible for leading information security and cybersecurity policies and practices in both the public and private spheres linked to critical sectors. Articles 157 to 160 of the same law also established conditions for interoperability and exchange of information. Similarly, Decree No. 232/010[11] was published that year, which promoted transparency and citizen access through the publication of open data by public entities.

In 2012, Law No. 19,030[12] was passed, ratifying Council of Europe Convention 108, promoting the protection of personal data in the context of automated processing and data

[7](2008, 18 August). Law No. 18,331. Law on personal data protection. *Official Information Centre*. *Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/18331-2008/34

[8](2009, 5 January). Decree No. 664/008. Creation of the register of personal databases. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/664-2008

[9](2009, 15 September). Decree No. 414/009. Regulation of Law 18,331 on personal data protection. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/414-2009

[10](2011, 5 January). Law No. 18,719. National budget for salaries, expenses and investments. Financial year 2010–2014. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/18719-2010/149

[11](2010, 10 August). Decree No. 232/010. Regulation of the law on the right of access to public information. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/232-2010/

[12](2013, 7 January). Law No. 19,030. Approval of the convention for the protection of individuals with regard to automatic processing of personal data. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/19030-2012

traceability. Subsequently, Decree No. 178/013[13] of 2013 regulated Articles 157 to 160 of Law No. 18,719[14].

In 2015, Law No. 19,355[15], Article 76, established the obligation for public bodies not to request documentation already issued by other State entities when this information could be accessed through computer systems. Furthermore, Article 82[16] determined that AGESIC would be responsible for technical standards on data and their metadata.

In 2018, Law 19,670[17] amended several articles of Law No. 18,331, extending the competences of the URCDP and adjusting aspects related to control and sanctions. In 2020, Decree No. 64/020[18] provided security recommendations and adopted the AGESIC Cybersecurity Framework. In the same year, Law No. 19,889 aligned national regulations with the European Union's General Data Protection Regulation (GDPR), strengthening the rights of personal data subjects and establishing greater obligations for those who manage these databases.

In 2021, Law No. 19,948[19] was passed, ratifying the Protocol amending Convention 108 (Convention 108+) and reaffirming the country's commitment to personal data protection. Law No. 20,075[20] of 2022 amended several articles of Law No. 18,331, improving the regulation of the processing of personal data.

In 2023, Decree No. 252/023[21] was issued regulating Article 76 of Law No. 19,355, and Law No. 20,212[22] was enacted, making AGESIC responsible for designing a National Data and

[13](2013, 25 July). Decree No. 178/013. Regulation of Articles 157 to 160 of Law No. 18,719, relating to the regulation of the exchange of information between public, state or non-state entities. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/178-2013

[14](2011, 5 January). Law No. 18,719. National budget for salaries, expenses and investments. Financial year 2010–2014. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/18719-2010/

[15](2015, 30 December). Law No. 19,355. National budget for salaries, expenses and investments. Financial year 2015–2019. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/19355-2015/76

[16](2015, 30 December). Law No. 19,355. National budget for salaries, expenses and investments. Financial year 2015–2019. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/19355-2015/82

[17](2018, 25 October). Law No. 19,670. Approval of the presentation of accounts and budget execution balance sheet. Financial year 2017. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/19670-2018

[18](2020, 21 February). Decree No. 64/020. Regulation of Art. 37 to 40 of Law 19,670 and Art. 12 of Law 18,331, on personal data protection. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/64-2020

[19](2021, 27 April). Law No. 19,948. Adoption of the protocol amending the Strasbourg Convention for the protection of individuals with regard to the processing of personal data. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/19948-2021

[20](2022, 3 November). Law No. 20,075. Approval of the presentation of accounts and budget execution balance sheet. Financial year 2021. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/20075-2022

[21](2023, 16 November). Decree No. 353/023. Regulation of Art. 76 of Law No. 19,355, regarding the procedure applicable by public entities, in order to simplify their procedures, following the guidelines of AGESIC. Amendment of Art. 15 and repeal of Art. 13 of Decree No. 178/013. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/353-2023

[22](2023, 17 November). Law No. 20212. Approval of the presentation of accounts and budget execution balance sheet. Financial year 2022. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/20212-2023/74

Artificial Intelligence Strategy. This law imposes obligations on public and private entities linked to critical services in the country and establishes the basis for both the creation of a national strategy, highlighting the importance of the controller, and AGESIC's oversight of compliance with these obligations.

This summary clearly shows that Uruguayan data regulation has evolved significantly, aligning with international standards and focusing on privacy protection, transparency and the promotion of a secure and collaborative environment for data sharing. This evolution has made it possible to establish a robust framework to ensure proper data management in a context of increasing digitisation.

Uruguay has developed a coordinated approach, reflected in the first instance in the Data 360° initiative[23] promoted by AGESIC in 2016. This initiative "refers to the holistic approach to data management in public administration" (AGESIC, n.d.), which "seeks to support digital government by addressing the different components of efficient data management" (AGESIC, n.d.).

Recently, with the above mentioned enactment of Law No. 20,212, which establishes AGESIC's obligation to develop a National Data and Artificial Intelligence Strategy, an organised approach encompassing the regulation of interoperability and data protection has been re-strengthened.

It is worth noting that this law also emphasises the need to make specific recommendations for public and private entities to comply with the necessary standards for data management, a factor that also contributes to coordinated governance.

[23](n.d.). "360° Data Initiative". "360° Data". *Agency for e-Government and the Information and Knowledge Society.* Available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/node/3557

3. Data governance in Uruguay: background and current situation

Decree No. 134/021[24], enacted on 4 May 2021, approved the Uruguay Digital Agenda (AUD, in Spanish) 2025 and entrusted AGESIC with the monitoring, evaluation of progress and results, and the mid-term review of the Agenda.

Objective 6 "Data as assets" of AUD 2025[25] proposes to optimise the intensive use of data and information as a key factor for effective decision-making and efficient public management, taking into account aspects of ethics, privacy, accountability, transparency and non-discrimination. In turn, target 27 sets the objective of strengthening public policy monitoring and evaluation processes by 2025, as well as the integration, openness and visualisation of public data, promoting data science.

Moreover, within the framework of AUD 2025, AGESIC defined the 5th National Action Plan for Open Government 2021–2024[26] in point 1.9 of which the National Open Data Strategy 2021–2024 was approved. The action plan mentions that "for the first time, the three branches of government converge in one plan, simultaneously integrating initiatives of Open Parliament, Open Justice, Central Administration bodies and Departmental Governments" (AGESIC, n.d., p. 03). It also mentions that it "reaffirms the country's strategy of conceiving action plans and co-creation processes in Uruguay as an instrument to generate new spaces for collaboration and collective construction between public institutions, civil society organisations, the private sector and academia, thus promoting a transversal agenda for all public policies".

Also within the framework of AUD 2025, in 2021, AGESIC defined the Digital Government Plan 2025[27], which includes the objective "Government as a platform", whose aims are related to "promoting the development of scalable and transversal platforms for the generation of public value services by public and private organisations; universalising interoperability and data integration in public administration; designing government architecture around a network of shared APIs and components, open standards and datasets, so that public

[24](2021, 12 May). Decree No. 134/021. Approval of "Uruguay Digital Agenda 2025". *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/134-2021%EF%BB%BF

[25](2023, 18 December). Uruguay Digital Agenda 2025 – Resilient digital society. "Uruguay digital". *AGESIC*. Download available at: https://www.gub.uy/uruguay-digital/comunicacion/publicaciones/agenda-uruguay-digital-2025-sociedad-digital-resiliente/agenda-uruguay

[26](n.d.). 5th National Action Plan for Open Government 2021–2024. *AGESIC and Uruguay Presidency*. Available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/book/6187/download

[27](n.d.). Digital Government Plan 2025. *AGESIC and Uruguay Presidency*. Available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/2021-07/Plan%20de%20Gobierno%20Digital%202025_0.pdf

agencies and the private sector can deliver services in a secure, innovative and responsible way" (AGESIC, n.d., p.15). Governance on data sharing between public bodies and the private sector is explicitly highlighted in this plan.

The Uruguay Digital Agenda 2025 reflects Uruguay's strategic positioning on data governance in both the public and private sectors, promoting interoperability, transparency, and the secure and responsible use of information. In this way, the strategy not only strengthens the country's digital ecosystem but also represents a continuity with the Agendas previously developed by Uruguay, reaffirming the country's commitment to digital transformation and collaborative governance.

Through clear objectives and concrete action plans such as the 5th National Action Plan for Open Government and the Digital Government Plan 2025, Uruguay consolidates its regional leadership in the implementation of open data strategies and digital integration, committed to a transversal and inclusive approach that involves all sectors of society.

This initiative is being complemented at the time of writing by a process of developing a national data strategy[28]. Consistent with past approaches, "this process contemplates the development of roundtable discussions, workshops and a public consultation mechanism. It also foresees the participation of representatives from the state, academia, civil society and the private sector throughout the different stages".

This process will result in the final version of the Artificial Intelligence Strategy and National Data Strategy documents. It is currently possible to participate in the public consultation via the following link: https://plataformaparticipacionciudadana.gub.uy/processes/estrategia-ia-datos/steps?locale=es

The strategy, recently published for public consultation, focuses on developing a data-driven economy with three key pillars: data governance, infrastructure and economic development based on a set of principles such as innovation, focus on data value, quality and availability, aligned with local and international regulations on security and privacy issues.

The draft strategy outlines the importance of creating mechanisms to enable data to be shared, integrated and made available securely and reliably, both domestically and across borders. To achieve this, it suggests the creation of data spaces with different levels of openness that are accessible to all sectors of society under a clear governance model that defines the licences, agreements and rules needed to ensure adequate and compliant participation.

There is a pressing need to create transversal spaces that guarantee the integration and exchange of data between public bodies in a secure and reliable manner, which would facilitate cooperation between different areas and systems according to the strategic

[28](2024, 17 July). "Process of reviewing the Artificial Intelligence Strategy and developing the National Data Strategy. "Policy and Management". *Agency for e-Government and the Information and Knowledge Society.* Available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/proceso-revision-estrategia-inteligencia-artificial-elaboracion-estrategia

objectives defined by the institutions. At the same time, it proposes to promote open data in a sustainable way, placing particular emphasis on strategic sectors, by strengthening the capacities, mechanisms and tools that enable effective and efficient openness.

Another key aspect of the text is the creation of a national interoperability plan addressing semantic, organisational, regulatory, technical and infrastructural aspects. It is noted that this plan should encourage greater data sharing and integration not only internally between organisations but also across borders, ensuring data quality and integrity at all times.

On the other hand, at a subnational level, Uruguay has the Montevideo Data Strategy[29], which focuses on improving the use and management of data to maximise the impact on the citizens of the country's capital. The strategy is organised into five core elements:

- **Governance:** establishes a Data Committee to ensure comprehensive data management, defining roles and responsibilities to ensure security, transparency and documentation.
- **Quality:** implements standards to ensure the consistency, accuracy and security of data through a Single Data Inventory. Each department of the City Council is responsible for updating and maintaining the information it manages.
- **Capacity:** includes a Training and Skill Building Plan to equip teams with skills in data management and analysis, ensuring the creation of a sustainable culture of data use throughout the City Council.
- **Transparency:** focuses on making internal and external data available, facilitating access through the systematic publication of open data. The data are published in accordance with a protocol that ensures confidentiality and compliance with current regulations.
- **Use:** promotes informed decision-making based on data analysis. The development of tools such as data integration platforms and a dashboard to prioritise public management is encouraged.

In turn, this subnational strategy is based on three fundamental principles:

1. Leadership to drive the use of data in day-to-day decision-making.
2. Resources to promote training.
3. Collaborative work and citizenship to ensure transparency and citizen participation in the access and use of data.

The strategy seeks to consolidate a data culture that improves the quality of life of the inhabitants of the city of Montevideo, increases transparency and allows the co-creation of solutions to public problems.

From the perspective of regulation and control, in Uruguay there is a set of autonomous units under the AGESIC linked to this topic: the Personal Data Regulatory and Control Unit (URCDP) and the Unit for Access to Public Information (UAIP, in Spanish), which act in response to

[29](2023, 18 May). Data strategy of the Montevideo City Council. *Montevideo City Council*. Available for download at https://montevideo.gub.uy/noticias/tecnologia/estrategia-de-datos-de-la-intendencia-de-montevideo

complaints or requests by issuing opinions when appropriate. They are governed by Executive Councils that are assisted in their tasks by Advisory Councils, multi-sectoral bodies made up of representatives from three areas: government, academia and civil society. In particular, as stated in the regulation, Advisory Councils must be involved when regulatory powers are exercised.

In line with the regulations presented and the technical guidelines and recommendations created, the country has developed a robust and modern data infrastructure that underpins its ability to effectively manage and share data between public bodies.

The Interoperability Platform (PDI, in Spanish)[30] is a technological infrastructure that enables the secure and efficient connection and exchange of data between systems of different public entities. This platform helps automate processes, improves the quality of public services and enables integrated information management, ensuring that data are shared using a standardised methodology and complying with security and data protection regulations. AGESIC ensured technical and semantic interoperability with the development of the User Guide for the Interoperability Platform[31].

The PDI has a service-oriented architecture (SOA), which allows the reuse and orchestration of services through standardised interfaces, promoting the efficient development of new solutions and the autonomous evolution of state systems. Within its structure, each of its elements plays a specific role in ensuring the provision, search, invocation and secure integration of services between agencies through standardised protocols. Its access control system allows authentication and authorisation for data sharing, acting as a gateway to the platform; this ensures that only authorised users and systems can access the data, reinforcing the security of information exchange.

Since its design and implementation in 2008, the PDI has enabled the development of several high-impact projects for the Uruguayan state, such as *Nacido Vivo* (birth certificate), *Trámites en Línea* (online procedures), *Expedientes Digitales* (digital records), *Notificaciones y Comunicaciones Digitales* (digital notifications and communications), *Historia Clínica Electrónica Nacional* (national electronic medical record) and *Ventanilla Única de Comercio Exterior* (foreign trade one-stop shop). These projects have significantly improved the capacity of public institutions to share and process data in a more competent way. The PDI's participation in these projects can be seen from the sustained growth in the number of annual transactions supported by the platform, demonstrating its stability and scalability.

By the end of 2023, the PDI was used by 98 Uruguayan public administration bodies to obtain and share information, while 27 of them published a total of 221 services available for data interoperation. This level of adoption underlines the importance of the PDI as an essential infrastructure for interoperability in the Uruguayan public sector, promoting data integration

[30](n.d.). Interoperability Platform. *AGESIC and Uruguay Presidency*. Available at https://centrodeconocimiento.agesic.gub.uy/web/ccio/plataforma-de-interoperabilidad

[31](n.d.). Conditions of use of the Interoperability Platform. Technical specification. Interoperability Platform. *AGESIC and Uruguay Presidency*. Available for download at https://centrodeconocimiento.agesic.gub.uy/documents/80442/88295/PGE-Condiciones-de-uso-Plataforma-v01-21.pdf/7786ceca-21b5-0a1d-254e-1293a1330876?version=1.0

and improved efficiency in public management[32].

[32](n.d.). Cross Border Digital Services. Programme for strengthening cross-border electronic transactions in Latin America and the Caribbean. "Regional Public Assets". *Reagealc*. Available at https://www.redgealc.org/site/assets/files/13516/anexo_1_-_servicios_digitales_transfronterizos_-_indice.pdf

4. Analysis cases

4.1 Data sharing and artificial intelligence

Data and Artificial Intelligence (AI) are closely related for a number of reasons whose analysis is beyond the scope of this document. In short, the implementation of AI requires a robust approach to data protection, management and governance to ensure the privacy and security of the information handled, at the same time as data laws and regulations directly impact how data can be used and stored to train and operate AI systems.

That said, Article 74 of Law No. 20,212, approved on 6 November 2023, is particularly relevant. It attributed to AGESIC the task of designing and developing a national data and artificial intelligence strategy based on international standards (in the public and private spheres), entrusting it, in turn, with drawing up recommendations on AI regulation for the Legislative Branch.

Within this framework, in 2024, AGESIC prepared and delivered to the Legislative Branch the report *Article 74 of Law No. 20,212. Recommendations for regulation of Artificial Intelligence (AI) focusing on ethical development, the protection of human rights and the promotion of technological innovation*[33], which mentions that it was developed using "a predefined methodology, and through a process that involved the participation of officials and consultants from different public bodies, with whom, after various meetings, a consultation document was defined and made available to other previously identified actors (organisations and private entities, academia and civil society), using the citizen participation platform managed by AGESIC for this purpose" (AGESIC, n.d., 09).

The public bodies that contributed were:

- Presidency of the Republic (Vice-secretariat of the Presidency and Secretariat of Human Rights).
- Ministry of Education and Culture (Copyright Council).
- Ministry of Economy and Finance (Consumer Defence Unit).
- Ministry of Industry, Energy and Mining (National Directorate of Telecommunications and National Directorate of Industrial Property).
- Ministry of Labour and Social Security (General Inspectorate of Labour and Social Security).
- Communications Services Regulatory Unit.

[33](n.d.). Report on Article 74 Law No. 20,212. Recommendations for regulation of Artificial Intelligence (AI) focusing on ethical development, the protection of human rights and the promotion of technological innovation. *AGESIC and Uruguay Presidency*. Available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Art%C3%ADculo%2074%20de%20la%20Ley%20N%C2%BA20.212%20recomendaciones%20para%20una%20regulaci%C3%B3n%20de%20la%20Inteligencia%20Artificial%20%28IA%29_0.pdf

- National Agency for Research and Innovation.
- Uruguay Innovation Hub Programme.
- Personal Data Regulatory and Control Unit.
- National Human Rights Institution and Ombudsman's Office (INDDHH, in Spanish).

In turn, the consultation process received contributions from:

- Association of Notaries of Uruguay (AEU, in Spanish).
- Data and Society Laboratory (DatySoc).
- DATA Uruguay.
- Uruguayan Chamber of Information Technology (CUTI, in Spanish).

As can be seen, the process of drafting the recommendations contained in the report involved the widespread participation of public and private actors of the most diverse nature within the framework of a very important issue for the country - the national data and AI strategy.

Although AGESIC, a public actor with a technical profile, has a clear and important leadership role in developing the aforementioned strategy, in the report it also recommends strengthening the mechanisms for intervention and collaboration of all stakeholders and explicitly includes specific measures and contributions suggested by the participating actors (e.g. creation of forums and public hearings with the collaboration of different actors, creation of multidisciplinary advisory groups that meet regularly, etc.). In addition, the report itself includes the full contributions of the INDDHH, DATA Uruguay, the Data and Society Laboratory (DatySoc) and the Association of Notaries of Uruguay (AEU) as an annex.

In addition, the recommendations set out in this document include aspects related to data sharing. In particular, with regard to the recommendations associated with institutionality and governance, it mentions "enabling the use of the interoperability platform provided for in Decree No. 178/013 of 11 June 2013 by private entities" (AGESIC, n.d., p. 100).

In relation to infrastructure and cybersecurity, it is mentioned that "in terms of regulatory support for secure data sharing, it is advisable to enable the use of the Interoperability Platform created by Decree No 178/013 for the use of services by private entities" (AGESIC, n.d., p. 115).

Both recommendations (under development by AGESIC at the time of writing) are presented as enablers and catalysts for a public-private ecosystem that enhances the development of quality digital services while still presenting challenges in relation to maintaining and ensuring guarantees and conditions in aspects of secure data handling and respect for privacy.

4.2 Cross-border data sharing

Uruguay has implemented specific regulations on international transfers of personal data. Resolution No. 23/021 of the URCDP of 2021[34] states that data may be transferred to

[34](2012, 8 June). Resolution No. 23/021. *Personal Data Regulatory and Control Unit*. Available for download at https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021

countries deemed appropriate; these include EU member states and other countries with a robust legal framework.

Uruguay was one of the first Latin American countries to obtain "adequate" status under the GDPR, which facilitates the transfer of personal data to and from the EU without the need for additional safeguards[35].

In addition, Uruguay actively participates in regional and international agreements that seek to facilitate the flow of data between countries, promoting cooperation in key areas such as digital trade and information security[36] [37] [38] [39]. These aspects are reflected in the draft National Data Strategy 2024–2030, which, as mentioned, includes aspects of cross-border exchange as part of its approach.

With regard to digital signatures, Uruguay has established a solid regulatory framework through Law No. 18,600[40], which regulates the use of electronic signatures and establishes certification standards. This means that digital signatures have the same legal value as handwritten signatures, facilitating secure electronic transactions at a national and international level. The UCE is the body responsible for overseeing the implementation of these technologies in the country, ensuring their interoperability with global systems.

Uruguay participates in discussion forums in the region on this issue, which implies a challenge in terms of adopting common regulations and rules for the countries that sign agreements, alliances or common action plans. One example is that in Latin America there is no governance space similar to the European Commission where issues are addressed, conclusions and agreements are reached, and regulations are eventually issued that must be adopted by all member countries.

As an example, in May 2024 the European Union – Latin America and Caribbean Digital Alliance (of which Uruguay is part) called for a policy dialogue to improve cooperation around digital governance. As a result, operational conclusions, areas for action and joint

[35](2024, 15 January). The European Commission confirms Uruguay's adequate level of data protection. Available from the *Personal Data Control and Regulatory Unit.*https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/comision-europea-ratifica-nivel-adecuado-uruguay-para-proteccion-datos-0

[36](2023, 13 December). New technical cooperation agreement on digital identification between Uruguay and Paraguay. "Official identification". *Agency for e-Government and the Information and Knowledge Society.* Available for download at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/nuevo-convenio-cooperacion-tecnica-identificacion-digital-entre-uruguay

[37](2023, 12 December). Uruguay and Brazil sign a technical cooperation agreement on digital identification. "Official identification". *Electronic Certification Unit.* Available for download at https://www.gub.uy/unidad-certificacion-electronica/comunicacion/noticias/uruguay-brasil-firman-convenio-cooperacion-tecnica-identificacion-digital

[38](2024, 18 September). Cross-border digital signature recognition agreements. *Electronic Certification Unit.* Available at https://www.gub.uy/unidad-certificacion-electronica/politicas-y-gestion/acuerdos-reconocimientos-transfronterizos-firma-digital

[39](2024, 3 April). Cross-border signature in Mercosur. "Digital signature". *Electronic Certification Unit.* Available at https://www.gub.uy/unidad-certificacion-electronica/comunicacion/noticias/firma-transfronteriza-mercosur

[40](2009, 5 November). Law No. 18,600. Electronic document and electronic signature. Admissibility, validity and effectiveness. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/18600-2009

interventions on cross-border data interoperability, digital identification and electronic signatures were established.

Uruguay expressed particular interest in the following activities with a view to the upcoming 2025 EU-LAC Summit:

Objective	Activity
Strengthen the community that facilitates cooperation between stakeholders. **Support the validation of cross-border data interoperability projects.** **Carry out a proof of concept.**	Promoting a regional initiative for digital consent (data access authorisation).
Share knowledge and experience on interoperability between LAC and EU countries.	Promoting strategies for citizen participation and awareness-raising about digital rights and the implications of regional interoperability.
Development of the LAC regional framework for cross-border digital identification and electronic signatures.	Identifying LAC and EU references with experience in cross-border e-signatures and digital identification.
Strengthen the community to plan further activities for the development and implementation of a cross-border recognition model for LAC countries.	Creating or improving working groups on digital identification and electronic signatures to discuss legal principles, international standards, common practices and common technical requirements.
Share knowledge and experience of digital and electronic identification between EU countries.	Developing the technical capacity and awareness of stakeholders regarding digital identification and e-signatures.

4.3 Digital health platform

Salud Digital (Digital Health)[41] is an evolution of the Salud.uy programme created in 2012. It aims to improve the efficiency and quality of health services through the integration and exchange of information in the health system and is a leading model in the region and a fundamental part of the digital transformation of the health system in Uruguay.

What is particularly remarkable is the strong governance established from the outset for this programme, with its broad and plural participation. Various bodies and their members carry out a range of tasks for the implementation and monitoring of objectives and processes, including the Management Committee, the highest authority responsible for defining and

[41](n.d.). Digital health platform. "Digital Health". *Agency for e-Government and the Information and Knowledge Society.* Available for download at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/programas/es-saluduy

approving policy and strategy as well as monitoring and approving budgets and investments; the Advisory Board, which provides technical advice; and various Advisory Groups.

This governance structure has undergone changes and updates over time, the most important of which are the following:

- Article 76 of Law No. 20,075[42], where the specific objectives of the Salud.uy programme were attributed to AGESIC and two Honorary Advisory Councils were added:

  - **Advisory Council on Digital Health Policies** composed of the Presidency of the Republic, the Ministry of Economy and Finance (MEF), the Ministry of Public Health (MSP, in Spanish), the National Health Board (JUNASA, in Spanish), the Agency for the Evaluation and Monitoring of Public Policies (AEMPP), the Agency for the Evaluation of Health Technologies (AETS, in Spanish), and the Agency for e-Government and the Information and Knowledge Society (AGESIC).
  - **Advisory Council for Inter-institutional Coordination in Digital Policies** composed of the Agency for e-Government and the Information and Knowledge Society (AGESIC), the National Telecommunications Administration (ANTEL, in Spanish), the State Health Services Administration (ASSE, in Spanish), the Social Prevention Bank (BPS, in Spanish), the National Resources Fund (FNR, in Spanish), the Integrated Network of Public Health Care Providers (RIEPS, in Spanish), Hospital de Clínicas, the Uruguayan Society for Standardisation, Exchange and Integration of Health Services Data and Information (SUEIIDISS, in Spanish), the Unions of Integral Health Care Providers (GREMCA, in Spanish), the Mobile Emergencies, the Faculty of Medicine and the Faculty of Engineering.

- Article 77 of Law No. 20,212[43] established that AGESIC would have the task of advising the MSP on the application of information technologies in the field of health in general, making the digital means for processing health information available to the ministry.

As well as being an example of governance, it is also an example of interoperability at all four levels. This can be demonstrated by Decree 242/017[44], which regulates information sharing

[42](2022, 3 November). Approval of the presentation of accounts and budget execution balance sheet. Financial year 2021. *Official Information Centre. Uruguayan regulations and legal notices.* Available at https://www.impo.com.uy/bases/leyes/20075-2022

[43](2023, 17 November). Law No. 20,212. Approval of the presentation of accounts and budget execution balance sheet. Financial year 2022. *Official Information Centre. Uruguayan regulations and legal notices.* Available at https://www.impo.com.uy/bases/leyes/20212-2023#:~:text=Cr%C3%A9ase%20una%20estructura%20integrada%20por,dependientes%20de%20la%20Direcci%C3%B3n%20General

[44](2017, 7 September). Decree No. 242/017. Regulation of Art. 466 regarding the mechanisms for the exchange of clinical information for health care purposes through the National Electronic Health Record System. Revocation of Decree No. 396/003. *Official Information Centre. Uruguayan Regulations and Legal Notices.* Available at https://www.impo.com.uy/bases/decretos/242-2017

mechanisms through the HCEN system and the Technology Reference Model[45].

Thus, Digital Health is a success story, an ecosystem that has existed for 12 years where data sharing between public and private actors of highly sensitive information takes place with strong governance, robust interoperability, ongoing reviews and improvements over time.

4.4 2023 census

The 2023 census in Uruguay was marked by a number of tensions regarding the privacy of personal data, the perception of privacy and the use of that information. Despite the INE's efforts to ensure the confidentiality of information, concerns about the handling of sensitive data persisted. The main controversy was related to the collection of sensitive data from the identity card[46] [47].

DatySoc conducted an extensive analysis of the issue and made some recommendations to citizens[48]. In this regard, the following points are worth mentioning:

- The ID number was mandatory in the digital format, while it was not mandatory in the in-person format, which raised doubts about the fairness of the treatment of citizens according to the modality chosen.
- There was little clarity on the specific use of both the ID number and its integration with other administrative records and its possible linkage with government databases.
- Fears were raised that this possible cross-referencing of data could open the door to increased state surveillance, as the census could allow the authorities to access sensitive information centrally.
- By requesting the ID number, discrimination by the government or third parties could be facilitated if the information collected is cross-referenced with other databases, especially in relation to issues such as income, health or ethnic characteristics.
- Although Law No. 18,331 establishes some standards of protection, it was questioned whether the handling of the ID number in the census fully complied with these regulations.
- Despite the INE's assurances that data protection standards would be followed, the lack of information on the specific measures taken to safeguard the data collected was noted, a factor that generated mistrust among the population.

[45](n.d.). HCEN reference architecture. *AGESIC and Uruguay Presidency.* Available at https://centroderecursos.agesic.gub.uy/web/arquitectura-salud.uy/inicio/-/wiki/Soluci%C3%B3n+peque%C3%B1os+prestadores/Arquitectura+Tecnol%C3%B3gica

[46](2023, 20 April). Census 2023: the first time the ID number will be requested and a warning will be issued about personal data protection. *El Observador*. Available at https://www.elobservador.com.uy/nota/censo-2023-pediran-el-numero-de-cedula-por-primera-vez-y-advierten-por-proteccion-de-datos-personales-2023420154121

[47](2023, 21 April). Census 2023: concern among organisations about the request for the ID number and "personal data protection". *La diaria.* Available at https://ladiaria.com.uy/usuarios/entrar/?article=106064

[48]DatySoc. (2023, 28 April). What you need to know about the ID number in the 2023 Census. *DatySoc.* Available at https://datysoc.org/2023/04/28/que-tenes-que-saber-sobre-la-cedula-en-el-censo-2023/#:~:text=El%20n%C3%BAmero%20de%20c%C3%A9dula%20de,deben%20responder%20el%20censo%20digital.

- Making the ID number compulsory in the digital census risks eroding citizens' trust in the census system and in the institutions in charge of handling their personal data.

Following this criticism, the INE modified the reasons for the mandatory request for the ID number and consulted the Personal Data Regulatory and Control Unit (URCDP), which issued an opinion seeking to provide the necessary guarantees within the scope of its competence[49].

From the above, it is clear that the different actors and regulations in force provided the necessary mechanisms for the protection of the human rights of citizens in this specific case. Secondly, it presents an opportunity for improvement at the necessary levels (regulatory, governance, etc.) to overcome these tensions in the future, even if Uruguay can be considered an example to follow in terms of data sharing and governance.

4.5 Automated facial recognition, cyber-patrolling and video surveillance

In February 2020, the Ministry of Internal Affairs procured a facial identification platform through a public tender.

In December of that year, Law No. 19,924[50] established the creation of a "facial identification database for administration and processing for public security purposes" (Articles 191 and 192) by the Ministry of Internal Affairs. However, despite the approval of these articles, no specific regulations, protocols for use or details of the automated facial recognition system have been developed, resulting in considerable discretion over the use of biometric data.

Civil society, through organisations such as DatySoc, highlights concerns and challenges related to the use of facial recognition in Uruguay.

By way of background, in November 2021, DatySoc addressed a request to the Ministry of Internal Affairs for access to public information within the framework of Law No. 18,381 regarding the acquisition of the facial identification platform and Automated Facial Recognition (AFR) software, a request that was rejected by the ministry in December of that year.

In March 2022, DatySoc published the report *Out of control: police use of automated facial recognition in Uruguay*[51] and that year sued the Ministry of Internal Affairs for refusing to provide the information mentioned. Even the UIAP ruled that "information that is public

[49](2023, 28 March). Opinion No. 4/023. *Personal Data Regulatory and Control Unit.* Available for download at https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/dictamen-n-4023

[50](2020, 30 December). Law No. 19,924. National budget for salaries, expenses and investments. Financial years 2020–2024. *Official Information Centre. Uruguayan regulations and legal notices.* Available at https://www.impo.com.uy/bases/leyes/19924-2020

[51]Díaz, Charquero Patricia. (2022). *Out of control. Police use of automated facial recognition in Uruguay.* Data and Society Laboratory (DatySoc) with the support of INDELA and Derechos Digitales América Latina. Available at https://datysoc.org/wp-content/uploads/2022/03/Informe-reconocimiento-facial-automatizado-Uruguay-2022-Datysoc.pdf

should be released, as well as classified information" (p. 4)[52]. In 2023, DatySoc published a document expanding on the report with the results of the lawsuit and the trial against the ministry[53].

Notwithstanding the specific results and the outcome of the case presented, the challenges are clear and include developing the discussion on the massive enrolment of the population in the AFR system, the prohibition or limitation of the use of AFR as a means of surveillance, the existence of regulations, public action protocols, impact analysis and risk assessment mechanisms, training on operation and risks, the need for citizen participation, and the existence of transparency and accountability processes.

In the same regard, DatySoc addressed cyber-patrolling in Uruguay and brought a lawsuit against the Ministry of Internal Affairs with similar characteristics to the case described above following another denial of access to public information[54] and finally, in June 2024, the ministry had to hand over information demonstrating that it collects personal data from open sources[55] for the prevention and/or investigation of crimes, and that it has conducted and approved studies, regulations, proposals for regulations or documents for which data has been collected from open sources. At the same time, it confirmed that it did not sign contracts with private companies involved in open-source data collection and analysis.

In this case, there are similar challenges that need to be addressed and that have to do with the review of Law No. 19,696 on the National System of State Intelligence and the use of Social Media Intelligence (SOCMINT) to collect information from open sources; the design of specific and public protocols for such activities; the review and/or creation of legislation; and transparency when establishing contracts related to the acquisition of technology used for surveillance activities, among others.

In Uruguay, the case of the ex-custodian of the President of the Republic was particularly significant, where chats in which he offered third parties contacts in the National Directorate of Information and Intelligence (DNII, in Spanish) and the tapping of mobile phones with El Guardián software were disseminated[56]. Despite the existence of a protocol for the legal interception of communications and an agreement between the Ministry of Internal Affairs, the Supreme Court of Justice, the Attorney General's Office and the telecommunications

[52]Executive council of the Access to Public Information Unit. (2022, 3 June). "Resolution No. 13 2022 / File No. 2021 – 2 – 10 0000432". Access to the Public Information Unit. *AGESIC and Uruguay Presidency* Available at https://www.gub.uy/unidad-acceso-informacion-publica/sites/unidad-acceso-informacion-publica/files/2022-06/RESUAIP22013-%20AA%20con%20MI.pdf

[53](n.d.). Out of Control: expanding on the report and results of the litigation on police use of automated facial recognition in Uruguay. *DatySoc*. Available at https://datysoc.org/fuera-de-control-ampliacion-del-informe/

[54]Díaz, Charquero Patricia and Gemetto, Jorge. (2024, July). *Cyber-patrolling: expanding on the report and results of the lawsuit on cyber-patrolling.* DatySoc with the support of INDELA and the Digital Rights Rapid Response Fund. Available at https://datysoc.org/litigio-ciberpatrullaje/

[55]Open source can be considered as any information that is accessible to anyone without the need for access credentials. In Uruguay, Article 3 of Law No. 19,696 (National State Intelligence System) defines it as "those from which a specific report can be obtained, with no other restriction than the task that requires it to be obtained".

[56]Silva, Laura. (2022). Astesiano's chats with important Argentinian agricultural businessman: he offered contacts in Intelligence, drones, mobile phone tapping with El Guardián and official vehicles. *La diaria*. Available at https://ladiaria.com.uy/usuarios/entrar/?article=99907

companies, there is still a long way to go[57].

[57]DatySoc. (2022, 24 November). On the Astesiano case and the need for regulation of police surveillance. *DatySoc.* Available at https://datysoc.org/2022/11/24/sobre-el-caso-astesiano-y-la-necesidad-de-regulacion-del-ecosistema-de-vigilancia-policial/

5. Conclusions, challenges and opportunities

Uruguay's coordinated and consistent digital strategy has positioned it as a regional benchmark in data governance and interoperability in the public sector. This progress has been driven by a sound and constantly evolving regulatory framework, accompanied by a robust technological infrastructure and a clear vision regarding data governance.

These aspects have been enhanced by institutional continuity in the data governance and data sharing agenda, an aspect in which Uruguay stands out in a region where the continuity of these policies faces multiple and complex challenges. However, this achievement has undoubtedly been the result of a long-term policy vision that has been sustained and enhanced through different governments and administrations that have allowed a constant and progressive evolution of the enabling framework in key areas such as personal data protection, information security and interoperability.

In any case, this consolidated differential in a positive regulatory process that improves transparency and facilitates inter-institutional collaboration should not fail to bring into focus that the path towards a more mature data sharing process poses important challenges that will require attention.

One of the most important aspects of the Uruguayan strategy is the creation of a digital architecture integrated into the public administration's data sharing ecosystem supported by the Interoperability Platform (PDI). This tool has enabled various agencies to share data efficiently and securely, which has improved the quality and speed of public services.

In addition, collaboration between public and private actors has fostered an ecosystem that has facilitated high-quality data sharing, helping to modernise the state and providing citizens with access to more services as in the emblematic case of Digital Health and the National Electronic Health Record.

This success story can provide important elements for replication in other priority areas where, despite good levels of data sharing in the public and private ecosystem, there is still room for further progress. In this regard, both the governance ecosystem and the technical discussion areas or data sharing architecture designed can be a helpful reference for data sharing in education, security, logistics, social welfare or finance.

At a regulatory level, Uruguay has a legal framework that is in line with international standards, a factor that ensures a favourable environment for personal data protection. Therefore, citizens have sufficient legal guarantees to defend their rights in the event of abuse or lack of transparency, which is essential for building an environment of trust in the handling of information.

This legal framework, together with the country's technological capabilities, creates the necessary conditions for democratic data governance. Recent cases such as the controversy over the 2023 census and the request for an ID number reveal the importance of ensuring that citizens perceive that their data is protected and that their privacy is respected with a state that proactively communicates any decisions that are taken.

Despite these advances, data sharing poses a number of risks that need to be carefully managed. In particular, privacy and personal data protection remain a concern, especially when handling sensitive data or in contexts where technologies such as artificial intelligence and facial recognition come into play.

These technological advances can be disruptive if they are not accompanied by a transparent regulatory framework and clear oversight to prevent abuse and mass surveillance. Their collective use in cases such as crime prevention adds complexity to the debate on digital rights and privacy. Therefore, without clear and transparent regulation, these mechanisms could generate a climate of distrust and perception of excessive surveillance, eroding trust in public institutions. It is therefore crucial that any technological advances are accompanied by robust communication and discussion policies, actively involving multiple stakeholders in the process.

In particular, it is important and necessary to enhance a trust-building perspective in the new strategies and governance schemes in development processes, accompanying the traditional perspectives of quality, data lifecycle, etc.

Another challenge lies in the involvement of the private sector and civil society in data governance. While AGESIC has been a key actor in the coordination of policies and practices, there continues to be room for coordination with the private sector and civil society, mainly in their participation in the monitoring of the defined policies, thus enhancing an inclusive, balanced and reliable ecosystem for decision-making regarding data. This aspect is particularly important in view of initiatives to include the private sector in public data sharing, as expressed in the recommendations proposed by AGESIC in this report.

Civil society organisations have also played a very important role in the area of transparency and open data, but their participation in data governance has been more reactive and limited by the spaces for dialogue provided by the government. Consequently, more effort is required to create inclusive and sustainable spaces for participation that allow these organisations to contribute in a meaningful way.

To consolidate the achievements and mitigate the risks, it is essential to institutionalise data governance spaces that ensure their continuity over time, integrating the private sector, academia and civil society in decision-making processes. Uruguay has the opportunity to continue progressing and building a sound governance system with the effective and proactive participation of different actors, that is, one that is not only conditioned by the creation of spaces for dialogue exclusively from the government at times of policy design. This will not only strengthen trust in data sharing but also foster innovation and the development of value-added services for society.

Similarly, it is crucial to achieve effective implementation of data interoperability between the public and private sector, facilitating the exchange of information by creating clear and transparent incentives. The use of technology platforms such as the Interoperability Platform (PDI) by private entities should be subject to strict rules to ensure data security and privacy. Complementing this point, the re-use of open data generated by public institutions can be enhanced with new incentive schemes, allowing the private sector to take advantage of it to develop new solutions.

In summary, Uruguay has come a long way in building a digital ecosystem that fosters data sharing in a secure and efficient way. However, the country still faces significant challenges in terms of engaging all sectors and in the practical implementation of policies, so it is necessary to continue promoting data governance that ensures the protection of citizens' rights while fostering collaboration and innovation. Public consultation processes such as those developed under the National Data and Artificial Intelligence Strategy are an excellent step in this direction, but they need to be strengthened and expanded.

As we move towards greater integration of technologies and expand interoperability capabilities, the risks also increase, so it is critical that the country maintains a balanced approach that prioritises technological innovation and the protection of citizens' rights by ensuring that data sharing remains a tool for development and inclusion without sacrificing privacy and public trust, because only in this way will it be possible to achieve a balance and systemic vision between open data, sharing, security of the information and privacy protection, building a future where data is a real driver for socio-economic development.

References

(2024, 18 September). Cross-border digital signature recognition agreements. *Electronic Certification Unit.* Available at https://www.gub.uy/unidad-certificacion-electronica/politicas-y-gestion/acuerdos-reconocimientos-transfronterizos-firma-digital

(2023, 18 December). Uruguay Digital Agenda 2025 – Resilient digital society. "Uruguay digital". *AGESIC.* Download available at: https://www.gub.uy/uruguay-digital/comunicacion/publicaciones/agenda-uruguay-digital-2025-sociedad-digital-resiliente/agenda-uruguay

European Commission. (2007). *Annex to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Interoperability Framework – Implementation Strategy.* Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017DC0134

(2022, 3 November). Approval of the presentation of accounts and budget execution balance sheet. Financial year 2021. *Official Information Centre. Uruguayan regulations and legal notices.* Available at https://www.impo.com.uy/bases/leyes/20075-2022

(n.d.). HCEN reference architecture. *AGESIC and Uruguay Presidency.* Available at https://centroderecursos.agesic.gub.uy/web/arquitectura-salud.uy/inicio/-/wiki/Soluci%C3%B3n+peque%C3%B1os+prestadores/Arquitectura+Tecnol%C3%B3gica

(n.d.). Conditions of use of the Interoperability Platform. Technical specification. Interoperability Platform. *AGESIC and Uruguay Presidency*. Available for download at https://centrodeconocimiento.agesic.gub.uy/documents/80442/88295/PGE-Condiciones-de-uso-Plataforma-v01-21.pdf/7786ceca-21b5-0a1d-254e-1293a1330876?version=1.0

(2023, 20 April). Census 2023: the first time the ID number will be requested and a warning will be issued about personal data protection. *El Observador*. Available at https://www.elobservador.com.uy/nota/censo-2023-pediran-el-numero-de-cedula-por-primera-vez-y-advierten-por-proteccion-de-datos-personales-2023420154121

(2023, 21 April). Census 2023: concern among organisations about the request for the ID number and "personal data protection". *La diaria.* Available at https://ladiaria.com.uy/usuarios/entrar/?article=106064

Executive council of the Access to Public Information Unit. (2022, 3 June). "Resolution No. 13 2022 / File No. 2021 – 2 – 10 0000432". Access to the Public Information Unit. *AGESIC and Uruguay Presidency* Available at

https://www.gub.uy/unidad-acceso-informacion-publica/sites/unidad-acceso-informacion-publica/files/2022-06/RESUAIP22013-%20AA%20con%20MI.pdf

DatySoc. (2023, 28 April). What you need to know about the ID number in the 2023 Census. *DatySoc*. Available at https://datysoc.org/2023/04/28/que-tenes-que-saber-sobre-la-cedula-en-el-censo-2023/#:~:text=El%20n%C3%BAmero%20de%20c%C3%A9dula%20de,deben%20responder%20el%20censo%20digital.

DatySoc. (2022, 24 November). On the Astesiano case and the need for regulation of police surveillance. *DatySoc*. Available at https://datysoc.org/2022/11/24/sobre-el-caso-astesiano-y-la-necesidad-de-regulacion-del-ecosistema-de-vigilancia-policial/

(2021, 12 May). Decree No. 134/021. Approval of "Uruguay Digital Agenda 2025". *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/134-2021%EF%BB%BF

(2009, 5 January). Decree No. 664/008. Creation of the register of personal databases. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/664-2008

(2020, 21 February). Decree No. 64/020. Regulation of Art. 37 to 40 of Law 19,670 and Art. 12 of Law 18,331, on personal data protection. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/64-2020

(2017, 7 September). Decree No. 242/017. Regulation of Art. 466 regarding the mechanisms for the exchange of clinical information for health care purposes through the National Electronic Health Record System. Revocation of Decree No. 396/003. *Official Information Centre. Uruguayan Regulations and Legal Notices.* Available at https://www.impo.com.uy/bases/decretos/242-2017

(2023, 16 November). Decree No. 353/023. Regulation of Art. 76 of Law No. 19,355, regarding the procedure applicable by public entities, in order to simplify their procedures, following the guidelines of AGESIC. Amendment of Art. 15 and repeal of Art. 13 of Decree No. 178/013. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/353-2023

(2009, 15 September). Decree No. 414/009. Regulation of Law 18,331 on personal data protection. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/414-2009

(2013, 25 July). Decree No. 178/013. Regulation of Articles 157 to 160 of Law No. 18,719, relating to the regulation of the exchange of information between public, state or non-state entities. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/178-2013

(2010, 10 August). Decree No. 232/010. Regulation of the law on the right of access to public information. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/decretos/232-2010/

Díaz, Charquero Patricia and Gemetto, Jorge. (2024, July). *Cyber-patrolling: expanding on the report and results of the lawsuit on cyber-patrolling.* DatySoc with the support of INDELA and the Digital Rights Rapid Response Fund. Available at https://datysoc.org/litigio-ciberpatrullaje/

Díaz, Charquero Patricia. (2022). *Out of control. Police use of automated facial recognition in Uruguay.* Data and Society Laboratory (DatySoc) with the support of INDELA and Derechos Digitales América Latina. Available at https://datysoc.org/wp-content/uploads/2022/03/Informe-reconocimiento-facial-automatizado-Uruguay-2022-Datysoc.pdf

(2023, 28 March). Opinion No. 4/023. *Personal Data Regulatory and Control Unit.* Available for download at https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/dictamen-n-4023

(2023, 18 May). Data strategy of the Montevideo City Council. *Montevideo City Council*. Available for download at https://montevideo.gub.uy/noticias/tecnologia/estrategia-de-datos-de-la-intendencia-de-montevideo

(2024, 3 April). Cross-border signature in Mercosur. "Digital signature". *Electronic Certification Unit.* Available at https://www.gub.uy/unidad-certificacion-electronica/comunicacion/noticias/firma-transfronteriza-mercosur

(n.d.). Out of Control: expanding on the report and results of the litigation on police use of automated facial recognition in Uruguay. *DatySoc.* Available at https://datysoc.org/fuera-de-control-ampliacion-del-informe/

(1991, 18 January). *610 – 1990 – IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. IEEE. DOI: 10.1109/IEEESTD.1991.106963

(n.d.). Report on Article 74 Law No. 20,212. Recommendations for regulation of Artificial Intelligence (AI) focusing on ethical development, the protection of human rights and the promotion of technological innovation. *AGESIC and Uruguay Presidency*. Available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Art%C3%ADculo%2074%20de%20la%20Ley%20N%C2%BA20.212%20recomendaciones%20para%20una%20regulaci%C3%B3n%20de%20la%20Inteligencia%20Artificial%20%28IA%29_0.pdf

(n.d.). “360° Data Initiative”. “360° Data”. *Agency for e-Government and the Information and Knowledge Society.* Available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/node/3557

International Standard. (2015, May). *Information technology – Vocabulary*. ISO / IEC 2382:2015. Available at https://www.iso.org/standard/63598.html

(2024, 15 January). The European Commission confirms Uruguay’s adequate level of data protection. Available at the *Personal Data Regulatory and Control Unit*. https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/comision-europea-ratifica-nivel-adecuado-uruguay-para-proteccion-datos-0

(2013, 7 January). Law No. 19,030. Approval of the convention for the protection of individuals with regard to automatic processing of personal data. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/19030-2012

(2021, 27 April). Law No. 19,948. Adoption of the protocol amending the Strasbourg Convention for the protection of individuals with regard to the processing of personal data. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/19948-2021

(2018, 25 October). Law No. 19,670. Approval of the presentation of accounts and budget execution balance sheet. Financial year 2017. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/19670-2018

(2022, 3 November). Law No. 20,075. Approval of the presentation of accounts and budget execution balance sheet. Financial year 2021. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/20075-2022

(2023, 17 November). Law No. 20212. Approval of the presentation of accounts and budget execution balance sheet. Financial year 2022. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/20212-2023/74

(2023, 17 November). Law No. 20,212. Approval of the presentation of accounts and budget execution balance sheet. Financial year 2022. *Official Information Centre. Uruguayan regulations and legal notices.* Available at https://www.impo.com.uy/bases/leyes/20212-2023#:~:text=Cr%C3%A9ase%20una%20estructura%20integrada%20por,dependientes%20de%20la%20Direcci%C3%B3n%20General

(2009, 5 November). Law No. 18,600. Electronic document and electronic signature. Admissibility, validity and effectiveness. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/18600-2009

(2008, 18 August). Law No. 18,331. Law on personal data protection. *Official Information Centre*. *Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/18331-2008/34

(2011, 5 January). Law No. 18,719. National budget for salaries, expenses and investments. Financial year 2010–2014. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/18719-2010/149

(2011, 5 January). Law No. 18,719. National budget for salaries, expenses and investments. Financial year 2010–2014. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/18719-2010/

(2015, 30 December). Law No. 19,355. National budget for salaries, expenses and investments. Financial year 2015–2019. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/19355-2015/76

(2015, 30 December). Law No. 19,355. National budget for salaries, expenses and investments. Financial year 2015–2019. *Official Information Centre. Uruguayan regulations and legal notices*. Available at https://www.impo.com.uy/bases/leyes/19355-2015/82

(2020, 30 December). Law No. 19,924. National budget for salaries, expenses and investments. Financial years 2020–2024. *Official Information Centre. Uruguayan regulations and legal notices.* Available at https://www.impo.com.uy/bases/leyes/19924-2020

Naser, Alejandra. (Coord.). (2011). "Digital governance and government interoperability. A guide to implementation". *Project documents*. (LC / TS. 2021 / 8°), Santiago. Economic Commission for Latin America and the Caribbean (ECLAC). Available at https://repositorio.cepal.org/server/api/core/bitstreams/6a12e389-3dcb-4cba-830a-99f038835423/content

(2023, 13 December). New technical cooperation agreement on digital identification between Uruguay and Paraguay. "Official identification". *Agency for e-Government and the Information and Knowledge Society.* Available for download at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/nuevo-convenio-cooperacion-tecnica-identificacion-digital-entre-uruguay

(n.d.). 5th National Action Plan for Open Government 2021–2024. *AGESIC and Uruguay Presidency*. Available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/book/6187/download

(n.d.). Digital Government Plan 2025. *AGESIC and Uruguay Presidency*. Available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/2021-07/Plan%20de%20Gobierno%20Digital%202025_0.pdf

(n.d.). Interoperability Platform. *AGESIC and Uruguay Presidency*. Available at https://centrodeconocimiento.agesic.gub.uy/web/ccio/plataforma-de-interoperabilidad

(2024, 17 July). "Process of reviewing the Artificial Intelligence Strategy and developing the National Data Strategy. "Policy and Management". *Agency for e-Government and the Information and Knowledge Society.* Available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/proceso-revision-estrategia-inteligencia-artificial-elaboracion-estrategia

(2022, 3 June). 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). Available at https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

(2012, 8 June). Resolution No. 23/021. *Personal Data Regulatory and Control Unit*. Available for download at https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021

(n.d.). Digital health platform. "Digital Health". *Agency for e-Government and the Information and Knowledge Society.* Available for download at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/programas/es-saluduy

(n.d.). Cross Border Digital Services. Programme for strengthening cross-border electronic transactions in Latin America and the Caribbean. "Regional Public Assets". *Reagealc*. Available at https://www.redgealc.org/site/assets/files/13516/anexo_1_-_servicios_digitales_transfronterizos_-_indice.pdf

Silva, Laura. (2022). Astesiano's chats with important Argentinian agricultural businessman: he offered contacts in Intelligence, drones, mobile phone tapping with El Guardián and official vehicles. *La diaria*. Available at https://ladiaria.com.uy/usuarios/entrar/?article=99907

UN. ECLAC and European Commission. (2007). *White book of e-government interoperability for Latin America and the Caribbean*. Available in: White book of e-government interoperability for Latin America and the Caribbean: version 3.0 (cepal.org)

(2023, 12 December). Uruguay and Brazil sign a technical cooperation agreement on digital identification. "Official identification". *Electronic Certification Unit.* Available for download at https://www.gub.uy/unidad-certificacion-electronica/comunicacion/noticias/uruguay-brasil-firman-convenio-cooperacion-tecnica-identificacion-digital

Annex: Legislative landscape

This section was prepared on a pro bono basis by the law firm **ECIJA Uruguay**, based on the connection facilitated by TrustLaw, the global legal pro bono network of the **Thomson Reuters Foundation**. Its purpose is to contextualise the legal framework applicable to data sharing, providing a legal basis that enriches the analysis of this case study.

Disclaimer of liability: This report is offered for information purposes only. It is not legal advice. Readers are urged to seek advice from qualified legal counsel in relation to their specific circumstances. We intend the report's contents to be correct and up to date at the time of publication, but we do not guarantee their accuracy or completeness, particularly as circumstances may change after publication. The Latin American Open Data Initiative (Iniciativa Latinoamericana por los Datos Abiertos, ILDA), ECIJA Uruguay and the Thomson Reuters Foundation accept no liability or responsibility for actions taken or not taken or any losses arising from reliance on this report or any inaccuracies herein..

ECIJA Uruguay has generously provided pro bono research to ILDA. However, the contents of this report should not be taken to reflect the views of ECIJA Uruguay or the lawyers who contributed.
Similarly, the Thomson Reuters Foundation is proud to support our TrustLaw member ILDA with their the work on this report, including the publication and the pro bono connection that made the legal research possible. However, in accordance with the Thomson Reuters Trust Principles of independence and freedom from bias, we take no position on the contents of, or views expressed in, this report.

Through a jointly developed questionnaire, ECIJA Uruguay was asked to answer the following questions on the Uruguayan regulatory framework:

1- What is the current legal framework, including laws, regulations, strategies and public policies, around the use, collection and processing of data in Uruguay?

A) Laws and regulations.

i. Article 72 of the National Constitution[58] recognises the right to the protection of personal data as an inherent right of the person.

ii. Law No. 19,948[59] approved Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol.

[58] https://www.impo.com.uy/bases/constitucion/1967-1967
[59] https://www.impo.com.uy/bases/leyes/19948-2021

iii. Law No. 18,331[60] regulates Personal Data Protection and the Habeas Data Action, which is regulated by Decree No. 664/2008 and 414/009.

iv. Decree 64/020[61] of Law No. 19,670 on Budget regulates Articles 37 to 40 subject to Law No. 18,331, concerning personal data protection.

v. Law No. 18,381[62] regulated by Decree 232/010[63] regulates the Right of Access to Public Information.

vi. Budget Law No. 19,355[64] and its Regulatory Decree 54/017[65] regulates the technical document called "Technical Guidelines for Open Data".

vii. Article 159 of Law No. 18,719[66] together with its Regulatory Decree No. 178/013[67] on Budget regulates the "Exchange of Information between State or non-State Public Entities".

B) Authority from which such regulations emanated, year of enactment and subsequent amendments or regulations.

i. The current National Constitution of Uruguay was established in 1967, emanating from a drafting process carried out by a Constituent Assembly, elected in 1966. It has been amended in 1989, 1994, 1997 and 2004.

ii. Law No. 19,948 was issued by the Legislative Branch and enacted in 2021 by the Executive Branch.

iii. Law No. 18,331 was enacted in 2008, issued by the Legislative Branch. Regulatory Decree No. 414/009 was enacted in 2009, issued by the Executive Branch.

iv. Law No. 19,670 was enacted in 2018, issued by the Legislative Branch, while Regulatory Decree 64/020 was enacted in 2008 by the Executive Branch.

v. Law No. 18,381 was enacted in 2008, issued by the Legislative Branch. Decree 232/010 was enacted in 2008, issued by the Executive Branch.

vi. Law No.19,355 was enacted in 2015, issued by the Legislative Branch, and Decree No. 54/017 was enacted in 2017, issued by the Executive Branch.

vii. Law No. 18,719 was enacted in 2010, issued by the Legislative Branch, while Decree No. 178/013 was enacted in 2013, issued by the Executive Branch.

C) Competent authorities.

In Uruguay, the regulation and control of the use, collection and processing of data falls under the purview of two main bodies:

1. **Personal Data Regulatory and Control Unit (URCDP)**[68] It was created by Article 31 of Law No. 18,331 on 11 August 2008. This is the supervisory body, with technical

[60] https://www.impo.com.uy/bases/leyes/18331-2008
[61] https://www.impo.com.uy/bases/decretos/64-2020
[62] https://www.impo.com.uy/bases/leyes/18381-2008
[63] https://www.impo.com.uy/bases/decretos/232-2010
[64] https://www.impo.com.uy/bases/leyes/19355-2015
[65] https://www.impo.com.uy/bases/decretos/54-2017
[66] https://www.impo.com.uy/bases/leyes/18719-2010
[67] https://www.impo.com.uy/bases/decretos/178-2013
[68] https://www.gub.uy/unidad-reguladora-control-datos-personales/

autonomy, in charge of ensuring compliance with Law No. 18,331 on Personal Data Protection and Habeas Data Action. Among others, its tasks and powers include the following: laying down the rules and regulations to be observed in the course of the activities covered by the law; carrying out out a census of the databases covered by the law and keeping a permanent record of them; supervising compliance with the law by individuals or by public or private legal entities that process personal data; controlling the observance of the legal regime, in particular the rules on legality, integrity, truthfulness, proportionality and data security, by the subjects concerned, and to this end carrying out the relevant oversight and inspections; hearing and deciding on complaints filed by data subjects, investigating possible violations of their rights and adopting the corresponding measures; providing guidance to citizens and organisations on their data protection rights and obligations; spreading the culture of data protection and conducting awareness campaigns on the importance of safeguarding privacy. Its competence extends to all sectors that process personal data, both public and private.

It is directed by a Council composed of three members: the Executive Director of AGESIC and two members appointed by the Executive Branch from among persons whose personal and professional background and knowledge in the field ensure independence, efficiency, objectivity and impartiality in the performance of their duties in accordance with the provisions of Article 31 of Law No. 18,331. With the exception of the Executive Director of AGESIC, the members will serve for four years and may be reappointed.

2. **Agency for e-Government and the Information and Knowledge Society (AGESIC)**[69] It was created by Article 72 of Law No. 17,930 in December 2005. It is an executing unit with technical autonomy that is dependent on the Presidency of the Republic of Uruguay. It has a broader approach covering data management within the framework of e-government and the information society. It drives the digital transformation of the state by promoting the use of information and communications technologies in public management. It promotes transparency and access to public information by ensuring that government data are accessible and understandable for citizens. It develops public policies on information and communications technologies, including those related to data management. It promotes the security of the state's IT systems and the protection of data against possible cyber-attacks. Its competence is mainly focused on the public sector, but it also has an impact on the private sector through its policies and standards.

   The law by which it was created established an Honorary Board of Directors (CDH, in Spanish), in charge of designing its lines of action, evaluating its performance and the results obtained, assisted by three other honorary boards: Information Society Council, Business Advisory Council and Public IT Advisory Council.

   Decree No. 184/015 sets out the mission, objectives and tasks legally attributed to AGESIC. This agency seeks to innovate and streamline the ways in which people

[69] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/

interact with the public administration, incorporating digital technologies and better ways of working, with a focus on people.

Additional information:

Open Data in Uruguay

Article 82[70] of Law No. 19,355 on Open Data establishes that public bodies must, as a minimum, publish in open format the information required by Article 5[71] of the Law on Access to Public Information. They may also publish as open data information that they consider useful for a particular sector of society, even if it does not fall within the scope of this article.

Its Regulatory Decree No. 54/017 sets the technical guidelines for the publication of data and is aimed at IT technical staff.

Article 159[72] of Law No. 18,719 together with its Regulatory Decree No. 178/013 are based on improving the exchange of information and optimising the provision of services, in line with principles of good governance and transparency.

Uruguay has established a sound regulatory framework for the use, collection and processing of data in the public sector. Open data is a valuable resource for strengthening democracy, improving governance and promoting sustainable development.

Open data allows citizens to access information about government activities, enabling an informed dialogue between government and society. In Uruguay there is quite a large amount of open data, and there is an Open Data Portal[73] that makes it easy to find it. Openly available public sector data usually include information that is publicly available and not subject to restrictions. The Portal provides access to a variety of datasets such as budget and public revenue information, public policy reports, documents analysing the implementation and impact of government policies, public procurement and environmental data.

Some examples of open data in the public sector are described below. The National Institute of Statistics (INE)[74] publishes statistical data on population, economy and society, which are used for research and public policy. The Ministry of Public Health[75] shares data including statistics on diseases, vaccination and health services. The National Road Safety Unit (UNASEV, in Spanish)[76] provides transport data, both traffic accidents and statistics on mobility and road safety in the country. The Council of Initial and Primary Education (CEIP, in

[70] https://www.impo.com.uy/bases/leyes/19355-2015/82
[71] https://www.impo.com.uy/bases/leyes/18381-2008/5
[72] https://www.impo.com.uy/bases/leyes/18719-2010/159#:~:text=Cuando%20proceda%20el%20intercambio%20de,competente%20y%20formalizar%20un%20acuerdo.
[73] https://ckan.montevideo.gub.uy
[74] https://www3.ine.gub.uy/rraa/contacto.html
[75] https://www.gub.uy/ministerio-salud-publica/
[76] https://www.gub.uy/unidad-nacional-seguridad-vial/

Spanish)[77] and other educational institutions publish information on enrolment, academic performance and other aspects of the education system.

National Catalogue of Open Data

It is a tool that facilitates access to open data, presenting it in an orderly manner by categories, organisations and tags, among other options[78]. In each section, it is indicated whether it is informative or mandatory. The informative sections provide context and definitions to facilitate the understanding of the document, and the mandatory sections prescribe guidelines to be complied with by the public bodies established in Article 82 of Law No. 19,355 mentioned above.

2- Are there any laws, regulations or provisions specific to data sharing or data exchange among government bodies or agencies?

A) Law and regulations

Although there is no specific regulation in Uruguay that exhaustively regulates the exchange of data among government agencies, various legal bodies and provisions have an impact on this practice. Law No. 18,331 on Personal Data Protection establishes the fundamental principles for the processing of data, including their transfer between public entities. Law No. 18,381 on Access to Public Information guarantees citizens' right of access to government information, which indirectly encourages inter-agency data sharing. Furthermore, Decree No. 134/021 and the National Cybersecurity Strategy establish general guidelines on information security and inter-agency collaboration, impacting on data sharing practices. Despite this regulatory diversity, the lack of a specific framework law makes harmonisation and uniform application of the established principles difficult.

B) Scope of application within the public sector.

The scope of data sharing in the public sector, in current legislation, covers all interactions between different state bodies involving the transfer of information. This means that any government entity, from ministries to local councils, that needs to share data with another is subject to the rules and regulations established for this purpose.

In general, there is an alignment between the different rules and policies regulating data sharing in the Uruguayan public sector. However, it is important to highlight some key points:

- Complementarity: The different rules complement each other, establishing a comprehensive regulatory framework. For example, Law No. 18,331 establishes general principles for data protection, while Law No. 18,381 guarantees access to public information, creating a balance between data protection and transparency.
- Implementation challenges: Despite the existence of a sound regulatory framework, the effective implementation of these standards presents challenges,

[77] https://uruguay.fandom.com/es/wiki/Consejo_de_Educación_Inicial_y_Primaria#:~:text=El%20Consejo%20de%20Educación%20Inicial,al%20ámbito%20de%20su%20competencia.
[78] https://catalogodatos.gub.uy/

such as the need for investment in technology, staff training and coordination among different agencies.

- Constant evolution: The regulatory framework is constantly evolving, adapting to technological changes and the new public administration requirements. This can lead to some complexity and the need for regular updates.

C) Coordination process for sharing data between national government bodies or agencies and local government bodies or agencies.

While there is no single, standardised procedure for data sharing among government agencies in Uruguay, there is a solid regulatory and political framework that establishes the fundamental principles and general rules for these types of transactions. This framework is composed of a variety of laws, decrees, resolutions and public policies designed to guarantee information security, protect individuals' privacy, promote transparency in government processes and ensure efficiency in data management.

The Law on Personal Data Protection (Law No. 18,331) is a fundamental pillar in this framework, establishing the principles and rules for the processing of personal data. In addition, the Law on Access to Public Information (Law No. 18,381) guarantees citizens' right to access public information and promotes transparency in government management. In addition, various sector-specific rules and inter-institutional agreements complement this framework, setting particular requirements for data sharing in different areas.

This legal and political framework seeks to strike a balance between the need to share information to improve decision-making and deliver public services and the protection of individual rights. Through this framework, mechanisms are established to ensure that data are processed lawfully, fairly and transparently, and that the necessary technical and organisational measures are taken to protect them from any unauthorised or unlawful processing.

Additional information:

Confidentiality is established in the procedure for the transfer of data, ensuring the protection of information and defining the entities' responsibilities in the handling of such information. It is established that AGESIC will make an Interoperability Platform (IPD)[79] available to Public Entities, where they will be able to exchange information in electronic format in a secure and reliable manner. Its objective is to facilitate and promote the implementation of Digital Government services, establishing guidelines for the interoperability of systems, facilitating the collection and efficient use of data.

79 https://centrodeconocimiento.agesic.gub.uy/documents/80442/88295/PGE-Plataforma-Interoperabilidad-Presentación-Técnica-v01.00.pdf/0ad91823-cd02-7edf-50c7-432c2838c3a7?version=1.0

Article 78 of Law No. 20,212 implemented a National Cybersecurity Strategy, and another one on digitalisation called "Uruguay Digital Agenda 2025"[80], which includes the use of new technologies such as interoperable platforms for the exchange of open data between agencies. This initiative seeks to strengthen the use of information technologies (ICTs) in the State to improve the quality of public services and promote the use of open data. As regards the National Cybersecurity Strategy, it advocates protecting the information handled by the State by implementing security protocols against possible cyber-attacks or unauthorised access. The aim is to prevent and mitigate risks in the use of technologies. The country's digital policy, through the Uruguay Digital Agenda 2025, seeks to promote transparency in public management through open data initiatives.

Interoperability facilitates efficiency in the public sector, allowing Uruguayan public institutions to share information in real time, avoiding duplication, streamlining administrative procedures and improving the provision of services to citizens when interacting with the State.

3- Bilateral or multilateral agreements in force that provide for data sharing between states

Uruguay has signed bilateral and multilateral agreements providing for data sharing between states, particularly in areas such as personal data protection, judicial cooperation, security and taxation.

Uruguay adheres to the international standards of the Organisation for Economic Co-operation and Development (OECD), such as the Common Reporting Standard (CRS), which establishes a framework for the automatic exchange of financial information between countries[81].

It is also a party to Agreements on Tax Information Exchange with the United States[82] and European Union countries, with the aim of combating tax evasion, which allow the exchange of financial information between the tax authorities of the signatory states under strict confidentiality and data protection rules.

In the area of health care, multilateral agreements were signed for the exchange of epidemiological and health data, particularly in the context of the Pan American Health Organisation (PAHO)[83] and the World Health Organisation (WHO). These Agreements facilitate the flow of information on infectious diseases and health emergencies, always under rules that protect sensitive personal data.

---

80 https://www.gub.uy/uruguay-digital/sites/uruguay-digital/files/documentos/publicaciones/Documento%20AUD%202025.pdf

81 https://www.gub.uy/ministerio-relaciones-exteriores/comunicacion/comunicados/uruguay-adhiere-recomendacion-ocde-sobre-inteligencia-artificial

82 https://www.ambito.com/uruguay/se-aprobo-la-ley-intercambio-informacion-financiera-estados-unidos-n6063690

83 https://www.paho.org/sites/default/files/cooperacion-tecnica-ops-uruguay-2022_0.pdf

Within the framework of Mercosur, it participated in several Agreements such as the Tax Information Exchange and Double Taxation Avoidance Method in 2012[84].

It participated in Agreements on Security and Justice Cooperation, related to the exchange of data on criminal investigations, immigration and border security, and Judicial and Criminal Cooperation Agreements, including Mutual Legal Assistance and Extradition Treaties with countries in Latin America and Europe[85].

4- Commitment towards international principles related to data sharing, such as the European Interoperability Framework

Uruguay has demonstrated a growing commitment to modernising its government systems and promoting data interoperability. Although it has not formally adopted the European Interoperability Framework, it has implemented several initiatives that are aligned with its principles.

Uruguay's Progress on Data Sharing

Interoperability Agreements: The Uruguayan government has signed framework agreements on interoperability between different institutions, such as the judiciary, the Ministry of Internal Affairs and the Attorney General's Office. These agreements aim to improve communication between systems and facilitate inter-institutional coordination.

Uruguay.uy platform: This digital platform integrates various government services, allowing citizens to access procedures and formalities more efficiently. While not a direct adoption of the European Framework, it represents an important step towards interoperability of government systems.

Participation in International Forums: Uruguay actively participates in international forums on e-government and digital transformation, which allows it to keep abreast of the latest trends and best practices in data sharing.

The European Union's General Data Protection Regulation (GDPR)[86] has influenced Uruguayan legislation as the European Union has recognised Uruguay as a territory that guarantees an adequate level of personal data protection[87].

On the other hand, and taking into account other international measurement mechanisms, according to the Regional Open Data Barometer (implemented by ILDA in Latin America)[88], which measures three dimensions – readiness in terms of open government data, the implementation of the dataset, and its political, social and economic impact, Uruguay's current position is as follows:

---

[84] https://www.argentina.gob.ar/normativa/nacional/ley-26758-201049

[85] https://www.mercosur.int/ciudadania/estatuto-ciudadania-mercosur/3-cooperacion-judicial-y-consular/

[86] https://www.boe.es/doue/2016/119/L00001-00088.pdf

[87] https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/comision-europea-ratifica-nivel-adecuado-uruguay-para-proteccion-datos-0

[88] https://idatosabiertos.org/proyectos/barometro-regional-de-datos-abiertos/

- Ranked 64th in the world.

- Ranked 1st in South America.

5- Case law and other relevant information.

In Uruguay, the concept of "data sharing" is beginning to gain importance, especially with the increasing use of technologies and the importance of personal data protection. As for legal scholars' opinions and case law on this subject, it is a developing area influenced by the regulatory framework of personal data protection, which has as its main source the aforementioned Law No. 18,331 (Law on Personal Data Protection and Habeas Data Action) and its regulation, which follows the principles of privacy and data protection established by the European Union's General Data Protection Regulation (GDPR) with regard to fundamental rights.

Legal scholarship:

Uruguayan legal scholarship in relation to data sharing has focused mainly on the analysis of Law No. 18,331 and its compatibility with international standards such as the GDPR. Studies and publications highlight the need for more detailed regulation of data transfer and sharing between companies, public entities and across borders. Some of the points covered in the analyses are:

- The limits of the data subject's consent to the transfer of data.
- The responsibility of data controllers and data processors.
- The role of the Agency for e-Government and the Information Society (AGESIC) as a regulatory authority.

Case law:

In terms of case law, while there are not many court decisions specifically on data sharing, some cases have addressed related issues, including the following:

Scope of the Law on Personal Data Protection: Cases have been analysed that have delimited the scope of the law and the rights of data subjects.

- Informed consent: Case law has established criteria to determine when the consent given for the processing of personal data is valid and effective. (e.g. Final Judgment No. 128/2017, 7th Civil Court of Appeal).
- Rights of data subjects: Case law has recognised and protected the rights of data subjects, such as the right of access, rectification, deletion and opposition to the processing of their data. (e.g. Final Judgment No. 109/2023, 1st Civil Court of Appeal).
- Responsibility of data controllers: Criteria have been established to determine the liability of entities processing personal data and the consequences of breaches of the law. (e.g. Final Judgment No. 43/2018, 6th Civil Court of Appeal).

Additionally, although it is not technically case law, AGESIC has issued guidelines and recommendations that interpret the regulations in data processing situations, such as the international transfer of data or the exchange of information between public and private bodies, issues that are linked to data sharing and which are gradually being taken into account by judges when making rulings.

Although Uruguay has advanced legislation on data protection, there is still a lack of further development in terms of specific regulations for data sharing, so legal scholarship and case law will continue to evolve on this issue.