A Report from the International Foundation for Electoral Systems

Solving the Puzzle: Making Political Finance Data Work

Steps Toward Interagency Interoperability

JULY 2026

About IFES

At IFES, we envision a world where people are free, societies are democratic, and elections are fair. We collaborate with civil society, public institutions, and the private sector to build resilient democracies that deliver for everyone. As a global leader in the promotion and protection of democracy, our technical assistance and applied research develop trusted electoral bodies capable of conducting credible elections; effective and accountable governing stakeholders; civic and political processes in which all people can safely and equally participate; and innovative ways in which technology and data can positively serve elections and democracy. Since 1987, IFES has worked in more than 145 countries, from developing to mature democracies. IFES is a global, nonpartisan organization and registered as a nonprofit organization [501(c)(3)] under the United States tax code.

International Foundation
for Electoral Systems

2000 M Street NW, Washington, DC, 20036, United States

www.IFES.org IFES1987

To request reprints or author engagment, please message Media@IFES.org

Solving the Puzzle: Making Political Finance Data Work

Steps Toward Interagency Interoperability

AUTHOR

CHELSEA DREHER

IFES RESEARCH & ANTI-CORRUPTION SPECIALIST

PUBLISHED JULY 2026

International Foundation for Electoral Systems

Sida

About This Paper

Political party and campaign finance transparency are essential to maintaining a level electoral playing field and preventing undue influence in politics. The effectiveness of accountability mechanisms, however, depends in large part on the quality and usability of underlying data. As legal and regulatory frameworks evolve to address new forms of campaigning and illicit interference, the volume and complexity of financial data continue to grow, making effective tracking and analysis increasingly challenging. Robust digital recordkeeping, coupled with targeted and timely interagency data sharing, can reduce reporting burdens, strengthen compliance and verification processes, and improve accountability for all actors involved in political finance oversight and government integrity.

Drawing on desk research and interviews with state and non-state political finance experts across diverse legal contexts, this guide provides a flexible and practical framework for improving the quality and interoperability of political finance data. It is designed to meet oversight institutions at different stages of digitalization and data management. The guide introduces key terminology to support engagement with data specialists and engineers; outlines steps to strengthen and clean internal datasets; identifies entry points for advancing interoperability; and offers recommendations for navigating inter-agency data-sharing arrangements – helping institutions to establish effective collaboration frameworks from the outset.

The author would like to sincerely thank Magnus Öhman, Regina Waugh, Cassandra Emmons, Erica Shein, and Christopher Le Mon for their thoughtful contributions to and review of this publication, and Jaime L. Jarvis for her exceptional copy editing and formatting assistance. Special thanks are also due to technical experts who provided interviews and supplemental reviews of this report, sharing their practical experience and insights to strengthen the text. These individuals include: Lina Petronienė (Chairperson of the Central Electoral Commission of Lithuania), Milda Pocevičiūtė (Head of the Political parties and political campaigns funding control unit, Central Electoral Commission of the Republic of Lithuania), Mariam Galstyan (Former Acting Chair, Armenia Corruption Prevention Commission), Lilit Aleksanyan (Former Member, Armenia Corruption Prevention Commission), Sandra Ximena Martínez (Political Finance Specialist and Program Director, Transparency International Colombia), Igor Feshchenko (Political Finance Expert), Septimius Pârvu (Election Expert, Expert Forum), Natalia Carfi (Executive Director, Open Data Charter), Mariam Hoveyan (Educational and Electoral Program Director, Transparency International Anti-Corruption Center, Armenia), Oriana Ivković Novokmet (Executive Director, Gong), and Nicolae Panfil (Program Director, Promo-LEX).

IFES extends its appreciation to the Swedish International Development Cooperation Agency (Sida) for generously supporting the development of this resource and for its commitment to strengthening democratic resilience worldwide. The views expressed herein are those of the author and do not necessarily reflect the official positions of Sida.

Table of Contents

Introduction

Political finance transparency is a cornerstone of democratic accountability. Laws and regulations governing party, candidate, and campaign finance are intended to limit undue influence and enable effective oversight, ensuring that all actors are playing by the same rules. Delivering on these objectives, however, depends heavily on the quality and usability of political finance data.

Tracking and verifying the accuracy and completeness of party and campaign finance reports is a significant challenge, particularly as legal and regulatory frameworks evolve to capture new forms of campaigning and illicit interference. As oversight mandates expand and reporting requirements grow more complex, political finance institutions and political actors must adapt. Robust digital recordkeeping, coupled with targeted and timely interagency data sharing, has the potential to reduce reporting burdens, strengthen and streamline compliance and verification checks, and improve accountability for all actors involved in political finance oversight and government integrity.

Interoperable data – standardized data that can be shared and understood across systems – can also help reduce reporting errors and burdens for political parties, campaigns, and candidates by pre-filling information based on past financial reporting, or forms submitted to other government agencies. Interoperable data can also help state institutions raise red flags about undue influence and conflicts of interest that may warrant follow-up investigation. Yet, the process of establishing strong databases and implementing data-sharing arrangements is a challenge that may require overcoming a range of roadblocks, including:

- lack of mutual understanding of technical needs, goals and skillsets among the political finance experts, data experts and engineers responsible for designing and implementing interoperability;
- inconsistently formatted or incomplete internal records on party and campaign or candidate finance;
- resistance to sharing data amongst peer agencies;
- limited human and financial resources to execute upgrades to data systems;
- resistance to change in operations and procedures within political finance oversight bodies; and
- lack of political will (e.g., among reporting entities and legislators) to tackle stronger transparency and reform more broadly.

This guide does not aim to be a comprehensive or authoritative framework for reform. Rather, it is intended to equip political finance oversight institutions and data specialists with a shared vocabulary around data standards and interoperability, along with practical insights on how to enhance internal data quality and pave the way for more effective interagency data sharing. Where digitalization agencies or task forces exist, they should be proactively engaged in efforts to enhance the interoperability of political finance data from the start, as they will be best situated to advise on how to standardize data definitions and formats, how to ensure compliance with data privacy laws, and how to better integrate data on money in politics into existing digital public infrastructure.

The guidance in the primary four sections of the paper builds on desk research, in-depth reviews of political finance reporting forms from six countries (including annual, quarterly and campaign reports for political parties; candidate filings; and third-party reports, where applicable) and 11 interviews with oversight institution representatives and political finance experts from civil society and the media, primarily in Europe and Latin America.

A NOTE ON TERMINOLOGY

Institutional mandates for political finance oversight vary broadly across countries and, in some cases, are spread across multiple institutions. Generally, institutions engaged with ensuring transparency and accountability around money in politics could include election management bodies, anticorruption commissions, supreme audit offices, courts of account, and similar mechanisms responsible for election administration and/or political integrity.

This paper uses the term **"oversight institutions"** to refer to state bodies that have a leading role in political finance monitoring and enforcement.

Conversely, it uses the term **"peer agencies"** to refer to the many types of government institutions that may house data that can help oversight institutions execute their political finance mandates. Illustratively, peer agencies could include tax authorities, public procurement offices or teams, census bureaus, and law enforcement agencies.

Using This Guide

This guide is designed to be flexible, recognizing that institutions undertaking data enhancement initiatives have different resource levels, data management experience, technical assistance needs, and goals.

For readers seeking a better understanding of what interoperability means in practical terms and the basic mechanics of data exchange, the "Annotated Glossary" section introduces key definitions and concepts in plain language. It is designed to provide political finance experts with basic vocabulary to articulate their data goals in conversations with information technology (IT) teams, data experts, and digitalization ministries.

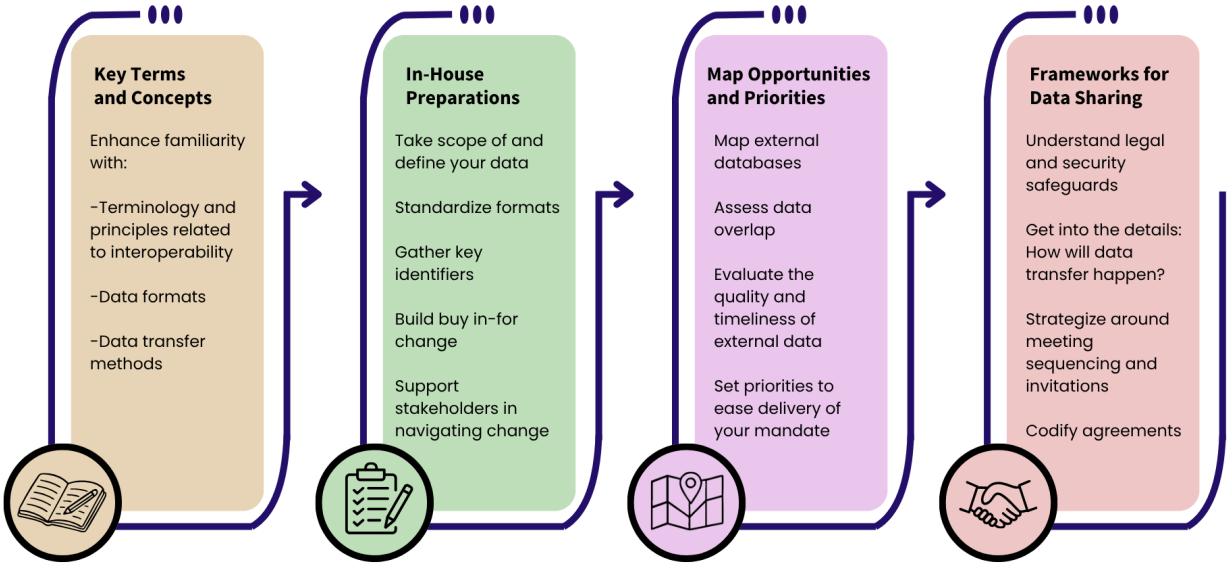
For readers in an oversight institution that is at an early stage of digitalization, or who have limited experience sharing data with peer agencies, the "In-House Preparation for Interoperability" section focuses on basic steps to strengthen internal data capture and management processes, easing the way for future data exchange.

For readers who have a basic understanding of data interoperability mechanics but are not sure where to invest limited resources to enhance data sharing, the "Identifying Opportunities and Setting Priorities for Interoperability" section provides insights into common areas of overlap between political finance databases and other government databases. This section outlines a range of common datasets that may be useful to oversight bodies in streamlining or automating their compliance and verification checks on financial reports from political parties, campaigns, and candidates. It also provides insights on how cross-referencing datasets can help raise red flags for conflicts of interest or undue influence that may warrant further investigation.

Finally, for readers who have identified clear data sharing priorities and are actively seeking to establish data exchange with peer agencies, the "Refining and Establishing a Framework for Interagency Data Sharing" section focuses on refining the request, articulating the mutual benefits of data sharing, and identifying safeguards to protect sensitive data.

Figure 1 provides additional information on the contents – and where applicable, suggested action items – of each of the sections.

FIGURE 1. NAVIGATING THIS GUIDE



Annotated Glossary

Start with this section if you are familiarizing yourself with the foundational vocabulary and mechanics of data interoperability.

General Terminology

> **Data interoperability:** Data interoperability relates to the feasibility of connecting and making different datasets work together.[1] For this paper, data interoperability can be understood as an oversight body's ability to confidently and efficiently combine and compare diverse government datasets managed by several different state agencies under an agreed interagency framework and in line with prevailing national laws.

In technical terms, data interoperability requires the overlap of one or more consistently defined data fields across datasets. Standardizing data formatting is also an important step to supporting easy comparison. Practically speaking, interoperability also requires interagency cooperation and agreement on data sharing policies and creation of a mechanism for exchanging data. The primary goal of establishing interoperability in the political finance arena is to support streamlined and effective cross-checking of the data in political parties and candidates' financial reports. Cross-verification may be achieved in the following ways:

- manually reviewing peer agencies' data against internally collated financial reports (e.g., if an election management body is granted only limited viewing privileges of datasets from a tax authority or an anticorruption agency or is only entitled to receive information in response to direct and targeted questions); and
- automated reviews via a data server.

Where oversight institutions have already established digital reporting systems for party and candidate submissions, having interoperable datasets may also enable auto-population of some reporting fields. However, data completeness, quality and format across datasets can also have an impact on the feasibility and value of a data exchange.

> **Semantic interoperability:** Data interoperability requires an overlap in data points, consistently formatted data and machine readability. Semantic interoperability goes a step further, ensuring consistency in *meaning and interpretation* across datasets.[2]

As an example from the political finance world, do all databases calculate an individual's total financial assets the same way? What are the components of this aggregated total? Does it include assets in their family members' names as well? When comparing data on a company's earnings for the year 2025, do you know whether the database is defining that period based on a calendar year or a fiscal year cycle?

To ensure that oversight institutions are interpreting peer agency data correctly and that external actors accessing the oversight bodies' data understand what they are seeing, it is helpful to document and share a number of details with peer agencies – to include metadata and *definitions* for each data field covered in political finance transparency portals/reports.

[1] Open Data Handbook. (n.d.). What is Open Data? (See discussion on interoperability.) https://opendatahandbook.org/guide/en/what-is-open-data/.
[2] European Commission. (n.d.). Glossary: Semantic Interoperability. Interoperable Europe. https://interoperable-europe.ec.europa.eu/collection/portal-support/glossary/term/semantic-interoperability

> **Common identifiers:** These attributes provide information about an individual or entity (e.g., name, job title or city of residence) and are present across multiple datasets. Unlike unique identifiers (discussed below), common identifiers – as the term is used in this guide – might be shared with other individuals or entities.

Common identifiers are important in political finance because they allow oversight bodies to cross-check the information in political finance reports with datasets managed by other agencies. To verify the legality of a donation, for example, an oversight body might check (1) an individual donor's information against a civil registry or tax registry to verify their citizenship or (2) a company register to learn whether a donor company is foreign owned, whether it has a record of operations and income to support the donation, and/or whether it was launched just before the election to funnel funding to specific parties or candidates.

Common identifiers are often insufficient for an oversight body to confidently connect two different datasets. For example, multiple individuals living in the same country or city are likely to share a first name, or even first and last names. When combined with other data fields, however – such as birthdate, age, registered address, and employer – an oversight body may be able to confidently identify the individual or entity across independent government datasets. This gets closer to creating a unique identifier.

> **Unique identifiers:** These identifiers are distinct codes, numbers, or text strings assigned to a discrete person, entity, object, or place that enable users to confidently distinguish between entries in a dataset – and to confidently make connections across datasets that contain the same unique identifier.[3] National ID numbers, tax numbers, and business registry numbers are all examples of unique identifiers. Unique identifiers are sometimes constructed by combining two or more common identifiers that allow users to distinguish between otherwise too similar cases.

An example of a unique identifier is the social security number, used in the United States. All social security numbers have the same format (`###-##-####`), but no two individuals have the exact same sequence or combination of digits. In Sweden, personal identifier numbers also use a common format (`######-####`), with the first six digits corresponding to an individual's birthdate (`YYMMDD`) and the last four digits enabling consistent and reliable distinction among individuals who share a birthdate.

Some unique identifiers combine two reliable and distinct fields, such as an individual's name and birthdate. For example, the name Jigon Kim may yield several results in a database, but searching for this first and last name in combination with a specific birthdate – inclusive of month, day, and year – is likely to narrow the search results significantly and help concretely identify a specific individual or entity.

Unique identifiers are incredibly valuable in establishing connections between datasets. Where they appear across multiple datasets, they allow an oversight institution to more rapidly and confidently confirm that they are looking at data records for the same individual or entity. Take the example of cross-checking a donation from an individual with a common name. If "Jan Novak" made a large donation to a party right before an election and the political finance oversight body needs to compare the value of the donation to his income to assess whether he was likely the original source of the significant contribution (and not a straw donor), the job of cross-verification is much simpler when the oversight body can use Mr. Novak's tax identification number. Using the tax ID allows the oversight body to request that the tax authority simply verify Mr. Novak's last reported income, rather than wading through tax records from several individuals with the same name.

[3] Open Data Handbook. (n.d.). Glossary: Unique identifier. https://opendatahandbook.org/glossary/en/terms/unique-identifier/

Website URLs, email addresses, and telephone numbers can also be unique identifiers, although they may be less reliable means of consistently identifying individuals for accounts set up anonymously or under pseudonyms, or where use or ownership of web portals and communication channels varies over time. Still, these types of identifiers can be valuable in connecting data entries for individuals and entities that commonly go by shortened names, nicknames, acronyms, or aliases. Consider this scenario: A party reports that it purchased promotional materials and services from Public Image Consultants Inc, Public Image Co., and PIC. Requiring the party to provide a URL or consistent contact information for the contracted companies could help an oversight body understand whether this is one company being logged under three names, or whether these are all different entities.

> **Open data:** The Open Data Charter defines open data as "digital data that is made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed by anyone, anytime, anywhere."[4] The benefit of open data is that users can compare, combine, connect, and evaluate data from multiple sources.

The Open Data Charter offers several principles – co-designed by governments, civil society organizations, and other stakeholders in 2015 – emphasizing that open data should be open by default, timely and comprehensive, accessible and usable, and comparable and interoperable.[5] Applying these principles, open data on political finance should be:

- **Proactively published and free:** Data should be published openly and with minimal redaction, not only accessible to users who request it (e.g., via a freedom of information request). Access to political finance data should also be free, rather than premised on subscription services or one-time fees.
- **Available within reasonable time frames:** Voters should be able to understand how money flows into and out of campaign accounts. This understanding requires rapid publication of data – in line with legally mandated timelines – once a candidate or campaign has reported it to an oversight body. Similarly, political parties' quarterly and annual reports should be published as soon as practicable. Rather than wait for an audit to be completed, agencies can publish preliminary data with a disclaimer that compliance and verification checks are in progress. Audit findings and amended party reports can then be filed in addition to (not instead of) the initial filings when the information becomes available.
- **As comprehensive as possible:** Users should have access to information that is as complete as possible and be able to see where the data has been changed or corrected over time. This requires maintaining a log of all reports, including those that have been corrected or amended with additional information. Although some personally identifiable information or donor data may need to be redacted for privacy or security purposes, limitations on the publication of data should be the exception, not the rule.
- **Accessible for a variety of stakeholders:** Accessibility may mean digitizing political finance reports and supporting documents rather than providing users with scanned or handwritten copies. Commissions may choose to make data available through a variety of means (e.g., viewable through an online portal, or viewable and downloadable) to support stakeholders' ability to integrate political finance data in their external analyses.
- **Usable by the public:** Ideally, data should be available for download in machine-readable formats so users can carry out their own analyses of the information.

Note that there are both important distinctions and areas of overlap between "open data" as described here, and laying the groundwork for inter-agency data interoperability, which is the main focus of this paper. Opening up data can benefit a wide variety of stakeholders, including peer agencies *and* non-government actors like civil society organizations, journalists, and everyday voters. Open data on political finance may provide the public with key insight on party assets and liabilities, and party and candidate donations and spending patterns – but it should not include sensitive information like individuals' personal identifiers (e.g., passport numbers, tax identifiers, or social security numbers). On the other hand, data interoperability as discussed in this guide is focused on sharing data directly and solely between state institutions. With robust privacy and security measures, interagency

[4] Open Data Charter (ODC). (n.d.). ODC Principles. https://opendatacharter.org/principles/.
[5] Ibid.

interoperability *may* allow for sharing of sensitive data (such as personally identifiable information) on a minimal and targeted basis, enabling oversight institutions to carry out their compliance and verification checks.

Despite these differences, both open data and data interoperability share several principles. For example, open data is most user-friendly when it is as comprehensive as possible, standardized (e.g., using broadly accepted formatting practices), and available in machine readable forms – which are also good practices for establishing data interoperability. As such, oversight institutions can draw lessons and good practices from existing research and the expertise of individuals and organizations working in the open data field. They can also strive to design data clean-up initiatives in a manner that will enhance both interagency interoperability and set the stage for publication of higher quality open data on party and campaign finance in the future (e.g., through adoption of standardized formatting practices, such as ISO formatting conventions).

> **ISO formatting conventions:** The International Standards Organization (ISO) is an international nongovernmental organization, founded in 1946, that convenes diverse experts and standard-setting bodies from around the world to deliberate on and develop data standards to apply across borders and sectors. ISO standards provide common frameworks for measurements, assessments, processes, and data formatting and management.

Dates are a common example of ISO formatting conventions. Oversight bodies can consistently register dates in the year-month-day format (`YYYY-MM-DD`), where January 13, 2025 is captured as `2025-01-13` rather than Jan-13, January 13th, and so on.[6] Other ISO code lists relevant for political finance reporting include country names, international currencies, banking information, and the language(s) in which data is collected and published.[7]

Adopting ISO standards to guide data collection from parties and campaigns, and internal formatting of datapoints can help prevent internal and external misinterpretation of datapoints and reduce the need for "translation" or data cleaning before sharing data with an external partner. Use of ISO codes may be particularly valuable for oversight bodies in countries concerned about "dirty money" entering politics from abroad, smoothing the way for information sharing with internationally based oversight bodies that may use different languages. For example, ISO abbreviations for countries would enable an English speaker and a French Speaker to recognize that the code "US" refers to the United States of America, even though the name for the country in French ("Les États-Unis") differs.

> **Metadata:** Metadata is information about a data point or a database itself. It can expand to explain the scope and timeframe of a database, details about how the data is gathered and released, and information about who is responsible for capturing data points and compiling a database.[8]

Metadata is important for setting user expectations. What should a peer agency expect to see regarding the timeframe covered by the political finance oversight institution's database? When was it last updated (and by extension, will it include information on donations and spending in the most recent election cycle, or the most recently closed reporting period for parties)? In turn, metadata may provide useful insights to oversight institutions that are seeking information from their peers. For example, if an oversight body is trying to verify information that a political party has reported on

[6] International Organization for Standardization (ISO). (n.d.). ISO 8601: Date and time format. https://www.iso.org/iso-8601-date-and-time-format.html

[7] See "Table 1: ISO Standards for Common Political Finance Reporting Fields" in the "In-House Preparation for Interoperability" section of this paper for additional information.

[8] Open Data Handbook. (n.d.). Glossary: Metadata. https://opendatahandbook.org/glossary/en/terms/metadata/. Note that many governments and organizations utilize a standardized Data Catalog Vocabulary (DCAT), currently in its 3rd version, to consistently structure metadata for the datasets they maintain. Use of a metadata standard helps to enhance discoverability and interoperability of databases, just as standardizing definitions and formatting of data does. W3. (n.d.). Data Catalog Vocabulary (DCAT) – Version 3. https://www.w3.org/TR/vocab-dcat-3/.

the purchase and sale of commercial office spaces, when was the real estate register last updated, and what is its geographic coverage?

Data Formatting

> **Machine-readable data:** Simply put, machine-readable data is information that a computer can interpret without human intervention. Machine-readable political finance data must be structured consistently, in line with a prevailing standard or set of rules, to allow computers to reliably identify the information.

Machine-readable data requires the adoption and consistent application of standard formats. It also requires interoperability. Widely used machine-readable data formats include CSV and JSON, both described below. Non-machine-readable content includes photos, handwritten notes, and most scanned PDFs.[9]

> **Comma-separated value (CSV) format:** CSV formatting – one of the most used and recognized machine-readable data formats – simply uses commas and line breaks to store information. CSV data can also be displayed in a spreadsheet or table format, with columns in place of commas and rows in place of line breaks to structure data.[10] Each row of a CSV file contains information on a specific observation (e.g., a political party), while each column contains information on a specific data field or variable (e.g., donor name).

Consistent formatting is critical to ensure that CSV data is machine readable; using a separate row for each entry ensures a computer can consistently identify where new donations or transactions are being logged, rather than conflating all donations as being from one individual. Consistent formatting and clear breaks between data entries (use of a comma to tell the computer to generate a new row) are essential for machine readability.

In Figure 2, an excerpt from a hypothetical donor report, each column has a clear data label. If asked to generate a list of all donor names, the computer would be able to identify Tina Lang and Nathalia Lazar as donors. Similarly, if a user ran a search for all donations from Tina Lang, they would be able to see that she made at least two donations during this campaign – one for Jane Smith's senatorial race and one for Philippe Moline's gubernatorial race.

FIGURE 2. EXAMPLE OF A CSV-FORMATTED CAMPAIGN DONATION SPREADSHEET

	A	B	C	D	E
1	Donation_Number	Campaign_Name	Donor_Name	Donor_Occupation	Donor_Address
2	4320260412	Jane Smith for Senator	Tina Lang	Retired	405 Spring Street
3	4320260415	Jane Smith for Senator	Nathalia Lazar	Teacher	507 Martin Avenue
4	5306370127	Philippe Moline for Governor	Tina Lang	Retired	405 Spring Street

> **JavaScript Object Notation (JSON) format:** JSON is a common human- and machine-readable data interchange format, popular for its flexibility in storing and transmitting data. It

[9] Open Data Handbook. (n.d.). Glossary: Machine readable. https://opendatahandbook.org/glossary/en/terms/machine-readable/

[10] File Format. (n.d.). Documentation: What is a CSV file? https://docs.fileformat.com/spreadsheet/csv/. For countries where commas are frequently used in writing numbers to include currency values (e.g., $1,234.56 or €7,89), oversight bodies may also use Tab-Separated Value (TSV) systems, which work similarly to CSV, but use tabs rather than commas to separate data points. See: Öhman, M., Klein, L., & Jouan-Stonestreet, B. (2024). Part 1 Implications of the Legislative Framework for Oversight Institutions. Oversight—A Toolkit for Political Finance Institutions. International Foundation for Electoral Systems. https://www.ifes.org/oversight/part-one

> is especially useful for transferring information between different databases or systems that may be based in different computing languages (e.g., API).

JSON is a popular data format because it is more intuitive (readable) to non-expert coders. It uses human language; hierarchies (denoted by indentations or "nesting") that showcase relationships between data points; and a limited set of data categories (e.g., a line of code clearly and consistently formatted to let a user know whether it holds a word or phrase, a number, a yes/no or true/false response, or a broader array of information about an entity).

Each line of JSON code is classified by the type of data it contains:

- A "string" entry lets the computer know the information in that line of code contains text. Candidate and donor names and street addresses, for example, are considered strings.
- If the data type is set to "integer," then the computer knows to expect a numerical entry; this is common for capturing ages and amounts of financial transactions.
- "Null" entries tell the computer there is no value in a stated field. For example, if a candidate has no middle name or no former names to report, then using a null entry alerts the computer that the candidate or party has not omitted or failed to submit this information; it just does not apply to them.
- "Boolean" fields contain true/false information for which there is either a yes or no answer. For example, if a reporting form asks whether the submitting candidate is an incumbent elected official, then this information could be captured in Boolean format.
- If the data type is set to "array," then the computer expects a list of information to follow. Arrays can include strings/text, integers, null entries or Booleans. Additional arrays or lists can be embedded into an overarching array – creating a hierarchical, or nested, way of viewing and understanding the relationship between different data points.[11]

A simplified example of JSON code capturing basic biographical data for a candidate could look something like the following. Note that curly brackets are used to introduce and close segments of JSON code.

```
{
   "candidate_first_name": "Ella",
   "candidate_middle_name": null,
   "candidate_surname": "Larson",
   "candidate_age": 42,
   "is_incumbent": false,
   "campaign_offices": ["Miami", "Orlando", "Tampa"]
}
```

In this example:

- `candidate_first_name` is a string or text field. It is followed by the candidate's first name, set off by opening and closing quotation marks that tell the computer where the text of the name begins and ends.
- The fictional candidate, Ella Larson, does not have a middle name, so that field contains a `null` response. The lack of quotation marks differentiates this line of code from the string (text) entry; quotation marks around a term would tell the computer that the candidate has entered a middle name.
- Similarly, integer entries – in this case, telling us the candidate is 42 years old – do not require opening and closing quotation marks. Computers identify integers based on the presence of numeric instead of alphabetical text.
- Next, a Boolean field tells us that Ella Larson is not the political incumbent. Use of the Boolean field here is appropriate because there are only two possible answers – Ella is either the incumbent (`true`) or not

[11] W3 Schools. (n.d.). JSON Data Types. https://www.w3schools.com/js/js_json_datatypes.asp.

(`false`). As with null and integer options, no opening and closing quotes are needed because there are only two possible values for the data field.

- Finally, an array in the final line provides the names of cities where the candidate has active campaign offices. Square brackets indicate where the list of office locations begins and where it ends. This array contains strings (text), so each city name is enclosed in quotation marks, letting the computer know where the name of each location starts and ends.

In the example above, information for each field would be captured in a standardized manner for all candidates that the file reports. With consistent JSON formatting, computers can differentiate between candidates with different names, ages, and other identifiers and extract information on their campaign incomes and spending patterns that are useful for analysis.

> **Extensible Markup Language (XML):** XML is a plain-text data storage and transmission format that allows users to add tags or labels to individual pieces of data, enhancing consistent and accurate interpretation and transfer of data. Political entities submitting reports to oversight institutions may use XML. Oversight institutions may also use XML to ensure the data can be understood.

XML can be highly valuable for institutions seeking to enhance interoperability with other datasets, because this "markup" language can provide crucial guidance for how to interpret and translate common datapoints (e.g., using tags to clarify whether currency values are documented with or without punctuation or currency symbols). XML also plays an important role in automating data validation – ensuring that parties or candidates are entering addresses, contact information, bank information and other details in a valid format that can be shared between agencies.[12]

Case-sensitive tags in XML are applied using an open tag format (`<tag>`) to start an entry and a close tag format (`</tag>`) at the end of the entry. Additional information can be sandwiched between an open tag and a close tag as "elements" of data. These "child" entries are indented, with plain text filling in the fields. The following is a simplified example, where `<party_treasurer>` is the open tag and `</party_treasurer>` is the close tag, with three child entries:

```
<party_treasurer>
      <first_name>Thomas</first_name>
      <last_name>May</last_name>
      <email>tmay@orangeparty.com</email>
</party_treasurer>
```

The tag could be built out further to require, and explain allowable formatting, for additional contact information. Examples may include instructions for logging a treasurer's phone number (e.g., requiring a country code or an area code), or a mailing address (e.g., requiring inclusion of the local postal code).

Data Transfer

Data transfer between oversight institutions and peer agencies can take many forms, from one-time requests for information communicated by phone or email to scheduled exchanges of spreadsheets and automated cross-referencing. Each method comes with its own limitations and challenges.

These final glossary entries provide basic information on common data sharing methods, followed by more detail in the Refining and Establishing a Framework for Inter-Agency Data Sharing section. **Where countries have established digital ministries, or where there are task forces or agencies responsible for executing a**

[12] Amazon Web Services (AWS). (n.d.). What is XML? https://aws.amazon.com/what-is/xml/

digitalization strategy, oversight bodies should coordinate directly with these specialized bodies from the start of their efforts to strengthen interoperability.

> **Limited database or portal access:** Staff in oversight institutions generally have some access to the vast amounts of party and candidate finance data housed in their internal databases. To protect personally identifiable information and other sensitive data, system administrators often provide individuals with limited access rights – only those they need for their jobs. In some contexts, institutions may grant staff at peer agencies very limited access to their internal data, applying similar permission restrictions to safeguard against leaks or exposure of sensitive information and data that are not pertinent to the oversight of money in politics.

> **Bulk downloads:** Bulk downloads pull information from a database in large quantities at once, often producing a CSV, JSON or XML file for users to review, analyze or transfer. Users may be able to use filters to narrow the scope of the downloaded data (e.g., pulling information on financial transactions that occurred between specific start and end dates).

In the realm of political finance, bulk downloads may be useful for long-term trend analysis of a political stakeholder's income and spending patterns or significant shifts in a political party's assets and liabilities, or for deeper investigation of a suspected regulatory breach. Bulk downloads can also be a cost-effective, low-effort means of establishing data sharing arrangements between agencies, with the data saved to a secure hard drive or file-sharing platform for rapid transfer.

However, using bulk downloads for interagency data sharing may present new challenges. For example, agency staff receiving the data may require additional time and assistance to understand how their counterparts have structured the data and to sort through and extract relevant information.

> **Application programming interface (API):** An API is a set of rules governing exchange between software applications. It allows one data system to send a request for specific data to another system; if the request aligns with pre-programmed rules, the system will send the specified data back to the requester.[13]

A common example of an API is a payment interface in a smartphone app. An individual who wants to purchase a good or service from inside the app enters their financial information, as prompted by the third-party application, which uses an API to verify and log the transaction with the bank or credit card company. If the data entered does not comply with the API's rules, then the user gets an error notification and may be prompted to correct or re-enter some information (e.g., bank account details or credit card number). Once the information complies with the API rules and is verified, the user will see a confirmation of payment.

Compared to bulk downloads, an API offers a much more targeted way of extracting and sharing data between systems, which can help protect agency data. However, it may be a less intuitive means of data sharing because it requires basic familiarity with how to access and read code.

[13] Goodwin, M. (n.d.). What is an API (application programming interface)? IBM. https://www.ibm.com/think/topics/api

In-House Preparation for Interoperability

Refer to this section if you are seeking to strengthen your data collection and management processes as you prepare to establish more effective interagency data sharing.

Updating or Establishing Written Policies for Data Management

Political finance data's utility hinges on whether it can be easily understood and interpreted. Establishing and regularly updating a unified codebook, data dictionary or explainer document supports internal knowledge transfer and collaborative analysis amongst oversight institution staff, while helping peer agencies interpret the data accurately.

First and foremost, your documentation should provide useful definitions for each data field. For example, where candidates are asked to report on "personal expenses" incurred during their campaign, what types of costs fall into this category? Documenting the scope of expenses that should be covered in this category can help prevent confusion or errors by reporting entities, and staff responsible for verifying the accuracy of a report. Developing and documenting this guidance can be time intensive, but it can improve reporting accuracy and reduce delays and workloads for your team.

If you are not sure how to get started on compiling or updating your codebook or similar documentation, consider reviewing existing financial reporting forms for parties and candidates. Reporting form fields generally correspond to fields in an oversight body's database. Consider:

- What are common questions that the oversight body receives from stakeholders filling out the forms?
- Are there any fields that users tend to fill in incompletely or incorrectly?

Answering questions like these can provide useful cues for fields that need better documentation of their scope or definition.

Robust documentation also explains the format and potential values for each data point. Regarding currency values in the database, for example, a codebook may:

- specify whether to use a currency symbol, name or abbreviation (e.g., ¥ versus a descriptive label "yen" versus the ISO currency code[14] "JPY")
- document proper use of punctuation to separate decimals from whole numbers or to denote thousands or higher values (e.g., $1,234.56 versus 7,89 €)
- distinguish between zero-value, null and missing data points (e.g., "the party received $0.00 in state funds during the specified period" versus "the party is ineligible to receive state funds" versus "the party failed to report or supply documentation about funds received from the state")

Documentation explaining institutional data should be updated regularly. Codebooks and similar documents should not be deleted or overwritten when they become outdated (e.g., due to a change in law and/or reporting form that alters the type or scope of data collected). Rather, the oversight body should (1) issue a new version of the documentation that clearly lists the date when it came into effect and (2) ensure that data viewers and users retain access to all codebooks for the life of the dataset so they can track how the database has changed over time.

For example, if the oversight body begins to integrate politically exposed persons (PEP) identifier numbers into a political finance data set in 2027 to better track when PEPs are donating to candidates and parties, it should be clear

[14] International Organization for Standardization (ISO). (n.d.). ISO 4217: Currency codes. https://www.iso.org/iso-4217-currency-codes.html

that the lack of PEP identifiers before 2027 does not imply that there were no PEPs donating to political groups and actors before 2027, only that the data had not been regularly tracked and documented before that date.

Documentation should extend to cover metadata. A codebook or similar documentation should include information on how often the data in the database is collected, through what means it is collected, and any quality control measures that are taken to review the data for accuracy and completeness. While this level of information may seem unnecessary for oversight body staff, it can be very useful when seeking to establish data interoperability with peer agencies.

Updating Data Collection and Formatting Practices

Using Unique Identifiers

Although bookkeeping and reporting requirements can vary drastically across jurisdictions, political finance datasets generally capture information on the same general categories of data.

For political parties, a simplified list of data points captured includes:

- party names and acronyms
- party offices and web addresses
- names and contact information for key party officers (e.g., leaders and treasurers)
- party bank account information (for regular operations and election campaigns)
- names and contact information for donors
- records of party contracts and issued payments (for regular operations and election campaigns)
- party assets (including real estate, moveable property and liquid assets)
- party liabilities (including details on loan status and holders)

For candidates or campaigns, a generalized and streamlined list of data points captured includes:

- candidate name and contact information
- candidate/campaign office(s) and web addresses
- names and contact information for key staff
- campaign bank account information
- names and contact information for donors (or, at minimum, value of donations)
- records of candidate or campaign contracts and payments issued (for materials and services related to the campaign)

Even within these simplified categories, there are several clear openings for introducing unique, government-assigned identifiers in a political finance database to enhance its future interoperability:

- **Individuals** listed as party officers, candidates and donors in the database have unique personal identification numbers or tax ID numbers. They are also likely to have unique physical addresses, email addresses and phone numbers that may be cross-listed in other government databases, with or without the individual's name.
- **Legal entities** listed as donors or service providers that are the recipients of party and candidate contracts and payments likely have unique entity identifiers assigned via a business registry, as well as their own tax ID numbers. As with individuals, they are also likely to have unique physical addresses, email addresses, web addresses and phone numbers.
- **Assets** are also likely to be cross-listed in alternate government databases (e.g., vehicle identification numbers for party-owned vehicles and unique property identifiers listed in corresponding registers for party-held lands and real estate).

Where it is legally allowable and appropriate, capturing these forms of information in political finance reporting forms and storing them in the political finance database can help forge interoperability links for the future. Ensuring that this data is stored securely, and that internal policies are in place to preserve data privacy (even amongst staff members) must be of the upmost importance if sensitive data (including personally identifiable information) is captured within the database.

Adopting Standardized Formats and Code Lists

Formatting common data fields in line with well-established standards and code lists can help lay the groundwork for easier data comprehension and interoperability. For example, oversight bodies that collect international bank account numbers (IBANs) or business identifier codes (BICs)[15] for political service providers already benefit from international standards that dictate consistent coding for banking information and make it possible to execute and track cross-border transactions. Because formats for IBANs, BICs and other standardized banking and entity identifiers are unique and used consistently within countries and across borders, they are useful reference points for establishing interoperability across diverse databases.

Many ISO standards can be adopted to capture common political finance data points, as illustrated in the non-exhaustive table below. Adopting and applying these standards is not directly equivalent to the use of IBANs, BICs, and similar codes (which act as unique identifiers, allowing institutions to pinpoint specific accounts and entities), but consistent application of these rules for standardization can help reduce the need for translation across databases operating in different languages or using specialized naming conventions. Additionally, oversight body staff need not be data experts to adopt these standards. They can work with data experts and engineers to identify and integrate well-established formats and code lists in their data collection and management processes in a manner that is appropriate to their contexts and the scope of their datasets.

TABLE 1. ISO STANDARDS FOR COMMON POLITICAL FINANCE REPORTING FIELDS

Common Data Fields	ISO Standards
Dates	Standard: ISO 8601[16] Format: `YYYY-MM-DD` • `YYYY` represents a four-digit year. • `MM` represents a two-digit month. • `DD` represents a two-digit day. Example: November 2, 2026 is formatted as `2026-11-02`.
Timestamps	Standard: ISO 8601[17] (generally used in combination with date format) Format: `hh:mm:ss:ms` • `hh` represents the hour of the day, based on a 24-hour time clock. • `mm` represents the minutes after the hour. • `ss` represents the number of seconds elapsed after the logged minute. • `ms` represents the number of milliseconds elapsed after the logged seconds. Example: 10:30 p.m. is represented as `22:30:00:00`.

[15] International Organization for Standardization (ISO). (n.d.) ISO 13616-1:2020: Financial services — International bank account number (IBAN). (n.d.). https://www.iso.org/standard/81090.html. See also: Swift. (n.d.). Business Identifier Code (BIC). https://www.swift.com/standards/data-standards/bic-business-identifier-code
[16] ISO 8601: Date and time format.
[17] Ibid.

Common Data Fields	ISO Standards
Country Names and Abbreviations	Standard: ISO 3166-1[18] Format: `XX`, `XXX`, or `###` • Country names are generally shortened to two-letter (Alpha-2) codes. • In some cases, database managers may prefer to use three-letter (Alpha-3) codes to identify countries, matching the abbreviation more closely to the full country name. • Alternately, a country may be identified by three digits (Numeric Code). The key value of these country codes, despite their variation, lies in the fact that they are applied universally across borders based on a list of established, pre-agreed country codes available online via a unified browsing platform. Example: The Republic of Ghana is represented as `GH`, `GHA` or `288`.[19]
Country Subdivisions (Subnational District Names)	Standard: ISO 3166-2[20] Format: `XX-YY` or `XX-YYY` • The first two digits correspond to the national-level Alpha-2 code. • The dash (`-`) acts as a separator. • The final two or three letters are assigned in unique combinations to distinguish between different regions of the country. Example: In Ghana, the Bono region is captured as `GH-BO`, while the Bono East region is captured as `GH-BE`.
Currency Names	Standard: ISO 4217[21] Format: `XXX` or `###` • Each global currency is assigned a unique three-letter code. Generally, this three-letter code builds on the ISO 3166 codes for country names. • Alternately, each global currency may be represented by a unique combination of three digits, logged in a master list. Example: The Ghanaian cedi is represented as `GHS` or `936`.[22]

Capturing Variations and Changes

Establishing connections between databases can prove challenging when there is internal or cross-database inconsistency in how names and contact information for key individuals and entities are captured, and when these details are subject to change over time.

There may be several reasons for mismatches or inconsistencies in datasets, such as the following:

- formal names transliterated across alphabets before being logged in the database
- reporting entities providing aliases, nicknames, shortened company names, acronyms, or abbreviated names in their filings

[18] International Organization for Standardization (ISO). (n.d.). ISO 3166: Country Codes. https://www.iso.org/iso-3166-country-codes.html
[19] ISO 3166 — Codes for the representation of names of countries and their subdivisions. Search results for “Ghana.” https://www.iso.org/obp/ui/#iso:code:3166:GH
[20] ISO 3166 — Codes for the representation of names of countries and their subdivisions.
[21] ISO 4217: Currency codes.
[22] Six Group. SIX: Your Source for Financial Data Standards. https://www.six-group.com/en/products-services/financial-information/market-reference-data/data-standards.html. (See Current and Historical Lists: Current Currency & Funds, “List One (XLS),” https://www.six-group.com/dam/download/financial-information/data-center/iso-currrency/lists/list-one.xls.)

- legal name changes made between reporting periods
- small variations in spelling or use of acronyms
- data entry errors

Any of these, individually or in combination, can yield duplicate records for a single entity. Indeed, Transparency International Colombia once identified some 50 naming variations for a single company in their review of the *Cuentas Claras* database, a tool the electoral authority used to assist with political finance monitoring.[23]

To mitigate these challenges, your team may find it useful to update existing reporting forms and associated instructions. For instance, you may wish to update instructions to specify that individuals and entities must record their full legal names and/or that they must report full legal names along with common names, shortened names, and abbreviations. Where permitted by law, the instructions may require users to submit supporting documentation, such as a copy of a government-issued ID or an entity's registration documents, to help validate the information they provide. Finally, your team could consider introducing new fields, such as simple yes/no checkbox to capture whether a reporting entity's name or contact information has changed since the previous reporting period. This helps establish a timeline for changes, which can be useful in matching records for an individual or entity in an external database.

Databases can also be built or expanded to log multiple identifiers for an individual or entity, capturing variations in formal and commonly used names and corresponding changes in these details over time. For example, the Labour Party is registered under its English name in the party register for Great Britain, but its record also contains its alternative name "Llafur" ("Labour" in Welsh). This allows database users to locate the party's information whether they are searching for information on "Labour" or "Llafur," and prevents confusion around whether these are two separate entities with similar names, or the same party.[24] Additionally, party records in this register capture the date of the party's registration and the date when the primary name of the party last changed (as authorized by the UK Election Commission).[25] These are helpful pieces of information in building out a complete array of financial records for a given party dating back to their launch, and ensuring continuity in identification of records relevant to a single party across any formal name changes.

Underlying Process Considerations

Updating data collection and management processes takes significant technical work, as illustrated by the preceding sections on documentation, data expansion and formatting. To maximize the impact of data cleaning and interoperability efforts, institutions also must ensure their projects are adequately funded, from planning through the rollout of new tools and forms, and they must engage with data providers and systems users to ensure they are willing and able accommodate changes.

This subsection includes brief recommendations on how to start strong with a data enhancement initiative – beginning with a long-term budgeting strategy, a robust and diverse team to execute the changes, and embedded opportunities for consultation with reporting entities. It ends with a list of guiding questions to support the successful launch of updated data collection and management practices. This content is not meant to offer comprehensive guidance. Rather, it focuses on highlighting common missed steps, costs, and opportunities.

[23] Author interview with a representative from Transparency International Colombia.
[24] The Electoral Commission. (n.d.) Labour Party: Registration summary. https://search.electoralcommission.org.uk/English/Registrations/PP53.
[25] The Electoral Commission. (n.d.). Registers search page. https://search.electoralcommission.org.uk/Search/Registrations?currentPage=1&rows=30&sort=RegulatedEntityName&order=asc&open=filter&et=pp&et=ppm&register=gb&regStatus=registered&optCols=EntityStatusName

Budgeting

Costs for enhancing data collection and management extend beyond updating internal documentation or launching an expanded database. In confirming you have the resources to launch a data interoperability project, remember to budget for the following elements:

- **Training.** Consider how you will prepare internal staff for the project. Additionally, assess whether you will need to adapt or develop new training materials on political finance reporting for parties and candidates or campaigns.
- **Updating reporting forms and user support materials (instructions).** Budget implications may vary, depending on whether your team uses paper forms, digital forms, or a mix of both. For paper reporting, consider the costs associated with design, printing, and dissemination of the updated reporting forms. For digital reporting, assess whether there are in-house staff who can update, test, and launch the revised forms; if not, this work may require support from an external vendor.

Assessing Team Capacities and Technical Assistance Needs

Before launching reform efforts, assess whether you have the right skills and bandwidth to tackle these updates in house – relying on your IT teams, data analysts, political finance experts, administrative support teams, and other groups. Database projects often involve a broad range of experts:[26]

- project managers and administrators to keep projects running on time and on budget
- subject-matter experts (e.g., political finance specialists) to help articulate the conceptual links between data points
- data engineers, web developers and IT experts to support database design and development and create the interfaces that oversight bodies will use to explore and analyze the data

It is also critical to coordinate with digital ministries or task forces already working in your country. Do this early in your planning process, taking note of the types and levels of assistance they can offer, including their availability compared with the timelines for completing the envisioned work.

Consultations and Buy-In

Oversight institutions may face **internal resistance** when it comes to data enhancement and interoperability projects. It can be a significant undertaking to allocate additional funds to revise reporting processes, update regulations and reporting forms, get staff ready to collect and review new forms of data, and amend training processes and support materials for the parties, candidates, and financial managers overseeing reporting. These are big changes that may require updating job descriptions, hiring new staff, and other changes in the work environment that could fuel anxiety and resistance.

Additionally, **external reporting entities** may not be willing to contribute to consultations or comply with expanded reporting requirements.[27] In some cases, the elected officials responsible for legal reforms related to money in politics may be hesitant or even openly hostile to expanding disclosure requirements in ways that would increase the burden

[26] Interviews with (1) a representative from TI Colombia who worked with engineers and election experts to support the design of Cuentas Claras and (2) a Ukrainian political finance expert who supported design and expansion of POLITDATA systems.
[27] As the Oversight Toolkit underscores, “If the reporting system does not take into account the way that political parties gather and maintain financial information, the risk of noncompliance increases. You should also consider the capacity of candidates at all levels of elections to prepare and submit financial reports.” Öhman, M., Klein, L., & Jouan-Stonestreet, B. (2024). 3.2 Compliance Control Mechanisms. Oversight—A Toolkit for Political Finance Institutions. https://www.ifes.org/oversight/3.2-Compliance%20Control%20Mechanisms

on them and their teams in future election cycles. Political finance reforms may gain less support than other policy issues when officials are facing a packed legislative agenda or when they could benefit from limited accountability with respect to political finance data.

Finally, **peer agencies** may balk at sharing data for a variety of reasons, from uncertainty about the legality of data sharing arrangements (or who has authority to approve them) to concerns about security and privacy, increased workload, or resistance to feeling monitored by external parties.

It is beyond the scope of this document to offer comprehensive guidance on navigating change management processes, but a starting point for institutional planning is to build a clear business case for interoperability that shows how stronger connections across datasets can benefit a variety of stakeholders. For example:

- **For oversight bodies and their staff,** receiving, analyzing, and verifying the accuracy and completeness of reports that document the financial assets, income, and spending of parties, candidates, and other political stakeholders are time-intensive and often politically sensitive tasks. The burden only increases during campaign cycles, when the number of financial reports grows to encompass individual candidates' campaign income and expenditures. Interoperability can help reduce the need for manual data reviews and time-intensive follow-up to secure missing data or verify the accuracy of information in the financial reports.
- **Political parties and candidates** can also benefit from improved interoperability of government datasets. Such capabilities streamline annual reporting on their assets, income, and spending as well as repeated financial reporting throughout an election campaign. Where databases are already linked (e.g., on tax payments or to land and property registers), it may be possible to pre-fill several fields in quarterly, annual, or campaign finance reports, reducing the burden on party and campaign officers tasked with compiling supporting documentation and filing regular reports.
- **Peer agencies** may benefit from interoperability and data sharing as well. In some cases, access to political finance data helps them deliver on their mandates (e.g., investigating conflicts of interest or illicit cross-border financial flows). In other cases, establishing interoperability may reduce burdens on their staff by reducing the number of ad hoc requests for support and data verification that they receive from oversight institutions.

In addition to being able to articulate the benefits that interoperability will yield to all these stakeholder groups, oversight bodies may be able to reduce resistance to change by building in opportunities for consultation and collaboration from the start of a new data project. This could take the form of internal meetings or workshops to better understand staff concerns and challenges with existing data collection methods, internal monitoring processes and other topics; another option is to hold consultations with reporting entities and individuals. These sessions can be used to better understand each stakeholder group's frustrations with the political finance reporting processes and brainstorm together how interoperability could reduce their burdens.

Topics to cover in meetings with external stakeholders include whether they have questions or concerns about existing reporting forms and their instructions and which aspects of reporting take the most time and effort for their teams to complete. The discussion could help the oversight body identify where it needs to adapt reporting forms, clarify formatting rules, and enhance the training or guidance it provides to reporting entities.

When planning and convening consultations, consider holding specialized sessions to ensure you are gathering diverse perspectives. For example, there may be value in holding separate sessions to gather feedback from smaller parties and new parties with less experience and fewer specialized staff available to navigate reporting, distinct from consultations with mainstream and well-established parties.

User Engagement and Education

Any changes to reporting forms and instructions must be clearly communicated to the affected parties. The oversight institution must develop a plan for logistics and communication before making any additional updates. The following are key questions to consider:

- Do internal staff need training or skills-building workshops to handle new data collection and management processes or to undertake additional compliance and verification checks on a broader set of data points?
- How will training be funded? Who will conduct the training, and when will it take place?
- Who needs to hear about the change to reporting requirements inside the oversight institution? How and when will this task be completed?
- Which individuals at which peer agencies (e.g., a party registrar office or an election management body) need to be informed of the update to reporting requirements? How and when will this task be completed?
- How will the change in reporting requirements be reported to other stakeholders (e.g., established parties, incumbents seeking re-election, first-time candidates)? Will standard training cover the changes sufficiently, or do the changes require a dedicated communications plan?
- How much time will elapse between announcing the change and submission of the first financial reports that include new data fields? Will parties and candidates have sufficient time to gather and provide the additional information?

Identifying Opportunities and Setting Priorities for Interoperability

Refer to this section if you have strong internal data management processes and are brainstorming about how interoperability with other datasets could help streamline your institution's compliance and verification work.

Oversight bodies generally have limited funding and personnel and tight timelines in which to carry out their mandates. Early analysis of opportunities and priorities for establishing interoperability is a critical step to maximize these finite resources. This section starts with a non-exhaustive inventory of common government datasets to help oversight institutions map opportunities for meaningful data interoperability in their own contexts. It concludes with a series of questions and recommendations to help identify priorities for interoperability.

Mapping Opportunities for Interoperability

Before requesting data from a peer agency, it can be useful to map relevant existing government datasets, assess whether there are natural overlaps between the peer agency's data and your own political finance records, and evaluate whether and how these external datasets could help with oversight of money in politics.

This section provides an illustrative list of common government databases and high-level observations on the kinds of data they tend to collect and store. Consider using this list as a starting point to scan useful databases in your own context, with the understanding that database names will vary by jurisdiction.

Civil Registers

A civil register tends to capture data on individuals and their major life events, such as:

- full legal name(s)
- birthdate, location, sex and parentage
- marriage details – spouse full name(s), location, date, and witnesses
- divorce, separation, and annulment details – former spouse full name(s) and date
- adoption details, where applicable

- death date, location, and cause[28]

Common identifiers useful in linking civil registers and political finance data may include individuals' legal name(s), used in combination with their birthdates or current ages and unique identifiers such as citizen numbers (social security numbers, personal insurance numbers, or license numbers).

Cross-comparing political finance data with a civil register can help confirm the identity of – or validate data submitted on – individuals who appear in political finance reports (e.g., candidates, party officers, and campaign treasurers). Civil registers are also useful for identifying and investigating potential relationships and conflicts of interest between individuals listed in reports. For example, are particular vendors receiving repeat contracts and payments from a party or candidate that has a personal relationship with one or more of their owners?

Population or Resident Registers

Population registers tend to track individuals residing in a country, capturing data on all legal residents in the nation's physical territory over time regardless of citizenship, death, or emigration. They may include information common to civil registers (name, birth details, and marital status) as well as information on:

- citizenship status
- dates of arrival in/departure from the country
- current residence
- country of origin/onward emigration
- details of an individual's occupation[29] (e.g., active employee, retiree, or student)[30]

Common fields useful for linking these registers to political finance data include individuals' legal names, used in combination with their birthdates or ages and current residential addresses.

As with civil registries, cross-comparing political finance data with a population or residential register can help confirm the identity of – or validate data submitted on – individuals who appear in political finance reports. Interoperability with a population register could also help identify unallowable financial transactions in contexts where the legal framework sets rules around non-citizen contributions and service provision. In Lithuania, for example, data on donations are checked against the residents' register to confirm that an individual has the citizenship or permanent residency status that provides them with a legal right to make political contributions in the country.[31]

Consistent and up to date employment data can also be used to identify trends in which a company's employees all seem to give coordinated donations to a specific party or candidate – a potential sign that an employer is masking large donations by having employees provide the funds to the political stakeholder under their own names.

[28] World Bank Group and World Health Organization (WHO). (2014). Global Civil Registration and Vital Statistics: Scaling up Investment Plan 2015–2024. https://openknowledge.worldbank.org/server/api/core/bitstreams/371e85c6-e7f6-529b-b6f0-800267108692/content

[29] Author interview with a representative of Expert Forum, a Romanian nongovernmental organization.

[30] United Nations Statistics Division (2017). Population registers. https://unstats.un.org/unsd/demographic/sources/popreg/popregmethods.htm. See also: OSCE's Office for Democratic Institutions and Human Rights (ODIHR). (2009). Guidelines on Population Registration. https://www.osce.org/sites/default/files/f/documents/7/d/39496.pdf

[31] Author interview with a representatives of the Lithuanian Central Election Commission. As established in the 2022 Electoral Code, citizens may donate to candidates across all types of election campaigns; permanent residents who also have citizenship in an EU country may donate to campaigns for the European Parliament and for municipal councils and mayoral elections; and permanent residents who do not have citizenship in an EU country may donate to campaigns for municipal councils and mayoral elections. See: The Electoral Code of the Republic of Lithuania. (2022, with subsequent amendment), Article 110(1), https://www.vrk.lt/en/teisine-informacija.

Voter Registers

Voter registers are used for a wide variety of purposes, depending on the jurisdiction, such as pre-identification of eligible voters for poll workers, mapping polling station locations among election administrators and establishing transparency around voter lists in advance of elections. The following are common fields found across voter registers:

- personal identifier number
- name and former names
- date of birth/age
- sex and gender
- place of birth and/or nationality
- addresses and former addresses (pertinent to assigning polling stations or mailing ballots)[32]

Common fields useful for linking these registers to political finance data include individuals' former and current legal names, used in combination with birthdates or ages and current residential addresses. Cross-comparison of political finance and voter data serves a purpose similar to cross-comparison with a civil or population register.

Tax Registers

A tax register captures information on a taxpayer's legal identity, income and financial standing. For legal entities, it also includes information on the entity's structure and operations. Common core fields may include:

- a unique domestic or foreign taxpayer ID
- legal name(s) of the individual or entity
- legal address(es) of the individual or entity
- tax status of the individual or entity
- taxpayer wages and employer information
- names and supplemental information for key corporate officers
- taxpayer familial relationships (e.g., for joint filers).[33]

Common fields useful for linking taxpayers to political finance data include individual and entities' legal names, which may be used in combination with other identifiers, such as birthdate or date of incorporation. Each individual or legal entity paying taxes to the state will also have a unique domestic or foreign tax ID number. Taxpayer IDs stay consistent over time; when they are captured in political finance data, they are a useful tool for establishing meaningful interoperability.

Connecting to tax registers can assist oversight bodies in validating or identifying unallowable financial transactions. For example, this type of link can help confirm that donors meet nationality requirements.[34] In Lithuania – where the total amount of an individual‘s donation to a campaign and the value of an individual‘s annual membership fee for a political party may not exceed 10 percent of their declared income in the previous year – connecting to the tax register also helps the oversight institution verify that no stakeholders exceed this cap on contributions.[35]

---

[32] ACE Project. (n.d.). Elections and Technology. See “Defining the Purposes of Voter Registration” (https://aceproject.org/main/english/et/etl01a.htm) and “Voter Registration System Input Sources” (https://aceproject.org/main/english/et/etl03.htm).
[33] High-level observations were derived from a review of 2025 tax forms available via the U.S. Internal Revenue Service. Tax reporting requirements and tax form design vary by country; oversight bodies interested in linking to tax registries in their jurisdictions should review relevant laws and available data to determine the scope of data housed in domestic tax databases and what forms of cross-checking are feasible.
[34] Interviews conducted with representatives of the Lithuanian Central Election Commission and a Ukrainian political finance expert confirmed the utility of linking to tax registers.
[35] For clarity, Lithuania's Electoral Code states in Article 110(5), “The total amount of donations made by a natural person to independent participants and the membership fee paid to a political organisation during a calendar year may not

Comparing political finance data with tax register data is also valuable to identify red flags that may warrant further investigation. For example, if an individual or entity with a relatively low reported income provides outsized financial donations, this *can* be a sign of a straw donor operation (although further review would be needed to confirm). Alternately, a surge in similarly timed, similarly sized donations from individuals working for a common employer could be a sign of a hidden corporate donation scheme (again, further investigation would be required).

Company, Entrepreneur or Legal Entity Registers

Company and entrepreneur registers tend to amass basic information on legal entities operating as businesses in a jurisdiction, such as the following:

- entity legal name
- unique identifier/registration number
- a list of founders
- details of ownership structure
- owner name(s) and contact information
- name(s) and contact information of legal agent(s)/representative(s)
- details of company/entity termination (if relevant)[36]

Formal legal names and common shortened names for the entity, office address(es), and founder or representative name(s) and contact details can all be used in combination with one another to make connections across databases. If a political finance register captures businesses' unique registration numbers, then this point of information can be valuable in establishing interoperability.

Linking business registers to political finance databases can help flesh out oversight body records, support data verification, or signal a need for follow-up investigations. For example, if a business provides services to multiple candidates but its name is listed differently across campaign reports (e.g., "Imaging Creatives and Associates" in one filing and "ICA Inc." in another), then an oversight body could identify all the candidates for which this company provided services if it had access to the company's unique business identifier, or if the company register captured both formal and common short names for the business. Comparison of political finance and business register data may help with confirming that a campaign or party service provider is a legitimate vendor, or that a business is a legitimate donor.

The dates or registration and dissolution of companies can also be valuable to oversight institutions. In Romania, civil society organizations have used public registries to spot suspicious donation patterns in which small companies are set up before elections and subsequently provide large cash donations to specific political campaigns. Identifying the rapid creation and dissolution of companies immediately before and after elections is not, on its own, proof of a straw donor arrangement, but is a useful way to generate red flags for follow-up investigation.[37]

exceed ten per cent of the amount of the annual income declared by the natural person for the last calendar year, for donations made after 1 May, or the amount of the annual income declared by the natural person for the calendar year preceding the previous year, for donations made before 1 May."

[36] The United Kingdom's Companies House is one example of a company register. A sample download illustrating the scope of information captured on legal entities under the Companies House scheme is available at https://download.companieshouse.gov.uk/en_output.html.

[37] Research from civil society suggests that in some cases, wealthy individuals set up and provide temporary companies with loans, which the company in turn donates to a party or campaign. This process may mask instances in which wealthy donors are providing significant funding to the same party or campaign and masking their total contributions by spreading donations across multiple entities. Author interview with civil society expert.

Public Official Income and Asset Declaration Registers

Public figures are required to disclose information on their income and assets and on their direct family members' income and assets. Common fields included in disclosures capture details on the following:

- non-moveable assets (e.g., real estate)
- moveable assets (vehicles, art, and jewelry)
- financial assets (foreign and domestic accounts, stocks, bonds, and cryptocurrency holdings)
- in-kind benefits (e.g., scholarships)
- gifts and hospitality received
- memberships, clubs, and other affiliations
- secondary employment
- liabilities and loans (and their terms)[38]

As with other public databases, common indicators across asset declarations and political finance reports include individual names and contact information, addresses, and birthdates or ages. However, there may also be a significant number of unique identifiers associated with public officials' assets (e.g., unique IDs for commercial properties, vehicle identification numbers, and bank account details) and loans that help forge connections across databases.

Bringing together data on money in politics and public officials' assets and incomes can help identify conflicts of interest, such as cases in which a candidate purchases services and issues payments to a company owned by a family member. It can also shine light on where a candidate is receiving offers of financial and in-kind support through personal loans (sometimes with beneficial terms or fully forgiven) rather than formal political donation channels.

Beneficial Ownership Registers

A beneficial ownership registry provides deeper insights on who ultimately owns, benefits from and/or controls a legal entity. Common data points captured in beneficial ownership registers may include:[39]

- Basic entity details:
  - entity type, name, and country of registration
  - other known identifiers, external identifier scheme codes/scheme names, and established entity URIs
  - information on whether it is a public listing (including relevant regulatory filings)
  - founding and dissolution dates
- Details on individuals linked to the entity:
  - individual type (known, unknown), name, place and date of birth, nationalities, place and date of death, tax residencies, and PEP details
  - other known identifiers, external identifier scheme codes, and names and URIs
- Details on relationship(s), such as:
  - whether and how ownership is nested
  - records of indirect relationships between an individual and an entity

Several of these fields can be combined to create confident links to political finance datasets, including entity and owner legal name(s), alternate and shortened names or acronyms for companies, dates of incorporation and

[38] This list of common fields was identified in an October 2025 interview with a researcher working for the civil society organization UNCAC Coalition, who led an in-depth research initiative on strengthening asset declaration systems.
[39] This list of common fields is derived from review of Open Ownership's Beneficial Ownership Data Standard (BODS). For more information on BODS and links to the full schema, see https://www.openownership.org/en/topics/beneficial-ownership-data-standard/.

termination, and registered address(es). Each individual and entity also will have a unique identifier in the database, which is crucial for identifying broader networks of relationships.

Beneficial ownership registers can help identify the ultimate source of a donation (which could be masked if an oversight body must rely solely on tax records or a company register) and who is benefiting from party- or campaign-issued payments.

Having access to beneficial ownership data could also help oversight bodies complete basic compliance checks, such as checking for breaches in donation limits. In some contexts, company owners may transfer funds between the entities they control before making donations, thereby masking that they have breached a cap on the cumulative amount of donations for a single contributor.[40] Beneficial ownership data can help identify tactics of this nature by allowing oversight bodies to trace donations back to their source and identify a true amalgamated total of the contributions.

Procurement Registers

Procurement registers gather detailed information on discrete procurement processes, such as:

- actors engaged in any aspect of the contracting process (consistently formatted identifiers, representative names and contact details, including for agencies launching an opportunity)
- buyers (identifiers, representatives and contact details)
- planning data (need/rationale for an award, budget, funding source, detailed specifications, and deliverables)
- tender data (procuring entity identifiers and contact details, anticipated work/deliverables, key dates, evaluation criteria, number of tenders, tendering organization identifiers, and log of tender amendments)
- award data (award status and date, value, supplier identifiers, key dates, expected deliverables, and log of award amendments)
- contract data (information on implementation, value/date of relevant transactions, payer and payee identifiers, milestone details, and log of amendments)[41]

Common identifiers overlapping with political finance data include legal names and contact information for individuals and entities.

Linking political finance and procurement registers can help oversight bodies conduct basic compliance checks (e.g., if companies receiving government contracts are barred from making donations for a specified period). Interoperability between these databases can also help identify potential conflicts of interest in political finance. For example, TI Colombia used publicly available data on campaign donations and public procurement processes to find that one in four significant political donors had received government contracts in the period immediately after elections – with many awards made on a noncompetitive basis. Although this was not proof of corruption, it raised a red flag about risks that political donations might have been granted in exchange for future government contracts.[42]

Lobbying Registers

Lobbying registers generally contain data on:

- names of individuals and interest groups or companies engaging in lobbying
- registered addresses of filers
- priority issue areas (or legislation) covered by filers

[40] Author interview with a representative of Expert Forum.
[41] This list of common fields was derived from review of the Open Contracting Data Standard (OCDS). For more information on OCDS and links to the full schema, see https://standard.open-contracting.org/latest/en/.
[42] Author interview with a representative from TI Colombia.

They may also include information on names of interest group staff, details on office locations and expenses, insights on contractual relationships with the government, and names of public officials (including elected officials) who accept lobbying meetings and dates of meetings.[43]

The level of detail captured in lobbying databases can vary widely, but common fields to establish links to political finance data once again include legal name(s) and contact addresses for individuals and entities. Comparing political finance data with lobbying registers can be particularly useful in contexts where there are bans or limits on lobbying donations to parties and candidates.

Other Registers

It may also be useful to establish links to **property registers, land registers, customs registers, and vehicle registers**, among other government datasets, to verify information that political parties submit on their current assets, sources of income, liabilities, and expenditures. Depending on what the law permits with regard to donations and third-party campaigning, oversight bodies may also find value in linking to **charity registers, nongovernmental organization registers, and religious organization registers**.

Setting Priorities

In deciding which databases to prioritize for connection, oversight bodies need to balance several competing factors. This section reviews some questions for oversight bodies to consider in determining how to invest their time and resources prudently.

Datasets That Complement Your Mandate

What data does the oversight body need to meet its mandate for control of political finance?

Planning for interoperability should start with a reflection on how connections to external datasets can reduce staff burdens and streamline delivery of the oversight body's existing mandate to ensure all stakeholders have respected the rules for donations, spending, and asset and liability management. As a first step, consider what current tasks demand the most time and effort from your team in reviewing and verifying party and campaign finance reports. For example, is it onerous – or impossible – to:

- verify the purchase or sale of party-held assets as currently logged in regular party finance reports?
- validate the identity of donors and loan providers and verify that they are permitted to offer political contributions under the existing legal framework?
- confirm the identity, operations, and services of vendors receiving payments from parties, candidates or campaigns?

The databases most likely to help with these forms of control over basic financial transactions, donations and spending are civil, population, or voter registers; tax registers; company registers; asset declaration registers; and a wide variety of state databases for tracking assets such as land, real estate developments, and vehicles. These sources provide detailed information that allows users to validate the identities of individuals and entities that commonly appear in party and campaign finance reports, and to track assets as they change hands.

Identifying database links that will advance your mandate may seem like an obvious entry point for establishing political finance interoperability, but it bears flagging as an initial planning step for two reasons. First, streamlining staff workloads through early data projects can build team buy-in and lessen internal opposition to changes in

[43] Katsaitis, A. (2024). Mapping and Analysing Lobbying Registers. Discussion Paper 1/2024. International IDEA. https://www.idea.int/sites/default/files/2024-03/mapping-and-analysing-lobbying-registers.pdf

administrative or operational processes associated with data clean up and navigating new data sharing arrangements. Second, donors and peer agencies do not necessarily share the same priorities; they may prioritize other open data connections, such as those advancing transnational asset tracing and recovery. These are valid aims of interoperability for anticorruption, and this observation is not a rebuke of competing priorities. Rather it is a reminder to establish the exact data sharing arrangements your institution needs to facilitate its own work, as you may have unique priorities.

What data does the oversight body need to identify "red flags" that may warrant deeper investigation?

Red flags are not proof of wrongdoing, but they are signals that something is out of the normal range and warrants investigation (e.g., a high-value donation compared to a company's declared liquid assets, or a company receiving a lucrative government contract after giving a major donation to an incumbent party's presidential candidate).

Each country has its own legal framework regulating money in politics and operates in a particular geopolitical context. Actors seeking to bypass political finance rules are likely to adopt different tactics based on local practice and the likelihood of detection and sanction. In some countries, this may result in significant in-kind or financial support to political actors during primary phases or before official campaign reporting periods kick off. In other contexts, stakeholders may use cryptocurrency exchanges to move money quietly to straw donors or non-contestant campaigners, hoping to tip the field in their favor. As tactics for bypassing political finance rules evolve, an oversight institution's standard compliance and verification checks on political finance data may become insufficient to detect all forms of violations, requiring new strategies or the use of red flags to help identify cases that need further investigation. Interoperability can help with these detection efforts.

For example, linking political finance data to the state tax registry and to public officials' asset declarations are an envisioned uses of the National Agency for Corruption Prevention's (NACP) newly updated[44] POLITDATA platform. Creating the link to tax data will allow the oversight body to identify red flags for further review, pinpointing where donors were providing significant financial contributions that seemed outsized compared to their declared incomes. Similarly, linking to asset declaration data will help the NACP identify where council members, members of parliament, and their family members were making declarations that outpaced their declared incomes and assets.[45]

A first step in establishing effective red flag indicators is to assess the most common and pressing violations in your political context. From there, it becomes possible to identify links to other databases that could be useful in identifying potential violations. The following table offers general, non-exhaustive guidance on how different government registers can support oversight. Linking to external databases to establish effective red flags is fundamentally about mapping relationships. Beyond providing more detail on individuals, entities, and ownership of physical assets – critical aspects of compliance and verification – these databases add additional layers of information about how actors are connected, including across borders.

TABLE 2. ILLUSTRATIVE GUIDANCE FOR LINKING DATABASES TO IDENTIFY HIGH-PRIORITY VIOLATIONS

If these violations are a priority …	… consider linking to these kinds of external government datasets.
Donations from single sources that exceed the legal limits for political giving	• **Civil or population registries:** Are multiple members of a single-earner family giving donations to mask the true source?

[44] POLITDATA is an online political finance portal, first launched in 2020, designed to streamline political parties' digital reporting and increase the transparency of data for the general public in Ukraine. An enhanced POLITDATA 2.0 was released in 2025. See: National Agency on Corruption Prevention. (2025, July 2). NACP launched an updated version of the POLITDATA 2.0 register. https://nazk.gov.ua/en/news/nacp-launched-an-updated-version-of-the-politdata-2-0-register/

[45] Author interview with a Ukrainian political finance expert.

If these violations are a priority …	… consider linking to these kinds of external government datasets.
	• **Company, entrepreneur or legal entity registry:** Is there a common founder of a string of companies that are making major donations, bypassing limitations on individual giving? • **Tax registries:** Is an individual exceeding legally allowable donation limits where caps are based on income?
Donations from foreign actors	• **Beneficial ownership registry:** Who controls legal entities providing election funding? • **Company, entrepreneur or legal entity registries:** Is the entity a subsidiary of a foreign company? Where is it registered? • **Civil or population registries and tax registries:** What is the donor's nationality or resident status?
Donations from banned domestic sources (e.g., corporations that have recently received government contracts)	• **Company, entrepreneur or legal entity registers:** Where is the entity registered? Was it established shortly before the election? Do its financial activities suggest that it has the means to provide the level of support it has offered to an electoral contestant? • **Public procurement database:** What awards has the entity received from the government, if applicable? When were these awards received? • **Voter register:** Is the donor a registered voter, where allowability of contributions is premised on active voter registration status?
Omissions or incorrect information in a candidate's reported personal contributions to their campaign (including loans)	• **Asset and interest declarations:** For a candidate who is already a public official, is the individual relying on personal loans to fund the campaign – and if so, who is providing the loans, and on what terms? • **Tax registries:** Is the amount an individual is contributing to their own campaign reasonable given their declared income and assets?
Donations in return for future kickbacks or benefits from the state[46]	• **Public procurement databases:** Did legal entities providing major donations to a winning party or candidate receive major contracts once their beneficiaries took office? • **Asset and interest declarations:** Has the public official received any major personal loans from politically exposed persons, company owners bidding for public awards, or registered lobbyists? • **Lobbying databases:** Have registered lobbying individuals or entities made contributions to a preferred party or candidate? Are these donations made in line with bans or limits established in the legal framework? Are there any longer-term indications of conflicts of interest, such as granting major policy concessions in line with the lobbyists' core interest or awarding government contracts to lobbying groups or their clients?

[46] In some countries, the institution responsible for controlling political finance may also be responsible for detecting and initially investigating conflicts of interest (e.g., where these mandates are concentrated in an anticorruption agency). In such cases, setting up cross-checks for conflicts of interest may be easily justifiable and prioritized. Yet even in countries where the mandates for political finance oversight and conflict of interest investigations are split across multiple agencies, setting up red flag systems can be beneficial to political finance bodies – saving them time and enabling them to respond rapidly to requests for information from peer agencies, including law enforcement.

Legal Feasibility and Timelines for Change

What changes are legally feasible in the near, medium and longer term?

What can you collect under the current legal framework, how frequently can you collect it, and with whom can you share the data? Moreover, what additional restrictions exist around the data you are seeking to access? Data interoperability projects must be grounded in a firm understanding of the legal framework. This means project managers must have a firm grip on the laws, bylaws, and regulations that shape party and campaign finance; national laws around data security and privacy; and possibly additional regulations and protection implemented by the peer agency from which they are requesting data.

Some changes to data collection may be uncontentious and easier to make in the short term, such as updating a form to require a full legal name and/or requesting that commonly used nicknames be reported for individuals.

Other changes might best be achieved in the medium term. Consider whether the oversight body can strengthen or clarify reporting rules through regulatory changes that fall short of formal legal reform (e.g., updating bylaws or institutional policies). For example, oversight bodies that are legally responsible for reviewing contracts or payments to vendors or assessing the national origin of companies providing donations to a political actor, may be able to update regulations to collect expanded data on companies – setting the groundwork for better links to company registers. This is only feasible if the extended data collection directly relates to the oversight institution's existing mandate and does not contradict other laws.

Finally, some change may take significant advocacy, alliance building, and time. This may be the case if the oversight body is seeking interoperability with datasets containing significant personally identifiable information, or where the oversight body is seeking access to data beyond its current mandate (e.g., in setting up new red flags). Additionally, more time and funding may be required if one or both bodies seeking to exchange data have not digitalized their reporting and recordkeeping.

In making internal decisions around data collection and management, consider that adding new data fields to party and candidate or campaign finance reports without a firm legal basis for doing so may lead to noncompliance from reporting entities. For example, parties and candidates may turn in blank or incomplete forms if they feel they have no legal obligation to provide the requested information. Additionally, updating financial reporting methods (e.g., moving from paper to electronic submissions) may take time, persuasion, and possibly legal amendments. This happened in Lithuania when the Central Election Commission began asking parties and candidates to submit reports via a digital information system instead of on paper. Initially, some stakeholders continued to file paper reports, refusing to use the new tool. After several election cycles and with advocacy, the election law was amended to require digital financial disclosure. Although parties and members of parliament were initially concerned about the additional workload, progress was based on the understanding that digital reporting and cross-agency data sharing could help parties and candidates meet their reporting requirements.[47]

Quality, Scope and Pre-existing Compatibility

Will quality, scope, or interoperability challenges prevent the oversight body from linking to external datasets? Before setting up a data exchange, oversight bodies with constrained time and resources may wish to assess the quality and scope of information in the database they are seeking to connect to, either through review of publicly accessible data portals, review of available metadata (e.g., when was the dataset last updated?), or through targeted meetings with peer agencies. For example, if they are seeking information on a public official's assets during the campaign period but public officials' declarations are only available for a period dating several years back, then they will miss critical information on the status of personal loans, income, and assets at the time of the election. Consider questions such as the following:

[47] Author interview with a representatives of the Lithuanian Central Election Commission.

- What is the time frame for data in the external database? Will it help the oversight institution verify the wealth and interests of parties, candidates, and other regulated entities during the campaign period?
- How frequently is the data in the external database updated?
- How complete is the data in the external database?
- How is the data sourced and how is it verified by the peer agency/third-party source?
- Are there any reasons to be concerned about the quality of the external dataset?

Ukraine offers an example of how incomplete datasets can undermine the value of interoperability. In the past, the NACP faced significant challenges in tracking and sanctioning political parties' regional branches for failing to file reports. They were missing a consolidated register of parties and relied on minimal data about regional branches that was partially available from other ministries. Over time, they enhanced cross-checks and were able to identify and sanction non-reporting regional party branches, but this first required the creation of a more robust and centralized list of party branches, pulling from Ministry of Justice data, paper copies of old political finance reports, and privately managed databases.[48]

At this exploratory stage, it can also be useful to map points of overlap between datasets. The following core questions should be considered in tandem with the analysis of the legal feasibility of interoperability:

- Are there common or unique identifiers across databases that will be useful in establishing interoperability?
- Are there new data fields that your institution would need to start collecting to forge meaningful links (e.g., company or charity registration numbers? additional contact details to help with consistent identification of individuals or entities across datasets? VINs for party owned vehicles)? If so:
    - Can your institution mandate disclosure in these new data fields from parties, candidates and other relevant stakeholders under the current legal framework?
    - Do you have the necessary funds and personnel to capture and manage this data?
    - For which of the new data fields are parties and candidates more likely to provide data, and why?

Building and maintaining large and accurate datasets can be a costly and labor-intensive undertaking. Data quality may suffer if managing agencies experience high turnover, constrained staffing and budgets or any number of other challenges. Understanding in advance the potential gaps or weaknesses in external databases and any overlaps in the existing datasets will help oversight bodies decide whether interoperability is worth pursuing and know which limitations they may encounter in using the external data to help validate political finance reports.

[48] Author interview with a Ukrainian political finance expert.

Refining and Establishing a Framework for Interagency Data Sharing

Refer to this section if you have a clear understanding of which data you need from a peer agency and are preparing to negotiate data sharing arrangements.

Safe and effective data sharing across agencies requires planning and, at times, a measure of salesmanship. A peer agency may initially resist requests to share more data for a range of reasons – a desire to avoid assigning additional tasks to overloaded staff, concerns about data privacy, uncertainty about the legality of a request and who has the authority to authorize data release, or even fear of external scrutiny or interference in how they manage their data. Before approaching a peer agency with a request, take the time to ensure you understand how the legal framework shapes interagency data sharing and reflect on how to manage coordination. This will help you refine the details of your request.

Laying the Groundwork

Before launching into interagency negotiations, invest time and effort into understanding what the domestic legal framework requires around interagency data sharing, data security, and data privacy. For example:

- Are laws or regulations already in place that require proactive or targeted data sharing between government agencies to support agencies in delivering on their mandates?
- Are you seeking data that should already be made public?
- In light of cybersecurity and data privacy laws, what reservations might peer agencies raise about sharing their data, and how can you mitigate these concerns?

This initial research may strengthen your ability to justify the data sharing request by enabling you to cite specific legal articles or regulations in your exchanges with peer agencies. Research may also help you refine the scope of your request, bringing it in line with prevailing privacy protections or prompting the team to identify more secure means of data exchange.

Framing the Request

Clarify *What* Data You Are Requesting from the Peer Agency

You likely do not need blanket access to the peer agency's files but rather access to a targeted portion of their available data. In seeking data on party or candidate finances from banks, for example, an oversight body may request information on specific transactions during a specific reporting period rather than a full list of all deposits and payments from an account.[49] Alternately, the oversight body may require only a list of account numbers and confirmation of their creation dates and status, to support verification that relevant stakeholders established dedicated accounts for electoral campaigns (where this is required by law). **Carefully targeting your data requests is best practice**. It can preserve privacy, mitigate potential reservations about data sharing, and prevent slowdowns in negotiations that could arise when the scope of a data request is too broad.

Articulate *Why* You Are Requesting the Data – For Yourself and the Peer Agency

Most of the staff you meet with across peer agencies will not be political finance experts. Consider preparing a streamlined pitch describing why your institution needs the data. For example:

[49] Author interview with representatives of the Armenian Corruption Prevention Commission.

> *"Our team would like access to your department's data on company registration dates. This will allow us to identify red flags for corruption – for instance, cases where a company is established just weeks before a campaign period and is able to make a large donation to a candidate's campaign."*

Be prepared to offer concrete examples of how and why you need access to the peer agency's data and specify how the specific data they hold will be critical to your own cross-checks (in the example above, company names and registration dates).

Just as important, identify how the peer agency can also benefit from linking datasets to make the exchange more appealing to them. Would linking your data on vehicles and other property owned by political parties help another government agency assess the accuracy of their own records? Would the link between databases save the peer agency time in responding to your ad hoc requests for data if a more streamlined and regular process were established for cross-checking data? Could it save both of your teams time and effort in trying to coordinate and respond to requests for information from police, prosecutors or other enforcement agencies during investigations? Be ready to highlight the ways that establishing interoperability of your datasets could save time, money, and effort for your team and the peer agencies.

Think Through *How* Data Sharing Will Occur in Practice

Be prepared to discuss the benefits and disadvantages of different data sharing options for both your institution and peer agencies. For example, consider your institution's ideal method of data transfer (e.g., API, direct database or portal access, or file transfer). What could you accommodate if the peer agency has a different preference?

- If API is the most convenient (e.g., the agency has one already and your team has the skills to pull from/access it): Which member(s) of your team will have authorization to pull this data? How often is it updated and how often can you access it?
- If the peer agency has data stored on a portal: Is there a way to grant your institution (or a designated user) access to the peer agency's portal? If yes, what permissions will the user(s) have (e.g., view only, download), and what are the rules for accessing the external system?
- If data will be transferred by a static Excel, CSV ,or other structured file: How can the file(s) be shared (e.g., via email, secure cloud server, USB ,or external hard drive)? Who is responsible for sending the most up-to-date data, and how frequently will it be shared? Can sharing be automated, or will the institution need to request it periodically?

Drawing on your initial research into the domestic legal framework for data sharing, security and privacy, be prepared to discuss how you will protect sensitive data points that are shared between agencies; for example, by redacting personally identifiable information from reporting forms and supporting documentation before they are published.[50]

Additionally, consider mapping out how you will ensure that rules for data projection are followed and how any breaches in data sharing agreements will be addressed and communicated between agencies. Data sharing can be a sensitive area of collaboration, so investing upfront time and effort into identifying safeguards for data protection could signal good intent and build trust.

Agree on *When* Data Sharing Will Happen

Is this a one-time exchange or an iterative exchange of data? If the data exchange process is not automated or completed on demand (e.g., via direct access to a portal or API pulls), then what is the timeline for requesting and

[50] Author interview with representatives of the Lithuanian Central Election Commission. In Lithuania, contracts between political stakeholders and vendors are uploaded with financial reports (e.g., for ad purchases). When this happens, the text of the contract is publicly available, with only sensitive information hidden (e.g., ID number, telephone and banking information). Thus, the supporting documents' content is partially available to the public.

providing the required data exchange between agencies? To avoid stress or delays, consider working backward to set reasonable timelines for issuing and completing data requests that work for both institutions:

- What are the important deadlines for political finance reporting and review or auditing that your institution needs to meet?
  - To meet these deadlines, when do you need the peer agency's data? Include time estimates for data compliance and verification checks, follow-up with parties and candidates/campaigns if data is missing and any deadlines for releasing data to the public.
    - How long does the peer agency need to review and respond to your data request?
      - ★ *When is the latest that the oversight institution must request the data from the peer agency to meet its mandated deadlines?*

Define *Who* Is Involved across the Data Sharing Process

Within your oversight institution, this includes who is responsible and has the authority for requesting data from the peer agency and who has the privileges to access or view the shared data. In turn, it is helpful to understand which contacts at the peer agency can answer questions about technical issues (e.g., loss of portal access, inoperable API, corrupted file), and whom to contact with more substantive questions about the data (e.g., missing data or the correct interpretation of a data point).

To streamline communication and cooperation, it can be useful to nominate a single point of contact at each institution who can receive all questions about the data sharing agreement and then direct those questions (through internal channels) to the right personnel who can respond.

Process Considerations

Think About Who Needs to Be in the Room and When

Sequencing can be important when you are initiating contact. If there are concerns about who can authorize data sharing, consider starting with high-level meetings. If senior staff are more likely to be responsive to data sharing efforts that come from their own teams, consider starting with outreach to operational teams. Alternatively, if data has been exchanged before and you are simply seeking to streamline and normalize data sharing, consider bringing IT, data and technical experts to the table to dig into the weeds about which data to share and how to complete transfers safely before you seek formal approval from leadership.

There is no single roadmap to assist with this step of planning, but stepping back to identify and assess the benefits and drawbacks of multiple entry points could save time and establish cross-agency buy-in.

Consider Formalizing Data Sharing Agreements in a Memorandum of Understanding

Representatives of relevant departments need to agree on a range of issues, including the what, why, how, when, and who of data transfer outlined above. Documenting each agency's agreements on these and other important points can be an important step in setting rules and building the trust needed to establish meaningful data sharing. Additionally, such agreements can serve as knowledge transfer tools for new staff adopting data interoperability responsibilities.[51]

[51] Author interview with representatives of the Lithuanian Central Election Commission. For each agency with which it shares data, the commission maintains robust memoranda of understanding covering a wide range of topics (e.g., data format data, general timelines and deadlines for sharing data and guidance on how to request additional information).

Annex: Steps Toward Data Sharing

In-House Preparations

1. Develop or update documentation to reflect the current scope and format of your data, and incorporate definitions of data fields, as needed, to support semantic interoperability.
2. Standardize data using broadly accepted formats and code lists.
3. Identify instances in which you are actively collecting unique and common identifiers – or could easily introduce new fields – to increase overlap with other databases.
4. Hold robust consultations with diverse stakeholders to collect feedback on and build buy-in for potential changes in reporting requirements.
5. Update reporting forms and your institution's internal data documentation to include approved changes in data collection.
6. Train staff *and* reporting entities on updates to reporting requirements and processes.

Practical reminders

- Budget in advance to cover all stages of the project, from the initial review of data through updates to reporting materials and training.
- Assemble a multidisciplinary team, including members who can keep projects on track, technology experts, data experts, and political finance experts.
- Build in time for genuine consultations and be transparent about how external recommendations are integrated into decision-making.

Identify Opportunities and Set Priorities

7. Identify relevant government datasets that can help verify political finance data.
8. Map common identifiers across political finance data and external datasets.
9. Assess legal feasibility and authority to share and request data.
10. Identify priorities for interoperability, starting with databases that directly support the oversight institution's ability to deliver on its mandate.
11. To the extent possible, assess the quality of data housed in the external datasets prioritized for interoperability. For example, are there clear gaps? Is the data up to date?
12. Prioritize interoperability projects based on legal feasibility and authority, degree of relevance to the oversight institution's mandate, and the quality of the external datasets.

Refine and Establish a Framework for Interagency Data Sharing

Lay the Groundwork

13. Ensure your team has a firm understanding of the domestic legal framework for interagency data sharing, paying particular attention to data security and privacy measures.

Frame Your Request

14. Clarify precisely **what** data is needed to establish interoperability and verify the completeness and accuracy of your political finance data.
15. Articulate **why** the data is needed, building a business case for internal staff, peer agencies, political parties, candidates, and other stakeholders.
16. Determine **how** data can be shared most appropriately, bearing in mind the constraints of both the oversight institution and peer agencies.
17. Define **when** exchanges will occur, building in time to troubleshoot errors and cross-check the data in advance of oversight deadlines.
18. Decide **who** has responsibility and access rights, keeping data privacy and security at top of mind.

Consider Process Elements

19. Strategize around sequencing for meetings. Who needs to be in the room – and when – to get authorization and operational buy-in for data sharing?
20. Formalize the data sharing agreement in writing, documenting the *what*, *why*, *how*, *when*, and *who* of decisions (the “Frame Your Request” steps) and identifying points of contact in case questions arise.


INTERNATIONAL FOUNDATION
FOR ELECTORAL SYSTEMS
IFES

2000 M Street NW, Washington, DC, 20036, United States

www.IFES.org