# 3. Using the data received

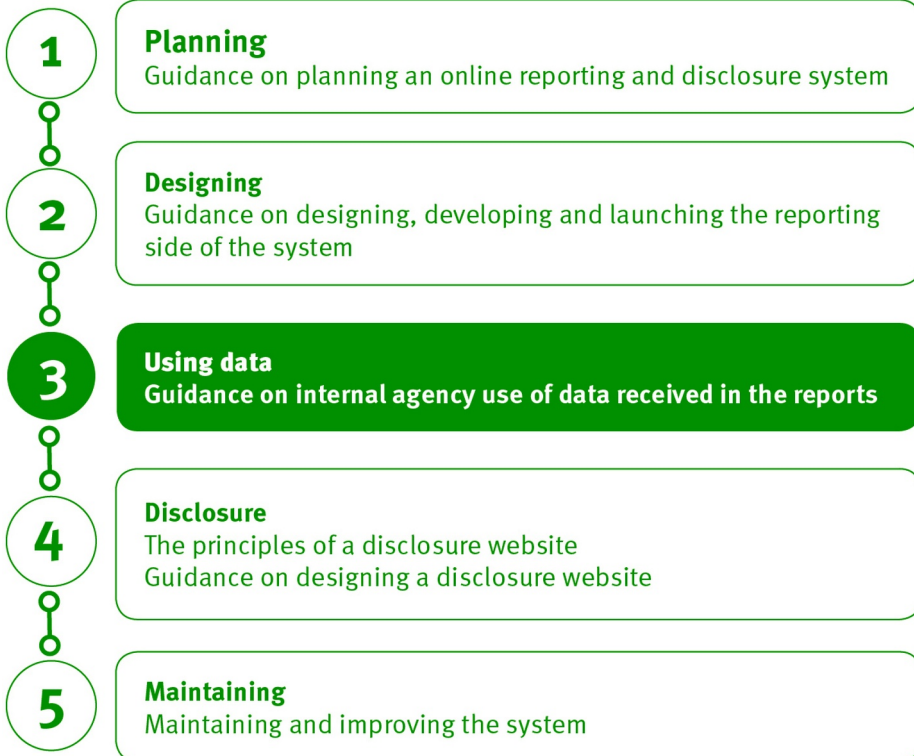| | |
|---|---|
| **1** | **Planning**<br>Guidance on planning an online reporting and disclosure system |
| **2** | **Designing**<br>Guidance on designing, developing and launching the reporting side of the system |
| **3** | **Using data**<br>**Guidance on internal agency use of data received in the reports** |
| **4** | **Disclosure**<br>The principles of a disclosure website<br>Guidance on designing a disclosure website |
| **5** | **Maintaining**<br>Maintaining and improving the system |

The oversight body can use the financial data received from political parties and candidates via the online reporting system in several ways, but most notably to monitor compliance with regulations; disclose data on their website for public scrutiny; verify the accuracy of data received; and analyse data for internal purposes.

## 3.1. Monitoring compliance with regulations

The user interface should have been designed to allow staff to easily see all areas of non-compliance, including late submissions and breaches of donation or spending limits. This ability is, of course, absolutely fundamental to the functioning of any online political finance reporting system.

For monitoring compliance, the system needs to produce specific reports on, for example, submission and compliance history. Make sure that there is a dedicated member of staff with the necessary expertise to analyse and interrogate the data. There will always be unanticipated questions about the data that need answering, so it may prove cheaper in the long run to employ skilled staff who can write database reports.

In the event of non-compliance, it is crucial to ensure that the data are robust enough for use as evidence. Auditable data, as discussed in section 3.3, helps greatly in this regard.

## 3.2. Verification of data

The extent to which the data received should be used to attempt to verify its accuracy will vary by country, depending on both the mandate of the oversight agency and the overall objectives of the online reporting and disclosure system. In more established democracies, the role of the oversight agency is often focused on monitoring compliance with reporting requirements and making the data public; civil society then scrutinizes and interrogates the data. If inaccuracies are discovered and reported to the oversight agency, it then follows up and investigates them. This is the case in democracies with a vibrant civil society and culture of investigative journalism, such as Australia, the UK and the USA.

In other countries, the political finance oversight agency has more of an anti-corruption mandate. This is typically the case in former Soviet and Eastern bloc countries. In Mexico, the online system was created to detect violations of campaign finance regulations, particularly spending limits, in a more timely manner. In these countries, verifying the accuracy of the political finance data submitted is a central task of the oversight agency.

Although an online reporting system can help to some extent to verify data, much of this work will still need to be done manually. Where this task falls to the oversight agency, it should dedicate staff time to detecting inaccurate or false data.

Below are three examples of how an online system can help with the verification process.

### Looking for anomalies

A system can be programmed to flag suspicious looking data entries that warrant further human investigation, such as particularly large sums of money or inconsistencies between different data sources. In Estonia, different sets of data can be compared to see if they tally. In Australia, donors are required to file reports on donations, in addition to parties and candidates reporting on receipt of these same donations. The eReturns system then compares these donation reports (made and received) and flags any discrepancies between the two.

In the USA, the system automatically checks for consistency between the current and previous report. For example, if the user's ending balances on the previous report do not match the starting balances on the current report, then this is flagged.

### Linking to other agencies and databases

If you expect data integrity to be an issue in your country, it may a good idea to link up with other official databases. Examples include:

- Cross-referencing social security numbers against civil registries, such as in Estonia, Finland and Georgia, to verify that only real, living people make donations. In Estonia, entries that contradict data contained in the population registry are automatically rejected.

- Linking to a business registry to check that donations come from legitimate entities, as in Estonia.

- Linking up with the tax registry, as in Estonia, where annual revenue and expenditures declared to the state are compared to reports submitted to the oversight agency. Latvia also intends to do this with its online system (under development at the time of writing). This comparison would detect whether donors contributed more than their total declared annual earnings according to their tax returns (which happens in an estimated 5 per cent of cases). In Colombia, if the electoral authorities deem it necessary to review the accuracy of financial information submitted to them, they can request data from the tax authorities.

- Cross-referencing political finance data with financial institutions, such as Mexico's Financial Intelligence Unit and National Bank and Monetary Commission. Ukraine has considered cross-referencing spending data with candidates' asset declarations during its planning process for an online political finance reporting system.

Where relevant data exists in other systems or is required to be exported from the political finance oversight agency's own system, consider automating the data transfer. This not only reduces ongoing labour costs but also ensures the accuracy and availability of the data.

### Batch together entities with multiple names

Where there is a risk that the same name might be written in more than one way, it is recommended to create rules to batch together these single entities with multiple names in order to avoid the system categorizing them separately. This is especially pertinent if the names are not being cross-checked with the databases of other agencies. In Australia, for example, where political donors have to file reports to the AEC, eReturns has been programmed to batch donors such as Coca Cola, Coke and Coke Corp together. Each year the system is updated with similar additional clustering. This saves staff from having to manually check and re-group filed returns. The system is also programmed to flag similar names that should be checked to see if they should be added to the list of groupings. Check, however, that there are no legal restrictions before setting this up. It is common for legislation to require information to be published exactly as it was submitted.

## 3.3. Data analysis for internal purposes

The oversight agency may wish to analyse data for its own internal purposes. In Colombia, for example, data are disaggregated by age, gender and ethnicity in order to analyse the dynamics of party and campaign funds, such as what percentage of donors are women, how much of a party's public funds are allocated to and spent by female candidates, how parties vary in the age of their donors and so on. If the provision of public funds is tied to its use by female candidates in some form, disaggregating financial data by gender may be crucial to the law's implementation.

---

**Summary of key considerations for using the data received**

- Is the oversight agency or civil society responsible for verifying the accuracy of data?

- Linking to other agency databases and cross-referencing data is a particularly effective way to verify political finance data.

- Consider how data can be analysed for your own internal purposes.