

## Case Study on the permissibility of donations

Source: IIDEM project – 2021.

### Methods used by political finance oversight bodies to check the permissibility of donations.

There are a variety of methods used for checking the permissibility of donations depending on country context and other factors. The oversight body in some countries do not undertake permissibility checks at all, some confirm the legitimacy of all donations, whilst others do so on a sampling basis. Permissibility checks are done manually in some countries whereas some oversight bodies have automated processes in place for the task.

To start, consideration must be given to the domestic political finance legislation setting out the criteria for permissible donations. For example, most countries ban foreign donations. Although such bans are very common, there can be wide variation in how ‘foreign donations’ are defined which may influence the oversight body’s approach to verification. In many countries, recipients must include the donor’s identification number in the reports submitted to the oversight institution, e.g., Estonia, Lithuania, Finland, and Albania. The oversight institution can then check the information against the citizen’s registry database. However, in other countries, such as the United Kingdom or Canada, there are no identify numbers or unique identifier for individuals. The UK legislation requires donors to be on an electoral register at the time of their donation. Political parties and candidates must include the donor’s name and address in the reports filed with the Electoral Commission. The Commission has access to copies of the electoral registers which it uses to confirm that the donor is registered on the electoral roll at the address provided in the submitted reports.

Domestic legislation governing the sharing of personal data also plays an important role in how oversight bodies approach permissibility checks. Lithuania and Canada offer two contrasting examples:

In **Lithuania**, all election contestants are required to use the Political Parties and Political Campaign Financing Control Subsystem of the VRK IS to report their membership fees, donations, expenditure and campaign contracts. The Lithuania Central Election Commission has a unified IT platform, meaning that it can be used by both the oversight body and the regulated community. The platform is interconnected with other state institutions. If the political party treasurer wants to check the permissibility of a donation, they can log into the electronic platform – which is linked with the tax inspectorate – and can get an answer in about 2 minutes. The search result is colour-coded, i.e., no colour means the donation is acceptable, yellow means the answer to the request is pending/ awaited or that the treasurer did not send a request to the STI, whereas red signals that the donation is impermissible. such as the State Tax inspectorate, the register of legal entities and banks. In addition to the State Tax Inspectorate, the platform has an interface with the register of legal entities and banking institutions. The CEC uses these interfaces in undertaking compliance checks.

- In **Canada**, privacy issues prohibit Elections Canada from accessing information held by other governmental agencies and there is no national identification number that can be used for determining citizenship for purposes of campaign donations. This presents challenges for verification of donor permissibility based on nationality. Company donations are also prohibited in Canada and there have been concerns about circumvention of this prohibition.

One technique used to monitor possible circumvention is through address verification. Fake donor addresses can be identified using Google API (<https://developers.google.com/google-ads/api/docs/start>). This service also identifies the nature of the address, e.g., residential or business. A business or a fake address serves as a red flag for the oversight body.

Some countries may obtain access to information about donors held by other governmental organisations but only after obtaining a court order. This is the situation in **Georgia** where the oversight institution has automatic access to some basic donor information (e.g. their national identification number and address) but must seek a court order to have access to other financial information that could shed light on the permissibility of the donation (e.g. bank accounts, tax declaration, status as a recipient of governmental assistance).

In addition to data protection issues, the availability of Informational Technology plays an important role in supporting automated systems for confirming permissibility of donations. Such systems require considered thought to get the design and scoping right. They also require time for development and proper testing. And, of course, they require adequate staff and financial resources to produce, maintain and update. The benefits of such systems are manifestly clear – they can provide a reliable and efficient way to ensure compliance with donation and other requirements as well as serving as the means to ensure transparency of political finance.

**Estonia** has developed an innovative and user-friendly system for reporting and disclosing information related to donors and donations, i.e. name, date of birth, donation amount and date of donation. The IT system relies entirely on OpenSource Software to disclose financial information contained in the reports submitted by electoral contestants and uses the civil register for conducting permissibility checks of donors. However, in the interest of personal privacy, while the ERJK, the oversight agency, requests donors' personal identification numbers, this information is withheld from the public website. To do so, the database operates through a two-stage approach: electoral contestants use an online reporting portal to submit their reports, then the information is processed and published on the public website of the ERJK.