TOSSD

Total Official Support for Sustainable Development

Anonymisation of TOSSD data in specific crises

TOSSD Task Force Issues Paper[1] - Agenda item 3
17th meeting of the International TOSSD Task Force
11-13 July 2022

Background

1. At the Task Force meeting in April 2022, the Secretariat explained the actions taken in mid-2021 to temporarily remove from the TOSSD website any reference to names, titles and descriptions of partners in Afghanistan for all providers.[2] This decision was taken as a temporary measure, under exceptional circumstances in order to protect lives. It was based on paragraph 75 of the Reporting Instructions which provides for an exception to activity-level reporting on TOSSD "to protect the lives or safety of people receiving the support or implementing the activities (e.g. in the field of human rights or in the context of violent conflicts)". The same action was taken earlier this year in the case of Ukraine, for the reporters who had made an explicit request to this effect[3].

2. The Task Force discussed the extent to which information on channels of delivery and other TOSSD data items can present security risks, and in which circumstances this information might be removed from the TOSSD data visualisation tool. Anonymisation of data was seen as a challenge since the aim of TOSSD is to increase transparency of official support for sustainable development, by providing data in a manner that is as disaggregated as possible. The Secretariat stressed that anonymising data too early in the process (e.g. aggregation by the reporter) might impact data quality assurance. In addition, it was clarified that removing information from the TOSSD data visualisation tool does not mean erasing it from the Secretariat's internal databases.

3. The Task Force requested the Secretariat to develop guidelines for the reporters on data anonymisation in specific crises, seeking balance between the pursuit of transparency inherent to TOSSD and the safety of implementing partners and beneficiaries. This paper presents the proposed guidelines for discussion at the Task Force meeting on 11-13 July 2022.

[1] Drafted by the TOSSD Task Force Secretariat.

[2] In line with the anonymisation of data in the CRS online database, the following fields were emptied from the downloadable files in www.TOSSD.online: Channel of delivery, Channel name (and other channel-related fields generated by the Secretariat such as the parent channel code and name in English and French), Project title, Project description, External link.

[3] Australia, Canada, France, Ireland, Japan, Korea, Netherlands, New Zealand, Norway, Poland, Sweden, United Kingdom and United States.

Data anonymisation guidelines to protect implementing partners

4. In the event of heightened security risks due to exceptional events (e.g. Afghanistan in August 2021), TOSSD reporters may feel the need to protect the identities of the recipients and implementing partners of their support.[4]

5. The anonymisation of data aims to prevent the identification of individuals or organisations for which individuals work for.[5] In the event of data anonymisation, the Task Force Secretariat will maintain the original granular data as reported by providers in its internal databases (i.e. databases only accessible to the Secretariat and not made available to the public), so that at some point in time, and once agreed with reporters, the anonymisation process can be reversed.

6. **The following steps provide guidelines on the course of action by reporters and the Secretariat:**

a) Request*:* A reporter should address a request to the Secretariat that prompt action must be taken to temporarily remove from the TOSSD website any potentially high-risk data included in its reporting. This request should specify the TOSSD fields that should be emptied [by default: Channel of delivery, Channel name, Project title, Project description, External link], as well as the transactions concerned (all transactions for a specified recipient and/or other specific transactions identified through their TOSSD identification number).

b) Information: The Secretariat will inform all TOSSD reporters of the heightened security risks and the steps it was requested to take to anonymise the TOSSD data of certain reporters. It will invite other reporters to indicate if they wish the same treatment for their data.

c) Action - anonymisation: The Secretariat will promptly anonymise TOSSD data as requested by reporters under steps a) and b)[6], entirely emptying the fields specified for the identified TOSSD transactions in www.TOSSD.online[7].

d) Review – reverse anonymisation: The removal of sensitive data contained in individual TOSSD activities must be seen as a temporary measure and the Secretariat will invite reporters to review the situation within a reasonable period, e.g. 6 months, to assess whether the data can be disclosed in a fully transparent manner again. If reporters consider transparent data still pose a risk to development partners, the full disclosure of data should be reviewed at regular intervals (e.g. every 6 months), until a time when reporters agree, the data may be published in a fully transparent manner again.

7. It is also proposed to amend the Reporting Instructions as shown in the Annex, to clarify the treatment of confidential data in TOSSD.

Issues for discussion

- **Do Task Force members have comments on the guidelines proposed in paragraph 6 on the course of action by reporters and the Secretariat on data anonymisation in specific crises (including on the TOSSD fields to be emptied by default)?**
- **Do Task Force members agree with the proposed amendments to the Reporting Instructions shown in Annex?**

[4] Noting that it is not intended that the TOSSD database should include personal data, and reporters are discouraged from including personal data in their submissions.

[5] High-risk data in the TOSSD context may also include geographical areas or locations and any descriptive information on individual activities.

[6] In addition, requests addressed to the OECD to anonymise CRS data will be automatically replicated in TOSSD.

[7] The Secretariat cannot be responsible for any detailed data that may have previously been downloaded by users from www.TOSSD.online before the anonymisation process.

Annex. Proposed amendments to the Reporting Instructions to clarify the treatment of confidential data in TOSSD

There are three paragraphs in the Reporting Instructions that deal with the treatment of confidential data in TOSSD, and the possibility offered to reporters to aggregate data and/or empty some TOSSD fields. The amendments proposed below aim to clarify the applicability of these two options, also in light with the data anonymisation guidelines proposed in this paper, keeping in mind the transparency objective which is at the heart of the TOSSD framework.

1.2.2 ACTIVITY-LEVEL REPORTING

Paragraph 24 - All TOSSD resource flows are reportable at the activity level. The term “activity” covers various types of operations, ranging from budget support to project-type interventions, investments and technical co-operation activities. In certain cases some aggregation is permitted to limit the reporting burden and number of records. (See section 4.2.)

Paragraph 25. All TOSSD data will be made publicly available, also at activity level. Any information linked to TOSSD activities subject to commercial confidentiality regimes (e.g. company names in the case of private sector instruments) should be filtered out upstream by the data providers.

[…]

4.2 REPORTING FORMAT AND OVERVIEW OF ITEMS COVERED

Paragraph 75. Data on TOSSD resource flows (including private finance mobilised through official interventions) are reported using a single file format. For transparency purposes, data are reportable at the activity level, although not all data fields of the TOSSD reporting format are necessarily filled for all types of financial instruments (see section 1.2.2). Anonymising data too early in the process might however impact data quality assurance, and when there is~~aggregation is warranted~~ a need to protect the lives or safety of people receiving the support or implementing the activities (e.g. in the field of human rights or in the context of violent conflicts), reporters are invited to refer to the ~~.~~Secretariat’s guidelines on data anonymisation. ~~Thus, a~~A certain level of aggregation in the information provided is also possible,~~. F~~ for example~~, aggregation is warranted to protect the lives or safety of people receiving the support or implementing the activities (e.g. in the field of human rights or in the context of violent conflicts). Another example is~~ in the case of contracts of individual experts involving many small-size transactions.

[…]