MINISTRY OF THE INTERIOR
OF THE CZECH REPUBLIC

AWARENESS RAISING FOR THE NPO SECTOR REGARDING THE FIGHT AGAINST TERRORISM FINANCING

2020

EXECUTIVE SUMMARY

Some non-profit organizations (NPOs)[1] or entities pretending to be NPOs can be abused for the purposes of terrorism financing (TF). TF can occur **with, but also without, the knowledge** of an NPO, and therefore due attention needs to be paid to this area. **TF is understood in its broader sense – that is including both material and non-material support of terrorist entities**, which, in effect, also broadens the area of risks that require appropriate attention.

The methods of abusing NPOs for TF can have various forms and can be **deliberate** as well as **inadvertent**, or **coercive**. Such methods may include, in particular, the following:

- affiliation of an NPO to a terrorist entity;
- abuse of the reputation or achievements of an NPO;
- creation of a fictitious NPO;
- the take-over of an NPO and its subsequent abuse, including abuse of its good name, in order to support terrorism;
- financial benefit from the activities of an NPO;
- and abuse of the NPO's facilities (e.g. for radicalization).

The risk associated with NPO abuse can be **mitigated**, inter alia, using the following methods:

- introduction of internal rules of operation;
- demonstrable reporting / record keeping and rigorous control of the use of funds;
- cooperation within the NPO sector;
- consistent use of sanction lists;
- use of secure payment channels;
- and screening of donors, staff, suppliers, and beneficiaries.

NPO abuse might be **prevented** or **detected**, inter alia, using the following methods:

- checking relevant persons against sanction lists;
- consistent setting of internal rules, their rigorous enforcement, and self-regulation;
- internal and external audits;
- cooperation within the NPO sector;
- and using up-to-date and complete information from the public, open sources, dedicated tools and/or databases, from competent authorities, or from various reports and evaluations.

[1] The Financial Action Task Force uses the term "non-profit organisations" or "NPOs", instead of "NGOs". For further information on how NPOs are understood in this framework, please see Footnote 2.

Should you suspect activities related to the financing and support of terrorism, please contact the Police of the Czech Republic or the Financial Analytical Unit.

INTRODUCTION

This document was created within the framework of a working group dedicated to the risks of abuse of non-governmental non-profit organizations (NPOs)[2], coordinated by the Ministry of the Interior, as part of the National Risk Assessment of Money Laundering and Terrorist Financing process in the Czech Republic. Representatives of the Ministry of the Interior, the Ministry of Finance, the Ministry of Foreign Affairs, the Office of the Government, the Financial Analytical Unit, the Police of the Czech Republic, and the General Financial Directorate participated in its creation. Representatives from the Ministry of Justice, the Ministry of Culture, and other authorities also had the opportunity to participate. The document is based on information acquired from practical experience, from materials of the Financial Action Task Force (FATF), and from consultations within the Czech NPO sector.

In the Czech context, NPOs play an important part in many areas, such as the building of civil society, provision of humanitarian and development aid, social services administration, development of advocacy and interest activities, or other public welfare activities. However, some NPOs, or entities pretending to be NPOs, can be abused for the purposes of money laundering schemes (and related criminal activities) and / or TF. This document, therefore, deals with the risk of abuse of NPOs for the purposes of TF and refers to several model cases. Although these cases **may not be currently common in the Czech Republic, considering their severity should they occur, it is necessary to pay due attention to their prevention**. Especially, since such an **abuse can take place without any actual knowledge, deliberate cooperation, or fault of the NPO representatives, employees, and collaborators. Thus, in this text, TF is understood in its broader sense – that is including material and non-material support of terrorist entities**[3].

This material is not intended to demonize or in any way undermine the legitimate and meritorious activities of the NPO sector – it aims to provide the NPOs with sufficient information and a helping hand in preventing TF (since they may encounter and / or be exposed to TF), explain the risks to the Czech or Czech-based NPOs, identify vulnerabilities, and thus help to effectively mitigate the risks of TF. The aim of this document is to focus on the prevention of NPO abuse and the detection of risks associated with TF. Another aim of this document is to serve as a basis for the introduction of good practices amongst NPOs and thus to reduce their vulnerability in relation to TF in areas where this is possible. This document will also be used as a basis for training NPOs in preventing terrorist financing and will be distributed to national authorities that provide grants or other support to NPOs.

[2] In line with the explanation of FATF Recommendation 8 (http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html), non-government non-profit organisations are understood according to a functional definition, i.e. as entities (which in the Czech context are usually legal entities) that collect or distribute funds for charitable, religious, cultural, educational, social or other purposes, or for other activities in the public interest.

[3] In the Czech context, these are criminal offenses of Terrorism Financing and Support and Promotion of Terrorism, which are described in Sections 312d and 312e of Act No. 40/2009 Coll., The Criminal Code.

HOW TO USE THIS DOCUMENT IN PRACTICE?

As mentioned above, the aim of this document is to provide NPOs with basic insight into the issue of NPO abuse for the purposes of financing and supporting terrorism, to acquaint them with the basic methods of such abuse, and to show examples of good practices. The text was conceived comprehensively, with regard to a wide range of NPOs. Therefore, many NPOs may not necessarily be at risk in all of the areas mentioned, especially if they are not (or are only marginally) involved in relevant activities. In addition, many NPOs have already established good practices in mitigating TF-related risks. It is important to mention that this document follows and complements the public version of the document "The Risk of an NPO abuse for the purposes of TF and money laundering," in which the list of risk indicators in this area is discussed in detail.

FACTORS INCREASING THE RISK OF AN NPO ABUSE

This text, just as the abovementioned document "The Risk of an NPO abuse for the purposes of TF and money laundering," understands that some of the risk factors and indicators of TF are also the determining features of some NPO activities (such as fundraising or presence in a specific geographical area), which makes them inextricably linked to specific NPOs and their missions. However, it is important to keep in mind that these risk factors, or their possible combinations, do not in themselves automatically indicate an abuse of NPOs. It is therefore always necessary to assess the specific situation and context. However, NPOs should be aware of these potential risk factors and should actively mitigate them through appropriate preventive measures, with this text serving as a helpful guide in the process.

Generally speaking, NPOs more at risk of abuse for terrorist financing are those that:

- **operate in conflict zones;**
- **operate in areas that are also targeted by terrorist organizations;**
- **do not conduct their activities in a transparent manner, their management and personnel structure or financing are not transparent either, and they do not have functional control mechanisms in place;**
- **do not fulfil their statutory obligations;**
- **do not inform the public or supervising authorities about their activities;**
- **do not communicate with the public authorities;**
- **and handle large amounts of funds, mostly in cash.**

However, the possibility of abuse of NPOs that carry out activities only in the Czech Republic, do not handle cash (or only to a minimal extent), and do not own any (or only negligible) assets, cannot be neglected. Even in such cases, NPOs (e.g. their facilities) can be abused for the purposes of radicalization and recruitment of foreign terrorist fighters. The risk of their abuse may increase due to the lack of the following two key factors:

1. **Effective risk management** of the risks to which the NPOs might get exposed – that is whether the NPO not only detects, but also effectively manages its risks, and thus prevents them.

2. **NPO Transparency** – it is important that the activities, administration, management and personnel structure, and funding are sufficiently transparent. This requires, in particular, to

have established demonstrable reporting / record keeping, functional control mechanisms, fulfilment of statutory obligations, and regular publication of true and complete information about the activities vis-a-vis the public and public authorities.

It should be added that according to available information, most Czech NPOs which operate in conflict zones already show sufficient awareness of the risks related to TF and have quite robust risk management systems. Rigorous control by international and state donors (e.g. EU and US grant schemes, etc.) also has a positive influence on mitigating the risks, namely in big NPOs working in multiple states. Similarly, it is the efforts of the NPOs themselves that help manage the risks – namely the transparent functioning of the organizations themselves, including their management and personnel structures. Thus, it is likely that the actual vulnerability of this type of NPOs is rather low.

FORMS OF NPO ABUSE

In general summary, the abuse of an NPO or its status can happen in the following manners:

1. **Deliberate abuse of NPO resources** – an NPO, or its staff member, abuses the NPO's resources – financial or other – in order to directly support a terrorist entity or its infrastructure; the resources may also be laundered through the NPO. The NPO's training or education programmes can also be abused.

Note - This example, as well as the examples below, are all fictitious and serve as an illustration of the possible ways NPOs can be abused.

An NPO employee sympathizes with a terrorist entity and knowingly provides its members with financial or material assistance from the resources of the NPO s/he works for. Alternatively, s/he facilitates, for example, the use of the communal spaces and technical facilities of this NPO to recruit new members of a terrorist group.

2. **Inadvertent abuse of NPO funds and outputs** – NPO assistance and/or the infrastructure built by NPOs (hospitals, schools, energy and water sources, etc.) are abused by a terrorist entity without the NPO's knowledge. NPO training or education programmes can be abused as well. This category can also include theft or embezzlement of NPO funds.

   According to Czech criminal law, those cases in which the abuse is not a result of deliberate actions of NPO staff, will not usually be considered a criminal offense, as criminal offenses related to terrorism require intention. Nevertheless, insufficiently prudent behaviour of the NPO staff can still have serious consequences.

An NPO helps to build a local school. However, the school premises can also be abused by a terrorist organization for radicalization and training.

An NPO develops a programme to improve agriculture in a developing country (e.g. by building drinking water wells, supplying ploughing tools, fertilizers, etc.). The program is a success and further funding and long-term support are needed to maintain its continuity. A terrorist organization operating in the area is aware that by providing social and other securities, it might win over at least a part of the population. In order to be able to sway the activities in the area to its advantage, its member or a supporter gets themselves hired as a coordinator or a collaborator for the given programme and,

thanks to the position s/he now holds, begins to spread the ideas of the terrorist organization among the population.

3. **Coerced abuse of NPO funds and outputs** – especially in areas with an ongoing conflict. Protection racket or sharing parts of the outputs are required of the NPO to get access to the area. It can also create a conflict between the fundamental principles of assistance, namely in the case of the provision of emergency health care.

An NPO wants to distribute food aid in an area with high malnutrition, which is located on the border of several hostile tribes. Negotiated consent to have safe access to the area is either directly conditioned by the inclusion of pre-selected recipients of assistance, or, during distribution, under threat of physical violence, the NPO is forced to hand over material assistance and possible cash in exchange for safe departure.

The FATF report on the risks of abuse of the non-profit sector for terrorist purposes[4] states that abuse may also occur at **various stages of the NPO work cycle**:

1. **Collection of resources** – this can be any activity undertaken by an NPO to acquire resources, either directly or through third parties (e.g. corporate volunteering).
2. **Retention of resources** – refers to the storage or maintenance of resources by an NPO. Retention includes activities ranging from the maintenance of funds within bank accounts to the management of property or facilities.
3. **Transfer of resources** – this can occur in multiple instances during NPO operations and refers to any point in which the NPO's resources are transferred between different actors.
4. **Expenditure of resources** – refers to any point in which the NPO's resources are exchanged for goods or services.
5. **Delivery of programs** – refers to the point in which an NPO is carrying out programme activities. This could include activities such as the distribution of aid, the provision of medical treatment, holding fundraising events, or hosting guest speakers.

BASIC METHODS OF NPO ABUSE

1. Affiliation of an NPO to a terrorist entity

An NPO supports a terrorist entity, provides it with information, is interlinked with it via its staff, legitimizes its activities, provides cover-ups, etc. It can also be a result of inadvertent affiliation, as the terrorist entity might present itself as a suitable partner in a conflict zone.

An NPO operates in an area, where it is not possible to earn the trust and contacts that are needed in order to fulfil its mission without having a local intermediary. However, due to imperfect, or non-existent, verification when selecting such an intermediary, the NPO unknowingly hires a person who sympathizes with a terrorist entity. This person will then use their position not only to divert parts of the aid, but also to promote the ideology of the terrorist group under the auspices of the NPO.

[4] https://www.fatf-gafi.org/documents/documents/risk-terrorist-abuse-non-profits.html

2. Abuse of the reputation or results of an NPO

A terrorist entity takes ownership of the success of an NPO and abuses it for recruitment or for gathering support from locals, or it pretends that it represents the NPO locally, while "collecting" funds for it. Abuse of programmes is also possible with the legitimate activities of NPOs being manipulated to support terrorism.

A terrorist organization knows that an NPO has been regularly active in an area currently controlled by this terrorist organization, and that the NPO's assistance has been appreciated by the local population. The organization, therefore, pretends to raise funds, which should allegedly enable this NPO to keep carrying out its activities, for this NPO. In reality, however, the finances were never intended for said NPO, but for the terrorist organization and its activities.

3. A fictitious NPO

A terrorist entity founds an NPO in order to get funds or to cover its real activities.

A terrorist organization needs to legalize proceeds gained through criminal activities and, at the same time, wants to gain access to potential new members. Under the guise of providing humanitarian aid, it establishes an NPO, the purpose of which, however, is to launder the proceeds of criminal activity and cover the organization's real agenda.

4. An NPO take-over and its subsequent abuse for the support of a terrorist entity

Abuse of the good name and history of an NPO. This can manifest e.g. as a personnel take-over based on a membership principle – a larger number of new members sign up and they, in the voting procedures, succeed in diverting the course of the NPO's activities; this can also manifest as taking over social media profiles that are managed by a particular NPO and their subsequent abuse.

An NPO providing assistance in a risk area has been successful with its activities and has earned a good reputation thanks to its work; owing to this, it has access to the population and local administration. However, this access would also be useful to a terrorist entity, which would thus gain both access and information useful for the dissemination of its agenda. The terrorist organization thus starts to gradually infiltrate its members into the NPO, with these members gaining voting and decision-making rights; over time, they will achieve membership prevalence. An already established organization with a good reputation can suddenly end up in the hands of a terrorist organization that will abuse the acquired platform for its agenda.

5. Financial benefit from NPO activities

This can be achieved by a direct diversion of NPO funds for TF purposes, caused by an unreliable employee who provides part of the funds to a terrorist entity, by a direct collection of funds from an NPO as a fee for enabling activities in the area controlled by a terrorist entity, or via local NPO suppliers who are connected to a terrorist entity, or have to pay taxes, fees, or other charges (e.g. protection racket) to such an entity.

An NPO provides assistance in a territory that is otherwise controlled by a terrorist organization. As the local civilian population suffers from the consequences of the conflict, assistance needs to be provided on the ground. However, the terrorist organization denies access to the village and provision

of assistance unless provided with protection racket in the form of bribes or portions of the humanitarian aid intended for the local population.

There is also evidence from abroad that a direct diversion of funds can take place when an NPO sends funds intended for a conflict zone via a non-cash transfer to the nearest third country. There, however, the NPO has to rely on cash withdrawals (and transfers) by a co-worker / contractor who abuses the situation and embezzles part of the funds for TF purposes.

6. Abuse of an NPO's facilities and recruitment support

Abuse of NPO premises, equipment, finances, or activities takes place in order to provide a base for recruitment for terrorism, meetings of terrorist entities, or preparation of materials propagating terrorist acts. This method may also apply to NPOs operating exclusively in the Czech Republic.

An NPO decides, in order to decrease its rent costs, to share its premises and equipment with another NPO or a group of people. However, this NPO or group of people support terrorism with their activities, e.g. by using common areas for indoctrination, preparation of explosives, or use the office equipment for printing and distribution of leaflets with propaganda, etc.

PREVENTION AND GOOD PRACTICE BASICS IN THE NPO SECTOR

Since NPOs cooperate with donors, beneficiaries, intermediaries, and other NPOs, it is in their interest not only to screen all the links in the chain, but also to be screenable themselves. This document, in conjunction with the above-mentioned text "The Risk of an NPO abuse for the purposes of terrorism financing and money laundering," which discusses in detail the individual risk indicator categories and shows how to screen and manage them, can serve as a guide in these processes.

The fundamentals of effective prevention are the development of and adherence to preventive measures to limit the risk of abuse for the purposes of financing and supporting terrorism. The introduction of some of these preventive measures may be a one-off undertaking, but in many cases, there is a need for a continuous evaluation and adjustment of these mechanisms, reflective of the current development of the international situation, NPO activities, but also domestic and foreign legislation. Since this is an area common to all NPOs, there are mechanisms in place embedded in international cooperation, where it is possible to use existing services and programmes. Similarly, there are established mechanisms at the national level to facilitate these preventive activities of NPOs.

As mentioned above, NPOs that receive funding from foreign donors are often well-prepared due to the rules that these donors require the recipients to follow[5]. There are also several guidance materials that shed light not only on the issue as such, but also present the NPOs with practical examples[6] of how to develop and consolidate good practices[7]. In the Czech Republic, basic information for NPOs

[5] More information on such rules can be found e.g. on the website of the British Charity Commission https://www.gov.uk/government/organisations/charity-commission, or USAID https://www.usaid.gov/forms/aid-500-13.
[6] Also covered e.g. by the FAU reports (https://www.financnianalytickyurad.cz/zpravy-o-cinnosti.html).
[7] Worth mentioning is the work of FATF, namely "Risk of terrorist abuse in non-profit organisations"

can be found on the website of the Financial Analytical Unit (FAU)[8]. One of the fundamental rules is to publicly distance activities and missions from any activity related to terrorism, e.g. in the founding documents or other materials associated with the description of the NPO mission.

If an NPO comes across any suspicious activity or suspicious persons while carrying out its activities or during its own screening, it should report them to the competent authorities at the national level (as specified below).

Introduction of internal rules

One of the basic building blocks of NPO activities is transparency, both their own and of the entities with which they are associated. Such transparency also includes regular and functional internal assessment and auditing. The basic rules for the functioning of an NPO should therefore include:

- a clearly defined mandate and mission, including that of individual programmes;
- a clear distancing from any support of terrorism or other criminal activity (e.g. in the statute, mission description, etc.);
- transparent management of finances; demonstrable reporting / record keeping, a transparent bank account, limiting the use of cash to the unavoidable minimum, strict control of the distribution and withdrawal of funds;
- strict application of the "four eyes" rule[9] (which will reduce, for example, the risk of fraudulent diversion of funds);
- worked out and regularly assessed risks;
- regular audits; ex-post assessment of the use of aid;
- checklists for individual steps within the working process, which will also facilitate work on other projects (e.g. guidelines for public procurements); application of the "know your client" principle (applies to donors, contractors, collaborators, intermediaries, and final beneficiaries);
- and regular publication of true and complete information about the NPO's activities.

Cooperation in the NPO sector

Within the NPO sector, active cooperation is taking place at both the national and international levels. Such cooperation helps individual NPOs in a number of areas, and is an important and positive element in the functioning of the NPO community.

The Government Council for Non-Governmental Non-Profit Organisations (RVNNO)[10] (at the Office of the Government of the Czech Republic) operates at the national level. It is a permanent consultative, initiative, and coordination body of the Government of the Czech Republic in the area of

http://www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html or "Best Practices on Combating the Abuse of Non-Profit Organisations" https://www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-combating-abuse-npo.html.

[8] https://www.financnianalytickyurad.cz/informace-pro-nestatni-neziskove-organizace.html

[9] That is at least two representatives acting together when representing an organisation.

[10] https://www.vlada.cz/cz/ppov/rnno/zakladni-informace-767/

non-governmental non-profit organisations. The Council collates, discusses and, through its chair, submits materials to the government relating to NPOs and the creation of a suitable environment for their existence and activities. It also cooperates with individual ministries and other government authorities in the area of the NPO sector, and ensures the availability and publication of information on NPOs and state policy measures related to them.

Furthermore, the **Czech Forum for Development Cooperation** (FoRS)[11] operating in the Czech Republic serves as a platform for Czech NPOs and other non-profit entities that deal with development cooperation, development education, and humanitarian aid.

The **Donors' Forum**[12] is another important Czech umbrella organization, which helps with the long-term shaping of the donor environment in the Czech Republic.

CONCORD[13] (European NGO Confederation for Relief and Development) operates at the European level and serves as a link amongst EU institutions and NPOs in the area of development cooperation. It aims at strengthening the impact of the work done by the European development NPOs in the context of European development policies and institutions.

Alliance 2015[14] is a strategic international network of several NPOs working in the area of humanitarian and development aid. Among others, it helps with sharing the experience and know-how in order to strengthen the positive impact of the activities of its members. Another entity, the **International NGO Safety Organization**[15], provides security support to humanitarian workers in high-risk areas.

Working with sanction lists

International sanctions are one of the "soft" tools that can be used to exert pressure on specific actors without the use of force. The current sanction regimes are targeted, which means that they are applied only to a defined (most often listed in an annex) list of persons, entities, services, goods, or technologies. An exemption for humanitarian purposes may be granted so that civilians do not unduly suffer from sanctions. Respective NPOs can contact the FAU, which is the national coordinator for the implementation of international sanctions, regarding the scope of such exemptions and with exemption requests.

The Czech Republic is bound by the international UN and EU sanction lists[16].

A basic tool for screening beneficiaries is the EU Sanctions Map[17], which lists all the persons and entities subject to international EU sanctions. The map, however, is only a source of information, while the binding wording of the relevant sanctions regime, including the sanctions lists, is available in the database of EU law – EUR-Lex (the sanctions map contains links to it).

[11] http://www.fors.cz
[12] https://www.donorsforum.cz/
[13] https://concordeurope.org
[14] https://www.alliance2015.org
[15] More information can be found here: https://www.ngosafety.org.
[16] More information can be found here: https://www.consilium.europa.eu/cs/policies/fight-against-terrorism/terrorist-list/.
[17] The map is available at www.sanctionsmap.eu.

Likewise, the UN maintains sanctions lists of persons and entities subject to restrictive measures by the Security Council. Both a consolidated list[18] and further supporting information[19] regarding the sanctions regimes can be found online, including information on how to apply for an exemption. The FAU informs about changes in the UN sanctions list on its website and you can subscribe on the FAU website to receive these updates by e-mail. The website also contains general as well as specific information on the implementation of international sanctions[20].

The list of so-called internal terrorists contained in Government Decree No. 210/2008 Coll., as amended, must also be added to these lists. The legal framework for the application of international sanctions is set out in Act No. 69/2006 Coll., On the implementation of international sanctions (hereinafter referred to as the Sanctions Act). Considering the risks posed by TF, it is appropriate to recall namely the prohibition to make available, directly or indirectly, any assets to persons subject to sanctions, who are listed on the relevant lists, which is an obligation stemming from the Sanctions Act, as well as the relevant and directly effective EU sanctions regulations.

Most states have their national sanctions lists, which either adopt sanctions to the extent adopted by the UN or add their own measures or expand the lists of sanctioned persons and entities beyond the UN framework. The best-known example is the USA's list at the OFAC – Office of Foreign Assets Control (at the US Department of the Treasury)[21]. These lists are not binding (enforceable) in the Czech Republic, but the donors (states / organizations) may still require compliance with them. The USA also applies so-called extraterritoriality to its sanctions, which means that it can penalize persons / entities for non-compliance, even in territories outside of its jurisdiction.

Due to the existence of different sanctions lists, which are frequently updated, commercial services are available offering a consolidated search of multiple sanctions lists at once. The disadvantage, especially for smaller NPOs, may be an increased financial burden. However, finding a match to a donor, beneficiary, intermediary, collaborator, or beneficial owner with the data on these national counter-terrorism lists, may indicate a suspicion of TF.

Use of secure payment channels

One of the basic tools for risk mitigation, including the already mentioned demonstrable reporting / record keeping, is using secure payment channels to transfer funds. Using transparent bank accounts and non-cash payments as much as possible is preferable. Nonetheless, considering the nature of assistance in a range of conflict or remote areas, it is not always possible to use secure payment channels. The alternatives are, among others, non-cash transfers of funds (i.e. from a bank account to a bank account) to the nearest country, or remittances (via a payment service provider), and subsequent cash withdrawals and cash transfers[22]. In cases where it is not possible to directly arrange a physical transfer of money, it is always necessary to track the cash flow all the way to the recipient, as well as the subsequent use of such cash. Special care and thorough verification of all the individuals or entities involved needs to be maintained. It is important to always ensure that records of

[18] https://www.un.org/securitycouncil/content/un-sc-consolidated-list
[19] For example here: https://www.un.org/securitycouncil/sanctions/1267.
[20] More information can be found here: https://www.financnianalytickyurad.cz/mezinarodni-sankce.html.
[21] https://www.treasury.gov/resource-center/sanctions/pages/default.aspx
[22] It should also be noted that in the majority of countries in the world, over-the-limit cross-border cash transfers are subject to a reporting obligation.

transactions within specific transaction channels are kept, including the identification of the final recipient. In general, the use of cryptocurrencies can also be considered risky.

Screening of donors

The receipt of subsidies and finances, thanks to which the activities and missions of the NPOs can be carried out, is key for the NPO. In addition to big donors, often linked to states or international institutions, it is also possible to make use of private or smaller foundations and donations from individuals. Particularly in such cases, it is necessary to properly screen both the donor and the origin of the funds, as they might possibly come from criminal activity or from an entity linked to terrorist or other criminal elements. If the donors themselves do not have any control systems, this in itself can constitute a risk. This also applies to some government actors, if the country is known to support terrorism. Generally speaking, long-term framework agreements[23] and funding from large donors with a good reputation, a proven track record, and a system of operation, constitute a lower risk.

Screening of collaborators, contractors, and suppliers

When providing financial and material assistance, especially in conflict zones, or areas that are cut off or otherwise politically isolated, it is often necessary – for both security and other reasons – to make use of the help and services of local organizations or individuals. In many cases, it is also necessary to work with cash, which can make it impossible to monitor a transparent cash flow. It is therefore crucial to have complete and up-to-date identification data available, so that the NPO could properly and continuously screen all the collaborators, both inside and outside their own organization. It may happen that there may be an individual, even in a completely legitimate local organization, who, without the knowledge of any of the parties, can abuse the aid provided for terrorist purposes. Due to the frequent fluctuation of people in the non-profit sector, a strict control in this chapter of the NPO activities is very important. For basic and formal screening of collaborators and suppliers, it is possible to use the EU sanctions map, the consolidated UN sanctions list, or information provided by OFAC. Electronic databases[24] or commercial tools can be used for further screening of cooperating organizations. However, on-site checks, including random rolling inspections, are likely to be needed in a number of areas. This equally applies to the screening of the core NPO employees, including those at the organization's headquarters.

Screening of beneficiaries

Generally speaking, it is necessary to screen aid and assistance beneficiaries when providing said aid and assistance. This is especially true if the assistance is provided in conflict and crisis zones, where entire communities might be under the control of a terrorist organization. It may happen that legitimately provided aid is collected by a representative, who promises to pass it on to the relevant beneficiaries, but passes the funds or material to terrorist entities instead. Another example might be

[23] It is a type of contract which is concluded in cases where both parties expect a longer-term cooperation. These agreements then set out, inter alia, the rules that are to be followed by both the parties in the framework of further cooperation and contractual relations, unless agreed otherwise.

[24] E.g. https://iatistandard.org/en/, http://www.d-portal.org/ctrack.html#view=search, or https://devtracker.dfid.gov.uk/.

a situation in which the real recipients are forced to hand over financial or material aid, or parts thereof, to a terrorist entity.

However, the principles of impartiality, neutrality, and non-discrimination[25]must be respected when providing exclusively humanitarian aid, which means that provision of medical treatment to a terrorist cannot be considered TF. In any case, though, both the people involved and the places where assistance is provided need to be screened and the relevant risks must be taken into account at the individual missions[26].

Procedures, which ensure a certain form of control, are considered to be good practice. This is namely the following:

- setting clear and transparent criteria for the selection of beneficiaries;
- vetting the list of beneficiaries[27];
- personal delivery of aid / assistance;
- delivery of aid / assistance by screened intermediaries;
- random on-the-spot checks;
- third-party monitoring;
- periodic review of processes and screening of collaborators;
- ongoing consultations with experts.

METHODS OF ABUSE AND DETECTION OF RISKY COOPERATION

In general, NPOs need to act responsibly both towards themselves and their employees, as well as towards donors and beneficiaries. This responsibility stems not only from the relevant legislation and the obligations resulting from donors' internal rules, but it is also in the interest of maintain the safety and the reputation of individual NPOs, especially should they operate in high-risk areas.

The amendment to Act No. 40/2009 Coll., The Criminal Code, with effect from 1 February 2017, created a new factual basis of the criminal offense of TF pursuant to **Section 312d of the Criminal Code**.

TF is, in fact, another (special) form of criminal cooperation, which otherwise corresponds to enabling or facilitating a criminal offense [Section 24, par. 1, letter c) of the Criminal Code]. The promotion of this form of facilitation to a separate crime stems from the international community's efforts to effectively prevent terrorist attacks. It is based on the idea that denying the terrorists and terrorist groups financial and material resources makes their operating more difficult, including planning and organizing terrorist attacks. Two interconnected acts are thus punishable: firstly, the act of financial or material support in itself, and secondly, the preparation of such financial or material support, i.e. the collection of funds or other resources.

[25] Comp. Section 214, para 2 of TFEU.
[26] That includes also assessing which mission to participate in or whether to stay in certain areas.
[27] Including assessment before the actual distribution that they indeed meet the set criteria.

Financial support has to be understood as the provision of financial resources, i.e. money and its substitutes. Material support then consists of, for example, the provision of weapons, accommodation, premises, food, means of transport, or other resources.

The above-mentioned stipulation lays down the legal responsibilities for NPOs: **they are legally obliged to inform, without delay, the public prosecutor or the police authority, should they learn in a credible manner, of any facts indicating that a crime of TF has been committed pursuant to Section 312d of the Criminal Code**. Should they not do so, they might face a penalty for the failure to report a crime or any of the means of criminal cooperation in relation to the crime of TF according to Section 312d in the form of instructions, assistance, or organization according to Section 368 of the Criminal Code.

Another piece of legislation in this area is Act No. 253/2008 Coll., On selected measures against legitimisation of proceeds of crime and financing of terrorism (hereinafter referred to as the "AML Act") and Act No. 69/2006 Coll., on Carrying Out of International Sanctions (hereinafter referred to as the "Sanctions Act"). **In accordance with these laws, the prevention of money laundering, TF, and national coordination in the application of international sanctions in the Czech Republic falls under the responsibility of the FAU**, which is an independent administrative authority functioning as the financial intelligence unit of the Czech Republic.

If an NPO encounters any conduct or comes across any facts that do not indicate a criminal offense has been committed, but could involve abuse of the financial system, including cash transactions for the purposes of TF, or the involvement of sanctioned persons or property, it should comply with the legal reporting requirements towards the FAU:

1. **A reporting obligation in the sense of Section 18 of the AML Act (i.e. notification of a suspicious trade):** Applies to so-called obliged entities. The obliged entities are listed in Section 2 of the AML Act and include, inter alia, entities that receive or issue cash in amounts equal or higher than EUR 10,000, provided that this value is also used as the final sum of the related payments. Such obliged entities also have to follow other obligations stipulated by the AML Act, such as customer identification (Section 7 et seq. of the AML Act) and customer due diligence process (Section of the 9 AML Act), or suspend the fulfilment of a transaction (Section 20 of the AML Act – security measures against property, which serves or is intended to finance terrorism). The notification of a suspicious transaction, i.e. of the circumstances that could indicate a suspicion of TF, must be submitted to the FAU without undue delay.
2. **Reporting obligation in the sense of Section 10 of the Sanctions Act:** Applies to all natural and legal persons, where a sanctioned property is located[28]. It further applies to situations when the donor, beneficiary, intermediary, collaborators, or any other party to the contractual relationship, or its real owner, is a person on a sanctions list by which the Czech Republic is bound. The notification must be submitted to the FAU without undue delay. Section 11 of the Sanctions Act also regulates situations in which the use of property subject to international sanctions may be restricted.

[28] According to Section 3 letter f) of Act No. 69/2006 Coll., it is property subject to international sanctions, any movable or immovable property owned, held or otherwise controlled by an entity subject to international sanctions, or a person subject to international sanctions, imported from the territory which is a subject to international sanctions, or intended for export to territories subject to international sanctions.

3. **Considering the gravity of the risk of TF**, the FAU also accepts other notifications of circumstances indicating suspicion of TF. Such situations include the match of the donor, beneficiaries, intermediary, collaborators, or other party to the obligation or its beneficial owner with the counter-terrorism lists of other jurisdictions. However, any other circumstances that could indicate a suspicion of TF, regardless of whether there is any involvement of sanctioned persons, also fall into this category. It should be highlighted that sanctions are only applied after allegations of terrorism are confirmed, and that the active terrorists and their supporters are not put on the lists until their actions are known, verified, and subsequently confirmed. The above-mentioned notification made to the FAU may also contribute to such investigations.

It is important to underscore that the information, which is the subject of notification and investigation by the FAU, is bound by strict confidentiality stemming from Section 38 of the AML Act and Section 16 of the Sanctions Act.

At the same time, a notification to the FAU does not in any way affect the notification obligation which concerns anyone[29] in relation to the most serious crimes[30] and must be made to the public prosecutor or the police authority.

The FAU contact details are listed on its website[31]. It is also possible to contact the FAU with questions in cases of ambiguities or a lack of clarity in connection to situations listed in points 1) - 3).

In general, the abuse or attempted misuse of NPOs can be prevented, or possibly detected, inter alia, thanks to the following[32]:

- diligent setting of the internal rules and control as well as regulatory mechanisms;
- internal and external audits;
- cooperation within the NPO sector;
- information from the public;
- information from whistle-blowers;
- open sources (press, social media, TV and radio broadcasting, Internet, etc.);
- relevant information tools and databases;
- information from competent authorities;
- reports and evaluations (e.g. annual reports of relevant organizations or bodies);
- and information from abroad (e.g. thanks to partner organizations).

CONCLUSION

Vulnerabilities in the area of NPO activities need to be assessed through the prism of all available information and adapted to the specific context of a relevant NPO, out of which the information stated above is only a fragment. The aim of this document is not to interfere in any way with the proper functioning of legitimate NPOs, but to provide guidance in order to raise awareness and to identify

[29] However, in the case of NPOs, there is an important exception granted under Section 368, para 3 of the Criminal Code: a person providing assistance to victims of crime does not have the obligation to report the crime of trafficking in human beings and deprivation of personal liberty.
[30] Listed in Section 368 of Act No. 40/2009 Coll., The Criminal Code.
[31] https://www.financnianalytickyurad.cz/
[32] Cit. FATF https://www.fatf-gafi.org/documents/documents/risk-terrorist-abuse-non-profits.html.

risks linked to TF in various parts of an NPO's legitimate working cycle. The aim, therefore, is to enable individual NPOs to assess possible risks in various areas and in individual steps related to their activities, to take measures to gradually reduce these risks, and thus also to reduce the likelihood of being misused for TF purposes.