



**SYSTEM OF INTERNAL PRINCIPLES, PROCEDURES AND
CONTROL MEASURES AIMING TO PREVENT THE
LEGITIMISATION OF PROCEEDS OF CRIME AND FINANCING OF
TERRORISM**

Internal directive for use in companies associated with the SYNOT Group.

Contents

- 1 List of acronyms4
- 2 Definitions of Terms4
- 3 Introduction8
- 4 Customer identification9
 - 4.1 Implementation of identification.....9
 - 4.1.1 Ascertaining identification data 9
 - 4.1.2 Identifying politically exposed persons11
 - 4.1.3 Detection of persons subject to international sanctions12
 - 4.2 Other identification options12
 - 4.2.1 Mediated identification12
 - 4.2.2 Takeover of identification13
- 5 Customer due diligence procedure and determination of the scope of customer due diligence in relation to the risk of legitimisation of proceeds of crime and financing of terrorism.....13
 - 5.1 Obtaining information about the purpose and intended nature of a transaction or business relationship14
 - 5.2 Identification of the ownership and management structure of a customer and its beneficial owner, and the adoption of measures to identify and verify the identity of the beneficial owner.....14
 - Procedures in cases where a customer’s beneficial owner cannot be identified from publicly accessible sources16
 - 5.3 Continuous monitoring of a business relationship, including a review of transactions carried out within the scope of the particular relationship17
 - 5.4 Reviewing sources of funds or other assets to which a transaction or business relationship relates.....17
 - 5.5 Measures taken to establish the origin of assets in the case of a business relationship with a PEP17
 - 5.6 Further information on customer identification and due diligence.....18
- 6 Simplified customer identification and due diligence.....18
- 7 Risk assessment20
 - 7.1 Risk categorisation of types of customers with regard to risk factors26
 - 7.2 Risk categorisation of products and related services which could be abused for ML or FT27
 - 7.3 A detailed demonstrative list of indications of suspicious transactions28
 - 7.3.1 Features that may indicate suspicious transactions28
 - 7.3.2 Features that definitely indicate suspicious transactions28
- 8 Rejected transactions29
- 9 Procedure for access of the competent authorities to stored data29
 - Storage of data29



- 10 Person authorised to manage matters of AML/CFT prevention and to supervise compliance with measures within the scope of the SIP30
- 11 Procedure after ascertaining a suspicious transaction until delivery of notification to the FAO, rules for dealing with a suspicious transaction, and identification of persons who evaluate a suspicious transaction.....30
 - 11.1 Situations where the FAO submits an STR.....30
 - 11.2 Contact details for the Financial Analytical Office31
 - 11.3 Requirements of an STR31
- 12 Measures to prevent hampering or substantial complication of seizing proceeds of crime by immediately carrying out a customer’s order.....33
- 13 Technical and personnel measures ensuring postponement of the fulfilment of a customer’s order and compliance with the information obligation within the stipulated time limit.....34
 - 13.1 Performance of the notification obligation34
 - 13.2 Measures when postponing the fulfilment of a customer’s order34
- 14 Description of additional measures for efficient management of the risk of legitimisation of proceeds of crime and financing of terrorism35
- 15 Confidentiality provisions.....35
- 16 Provisions for ensuring staff training.....36
- 17 Binding force and effect.....36

1 List of acronyms

AML Act	Act 253/2008 Coll., on Selected Measures Against the Legitimation of Proceeds of Crime and Financing of Terrorism, as amended (the Anti-Money Laundering Act)
AML Decree	Decree No. 67/2018 Coll., on Certain Requirements for a System of Internal Principles, Procedures and Control Measures against the Legitimation of Proceeds of Crime and Financing of Terrorism, as amended
AML/CFT prevention	Measures Against Money Laundering / Countering the Financing of Terrorism
ML/FT	Legitimation of proceeds of crime (Money Laundering) / Financing of Terrorism
CNB	Czech National Bank
EEA	European Economic Area
EU	European Union
FAO	Financial Analytical Office
NST	Notification of suspicious transactions
PEP	Politically Exposed Person
SA	Act No. 69/2006 Coll., on the implementation of international sanctions, as amended (the Sanctions Act)
SIP	System of internal principles, procedures and control measures aiming to prevent the legitimation of proceeds of crime and financing of terrorism
IND	Individual
LP	Legal Person

2 Definitions of Terms

Financing terrorism	of	<p>Gathering or providing financial means or other assets in the knowledge that such assets, even if only partially, will be used to commit a criminal act of terror, a terrorist attack, or a criminal offence intending to facilitate such a crime or to support a person or group of persons planning to commit such a criminal offence.</p> <p>Acting with the intention to remunerate or indemnify a person who has committed a criminal act of terror, a terrorist attack, or a criminal offence intended to facilitate such a crime, or to remunerate or indemnify someone in a close relationship to such a person within the meaning of the Criminal Code, or acting with the intention of collecting assets to pay such remuneration or indemnification.</p>
----------------------------	-----------	--

	<p>For the purposes of the AML Act, financing of terrorism also means financing proliferation of weapons of mass destruction, i.e. gathering or providing financial means or other assets in the knowledge that such assets, even if only partially, will be used by a disseminator of weapons of mass destruction, or will be used to support proliferation of such weapons in conflict with the requirements of international law.</p> <p>The fact that such actions have occurred or are to occur, in whole or in part, in the Czech Republic or abroad is not important.</p>
Legitimation of proceeds of crime	<p>Actions performed to conceal the illicit origin of proceeds of crime with the intention of presenting such illicit proceeds as legal income. Such actions include:</p> <ul style="list-style-type: none"> - converting or transferring assets, knowing that such assets are proceeds of crime, for the purpose of concealing or disguising the illicit origin of the assets or assisting a person involved in such activity to avoid the legal consequences of such conduct, - concealing or disguising the true nature, source, location, disposition or movement of assets, or changing ownership rights to such assets in the knowledge that the assets are proceeds of crime, - acquiring, possessing, using or handling assets knowing that they originate from crime, - criminal association or any other type of cooperation serving the purpose of the conduct specified above. <p>The fact that such actions have occurred or are to occur, in whole or in part, in the Czech Republic or abroad is not important.</p>
Non-transparent ownership structure	<p>A situation where a beneficial owner or the ownership and control structure of a customer cannot be determined from:</p> <ul style="list-style-type: none"> - a public register, records of trust funds or records of data on beneficial owners kept by a public authority of the Czech Republic, - a similar register or records another country, - another source or combination of sources which SYNOT reasonably deems to be credible and which give reason to believe that they provide, as a whole, complete and up-to-date information on a beneficial owner and the ownership and control structure of a customer, particularly if issued by a public authority or officially authenticated.
Trade	<p>Any conduct of SYNOT together with another entity, if such conduct is aimed at the disposal of assets of that other entity or at the provision of a service to that other person.</p> <p>If a payment is divided into several instalments, the value of the transaction or payment shall be the sum of these instalments, provided they are related.</p> <p>The concept of trade is twofold. Firstly, it refers to individual/one-off/occasional trade (e.g. the purchase of goods and payment) without establishing a business relationship. Secondly, after the establishment of a business relationship, it refers to individual (partial) transactions of the same or similar type within such a relationship (e.g. money transfer).</p>

Business relationship	A contractual relationship between SYNOT and another entity, the purpose of which is disposal of the assets of that other entity or the provision of services to that other entity if, taking into account all circumstances, it is clear that it will contain repeated transactions.
Suspicious transaction	<p>A transaction made under circumstances that raise suspicion of efforts to legitimise proceeds of crime or suspicion that the transaction is made using funds intended to finance terrorism, or that the transaction is otherwise related to or connected with financing of terrorism, as well as any other fact that could raise such suspicion.</p> <p>Circumstances that raise suspicion include, for instance, anomalies in the behaviour of a customer compared to the customer's usual behaviour or the behaviour of a group of customers of a similar type.</p>
Politically exposed person	<p>a) an individual who holds or has held a significant public position with nationwide or regional importance, in particular positions such as the head of state, prime minister, head of a central organ of state administration or his/her proxy (deputy, assistant secretary), a member of parliament, a member of a steering body of a political party, a leading representative of a municipal authority, a judge of a supreme court, constitutional court or other body of supreme justice against whose decision no remedies may be used (with some exceptions), a member of a bank council of a central bank, a high-ranking officer of armed forces or corps, a member or representative of a member (if the member is a legal entity) of a statutory body of a business corporation controlled by the state, an ambassador or a head of an embassy or an individual who holds or has held a similar position in another country, in an EU body, or in an international organization,</p> <p>b) an individual who is:</p> <ol style="list-style-type: none"> 1) a person in a close relationship to a person specified under letter a), 2) a partner or the beneficial owner of the same legal entity or, as the case may be, a trusteeship fund or other legal organisation without legal personality, as a person listed under letter a), or a person who SYNOT knows to be in any other close business relationship with a person listed under letter a), 3) the beneficial owner of a legal entity or, as the case may be, a trusteeship fund or other legal organisation without legal personality which SYNOT knows to have been created for the benefit of a person listed under letter a).
Identity card	A document issued by a public administrative body which specifies the holder's full name and date of birth, and from which the likeness of the holder or other details enabling identification of the person presenting the document as its authorised holder are apparent.
High-risk countries	High-risk countries in terms of legitimisation of proceeds of crime, financing of terrorism, or spreading of weapons of mass destruction. A list of these countries is determined by the Commission Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, as amended. Further high-risk countries are specified in an Annex, which is part of the SIP.

<p>Beneficial owner</p>	<p>An individual (or several individuals) who has (have) a factual or legal opportunity to exercise, directly or indirectly, a decisive influence within a legal entity, a trust fund or another legal organisation without legal personality. It shall be assumed that when meeting such conditions, the beneficial owner is:</p> <p>a) in the case of a business corporation, an individual</p> <ol style="list-style-type: none"> 1. who alone, or together with persons acting with him/her in concert, holds more than 25% of voting rights in that corporation or owns a share of more than 25% of its registered capital, 2. who alone, or together with persons acting with him/her in concert, controls the entity specified in item 1, 3. who is to receive at least 25% of the profit of this business corporation, or 4. who is a member of a statutory body, a representative of a legal entity within such a body, or in a position similar to that of a member of a statutory body, if he/she is not the beneficial owner or cannot be identified as a person according to points 1–3, <p>b) in the case of a society, a public benefit organisation, an association of unit owners, a church or religious association or other legal entity regulating the position of the church and religious associations in accordance with the applicable law, an individual</p> <ol style="list-style-type: none"> 1. who holds more than 25% of its voting rights, 2. who is to receive at least 25% of the funds it distributes, or 3. who is a member of a statutory body, a representative of a legal entity within such a body or in a position similar to that of a member of a statutory body, if he/she is not the beneficial owner or cannot be identified as a person according to points 1 or 2, <p>c) in the case of a foundation, an institute, an endowment fund, a trust fund or other legal organisation without legal personality, an individual or the beneficial owner of an individual, who is in the position of</p> <ol style="list-style-type: none"> 1. founder, 2. trustee, 3. beneficiary, 4. a person in whose interest the foundation, institution, endowment fund, trust fund or other organisation without legal personality was established, provided that a beneficiary has not been determined, and 5. a person authorised to supervise the management of the fund, institution, endowment fund, trust fund or other legal organisation without legal personality.
<p>Country of origin</p>	<ul style="list-style-type: none"> - in the case of a customer who is an individual, country of origin refers to each country of which the person is a citizen, as well as to any other countries where the person is registered as a temporary resident for more than 1 year or as a permanent resident, if known to SYNOT, - in the case of a customer who is a legal entity, country of origin means the country in which it has its registered office and, at the same time, all countries in which it has a branch.
<p>Gaming licence</p>	<p>Authorisation to operate a game of chance issued by decision of a public authority.</p>

Risk management	Risk management is a set of measures that are used to identify the key risks that SYNOT faces. It also serves to set up the inspection mechanisms available to the company to mitigate these risks. The risks can be both external and internal for the company. The objectives of risk management are to determine the risk profiles of customers, to measure the overall resilience of the company to the risks that it faces, and to plan measures to reduce those risks.
Due diligence	The process of implementing policies and procedures designed to help monitor and evaluate the financial or other risk represented by a customer, i.e. an audit of a particular customer. Due diligence includes, but is not limited to, identification of customers, determination of expected customer behaviour, and/or monitoring of account activity to identify transactions that do not correspond to normal or expected transactions for a particular customer or type of account, and categorisation of customers into individual risk groups.
Due diligence form - individual	A form intended to ensure the necessary identification and other information about a customer, who is an individual, involved in trade or a business relationship. This information subsequently serves to assess the risk level of the customer and to determine his/her risk profile.
Due diligence form - LP	A form intended to ensure the necessary identification and other information about a customer, who is a legal person, involved in trade or a business relationship. This information subsequently serves to assess the risk level of the customer and to determine his/her risk profile.
Due diligence form - LPG	A form intended to ensure the necessary identification and other information about a customer, who is a legal person whose line of business is in the field of gaming, involved in trade or a business relationship. This information subsequently serves to assess the risk level of the customer and to determine his/her risk profile.
KYC process	KYC is an abbreviation meaning “know your customer”. It is the process of identifying a customer together with regular periodic inspections of the customer according to his/her/its risk profile.

3 Introduction

SYNOT is a respected international group of companies operating in more than 20 countries around the world. The group provides work for around 3000 people. The core of the SYNOT Group’s business is the gaming industry and provision of first-rate technologies, gaming content and solutions representing a complete product package for the online and land-based entertainment industry.

The group is also involved in a wide range of other business activities - sales and servicing of luxury BMW vehicles, investment in tourism, media activities, IT technologies and support for start-up projects, modern security services and, last but not least, broad support for sport and the non-profit sector.

Individual companies use international know-how not only in the field of technologies and trade, but also in the area of legislation, finance and marketing. The SYNOT Group operates in Europe and beyond, specifically in Slovakia, the Czech Republic, Spain, Greece, Poland, Latvia, Romania and many other countries of Europe, Africa, Asia, Central America and South America, with plans to expand its activities in the coming years.

4 Customer identification

4.1 Implementation of identification

SYNOT carries out customer identification:

- at the latest when it is clear that the value of a one-off transaction within a company belonging to the SYNOT group exceeds the amount of 3% of the annual turnover of the particular company (each company of the SYNOT group has a set individual limit)
- in all cases, regardless of the above-stated limit, where matters concern:
 - a suspicious transaction;
 - the establishment of a business relationship where it is clear that individual partial transactions within the scope of this business relationship will exceed the value of €20,000;
 - a potential high-risk customer;
 - transactions, which have no apparent economic reason;
 - transactions directed to a country that insufficiently applies or does not at all apply anti-money laundering measures. List of countries that do not apply anti-money laundering measures at all.

If a transaction is divided into several separate instalments, the value of the transaction shall be the sum of these instalments, provided they are related. Clearly related instalments must thus be totalled and considered as a single transaction.

4.1.1 Ascertaining identification data

When identifying a customer who is:

- **an individual:** SYNOT shall ascertain all names and surname; birth registration number or date of birth if a birth registration number has not been allocated; place of birth; sex; domicile or other place of residence; nationality. SYNOT shall record this data and verify it from an identity card (if the card specifies such data), and shall further record the type and number of the identity card, the country or authority that issued the card, and the validity period of the card. At the same time, SYNOT shall make sure that the identity card photo matches the semblance of the holder;
- **an individual (entrepreneur):** SYNOT shall ascertain all names and surname; birth registration number or date of birth if a birth registration number has not been allocated; place of birth; sex; domicile or other place of residence; nationality. SYNOT shall record this data and verify it from an identity card, and shall further record the type and number of the identity card, the country or authority that issued the card, and the validity period of the card. At the same time, SYNOT shall make sure that the identity card photo matches the semblance of the holder. It is also necessary to record the business name, distinguishing description or other designation, the place of business and the identification number of the individual;

- **a legal person:** SYNOT shall ascertain the business name, including a distinguishing description or other designation, registered office and business identification number or a similar number allocated abroad. SYNOT shall record these identification data and verify them against a document of the existence of the legal person, which shall be a valid record from the Commercial Register or other business register. If the customer is a legal person registered in the Czech Commercial Register, SYNOT may either verify the identity by means of a printout of the entry from the Commercial Register submitted by the customer on the portal justice.cz, or download the data directly from this electronic register to identify the customer, or verify the data provided by the customer in a verbal or written communication. If a foreign legal person is involved, SYNOT must be provided with an original or a copy of a valid entry from the Commercial Register, unless it is publicly accessible in a similar authenticated form as a current entry from the Commercial Register in the Czech Republic. SYNOT shall further identify individuals who act on behalf of such a legal person in a particular transaction or business relationship. For individuals who are members of a statutory body of such a legal person, but who are not involved in the negotiation of a particular transaction or business relationship, only data for determining and verifying their identities shall be recorded. This means data that can be ascertained from accessible sources, typically the Commercial Register, in particular the person's name, surname, date of birth and address. If a customer's statutory body (or member or controlling person of the statutory body) is a different legal person, the identification data of this legal person shall also be recorded.
- **a trust fund or other legal organisation without legal personality:** SYNOT shall ascertain the designation and identification data of its trustee or manager, or another person in a similar position, to the extent specified above, depending on whether this concerns an individual or a legal person.

Ascertaining individual data:

- **Birth registration number or other unique identifier of a citizen of a particular country:** an obligatory data item for citizens of the Czech Republic, foreign nationals with a permit to reside in the Czech Republic, refugees and other persons, in the form of a birth registration number allocated in accordance with Section 16 of Act No. 133/2000 Coll., on the registration of the population, as amended.
- **Date of birth:** a mandatory data item for persons who have not been allocated a birth registration number or other unique identifier of a citizen of a particular country.
- **Sex:** a data item which is particularly required of foreign nationals whose names do not indicate their sex (for example they do not have a suffix like "-ová", as found on Czech women's surnames), or if it is not apparent from their birth registration number.
- **Place of birth:** the format for recording the place of birth should be comprehensible and clear. From a language viewpoint, the "place" cannot be just a country, but a place specified in an appropriate manner, for instance the name of a village, town or city + country.
- **Permanent or other residential address:** identification of an appropriate residential address. Residential addresses should be real, traceable (verifiable on the internet) and verifiable from appropriate documents. If a person uses several addresses, it is appropriate to record all of them.
- **Identity card issuer:** this data item must particularly be recorded in the case of foreign nationals. In situations where the customer is a citizen of the Czech Republic, it is clear that such a document could not be issued by anyone other than a Czech government authority (except in cases where the customer has dual citizenship and presents an identity document issued by a country other than the Czech Republic).
- **Required types of identification documents:**
 - A national identity card, passport, driving licence, a residence permit for foreign nationals, a firearms licence, etc.

- The specified types of identity documents can be only accepted if they meet the following requirements:
 - ✓ it must be a valid document issued by a given country;
 - ✓ It must not be damaged beyond an ordinary degree of wear and tear (e.g. must not have missing pages, be stuck together, written over, illegible, etc.);
 - ✓ the photo of the document holder must match the actual appearance of the holder and must be sufficiently clear and undamaged to allow identification of its holder with sufficient degree of probability;
 - ✓ it must be possible to identify which authority issued the document and in which country;
 - ✓ the document must not raise doubts about its authenticity for any reason.

Some identification data (e.g. sex and residential address) need not be specified in every identity document. Such information may be established on the basis of a declaration of the identified person, or from another supporting document.

SYNOT may procure copies of or extracts from any of the presented documents and process the acquired information for the purposes of the KYC process. Procurement of copies of personal documents for the purposes of personal identification is only possible with the consent of their holder.

If, when concluding a transaction or business relationship, SYNOT suspects that the customer is not acting in his/her/its own name, or is concealing the fact that he/she/it is acting on behalf of a third party, SYNOT shall ask the customer to present an original or authenticated copy of a power of attorney for such agency. All persons are obliged to accommodate this request.

4.1.2 Identifying politically exposed persons

As part of customer identification, SYNOT shall ascertain and record whether the customer is a politically exposed person. To this end, it is necessary to verify the customer, as well as all persons who are beneficial owners of the customer, if this has been established.

Whether or not a customer is a PEP can be ascertained:

- through active searches, e.g. by searching through open sources and other information (media, internet, personal knowledge and potential relevant information from other institutions);
- through a declaration of the customer made during identification at the beginning of a transaction or business relationship. This declaration shall include the customer's obligation to report any changes in its status, if such a change occurs within the duration of the business relationship;
- by using the national list of functions of PEPs (Annex No. 1) and comparable functions in another country where SYNOT operates;
- using one of the systems for the control and tracing of "risky" clients, which are based on public resources and which are provided as a paid service by certain specialized business entities.

Other obligations are also linked to establishing whether a customer is a PEP. Among other things, the situations specified below require the approval of the person authorised to manage the AML/CFT measures as specified in Article 10 of this Directive (if such a person does not give his/her approval, it will not be permissible to conduct a transaction or to establish a business relationship with a PEP, or to continue such a transaction or relationship if the customer becomes a PEP during the course of the business relationship);

Whether or not customers are PEPs must be determined prior to the execution of a transaction or the conclusion of a business relationship. Business relationships are subject to ongoing

customer control (once every 12 months or every 24 months depending on the level of risk), which will make it possible to establish whether a customer has become PEP during the course of the relationship.

SYNOT shall apply obligations and restrictions relating to politically exposed persons for a period of at least another 12 months from the date on which a politically exposed person ceases to perform the relevant function. These obligations and restrictions shall be applied for the same period of time to customers whose beneficial owner is a politically exposed person, and to persons in cases where SYNOT knows that they are acting for the benefit of a politically exposed person.

4.1.3 Detection of persons subject to international sanctions

As part of customer identification, SYNOT determines and records whether a customer is a person against whom the Czech Republic, Slovakia or another EU country has applied international sanctions of a financial nature (hereinafter referred to as the “sanctioned entity”). In this way, it is necessary to verify the customer and persons authorised to act on the customer’s behalf in the relevant transaction (or business relationship) and, in the case of a customer who is a legal person, to verify all persons who are members of the customer’s statutory body, all identified beneficial owners of the customer, and all persons identified on the basis of information obtained from a survey of the customer’s management and ownership structure.

Information on current sanctions and sanctioned persons and entities can be obtained through the EU

- sanctions map, which is published on [the website www.sanctionsmap.eu](http://www.sanctionsmap.eu), and simultaneously
- from Government Regulation No. 210/2008 Coll., regarding the implementation of special measures in the fight against terrorism, as amended;
- SYNOT also identifies persons who are subject to international sanctions by means of automated systems of a third party with whom SYNOT has entered into a contractual relationship. As part of this control, SYNOT also takes into account OFAC sanctions.

Verification with sanctions lists must be carried out before a transaction is conducted or a business relationship is established.

If a person is matched with sanctions lists, a transaction or business relationship may only be continued in accordance with the legal regulation based on which the sanction was imposed. This usually means complete freezing of all of the customer’s funds and a ban on the provision of any funds; possible exceptions may be permitted by the FAO. A suspicious transaction report is always promptly submitted.

4.2 Other identification options

Besides identification carried out in the physical presence of the customer, SYNOT may also use the following options to identify a customer.

4.2.1 Mediated identification

At the request of a customer or an obliged person, the identification of a customer who is an individual and every individual who acts on behalf of a customer who is a legal person may be carried out by a notary or a state administration contact point (“CzechPOINT”) in the physical presence of the person to be identified. The notary or state administration contact point shall draw up an identification document, which shall serve as a public document. This public document must be stored by SYNOT before making a transaction or establishing a business relationship.

4.2.2 Takeover of identification

SYNOT may replace the typical identification procedure pursuant to Article 4.1 by conducting the identification process in such a way that:

a) a customer who is

1. an individual shall send SYNOT copies of the relevant parts of an ID card, from which it is possible to ascertain the data pursuant to Article 3.1.1,

2. a legal person shall send SYNOT proof of its existence and its identification data, or SYNOT shall ascertain the customer's existence and identification data from a public register or records of trust funds,

3. a trust fund shall send SYNOT proof of its existence and its identification data,

b) if a different person acts on behalf of a customer, the customer shall send copies of the documents according to letter a) item 1 of an individual who is authorised to act on behalf of the customer in a transaction or business relationship, and the authorisation of such an individual to act on behalf of the customer,

c) SYNOT records and verifies the data and authorisations sent pursuant to letters a) and b) and has no doubt about the actual identity of the customer or person acting on the customer's behalf – due diligence process,

d) SYNOT enters into a contract for a transaction or business relationship with a customer, the content of which will be recorded in text form,

e) the customer proves the existence of a payment account maintained in his/her/its name in a credible manner,

f) the first payment from such a contract shall be made by the customer via an account pursuant to letter e).

5 Customer due diligence procedure and determination of the scope of customer due diligence in relation to the risk of legitimisation of proceeds of crime and financing of terrorism

By carrying out customer due diligence and with a declaration from the customer, SYNOT obtains the information it needs to assess whether or not a transaction is suspicious.

An insufficiency or inability to ascertain or verify an adequate amount of information for customer due diligence is a significant risk factor to be applied when deciding on the possibility of not conducting a transaction or submitting a suspicious transaction report.

SYNOT always conducts customer due diligence:

- prior to conducting a transaction outside the scope of a business relationship
 - at the latest when it is clear that it will reach the value of 3% of the annual turnover of the company (each company of the SYNOT group has a set individual limit);
 - with a PEP;
 - with a person established in a country that must be considered extremely high risk on the basis of a European Commission designation or for any other reason. *This means a person with a nationality, a residence (permanent or temporary), a registered office, a branch or an organisational unit in a so-called high-risk country (see the chapter Definition of Terms);*

- before carrying out a suspicious transaction;
- upon establishment of a business relationship, where it is clear that the value of individual partial transactions within the business relationship will exceed €20,000 (at the latest before the first transaction takes place);
- for the duration of a business relationship within the framework of ongoing due diligence - for customers with normal risk once every 24 months, and for customers with high risk once every 12 months;
- before making a cash transaction in the amount of €8,000 (CZK 200,000) or higher, but not more than €10,800 (CZK 270,000) in accordance with Act No. 254/2004 Coll., on the limitation of cash payments and amending Act No. 337/1992 Coll., on the administration of taxes and fees, as amended;

If a transaction is divided into several separate instalments, the value of the transaction shall be the sum of these instalments, provided they are related. Clearly related instalments must thus be totalled and considered as a single transaction.

Customer due diligence includes:

- obtaining information about the purpose and intended nature of a transaction or business relationship;
- determining the ownership and management structure of a customer and its beneficial owner if the customer is a legal person, trust fund or other legal organisation without legal personality, and adoption of measures to ascertain and verify the identity of the beneficial owner;
- continuous monitoring of business relationships, including re-examination of transactions conducted within a particular relationship for the purpose of determining whether the transactions are in harmony with what SYNOT knows about the customer and the customer's business and risk profile – KYC process;
- reviewing sources of funds or other assets to which a transaction or business relationship relates;
- within the scope of a business relationship with a PEP, adequate measures to ascertain the origin of his/her assets;
- in the case of a customer who is an operator of games of chance, proof of a gaming license is always required.

5.1 Obtaining information about the purpose and intended nature of a transaction or business relationship

This information is obtained in order to create conditions for the future assessment of whether partial transactions show signs of a suspicious transaction.

The information obtained by SYNOT must be of such a volume that makes it possible to assess the customer in terms of potential risks in the areas of ML/FT.

5.2 Identification of the ownership and management structure of a customer and its beneficial owner, and the adoption of measures to identify and verify the identity of the beneficial owner

Obtaining information about a customer's ownership structure and identifying the customer's beneficial owner is necessary for assessing customers in terms of possible risk in the areas of ML/FT.

SYNOT identifies the scope of relevant relationships all the way to a particular individual or multiple individuals that have a significant impact on the activities of a customer, even if indirectly (through other individuals or legal persons).

The identification of a beneficial owner therefore requires the acquisition of information about the customer's ownership and management structure. In order to gain knowledge of the beneficial owner, it is necessary to adopt measures that help to understand a customer's ownership and management structure, i.e. to obtain information about the customer's status, shareholders and management bodies.

To determine the necessary information, SYNOT shall send a due diligence questionnaire to the customer, which the customer shall then fill in and, at the same time, submit the required annexes, which will make it possible to subsequently identify and verify the beneficial owner. If the customer is obliged to make a record in a register of beneficial owners or another similar register, SYNOT shall always ask the customer to provide an entry from such a register or other similar register, and evidence from one other source.

If the beneficial owner is listed in a public register and there is no doubt as to the accuracy and currency of that information, that source of information and a link to it shall suffice.

When conducting customer due diligence in the case of a legal person, SYNOT ascertains and records:

- data for verifying the beneficial owner's identity and the procedure for his/her identification.

Possibilities for verifying certain facts which are significant for identifying the beneficial owner of a customer in selected cases:

a) Trading companies

It is currently possible to use the Commercial Register maintained in the Czech Republic or a similar register maintained in another state in particular to identify partners of partnerships (public partnerships and limited partnerships), directors, partners and statutory bodies of limited liability companies, statutory bodies and 100% owners (single shareholders) of joint-stock companies, and statutory bodies of cooperatives. It should also be possible to use the collection of documents to access other documents such as annual reports or minutes of meetings of company bodies and documents on profit distribution, where it is also possible, as of the date of the respective event, to identify the ownership structure of joint-stock companies and cooperatives, including any silent partners (approval of a silent partnership agreement falls under the competence of the general meeting in the case of limited companies, or a meeting of members in the case of cooperatives; silent partners are entitled to a share in the profit corresponding to their contribution).

b) Trust funds or other legal organisations without legal personality

The essence of a trust fund consists in the fact that its founder will set aside some of its assets and entrust them to a certain purpose. This creates separate and independent ownership, to which neither the original owner nor any other person already has any ownership rights. Those rights shall be exercised for and on behalf of the trust by a trustee, who acts as the owner of property in the trust fund. Just as in the countries of Anglo-Saxon law, trust funds in the Czech Republic are also very high-risk instruments which can be abused for the purpose of money laundering and other illegal activities, including support of terrorism. Establishing a trust fund is subject to certain obligations: it is established by way of a statute issued by the founder in the form of an authentic instrument, generally a notarial deed, and its trustee is then bound by this statute in his/her actions. The trustee, as the only person entitled to dispose of the assets in the trust fund, shall be recorded in any register as the owner of such assets with the note "trustee".

Other legal organisations without (separate) legal personality, such as mutual funds, may be established under Czech and foreign law. In all such cases, as in the case of trust funds, it is always necessary to identify as beneficial owners all persons (who come into consideration) specified in this Directive within the definition of beneficial owner under letter c).

c) Bodies of churches and religious societies, associations, foundations and similar entities

For the purposes of identifying managers in the above cases, it is possible to use other public registers established beyond the Commercial Register (Register of Societies, Register of Foundations, Register of Institutions, Register of Associations of Unit Owners, Register of Public Benefit Companies).

d) Local government units, state authorities and institutions

In the case of municipalities and higher local government units and institutions established by them, just as in the case of government bodies and institutions or state enterprises established by them, a beneficial owner cannot in fact be considered. It will always be necessary to identify the founder and to specify an individual who directly performs the highest management function for such a legal person as its beneficial owner.

Identification of a beneficial owner is also carried out in the course of a business relationship, and is conducted in a manner that ensures that the periodicity of checks will cover all changes that occur.

After identifying the beneficial owner and ownership structure, it is necessary to verify whether or not the entities thus identified are on the list of sanctioned entities. For conformity assessment procedure, see chapter 4.1.3.

Procedures in cases where a customer's beneficial owner cannot be identified from publicly accessible sources

In situations where it is not possible to identify a customer's beneficial owner from publicly accessible sources, SYNOT shall proceed as follows:

- SYNOT shall call upon a person acting on the customer's behalf to submit documents proving the customer's ownership structure in the form of due diligence documents (articles of association, lists or declarations of shareholders, minutes of general meetings, etc.);
- if such documents are not submitted by a person acting on the customer's behalf (because these documents do not exist or are not available), SYNOT shall identify the beneficial owner by means of a sworn statement; in such cases, SYNOT must adequately reflect this fact in the customer's risk profile and take appropriate measures against the customer according to established SYNOT regulations. The customer shall be classified under the category High Risk.
- When identifying a customer's beneficial owner, SYNOT may conclude that no such person exists (e.g. if no individual within the customer's ownership structure has a share higher than 25%); in such cases, the individual or individuals who performs/performs the customer's highest management function (who genuinely exercise a decisive influence on the management of the company, e.g. members of a statutory body) must be identified as the beneficial owner(s). If such data cannot be evidenced by an official document, it must be evidenced by a written statement from a responsible representative of the customer;
- if a customer fails to cooperate, or if there are doubts about the truthfulness or credibility of the information provided, SYNOT may consider such conduct to be reason to refuse to carry out a transaction or to establish a business relationship, or to terminate an existing transaction or relationship.

5.3 Continuous monitoring of a business relationship, including a review of transactions carried out within the scope of the particular relationship

SYNOT must obtain information necessary for carrying out continuous monitoring of a business relationship (in accordance with other points specified herein), including scrutiny of transactions undertaken during the course of such a relationship to ensure that these transactions are consistent with SYNOT's knowledge of the customer, its business and its risk profile. SYNOT must assess whether individual transactions are genuinely related, for instance, to the business operations of the customer or its usual income, whether they correspond to the customer's standard operations, etc. For these purposes, SYNOT shall use a due diligence form and local and personal knowledge of customers.

If a customer carries out financial transactions that are excessive in comparison to its typical transactions, such transactions shall be verified by an employee of SYNOT's economic department in cooperation with the Division of Prevention of Money Laundering and Financing of Terrorism. For the purpose of ascertaining information about a customer's financial transactions, SYNOT employees are entitled to contact the customer by e-mail or by phone. Such customers may subsequently be moved into higher risk categories, and the continuous monitoring of the business relationship with these customers shall be stricter.

SYNOT must understand the purpose and sense of transactions conducted by a customer; for this purpose, SYNOT may request the provision of all documents (business contracts, invoices and delivery notes) and make copies of these documents. SYNOT must know the trading counterparties and obtain such information from the customer so as not to participate in a breach of international sanctions, i.e. counterparties (and persons involved in their activities) must be verified against the relevant lists; their goods or services must also not exceed the relevant limits ensuing from international sanctions.

5.4 Reviewing sources of funds or other assets to which a transaction or business relationship relates

It is essential to ascertain the source of funds that a customer uses in a transaction or business relationship. In the case of a business relationship, this part of customer due diligence should especially be carried out upon the establishment of the relationship (acquisition of so-called input information).

As part of SYNOT's KYC and due diligence process, SYNOT identifies and requires the completion of information about the source of funds used in a transaction or business relationship. For this purpose, SYNOT shall provide the customer with a Due Diligence form for an individual, a Due Diligence form for an LP, or a Due Diligence form for an LPG (depending on the type of customer).

The term 'source of funds' in the case of an LP indicates the person who has provided or will provide funds that are to be used to finance the customer's business, and where the funds come from, for example, the company's working capital, a loan or funding by a third party. The term 'source of funds' for an individual refers to the origin of funds that the particular person intends to use to finance a transaction or business relationship, for example a gainful activity, an inheritance, a prize, a loan, a gift or other such source.

5.5 Measures taken to establish the origin of assets in the case of a business relationship with a PEP

Before making a transaction or entering into a business relationship with a politically exposed person, SYNOT shall identify and inspect the particular customer.

SYNOT employees shall not conduct a transaction with a politically exposed person, if the origin of the assets used in the transaction is unknown.

Upon the establishing a business relationship or before conducting a transaction with a politically exposed person, the consent of the authorised person pursuant to Article 10 shall be required, otherwise the transaction shall not take place.

5.6 Further information on customer identification and due diligence

Customers must always provide SYNOT with information that is essential for customer identification. At the same time, SYNOT expects the active cooperation of the customer, that may consist, for instance, in the submission of the relevant documents and declarations. The information obtained is required in accordance with the AML Act.

SYNOT may make copies of or obtain extracts from the presented documents and process the acquired information in accordance with legislation. If a customer does not allow SYNOT to make copies, this shall constitute a failure to provide cooperation, and such conduct may be classified as a suspicious transaction.

In case of doubt, SYNOT may request further supporting or clarifying information, and if these should be insufficient or unclear, SYNOT shall not make the transaction or may file an STR. If the customer refuses to cooperate, SYNOT shall not make the transaction. Doubts of potential abuse that persist even after due diligence checks have been made shall constitute a reason for submitting an STR.

All data are recorded in a due diligence questionnaire, which serves as a basis for the Division of Prevention of Money Laundering and Financing of Terrorism to compile customer risk profiles.

When establishing a business relationship with a customer, as well as during the course of the relationship and when conducting transactions that are not part of a business relationship, SYNOT:

- a) shall determine and keep on file information about the customer which will enable SYNOT to assess whether or not the customer carries a risk,
- b) shall check the validity and completeness of details about the customer, and shall update these details,
- c) shall pay increased attention according to this Directive to selected transactions (high-risk circumstances):
 1. with any of the risk factors described above,
February politically exposed persons,
 3. where SYNOT is aware that the customer's beneficial owner is a politically exposed person, or that a politically exposed person participates in some other way, or
 4. with an unusually large volume or high level of complexity, especially with regard to the type of customer, subject matter, amount and method of settling the transaction, the purpose of the business relationship, and the customer's line of business.

6 Simplified customer identification and due diligence

SYNOT may carry out simplified customer identification and due diligence with regard to customer categories with a potentially lower risk of abuse for legitimising proceeds of crime or financing terrorism, providing that the customer is:

- a) a credit or financial institution,
- b) a foreign credit or financial institution operating in the territory of a country which imposes on that institution applicable obligations equivalent to requirements of the European Union law

focusing on combating legitimisation of proceeds of crime and financing of terrorism, and therefore this institution is supervised,

c) a company whose securities are accepted for trading on a regulated market and which is subject to disclosure requirements equivalent to those of European Union law,

d) the beneficial owner of funds deposited in the escrow account of a notary, lawyer, court bailiff or court,

e) a central government authority of the Czech Republic, the Czech National Bank, a high-ranking local government authority, or a similar institution within the framework of the EU,

f) a customer

1. who has been entrusted with important public functions under EU regulations,
2. whose identification data are publicly accessible, and there is no reason to doubt their correctness,
3. whose activities are transparent,
4. whose accounts present a true and fair picture of the subject matter of their accounting and financial situation,
5. who is responsible either to a body of the EU or to bodies of a member state of the EU or the EEA, or for whom there are other appropriate due diligence procedures allowing for proper inspection of its activities.

g) SYNOT may also apply simplified customer due diligence for other products, provided that they pose a low risk of abuse for the purposes of legitimisation of proceeds of crime or financing of terrorism, and also meet the following conditions:

1. the contract for the provision of the product is always drawn up in writing,
2. payments for this product are made exclusively through an account kept in the customer's name by a credit institution or a foreign credit institution operating in the territory of an EU or EEA Member State, or operating in the territory of a country that imposes obligations on this institution in the area of combating legitimisation of proceeds of crime and financing of terrorism that are equivalent to the requirements of EU law, and supervises the fulfilment of these obligations,
3. neither the product nor individual payments are anonymous, and their nature allows for identification of a suspicious transaction,
4. the product in question has a pre-determined maximum value for trade, which shall not exceed €40,000.

h) a customer who does not pose a risk of legitimisation of proceeds of crime or financing of terrorism. This means a customer in whose case there are no doubts regarding the possibility of legitimisation of proceeds of crime or financing of terrorism, and a customer who SYNOT knows and has verified. In such a case, the consent of the authorised person pursuant to Article 10 of this Directive is required.

In cases where simplified customer identification and due diligence is used, SYNOT shall at least ascertain and record the following in an appropriate manner:

1. basic identification data of the customer and a person acting on behalf of the customer; this includes ascertaining whether or not international sanctions have been applied against the customer,
2. data for verifying the identity of the beneficial owner of the customer,

where appropriate, SYNOT shall perform other activities within the scope of customer identification and due diligence to the extent necessary for effective risk management.

7 Risk assessment

The management of the SYNOT Group is the overall owner and controlling unit of the risk environment. Risk assessment is delegated to the Division of Prevention of Money Laundering and Financing of Terrorism, for which the authorised person specified in Article 10 of this Directive is responsible, and which bears primary responsibility for the initiation and implementation of aspects of an ML risk assessment. This includes, but is not limited to, tasks such as methodology development, maintenance, periodic process renewal/initiation of activities and record-keeping of completed assessments. The cooperation of all companies of the Group and their departments is also required.

Risk assessment must include at least:

- risk categorisation for types of customers in view of their risk factors;
- risk categorisation of products and related services which could be abused for ML or FT;
- exemplary signs of suspicion that could indicate suspicious behaviour in individual types of customers, suspicious transaction patterns, etc.

The above-mentioned minimum requirements also cover:

- the high-risk country factor;
- the distribution channel factor.

Based on the information obtained during customer identification and due diligence, SYNOT determines the risk profile of the particular customer. SYNOT shall always compile and assess risk profiles with respect to at least the following risk factors:

- a) the fact that a country of origin of customers or persons who SYNOT deals with on behalf of customers, or a country of origin of beneficial owners of customers is a country which insufficiently applies or does not at all apply measures against legitimisation of proceeds of crime and financing of terrorism, or is a country which SYNOT considers high-risk based on its assessment;
- b) the fact that, according to information available to SYNOT, the subject matter of a transaction has been or is intended to be transferred or provided in connection with the transaction from a country which insufficiently applies or does not at all apply measures against the legitimisation of proceeds of crime and financing of terrorism, or from a country which SYNOT considers high-risk based on its assessment, or the subject matter of a transaction has been or is intended to be transferred to such a country in connection with a transaction;
- c) a customer or a person who deals with SYNOT on behalf of a customer or on behalf of the beneficial owner of a customer, persons with whom a customer carries out a transaction or, if they are known to SYNOT, the final beneficiary of the subject matter of a transaction or the beneficial owner of an entity with whom a customer carries out a transaction has a record on a list of persons or movements against whom sanctions have been applied;
- d) non-transparent ownership structure of a customer;
- e) unclear origin of a customer's funds;
- f) facts that give rise to a suspicion that a customer is not acting on its own behalf, or is concealing the fact that it is acting on the instructions of a third party;
- g) an unusual method of conducting business, especially considering the type of customer and its previous business activities, subject matter, volume and method of settling business, the purpose of its business relationship and the customer's line of business;
- h) evidence suggesting that a customer is conducting a suspicious transaction;

i) the fact that, based on information available to SYNOT, a customer's business activities are associated with an increased risk of legitimisation of proceeds from crime or financing of terrorism.

Risk profiles and risk factors

- **in relation to a customer**

- a business relationship takes place under unusual circumstances (for example, a significant inexplicable geographical distance between the financial institution and the customer),
- the customer is not resident in the relevant country,
- a company has authorised shareholders or bearer shares,
- business activities require large amounts of cash,
- the ownership structure of a company seems unusual or excessively complex with regard to the nature of its business,

- **in relation to a country or a geographical area**

- countries identified by credible sources as countries without an appropriate AML/CFT system,
- countries subject to international sanctions,
- countries identified by credible sources as countries with a significant degree of corruption or other criminal activity,
- countries identified by credible sources as countries providing funding for or supporting terrorist activities,

- **in relation to a product, service, transaction or distribution channel**

- private banking,
- anonymous transactions,
- non-personal business relationships or transactions,
- payment received from unknown or non-associated third parties.

Overview of criteria related to the level of risk and the compilation of a customer's risk profile:

Level of risk Criterion	Low risk	Standard risk	High risk
Territorial principle and country of origin of the customer	Individual – Country of origin EU or EEA Member State	Other countries	Individual – country of origin is found on a list of high-risk countries or on a list of countries subject to international sanctions
		Other countries	LP – country of origin is found on a list of high-risk

	LP – country of origin EU or EEA Member State		countries or on a list of countries subject to international sanctions
Type of customer	A customer pursuant to Article 5, with simplified identification and due diligence (i.e. central government authorities, CNB, high-ranking local government units, credit or financial institution, etc.)	Standard customers	<ul style="list-style-type: none"> - PEPs - international sanctions are applied and no obligation to trade is imposed; - LP with its registered seat in an off-shore centre; - non-transparent ownership structure of a customer; - customers from countries with a high level of crime or corruption; - an entity is listed in an insolvency register or another similar register; - facts that give rise to a suspicion that a customer is not acting on its own behalf, or is pretending to act according to the instructions of a third party; - evidence suggesting that a customer is conducting a suspicious transaction;
Method of ascertaining information on a customer	An excerpt from a register	<ul style="list-style-type: none"> - a declaration of the company, - public sources and documents submitted for customer identification and due diligence 	A declaration of the customer, public resources, documents submitted for customer identification and due diligence, additional findings, independent verification of documents, or

			additional due diligence checks
Customer monitoring	Simplified monitoring.	Standard monitoring.	Increased monitoring.
Customer's line of business and business focus	Customers who SYNOT has been cooperating with for a long time, where there are no reasonable suspicions of ML/FT and there is no doubt about their transparency – the customer has a verified business history in relation to SYNOT.	<ul style="list-style-type: none"> - standard services used by companies of the SYNOT Group, - activities related to the gambling industry and the operation of games of chance, - charities and NPOs, - real estate, - IT technologies, - the customer has no verified business history in relation to SYNOT, 	<ul style="list-style-type: none"> - retail trade with precious stones/metals, - second-hand shops, - nightclubs, - trade in strategic materials, - trade in military material, - arms dealing, - private military companies, - digital currency and cryptocurrency providers, - the customer's line of business is associated with an increased risk of legitimisation of proceeds of crime or financing of terrorism, - an unusual method of conducting a transaction.
Method and volume of financial transactions made by a customer	Cashless transfer up to €50,000 (CZK 1,300,000).	Cashless transfer exceeding €50,000 (CZK 1,300,000). In cash up to €8,000 (CZK 200,000).	In cash exceeding €8,000 (CZK 200,000) up to €10,800.
Method of customer identification	Identification in the physical presence of the customer.	Identification without the physical presence of the customer. - so-called problem-free identification	Identification without the physical presence of the customer. - failure to provide full cooperation during the identification process
Legislation in force in a customer's country of origin applicable to the	Participation in gambling is only possible for registered players.	-	Participation in gambling is possible even without

identification and registration of participants in gambling	This does not create anonymous gamblers.		registration. Risk of the creation of anonymous gamblers.
Country of origin of a customer taking into account legislation in the gambling industry	The customer's country of origin has a codified system of conditions for operating games of chance, expressed in the form of a law.	-	The customer's country of origin does not have a codified system of conditions for operating games of chance expressed in the form of a law.
Due diligence process	The customer provides all cooperation, i.e. duly completes the presented form and submits the required annexes.	-	The customer does not provide cooperation, i.e. does not complete the presented form or does not submit the required annexes.
PEP	Domestic – Czech Republic, Slovakia	EU, EEA	Other countries
Origin of the customer's funds	- gainful activity, - income from business activities, - inheritance	-	- won, - loan, - origin of funds unclear, - other

Based on the information ascertained about the customer, the Division of Prevention of Money Laundering and Financing of Terrorism shall compile a risk profile. The risk profile shall be compiled as follows:

A low-risk indication is evaluated with a coefficient of 0.5

A standard risk indication is evaluated with a coefficient of 1

A high-risk indication is evaluated with a coefficient of 1.5

Example risk coefficient calculation: the customer has 4 low-risk indications, 3 standard risk indications and 1 high-risk indication. $4 \times 0.5 + 3 \times 1 + 1 \times 1.5 = 6.5$ (resulting risk coefficient).

Based on the resulting risk coefficient, the customer will be assigned to the relevant category. If only indications from one category will occur in a customer's case, such a customer will automatically be classified in the relevant category regardless of the resulting coefficient.

The system is set up in a way that ensures that customers can be moved quickly between groups.

Other risk factors

A customer's risk profile must be supplemented by other risk factors in specific situations. Below is a non-exhaustive list of other risk factors:

- **personal risk** – individuals (including statutory representatives or beneficial owners of legal persons) with a criminal or otherwise dubious (unclear) past or associated with such persons; persons with property of dubious/unclear origin; persons associated with PEPs, “godfathers”, lobbyists, persons from high-risk territories, persons associated with participation in a large number of business entities, chronic “bankruptors”, etc.
- **payment risk** – intensive cash payments, over-limit cash payments, frequent payments that do not correspond to the type of customer or the customer’s line of business, transfers to/from high-risk jurisdictions or to areas subject to international sanctions, etc.
- **distribution risk** – cashing of foreign cheques, use of so-called new payment methods (payments by mobile phone, remote payments, digital wallets above the specified limits), etc.
- **commodity risk** – the subject matter of transactions are weapons or their (potential) carriers, military material, dual-use items or advanced technologies, precious metals or stones, strategic materials, precursors, etc.
- **product risk** – investments in mutual funds, flexible investment life insurance with a buy-back option, virtual or digital currencies (Bitcoin, etc.), provision of strategic material trading, or territorial, volume and other risks.

The risk may also increase the subjective evaluation of a SYNOT employee present at the establishment of a business relationship or conclusion of a transaction (e.g. local and personal knowledge, mistrust of provided information, and doubts about the authenticity of documents submitted for customer identification and due diligence). Based on the identified risks, it is ensured that the measures put in place for AML/CFT prevention are proportionate to the risks identified, i.e. higher ML/FT risk justifies enhanced measures, while reduced risk may justify less thorough customer due diligence.

The authorised person pursuant to Article 10 of this Directive must ensure that employees of all companies of the SYNOT Group are familiar with this SIP. SYNOT Group companies meet twice a year (every six months) at corporate presentations and meetings. The agenda of these meetings includes, but is not limited to, sharing information on issues of combating legitimisation of proceeds of crime and financing of terrorism and information on any changes in AML/CFT legislation in the Czech Republic, the EU or any country where SYNOT Group companies operate.

Within the scope of risk assessment, SYNOT particularly takes into account:

- Act no. 253/2008 Coll on selected measures against legitimisation of proceeds of crime and financing of terrorism;
- Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, and Directives 2009/138/EC and 2013/36/EU (“5th AML Directive”);
- Act No. 186/2016 Coll., on gambling, as amended;
- regulations issued pursuant to the Czech Gambling Act and the gambling acts of countries where the SYNOT Group operates;
- Act No. 370/2017 Coll., on payments;
- Act No. 256/2004 Coll., on capital market business, as amended;
- Act No. 69/2006 Coll., on the enforcement of international sanctions;
- other relevant legislation of the EU and other countries where the SYNOT Group operates.

7.1 Risk categorisation of types of customers with regard to risk factors

Low risk – customers with a resulting risk coefficient of up to 6.5

Low risk is the usual risk of money laundering and financing of terrorism, which is the assessment of most of SYNOT's customers. This covers customers that are not normally connected with money laundering, financing of terrorism, embezzlement or other criminal acts. The products and services used by such customers do not create an increased risk of money laundering, and the geographical operation of these customers and their transactions do not necessarily lead to increased concerns about money laundering and financing of terrorism. No increased attention and supervision are required for customers in this category. The proper process of conducting a transaction or entering into a business relationship should be sufficient to verify the identity of the customer and to understand who the customer is, and how the customer intends to use offered products and services. Similarly, increased supervision (monitoring) is not required. It is sufficient to record any abnormalities that may develop during the relationship.

Medium risk – customers with a resulting risk coefficient of 7 to 13

Medium risk entails an increased risk of money laundering and financing of terrorism. If an increased risk is present, the attention and level of monitoring must be increased accordingly to the degree of perceived risk. Increased supervision (monitoring) is required as part of periodic customer due diligence once every 24 months. Any abnormalities that may develop during the relationship shall also be recorded.

High risk – customers with a resulting risk coefficient of 13.5 and up

High risk entails a high increase in the possibility of money laundering and financing of terrorism for customers through our products and services. SYNOT must implement appropriate measures and controls to mitigate the risks of possible money laundering and financing of terrorism for those customers with a high risk. Such measures and controls shall include the following:

- An increased level of knowledge about the customer and increased caution;
- A stricter approval process for transactions or when entering into a business relationship;
- Increased monitoring of transactions;
- An increased level of continuous monitoring and evaluation of the relationship, i.e. once every 12 months.

Unacceptable customers

- customers or their beneficial owners who are subject to international sanctions imposed by the EU;
- customers who refuse to be identified or refuse to provide the necessary cooperation during due diligence checks;
- customers who do not act on their own behalf or who conceal the fact that they are acting on behalf of a third party and refuse to identify such a person;
- a legal person with a non-transparent ownership structure;
- the origin of the customer's funds is not clear;
- evidence suggests that a customer is conducting a suspicious transaction;
- a customer in whose case other facts foreseen by this internal directive occur;
- a customer who is identified as an unacceptable client by the authorised person under Article No. 10 of this Guideline.

7.2 Risk categorisation of products and related services which could be abused for ML or FT

High degree of risk

- B2B provision of technical gaming equipment intended for the operation of games of chance;
- provision of software, consulting in the field of information technologies, data processing, hosting and related activities, and web portals;
- development of applications and platforms intended for the operation of games of chance;
- support for start-up projects;
- investment activities;

Medium degree of risk

- wholesale and retail (B2B and B2C) - mainly sales of vehicles, security equipment, camera systems, etc.;
- advertising, marketing and media representation;
- provision of additional products and services relating to the operation of games of chance;

Low degree of risk

- other products and services provided by the SYNOT Group, especially accommodation and catering services, wellness, etc.

7.3 A detailed demonstrative list of indications of suspicious transactions

7.3.1 Features that may indicate suspicious transactions

A transaction may be considered suspicious if, for instance:

- the customer presents him/her/itself as a person acting on behalf of or for another person, and is accompanied or followed by another person or persons who wish to remain anonymous;
- the customer performs actions which could help to conceal his/her identity or the beneficial owner's identity;
- the customer or beneficial owner is a person from a high-risk country;
- SYNOT has doubts about the truthfulness or completeness of the obtained customer data. From the context, it follows, for instance, that the customer has made an effort to provide inaccurate or incomplete information about him/herself;
- identification documents have a dubious appearance;
- the customer is nervous, refuses to identify him/herself or only identifies him/herself unwillingly, or provides false information during the identification or due diligence process (e.g. concerning the origin of funds or the line of business);
- the customer is known to have a criminal history or contacts or relationships with persons associated with criminal groups or who directly commit crimes;
- the customer has contacts or links to high-risk countries, e.g. permanent or temporary residence, or the customer or its business partners have a registered office in such a country;
- the customer requires unusual transactions, conducts transactions in an unusual manner, or is in an unusual hurry to conclude a transaction;
- the customer makes transfers of assets that have no obvious economic sense, or makes complicated or unusually large transactions;
- the customer makes numerous transactions within one day or within a period of time that is shorter than usual for its activities or the activities of a comparable type of customer;
- funds handled by the customer clearly do not correspond to the nature of its business activities and financial situation;
- the customer does business in a field associated with a risk of involvement of criminal groups (e.g. erotic services or trade in military material, particularly weapons, etc.);
- the customer consciously carries out loss-making transactions or transactions characterised by a disproportionately high contractual penalty;
- transactions are made with a large number of low value banknotes, or carries a high volume of cash in an unusual manner (e.g. in plastic bags, clothes pockets, etc.);
- transactions are channelled into or out of areas where the customer does not usually have business interests or where it cannot be assumed that the customer has business interests;
- customers refuse to reveal identification data of persons who they are representing, or refuse to undergo the due diligence process;
- transactions are made in amounts just below the threshold for obligatory customer identification or due diligence.

7.3.2 Features that definitely indicate suspicious transactions

In the situations stated below, transactions are always suspicious and it is therefore reasonable to submit a Suspicious Transaction Report

- the customer, a person in the ownership or management structure of the customer, the beneficial owner of the customer, a person acting on behalf of the customer or a person who otherwise does not participate in transactions is known by SYNOT to be a sanctioned person;
- the subject matter of a transaction is to be goods or services against which the EU has imposed international sanctions under the Sanctions Act.

8 Rejected transactions

SYNOT can reject a transaction or establishment of a business relationship, or can/shall terminate a business relationship if

- the customer refuses to undergo identification;
- the customer refuses to submit a power of attorney in cases where the customer is represented by an agent;
- the customer fails to provide the necessary cooperation for due diligence;
- customer identification or due diligence is not possible for some other reason;
- SYNOT has doubts about the truthfulness of the information provided by the customer or about the authenticity of documents submitted (in such cases it is imperative to simultaneously submit an STR);
- the customer, beneficial owner of the customer, a person acting on behalf of the customer, or a member of the customer's statutory body is found on the list of persons subject to sanctions (in such a case, it is imperative to simultaneously submit an STR);
- a transaction, even in the context of a business relationship, is made with a PEP, and the obliged person is not aware of source of the funds used in the transaction or business relationship;
- the person authorised to manage AML/CFT prevention does not give consent to a business relationship with a PEP;

9 Procedure for access of the competent authorities to stored data

Storage of data

SYNOT keeps the following information for a period of 3 years after the implementation of the last part of the relevant transaction or from the end of a business relationship with a customer:

- identification data, other information concerning the identity document of a customer who is an individual or a legal person acting on behalf of the customer;
- records of whether or not a customer is a PEP or a person who is subject to international sanctions imposed by the Czech Republic pursuant to the Sanctions Act;
- copies of documents presented for identification purposes, if procured;
- information and copies of documents obtained within the scope of customer due diligence;
- documents justifying a customer's exemption from customer identification and due diligence.

The record keeping time limit begins on the first day of the calendar year following the year in which the last transaction act known to the mandatory person was performed, or in which the business relationship was terminated. The method of data storage is governed by the SYNOT Group Security Directive.

10 Person authorised to manage matters of AML/CFT prevention and to supervise compliance with measures within the scope of the SIP

The authorised person for these purposes shall be:

JUDr. Andrej Kucbel', Head of the AML / CFT Division

Mobile: +420 739 604 165

Landline: +420 572 410 126

E-mail: Andrej.Kucbel@synot.cz

11 Procedure after ascertaining a suspicious transaction until delivery of notification to the FAO, rules for dealing with a suspicious transaction, and identification of persons who evaluate a suspicious transaction

11.1 Situations where the FAO submits an STR

SYNOT shall report suspicious transactions on the basis of the information specified above, and particularly if:

- doubts concerning potential abuse for the purpose of ML/FT persist, even after customer due diligence has been carried out;
- customers refuse to identify themselves before making a transaction or entering into a business relationship and SYNOT has partial information concerning the customer or (in such cases all information from SYNOT representatives concerning the description, behaviour and progress of negotiations with unidentified parties to the transaction, their arrival and their departure, shall be included in the STR; the STR shall also include basic identification data of the SYNOT staff who negotiated with unidentified parties to the transaction and could eventually supplement a description of such unidentified parties and subsequently identify them);
- customers fail to cooperate in the acquisition of data and information within the scope of customer identification and due diligence (in which case, SYNOT, depending on the current situation, shall consider whether there is a possibility of obtaining an appropriate explanation from a customer, who is for instance only temporarily unavailable. In such cases, the customer may be provided with an adequate grace period to fulfil its obligations, and the submission of an STR can be postponed until such a period elapses);
- SYNOT has no information from public sources about the origin of the funds used in a transaction with a PEP, and such a person refuses to explain the origin of the funds;
- there are compulsory reasons in accordance with Article 8 of this Directive;

- the matter does not concern a specific suspicious transaction but there are “other facts” which could indicate the legitimisation of proceeds of crime and transactions related to terrorism.

If, in the course of its activities, SYNOT detects a suspicious transaction, it shall report such a suspicious transaction to the FAO without undue delay and no later than 5 calendar days after such detecting transaction. If this period ends on a Saturday, Sunday or public holiday, the last day shall be the nearest business day.

Should the circumstances of a suspicious transaction so require, particularly if there is a danger of a delay, SYNOT shall report the suspicious transaction immediately after its detection. This process is necessary in a situation where there is a risk that the assets which are the subject matter of the transaction or the funds used in the transaction could escape the reach of law enforcement authorities. In such a case SYNOT, must report the suspicious transaction immediately upon its detection, even if the report will not contain all relevant information (the report will be complemented later).

If there is a risk that the immediate fulfilment of a customer’s order could hamper or substantially impede the seizure of proceeds of crime or funds intended to finance terrorism, the obliged entity may fulfil the customer’s order concerning such a suspicious transaction at the earliest after 24 hours have elapsed from the submission of an STR (for more details see chapter 12).

The STR shall be delivered to the FAO in writing by registered post or verbally in a report at a place specified by the FAO after a prior agreement. Written notification shall also mean a communication submitted by electronic technical means ensuring special protection of the transferred data, i.e. the encrypted electronic system “MoneyWeb Lite” connected to the FAO, or via a data mailbox.

The person authorised pursuant to Article 10 of this Directive shall decide whether or not the submission of an STR is necessary. The Division of Prevention of Legalisation of Proceeds from Crime and Financing of Terrorism shall always assess whether or not the indications for submitting an STR have been met.

11.2 Contact details for the Financial Analytical Office

Telephone (7:45 a.m. – 4:15 p.m.): +420 257 044 501
(4:15 p.m. – 7:45 a.m., + weekends and holidays): +420 603 587 663
Fax: +420 257 044 502

Address for delivery in person: Washingtonova 1621/11, 110 00 Prague 1

Correspondence address: P.O. BOX 675, Jindřišská 14, 111 21 Prague 1

E-mail: fau@mfcz.cz (cannot be used for submitting an STR)

Data mailbox: egi8zyh

11.3 Requirements of an STR

An STR must contain all information which is available to the reporting party about a suspicious transaction, its circumstances and participants, specifically:

- 1. identification details of the person reporting a suspicious transaction:** trade name (name and surname or name including a distinguishing description) or other designations, registered office (possibly also a correspondence address), business identification number, line of business according to a record in the Commercial Register or according to a certificate for trading or other business activities (specify only lines of business relevant to the report)
- 2. identification data of the person to whom the report applies as follows, if it concerns:**

- **an individual - non-entrepreneur:** name and surname including other names and surnames used (in unclear cases clearly distinguish the name and surname); domicile in the Czech Republic and potentially outside the Czech Republic and other addresses used; birth registration number or date of birth; place of birth; type and number of identity document, when and by whom it was issued and its information on its validity; citizenship; sex (if not apparent from other data) and possibly any other identification details specified in the identity document;
- **an individual - entrepreneur:** in addition to the data specified for an individual who is not an entrepreneur, designations used in business, possibly a trade name registered in the Commercial Register and a business identification number, lines of business according to a trade licence or an entry from the Commercial Register, and place of business;
- **a legal person:** a trading name or company name including distinguishing descriptions or other designations; registered office; business identification number or a similar number allocated under foreign law; name and surname; birth registration number or date of birth and residential addresses of the persons who are statutory bodies or members of a statutory body, if the statutory body or its member is a legal person; and further a trading name or company name including distinguishing descriptions and other designations; place of business; identification number and identification data of persons who constitute a statutory body or members of a statutory body and identification data of the majority shareholder or controlling entity;
- in the case of representation of an individual, and always in the case of a legal person, identification details of a person acting on behalf of the person concerned by the report shall be provided;

3. identification data of all other parties to the transaction, which are available to SYNOT at the time of the report;

4. a detailed description of the subject matter and fundamental circumstances of the suspicious transaction, especially:

- the reason for the transaction specified by a party to the transaction;
- description of cash or other payment methods used, and other circumstances of a cash payment;
- time details;
- numbers of bank accounts in which the funds concerned by the report are located, and the numbers of all accounts to which or from which money has been or is to be transferred, including identification of their owners and people entitled to handle the accounts, if such details are available to the reporting person;
- currency;
- the suspicious aspect of the transaction;
- information about related transactions;
- a description of the conduct of the party to the transaction and any partners;
- as the case may be, ascertained telephone and fax numbers, and a description and registration numbers of means of transport;
- other information, which could be of importance to involved persons or the concerned transaction, or other data that may be related to the suspicious transaction and that are significant for its assessment in terms of AML/CFT prevention;
- integral parts of the report include copies of all documents specified in the report and relevant to the subject matter of the report, which are available to the reporting person;

5. notification of a case where the report also concerns assets that are subject to international sanctions declared with the purpose of keeping or restoring international peace and security, protection of human rights or the war on terror. Together with such notification, a brief description of such assets shall also be provided, including their location and owner, if known to the reporting party. Furthermore, the reporting person must provide information as to whether there is an imminent risk of damage, devaluation or use of these assets in conflict with the law;

6. the reporting person shall state whether and when the transaction was made, or whether it has been suspended, or the reason for conducting or not conducting the transaction. If the fulfilment of an order has been postponed, SYNOT may not inform the customer of this fact (see the confidentiality provisions);

7. contact details

- The STR must contain the name, surname and job position of the person obliged to submit the STR and contact details so that the FAO may send instructions, including means of contacting the reporting person outside of standard working hours (telephone, fax, e-mail). The person authorised to conduct matters concerning AML/CFT specified in Article 10 of this Guideline shall always submit STRs on behalf of SYNOT.
- the STR shall also contain the date, time and place of its submission, as well as the signature of the person fulfilling the reporting duty;
- Information about the employee of the obliged entity or a person in a similar labour-law relationship who detected the suspicious transaction is not specified in the STR;

SYNOT may not notify the customer of the submission of an STR.

12 Measures to prevent hampering or substantial complication of seizing proceeds of crime by immediately carrying out a customer's order

Fulfilling a customer's order in such a case is understood to mean completion of any transaction with a suspicion of ML/FT.

If there is a risk that immediate fulfilment of a customer's order could impede or substantially complicate the seizure of proceeds of criminal activities or funds intended for financing terrorism, SYNOT may not fulfil the customer's order concerning a suspicious transaction until 24 hours have elapsed from the moment that the FAO receives the STR. The obliged entity shall make sure, in a suitable manner, that the assets concerning the customer's order will not be handled in violation of the AML Act.

Fulfilment of the customer's order shall not be delayed if such postponement is not possible, or if SYNOT is aware that such postponement could hamper or otherwise jeopardise the investigation of the suspicious transaction; SYNOT shall immediately inform the FAO of the fulfilment of the customer's order. If the transaction takes place before the STR is submitted, SYNOT shall provide information of the fact that the transaction has already taken place directly in the STR; if the transaction takes place later, SYNOT shall provide the information with a reference to the submitted STR stating the exact time that the transaction took place.

If there is a risk that the immediate fulfilment of a customer's order might impede or significantly complicate the seizure of proceeds of crime or funds intended to finance terrorism, and the investigation of a suspicious transaction requires a longer period of time due to its complexity, the FAO may decide:

- to extend the period of suspension of the customer's order, but for a maximum period of 2 business days, or
- to postpone the fulfilment of the customer's order or to seize the assets that are supposed to be the subject matter of a suspicious transaction from SYNOT, with whom the assets are entrusted for up to 3 business days.

The above-specified time limits do not apply to seizure of assets, if such assets are seized according to applicable legislation issued to implement international sanctions. Assets are seized on the basis of the applicable regulation on sanctions; it is not therefore necessary (or even possible to consider) any seizure measures under the AML Act. At the same time, such a case is always a suspicious transaction pursuant to Section 6(2) of the AML Act, and it therefore obligatory to submit a STR. Confidentiality pursuant to Section 38(1) of the AML Act in such cases shall apply only to the STR, not to the seizure of assets pursuant to sanctions regulations. The party affected by the seizure of assets may be informed and has the possibility to seek annulment of the restriction in court. This person may also contend that he/she is not the party upon whom the sanctions should be imposed (identical or similar names, misidentification, etc.). Such seizure is not limited in time like the seizure measure pursuant to Section 20 of the AML Act, but prevails for the duration of the sanctions.

13 Technical and personnel measures ensuring postponement of the fulfilment of a customer's order and compliance with the information obligation within the stipulated time limit

All necessary acts shall be ensured by the Division of Prevention of Money Laundering and Financing of Terrorism. The authorised person pursuant to Article 10 of this Directive is responsible for its activities.

13.1 Performance of the notification obligation

At the request of the FAO and within a time limit that the FAO sets, SYNOT shall:

- provide information about transactions related to the identification obligation or transactions investigated by the FAO;
- submit documents about these transactions or permit authorised FAO staff to access them during the verification of an STR and performance of administrative supervision;
- provide information about persons involved in the concerned transactions in any way.

Before establishing a business relationship or carrying out a transaction outside of a business relationship, SYNOT shall provide customers with the information required under Act No. 101/2000 Coll., on personal data protection, or other similar legislation. This information consists mainly in a general notification about SYNOT's obligations to process personal data for the purposes of preventing ML/FT.

13.2 Measures when postponing the fulfilment of a customer's order

A decision of the FAO to suspend the fulfilment of a customer's transaction may be conveyed verbally, by telephone or by electronic means, although a written copy of the decision must always be subsequently delivered.

If SYNOT reports a suspicious transaction to the FAO, the basic postponement period, including any extensions, applicable to the customer's transaction shall begin to run from the moment the FAO receives the report.

If SYNOT fails to report a suspicious transaction to the FAO, and the latter decides to postpone the customer's transaction or to seize its assets, the start of this time limit shall be determined in an announcement of the decision of the FAO.

SYNOT shall promptly confirm to the FAO the postponement of the fulfilment of the customer's order, the extension of the time limit, or the seizure of the relevant assets, and confirm the time when this period starts to run.

SYNOT shall further provide the FAO with information about all substantial facts related to the assets specified in the decision (e.g. attempts to break the freezing of the assets).

If the FAO fails to notify SYNOT by the end of the stipulated period that it has filed a criminal complaint, or cancels its decision before the lapse of the freezing period, SYNOT may fulfil the customer's order.

If the FAO files a criminal complaint with the criminal authorities, the suspension of the customer's order or seizure of the customer's assets shall be extended by 3 business days from the date on which the relevant criminal complaint is filed. The FAO shall notify SYNOT of the filing of a criminal complaint. SYNOT shall thus fulfil the customer's order at the earliest upon the lapse of 3 business days from the filing of the criminal complaint, but only in cases where the criminal authorities decide not to confiscate or freeze the assets concerned in the suspicious transaction. The period of 3 business days shall end either upon the expiry of this period, or sooner if the criminal authorities take the necessary measures to confiscate the assets before the expiry of this period. (The period of 3 business days is counted from the beginning of the day following that on which the FAO files a criminal complaint).

14 Description of additional measures for efficient management of the risk of legitimisation of proceeds of crime and financing of terrorism

SYNOT applies customer control and record-keeping measures at least equivalent to the requirements of European Union law in its branches, establishments and subsidiaries of business corporations operating in third countries. To that end, SYNOT transmits relevant information to these entities on the methods and procedures applied, to the extent permitted by the law of the particular country.

If a SYNOT branch or establishment is located in another Member State of the European Union or in a country forming the European Economic Area, SYNOT shall ensure that the branch or establishment complies with national regulations in the field of combating money laundering and financing of terrorism of that other Member State of the European Union or country of the European Economic Area.

15 Confidentiality provisions

The confidentiality obligation particularly serves for:

- uninterrupted progress of the investigation of a suspicious transaction;
- protecting processed and stored data for the duration of the period until the results of the investigation are handed over to another authority;

- preserving the possibility of using measures to seize assets in potential subsequent criminal proceedings;
- protecting persons who report suspicious transactions from threats or hostile acts.

The confidentiality obligation applies to:

- the submission of an STR and its investigation;
- seizure of assets;
- fulfilment of the notification obligation to the FAO.

The confidentiality obligation applies to SYNOT and its employees, and does not expire upon the re-assignment of SYNOT employees to other work, the termination of their labour-law or other contractual relationship with SYNOT, or even in the event that SYNOT ceases to perform its activities.

All persons who learn any confidential facts are obliged to keep them secret.

16 Provisions for ensuring staff training

SYNOT shall ensure at least once during a period of 12 calendar months training of employees who could encounter suspicious transactions in the course of their work activities, and training of all employees prior to their assignment to such job positions.

SYNOT shall also ensure and take responsibility for training of persons involved in its activities under an agreement other than an employment contract, if such persons could encounter suspicious transactions when performing their duties.

The content of training particularly includes classification and indications of suspicious transactions, requirements set by the obliged party for identifying and verifying customers, procedures for detecting customer risk factors, and procedures to follow when a suspicious transaction is detected. SYNOT continuously complements and updates its training.

17 Binding force and effect

SYNOT continuously monitors development and changes in the fight against ML/FT (i.e. laws, decrees, government regulations, etc.) and trends in the development of risks related to this area. The relevant regulations are published by the FAO at the website <http://www.financnianalytickyurad.cz/> and the Czech National Bank at the website www.cnb.cz/cs/dohled_financni_trh/legislativni_zakladna.

If the relevant regulations are amended or new regulations come into force, SYNOT shall always amend the content of this document to comply with such regulations, and shall also ensure training for all persons affected by such changes. Similarly, SYNOT shall adopt necessary additional measures aiming to mitigate newly detected risks.

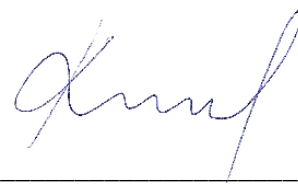
This Directive is binding for all employees of SYNOT Group and all persons performing relevant activities for SYNOT who may encounter suspicious transactions during their activities. The Directive shall enter into force and effect on 1 June 2021.

Some companies belonging to the SYNOT Group apply their own measures against legitimisation of proceeds of crime and financing of terrorism, and have their own system of internal principles, procedures and control measures aiming to prevent

legitimation of proceeds of crime and financing of terrorism, as they are primarily obliged entities pursuant to the AML Act and this obligation is directly imposed on them by law.



Ivo Valenta
founder of the SYNOT Group



JUDr. Andrej Kucbel
Head of the AML / CFT
Division

List of countries considered high-risk by the EU and FATF:

<u>Country</u>	<u>ISO</u>
<u>Afghanistan</u>	<u>AFG</u>
<u>Albania</u>	<u>ALB</u>
<u>Bahamas</u>	<u>BHS</u>
<u>Barbados</u>	<u>BRB</u>
<u>Botswana</u>	<u>BWA</u>
<u>Ghana</u>	<u>GHA</u>
<u>Iraq</u>	<u>IRQ</u>
<u>Iran</u>	<u>IRN</u>
<u>Iceland</u>	<u>ISL</u>
<u>Jamaica</u>	<u>JAM</u>
<u>Yemen</u>	<u>YEM</u>
<u>Cambodia</u>	<u>KHM</u>
<u>North Korea</u>	<u>PRK</u>
<u>Laos</u>	<u>LAO</u>
<u>Mauritius</u>	<u>MUS</u>
<u>Mongolia</u>	<u>MNG</u>
<u>Myanmar</u>	<u>MMR</u>
<u>Nicaragua</u>	<u>NIC</u>
<u>Pakistan</u>	<u>PAK</u>
<u>Panama</u>	<u>PAN</u>
<u>Syria</u>	<u>SYR</u>
<u>Trinidad and Tobago</u>	<u>TTO</u>
<u>Uganda</u>	<u>UGA</u>
<u>Vanuatu</u>	<u>VUT</u>
<u>Zimbabwe</u>	<u>ZWE</u>

List of countries with international sanctions:

<u>Country</u>	<u>ISO-3</u>	<u>ISO-2</u>
<u>Afghanistan</u>	<u>AFG</u>	<u>AF</u>
<u>Belarus</u>	<u>BLR</u>	<u>BY</u>
<u>Bosnia and Herzegovina</u>	<u>BIH</u>	<u>BA</u>
<u>Burundi</u>	<u>BDI</u>	<u>BI</u>
<u>Democratic Republic of the Congo</u>	<u>COD</u>	<u>CD</u>
<u>Egypt</u>	<u>EGY</u>	<u>EG</u>
<u>Guinea</u>	<u>GIN</u>	<u>GN</u>
<u>Guinea-Bissau</u>	<u>GNB</u>	<u>GW</u>
<u>Iraq</u>	<u>IRQ</u>	<u>IQ</u>
<u>Iran</u>	<u>IRN</u>	<u>IR</u>
<u>Yemen</u>	<u>YEM</u>	<u>YE</u>
<u>South Sudan</u>	<u>SSD</u>	<u>SS</u>
<u>Lebanon</u>	<u>LBN</u>	<u>LB</u>
<u>Libya</u>	<u>LBY</u>	<u>LY</u>
<u>Mali</u>	<u>MLI</u>	<u>ML</u>
<u>Moldova</u>	<u>MDA</u>	<u>MD</u>
<u>Myanmar</u>	<u>MMR</u>	<u>MM</u>
<u>Nicaragua</u>	<u>NIC</u>	<u>NI</u>
<u>Russia</u>	<u>RUS</u>	<u>RU</u>
<u>North Korea</u>	<u>PRK</u>	<u>KP</u>
<u>Somalia</u>	<u>SOM</u>	<u>SO</u>
<u>Central African Republic</u>	<u>CAF</u>	<u>CF</u>
<u>Sudan</u>	<u>SDN</u>	<u>SD</u>
<u>Syria</u>	<u>SYR</u>	<u>SY</u>
<u>Tunisia</u>	<u>TUN</u>	<u>TN</u>
<u>Turkey</u>	<u>TUR</u>	<u>TU</u>
<u>Ukraine</u>	<u>UKR</u>	<u>UA</u>
<u>Venezuela</u>	<u>VEN</u>	<u>VE</u>
<u>Zimbabwe</u>	<u>ZIM</u>	<u>ZW</u>

National list of PEPs:

President of the Republic + Head of the Office of the President of the Republic

Prime Minister

Head of the Central Government Authority and its representatives (Deputy Minister, Secretary of State):

- Ministry – Minister, Deputy Minister, Deputy Minister for Section Management, Secretary of State,
- Czech Statistical Office - President, Vice-Presidents,
- State Administration of Land Surveying and Cadastre – President, Vice-President,
- Czech Mining Office – Chair, Deputy Chair – Director of the Mining Administration Section,
- Industrial Property Office - President, Representatives,
- Office for Protection of Economic Competition – President, Vice-Presidents,
- State Material Reserves Administration – President, Deputies,
- State Office for Nuclear Safety – President, Section Directors,
- National Security Authority – Director, Deputy Directors,
- Energy Regulatory Office – President of the ERO Council, members of the ERO Council,
- Office of the Government of the Czech Republic – Head of the Office of the Government, Deputy Minister for Section Management, Secretary of State,
- Czech Telecommunications Office – President of the CTO Council, members of the CTO Council,
- Personal Data Protection Office – President, Vice-Presidents,
- Council for Radio and Television Broadcasting – President, Vice-Presidents,
- Office for Economic Supervision of Political Parties and Political Movements – President, Members of the Office,
- Transport Infrastructure Access Authority – President, Vice-President,
- National Cyber and Information Security Agency – Director, Deputies,
- National Sports Agency – President, Vice-Presidents,

Member of Parliament of the Czech Republic

- Deputy,
- Senator,
- Head of the Office of the Chamber of Deputies,
- Head of the Office of the Senate,

Member of a political party's and political movement's governing body – President, Vice-Presidents,

Heads of local governments

- Mayor
- Deputy Mayor,
- Secretary of the Municipal Authority,
- Director of the Prague City Hall,
- Regional Council President,

- Regional Council Vice-President,
- Director of the Regional Office,
- Mayor of a Municipality with Extended Powers,

Judge of the Supreme Court, Constitutional Court or other supreme judicial authority against whose decision, generally with a few exceptions, no appeals may be lodged

- Constitutional Court Judge,
- Supreme Administrative Court Judge,
- Supreme Court Judge,
- Prosecutor General,

Member of the Bank Board of the Central Bank

- Governor,
- Vice-Governor,
- member of the Bank Board of the Czech National Bank

High-ranking officer of armed forces or corps

- Police of the Czech Republic – Police President, Heads of Regional Directorates of the Police of the Czech Republic,
- General Inspection of Security Forces — Director,
- Security Information Service – Director,
- Military Intelligence – Director,
- Office for Foreign Relations and Information – Director,
- Army of the Czech Republic – Chief of General Staff of the Army of the Czech Republic, Heads of Regional Military Commands,
- Castle Guard – Commander,
- Military Office of the President of the Czech Republic – Chief of Staff,

Member or representative of a member, if it is a legal person, statutory body of a business corporation controlled by the state – a member of the Board of Directors, as well as any other member of the administrative, management or control body of a business corporation owned by the state (a business corporation in which the Czech Republic directly or indirectly owns more than a 50% share),

An ambassador or head of a diplomatic mission, or a natural person who exercises or has exercised any similar function in another country, body of the European Union, or an international organisation,

- Ambassadors,
- Consuls General,
- Chargé d'affaires,
- MP of the European Parliament,
- Member of the European Commission,
- Judge of the Court of Justice of the European Union, of the European Court of Human Rights, of the International Court of Justice, of the International Criminal Court, or of another international court,
- Representative of the Czech Republic in the European Central Bank, the European Court of Auditors, the Council of Europe, NATO, the United Nations (including its funds, programmes, associated organisations and specialised agencies such as IMF, UNESCO, WTO, etc.), OECD, WTO, EUROPOL, MOV, OSCE, etc.