Metodické doporučení

KTERÝM SE DEFINUJE MINIMÁLNÍ ROZSAH DUE DILIGENCE A ŘÍZENÍ RIZIK SPOLUPRÁCE S TŘETÍMI STRANAMI V RÁMCI POSILOVÁNÍ ODOLNOSTI VYSOKOŠKOLSKÉHO A VÝZKUMNÉHO PROSTŘEDÍ VŮČI NELEGITIMNÍMU OVLIVŇOVÁNÍ

(METODICKÉ DOPORUČENÍ KE SPOLUPRÁCI S TŘETÍMI STRANAMI)

Tento dokument byl, i na základě požadavků českých vysokoškolských a výzkumných institucí a ve snaze o slaďování přístupu daných institucí k problematice nelegitimního ovlivňování na základě osvědčené praxe, vypracován v rámci Mezirezortní pracovní skupiny pro potírání nelegitimního ovlivňování ve vysokoškolském a výzkumném prostředí Ministerstvem vnitra a Ministerstvem školství, mládeže a tělovýchovy, ve spolupráci s Akademií věd ČR a v konzultaci se zástupci dalších českých vysokoškolských a výzkumných institucí.

Pro lepší přehlednost textu využíváme v textu generického maskulina, tudíž pokud hovoříme o výzkumných pracovnících, studentech apod., vždy zahrnujeme muže, ženy i nebinární osoby.

VÝKLAD POJMŮ

Pro účely této metodiky a souvisejících materiálů *Metodické doporučení, kterým se definuje minimální rozsah due diligence a řízení rizik spolupráce s třetími stranami v rámci posilování odolnosti vysokoškolského a výzkumného prostředí vůči nelegitimnímu ovlivňování*, a *Metodické doporučení k řízení rizik v oblasti bezpečnosti výzkumu na institucionální úrovni* se pojmy uvedené níže vykládají takto:

Akademická instituce

Označení používané jako alternativní pojem pro vysokoškolské a výzkumné instituce, podle kontextu společně i zvlášť.

Bezpečnostní výzkum

Bezpečnostním výzkumem se rozumí výzkumné, vývojové a inovační činnosti, jejichž cílem je identifikace, prevence, příprava a ochrana proti nezákonným jednáním nebo jednáním úmyslně poškozujícím (evropské) společenství, lidské bytosti, organizace nebo struktury, hmotné i nehmotné statky a infrastruktury, včetně zajištění operační kontinuity po takovém jednání a zmírnění jeho důsledků (také aplikovatelné v případě přírodních katastrof a průmyslových havárií).

Bezpečnost výzkumu

Bezpečností výzkumu se rozumí organizační a systémové postupy pro vyhodnocování a zvládání bezpečnostních rizik v oblasti výzkumu a vzdělávání, které snižují rizika spojená s nelegitimním

ovlivňováním ve vysokoškolském a výzkumném prostředí. Primárním cílem bezpečnosti výzkumu je komplexní ochrana výzkumného ekosystému a s ním také spojená ochrana národních a ekonomických zájmů.

Citlivá data/informace

Označení pro data a informace, které akademická instituce chrání jako předmět znalostí v rámci citlivé oblasti výzkumu a vzdělávání, nebo je považuje za důvěrné z vlastního rozhodnutí, nebo jde o data a údaje, které musí chránit na základě regulatorního požadavku státu.

Citlivé oblasti výzkumu a vzdělávání

Jde o označení oblastí výzkumu a vzdělávání, které nesou zvýšená rizika nelegitimního ovlivňování a u nichž se usiluje o jejich zvýšenou ochranu, a to:

- kritické technologie pro ekonomickou bezpečnost EU,
- vybrané obory výzkumu a vzdělávání,
- vybraná spolupráce s třetími stranami,
- zboží a technologie dvojího užití a vojenský materiál,
- to, co se daná akademická instituce sama rozhodne do této oblasti zařadit.

Cizí moc

Rozumí se tím cizí stát nebo jeho orgán anebo nadnárodní nebo mezinárodní organizace nebo její orgán, jakož i jakékoliv další fyzické osoby bez ohledu na jejich státní příslušnost a právnické osoby bez ohledu na jejich sídlo anebo místo působení, pokud se podílí, byť i jen částečně, na prosazování zájmů cizího státu či organizace formou nelegitimního ovlivňování.

Due diligence

Rozumí se tím náležitá péče představující soubor opatření, která mají eliminovat či snížit rizika nelegitimního ovlivňování akademických institucí vyplývající ze spolupráce s třetími stranami.

Identifikační údaje

1. jméno, příjmení, datum narození a státní příslušnost, jde-li o fyzickou osobu,
2. název a sídlo, jde-li o právnickou osobu, nebo
3. označení nebo název v ostatních případech, popřípadě další údaje nezbytné k jednoznačné identifikaci partnera.

Kritické technologie pro ekonomickou bezpečnost EU

Rozumí se tím seznam technologických oblastí definovaných v Doporučení Evropské komise ze dne 3. 10. 2023 o kritických technologických oblastech pro hospodářskou bezpečnost EU pro další posouzení rizik s členskými státy[1] a jeho přílohu[2].

1 COMMISSION RECOMMENDATION of 3.10.2023 on critical technology areas for the EU„s economic security for further risk assessment with Member States; C(2023) 6689 final

2 ANNEX to the Commission Recommendation on critical technology areas for the EU„s economic security for further risk assessment with Member States, C(2023) 6689 final,

Nelegitimní ovlivňování

Označení pro nežádoucí působení na lidi, rozhodování, či procesy. Zahrnuje jak vlivové působení cizí moci, tak i kriminální (např. korupční) jednání a nežádoucí lobbování. Obvykle jde o aktivity, které jsou skryté, klamavé, vynucující či korupční a které původce či původkyně nelegitimního ovlivňování (cizí moc, korupce, lobbing postupující v rozporu se zákonem, případně obecně uznávanými společenskými etickými pravidly) vykonává sám či sama anebo prostřednictvím třetí strany a které ohrožují či poškozují zájmy vysokoškolských a výzkumných institucí.
Alternativně se používá i pojem nelegitimní působení.

Partner

Rozumí se jím jakákoliv právnická či fyzická osoba, se kterou vstupují, anebo již jsou, vysokoškolské a výzkumné instituce v partnerském vztahu.

Partnerský vztah

Takový vztah či spolupráce, který je založen smlouvou o spolupráci či jiným zpravidla písemným ujednáním (např. memorandum o porozumění, o rozdělení kompetencí v řešitelských týmech) mezi akademickou institucí a třetí stranou. V některých případech se může jednat i o méně formálně či zcela neformálně uzavřený smluvní vztah (včetně konkludentního) mezi zaměstnancem či zaměstnankyní akademické instituce a třetí stranou.

Pracovník či pracovnice vysokoškolské a výzkumné instituce/ akademické instituce

Rozumí se jím student či studentka, stážista či stážistka, vysokoškolský a výzkumný pracovník či pracovnice, další zaměstnanci v pracovněprávním poměru nebo fyzické osoby v jiném smluvním vztahu s akademickou institucí, jakož i další osoby podílející se na činnosti akademické instituce.

Původce nelegitimního ovlivňování

Rozumí se jím vždy osoba, bez ohledu na to, zda jedná sama či ve prospěch nějakého státu, firmy, organizace a bez ohledu na to, jaké formy a metody nelegitimního ovlivňování využívá. Někdy je rovněž používán pojem útočník. Svoje zájmy prosazuje zpravidla v rozporu s demokratickými principy, právním řádem, ale i dobrými mravy. Snaží se najít si co možná nejjednodušší cestu k prosazování svých zájmů, přičemž v absolutní většině případů takové aktivity směřují proti nějaké fyzické osobě (v tomto případě členovi či člence akademické obce nebo zaměstnanci či zaměstnankyni akademické instituce).

Regionální studia

Označení pro vědní obory zabývající se studiem lokálních a regionálních souvislostí vývoje společnosti a životního prostředí, resp. kontextem a reáliemi daného regionu.

Třetí strana

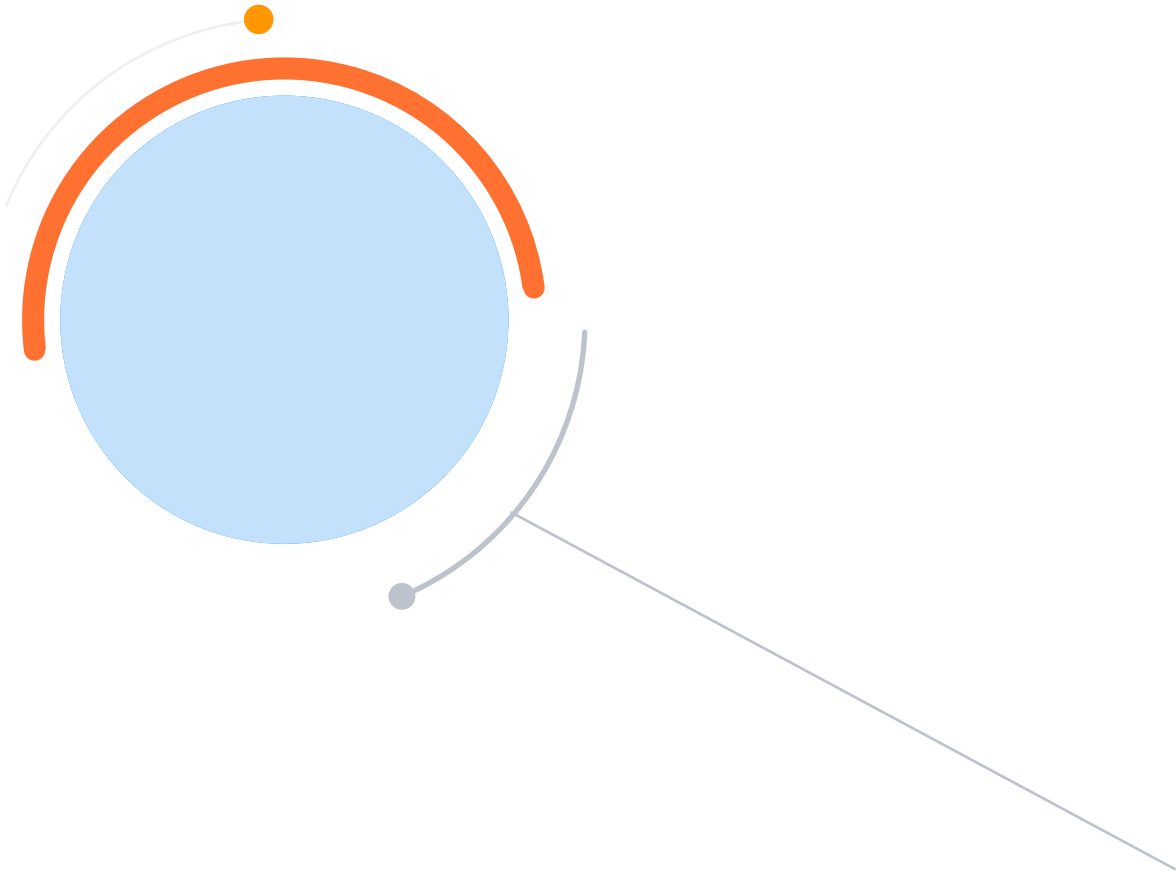
Rozumí se jí jakákoliv právnická či fyzická osoba, orgán veřejné moci nebo jiný subjekt, který zastupuje či jedná ve prospěch státu, který není členským státem Evropské unie (EU)[3], Evropského hospodářského prostoru (EHP)[4] nebo Evropského sdružení volného obchodu (ESVO)[5].

Třetí země

Rozumí se jí jiná země než ČR. Alternativně je též používán termín třetí stát.

VaVaI

Zkratka VaVaI odkazuje na výzkum, vývoj a inovace.
Ostatní použité pojmy jsou vykládány ve smyslu Sdělení Evropské komise o rámci pro státní podporu výzkumu, vývoje a inovací (2022/C 414/01).



3 https://european-union.europa.eu/easy-read_cs

4 https://www.europarl.europa.eu/factsheets/cs/sheet/169/the-european-economic-area-eea-switzerland-and-the-north; Norsko, Island a Lichtenštejnsko

5 https://eur-lex.europa.eu/CS/legal-content/glossary/european-free-trade-association-efta.html; Island, Lichtenštejnsko, Norsko a Švýcarsko

ÚVOD

Spolupráce s třetími stranami je nedílnou součástí činnosti každé vysokoškolské a výzkumné instituce. Každá taková spolupráce s sebou nese různou míru rizik, přičemž zejména rizika nelegitimního ovlivňování byla doposud řešena pouze okrajově, případně nebyla řešena vůbec. Většina této spolupráce je přínosná a nevykazuje žádná anebo jen minimální rizika nelegitimního ovlivňování. Zároveň ale existují i oblasti spolupráce vysokoškolských a výzkumných institucí s třetími stranami, které s sebou nesou rizika nelegitimního ovlivňování v takové míře, že je velmi žádoucí se ze strany vysokoškolských a výzkumných institucí pokusit tato rizika v rámci možností snižovat.

Toto metodické doporučení je součástí širší snahy vlády ČR o posílení odolnosti společnosti vůči rizikům nelegitimního ovlivňování[6]. Jeho cílem je popsat metodologický základ a minimální rozsah a postupy při provádění due diligence a řízení rizik spolupráce s třetími stranami v rámci posilování odolnosti vysokoškolských a výzkumných institucí v ČR vůči nelegitimnímu ovlivňování. Dokument slouží jako prováděcí text metodiky k „Posilování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí".

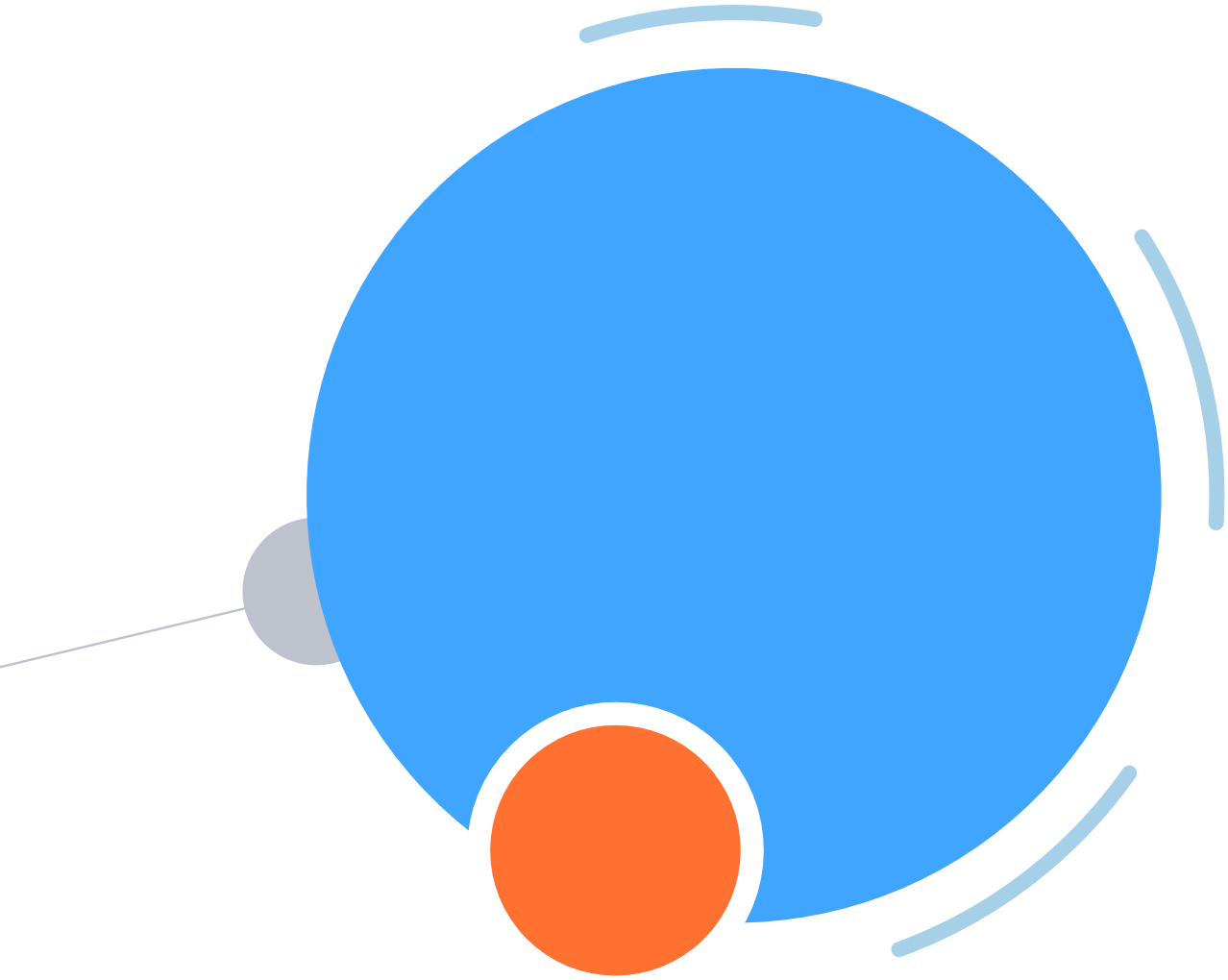
Cílem řízení rizik spolupráce s třetími stranami v žádném případě není omezování akademických práv a svobod, případně rozsahu a šíře spolupráce s externími partnery. Naopak, snahou je dosáhnout stavu, kdy budou moci vysokoškolské a výzkumné instituce a jejich zaměstnanci a členové

6 např. usnesení vlády č. 794 z 25. října 2023

akademické obce vykonávat svoje akademická práva a svobody a spolupráci s externími partnery bezpečněji.

Tento metodický dokument se primárně zaměřuje na vysokoškolské a výzkumné instituce financované z veřejných prostředků. Vysokoškolské a výzkumné instituce financované plně ze soukromých zdrojů jsou podporovány v tom, aby i ony využívaly toto metodické doporučení ve své každodenní činnosti podle svého uvážení.

Pojmy používané v tomto metodickém doporučení mají význam uvedený ve Výkladu pojmů v metodice k „Posilování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí".



I. DUE DILIGENCE

ČLÁNEK 1 ROZSAH DUE DILIGENCE

Due diligence probíhá v několika na sebe navazujících fázích od přípravy, přes vyhledávání informací z veřejně dostupných zdrojů, dalších vysokoškolských a vědeckých databází, interních informačních zdrojů, ale i informací a zkušeností získaných v rámci spolupráce s třetími stranami a dalšími akademickými institucemi, dále analýzy rizik vyplývajících z takto dohledaných informací, až po vyhodnocení a stanovení doporučení k mitigaci jednotlivých rizik.

Dělí se na **základní a podrobnou**. Základní due diligence by měla být aplikována v co možná nejširší míře, ideálně vždy když dochází k nastavování vztahů akademické instituce s novým partnerem, změně vztahů se stávajícím partnerem nebo opakovaně v průběhu dlouhotrvající spolupráce. Podrobná due diligence by měla být využívána zejména v případech, kdy jsou při provádění základní due diligence získány informace naznačující, že prověřovaná spolupráce s sebou nese rizika, která popisuje toto metodické doporučení. Každá vysokoškolská a výzkumná instituce se může rozhodnout rozšířit provádění podrobné due diligence i nad tento rámec.

Zároveň je pro obě tyto úrovně **stanoven jejich minimální rozsah**, v němž by měly být provedeny. Vysokoškolské a výzkumné instituce jsou podporovány v tom, aby využívaly informační zdroje, které mají k dispozici, i pokud nejsou v tomto textu zmíněny, neboť takové zdroje informací můžou pomoci v procesu hodnocení rizik nelegitimního ovlivňování.

V mnoha případech se také uplatní i konkrétní legislativa či další smluvně s partnerem zakotvené podmínky. Může také docházet ke změnám regulatorních požadavků ze strany vlády či zřizovatele (např. nastavením nových pravidel, uvalením sankcí na některého z partnerů, se kterými již probíhá spolupráce apod.). V takovém případě je potřeba zareagovat bez zbytečných odkladů, upravit interní dokumenty vztahující se k řízení rizik nelegitimního ovlivňování a provést úpravy i v dotčených smluvních vztazích, např. formou dodatku k původní smlouvě.

ČLÁNEK 2 ZÁSADA „POZNEJ SVÉHO PARTNERA"

Vysokoškolské a výzkumné instituce potřebují znát rizika, která se vážou na třetí strany, s nimiž mají či plánují navázat partnerské vztahy. Ve snaze o minimalizaci těchto rizik je potřeba v co nejširší míře uplatňovat zásadu „Poznej svého partnera" a to tak, aby v rámci procesu prověřování partnera a jeho důvěryhodnosti dospěla akademická instituce a její představitelé k dostatečnému poznání partnera ještě předtím, než dojde k navázání jakékoliv formální spolupráce. K naplnění zásady „Poznej svého partnera" slouží due diligence a vyhodnocení rizik, která byla takto zjištěna.

Vysokoškolské a výzkumné instituce by měly hledat odpovědi zejména na následující otázky:

1. Kdo je přesně partnerem?
2. Kde partner sídlí?
3. Kdo partnera v dané spolupráci reprezentuje?
4. Respektuje partner základní lidská práva a svobody?
5. Uvádí o sobě partner nějaké informace, které nelze jinak doložit?
6. Snaží se partner některé informace o sobě zamlčet?
7. Jak partner spolupracuje s dalšími subjekty (včetně např. řešení sporů)?
8. Podléhá partner kontrole či vlivu nedemokratických režimů?
9. Nepodílí se partner na činnosti, která by byla v ČR považována za protiprávní?
10. Neprovádí partner činnosti, které jsou v ČR považovány za neetické?

ČLÁNEK 3 RIZIKA

Absolutní většinu rizik nelegitimního ovlivňování lze zařadit do tří kategorií:

- **reputační rizika,**
- **finanční rizika a**
- **operační rizika[7].**

Ve většině případů bude docházet ke kombinaci těchto rizik. Asi největší dopad budou zpravidla všechny vysokoškolské a výzkumné instituce řešit v oblasti reputačních rizik. **Poškození dobrého jména akademické instituce mohou způsobit i aktivity, které nejsou v rozporu s právním řádem ČR a ve své ojedinělosti se mohou zdát jako bezproblémové.** Příkladem by mohla být publikační činnost v rozsahu základního výzkumu s akademiky působícími v akademické instituci třetího státu, vůči níž existují platná a právně závazná sankční (omezující) opatření. Reputační škodu způsobí ale i akade-

7 https://www.essex.ac.uk/staff/research-governance/due-diligence-risk-approach-and-policy#:~:text=Our%20Approach%20to%20Due%20Diligence,is%20able%20to%20go%20ahead

mik, který se rozhodne zpravidla kvůli získání osobního prospěchu spolupracovat se zpravodajskou službou cizí moci, nebo akademik omezující např. akademická práva a svobody ve prospěch cizí moci.

Rozsáhlé finanční škody může akademické instituci způsobit akademik, který ve snaze získat osobní prospěch předá (např. za úplatu) zástupcům cizí moci duševní vlastnictví, ke kterému má přístup. Stejně tak může závažné finanční škody zapříčinit někdo, kdo způsobí, že se takové duševní vlastnictví dostane do rukou zástupců cizí moci např. z nedbalosti. Dalším z příkladů je pak i nemožnost dosáhnout na zahraniční financování např. formou grantů v situaci, kdy je veřejně dohledatelná spolupráce akademické instituce či členů její akademické obce a zaměstnanců se subjektem sankcionovaným ze strany státu, o jehož financování se uchází.

Operační rizika[8] se mohou projevovat např. v oblasti IT, i když neplatí, že by byla nutně vázána jen na kybernetický prostor a přístup k němu. Může tak např. dojít k napadení počítačů škodlivými kódy, které způsobí jejich zašifrování a následnou nemožnost pokračovat v práci. Může také dojít k napadení systémů elektronické kontroly vstupu do určitých prostor apod. Může ale dojít i k narušení fyzické ochrany ať již u objektů, nebo u chráněných prostor uvnitř objektů a v jeho důsledku krádeži duševního vlastnictví nebo krádeži či poškození nemovitého či movitého majetku (včetně např. poškození budov a jejich zabezpečení, krádeže vybavení laboratoře, kanceláře, ...).

ČLÁNEK 4 ETICKÉ ASPEKTY

V dnešní době je pro absolutní většinu vysokoškolských a výzkumných institucí běžné, že součástí jejích vnitřních předpisů je i etický kodex. V absolutní většině případů nebylo při jejich tvorbě předpokládáno, že by mohly být využívané i jako jeden z nástrojů pro řízení rizik nelegitimního ovlivňování. I přesto lze etický kodex vnímat jako jeden z interních předpisů, jehož prostřednictvím je možné určitou část rizik nelegitimního ovlivňování ošetřit. Doporučujeme proto jednotlivým akademickým institucím zvážit provedení novelizace znění jimi užívaných etických kodexů.

Některé etické kodexy již dnes obsahují požadavky, které mohou být v procesu řízení rizik nelegitimního ovlivňování využitelné. Jedná se např. o:

1. požadavek, aby nedocházelo ke střetu zájmů akademika jako zaměstnance a reprezentanta akademické instituce s jeho soukromými aktivitami, a pokud k takovému střetu zájmů dojde, pak požadavek na to střet zájmů otevřeně deklarovat,
2. požadavek, aby si akademik byl vědom že reprezentuje akademickou instituci i navenek a choval se dle toho,
3. odmítnutí užívání nevědeckých přístupů a rasistických, genderových, náboženských, nacionalistických a politických hledisek ve vědě,
4. dodržování principů nestrannosti a nezávislosti na ideologických a politických tlacích a na zájmech nátlakových skupin.[9]

8 Operační rizika, si můžeme zjednodušeně představit jako riziko vzniku ztráty v důsledku provozních nedostatků a chyb.

9 např. https://www.avcr.cz/cs/o-nas/pravni-predpisy/eticky-kodex-vyzkumnych-pracovniku-v-av-cr/, https://www.muni.cz/o-univerzite/uredni-deska/eticky-kodex-mu a https://cuni.cz/uk-5317.html

Ne všude na světě ale přistupují k otázkám etiky a integrity stejně zodpovědně jako česká akademická obec. Řada zejména nedemokratických a totalitních režimů buď vůbec otázky etiky a integrity neřeší, anebo k nim přistupuje jako k nástroji prosazování svých zájmů.

Příklad č.1:

Zákony některých zemí požadují, aby všechny firmy, ať již státní, polostátní anebo soukromé, které operují v zahraničí, sbíraly zpravodajské informace o cizích entitách (fyzické/právnické osoby, zájmové spolky, ...) a tyto předávaly domácím úřadům.[10]

Příklad č.2:

Studenti a akademici některých zemí prochází školením v oblasti národní bezpečnosti a učí se odhalovat zahraniční špiony. V řadě případů jsou i obyčejní lidé terčem masivní mediální kampaně domácích bezpečnostních a zpravodajských složek cílící na odhalování zahraničních špionů. Za zahraniční špionáž či pokus o ni mohou být v těchto zemích považovány ale i zcela legitimní akademické aktivity. Bezpečnostní a zpravodajské složky těchto zemí si zřizují kontaktní body, kam lze podezřelé špiony hlásit. Za nahlášení zahraničního špiona lze získat finanční odměnu, která v některých konkrétních případech může dosáhnout až do výše cca 68 500 USD.[11]

Příklad č.3:

Kodexy chování vydané akademickými institucemi některých zemí zakazují akademikům vyjadřovat se k jakýmkoliv tématům, která se netýkají jejich expertízy. Zavádí mj. i společenský dohled nad akademiky nebo povinnost, aby veřejná prohlášení akademiků byla v souladu s politikou vlády a aby podporovala národně bezpečnostní zájmy státu.[12]

ČLÁNEK 5 STŘET ZÁJMŮ

Střetem zájmů rozumíme situaci, kdy více protichůdných zájmů dané osoby (zaměstnanec či člen orgánu) narušuje objektivitu jeho rozhodování nebo jednání. Typicky jde o střet mezi zájmem na vlastním prospěchu a povinnostmi vůči zaměstnavateli. Střet zájmů obvykle vede k ohrožení nestrannosti dané osoby či nestranného výkonu jeho funkce a následné možnosti vzniku neoprávněného prospěchu pro něj samotného nebo pro osobu jemu blízkou[13].

Některé vysokoškolské a výzkumné instituce ze zemí demokratického světa řeší část rizik nelegitimního ovlivňování i posuzováním toho, zda u jejich zaměstnanců nedochází ke střetu zájmů. Jednotliví akademici zpravidla jednou ročně vyplní čestné prohlášení, kam zaznamenají svoje zahraniční aktivity, spolupráci s akademiky a dalšími partnery z třetích států a dále také veškeré zahraniční financování, které v daném kalendářním roce získali anebo o něž se uchází. V případě zvýšeně chráněných citlivých oblastí výzkumu a vzdělávání jsou tato čestná prohlášení důkladně zkontrolována

10 https://foreignpolicy.com/2023/09/20/china-shipping-maritime-logistics-lanes-trade-ports-security-espionage-intelligence/

11 https://www.economist.com/china/2023/09/21/china-tells-its-citizens-to-be-on-the-lookout-for-spies

12 https://www.universityworldnews.com/post.php?story=20230914145456163

13 https://www.muni.cz/o-univerzite/uredni-deska/eticky-kodex-mu

a provedením due diligence je ověřeno, zda předkladatel čestného prohlášení neopomněl či záměrně nevynechal některé informace zejména o spolupráci či financování ze strany rizikových partnerů. U ostatních čestných prohlášení bývá taková kontrola provedena jen na náhodném vzorku. Pokud jsou ale ze strany akademické instituce kdykoliv v průběhu roku zjištěny informace, které by mohly naznačovat, že některý z akademiků by se mohl dopouštět spolupráce s partnery, kteří by jinak byli vyhodnoceni jako rizikoví, či od nich přijímá nedeklarované a ze strany akademické instituce předem neschválené financování, tak je využívána možnost podívat se i do čestných prohlášení a porovnat jejich obsah se zjištěnými skutečnostmi. Zejména v případě zamlčení spolupráce s partnery či financování ze zemí s vysokými riziky nelegitimního ovlivňování pak bývají vyvozeny pro tyto akademiky i pracovněprávní důsledky.

Pokud se některá z českých akademických institucí rozhodne využívat tento nástroj, pak se doporučuje, aby se týkal pouze oblastí definovaných v článku 6 a aby v žádném případě nedocházelo k jeho nadužívání. Obsah čestného prohlášení si stanoví každá akademická instituce sama, nicméně neměl by překračovat rámec spolupráce s partnery (včetně získaného financování) z vysoce rizikových států (článek 7, písm. B) a spolupráce s partnery, vůči nimž jsou uplatňována platná omezující opatření (v rozsahu základní due diligence, článek 7, písm. C). Kontrola možného střetu zájmů by pak byla založená na ověření informací uvedených v čestném prohlášení a prováděna za pomoci due diligence.

ČLÁNEK 6 CITLIVÉ OBLASTI VÝZKUMU A VZDĚLÁVÁNÍ

Na základě zhodnocení dosavadních zkušeností s posilováním odolnosti akademické sféry vůči nelegitimnímu ovlivňování z ČR i zahraničí lze definovat pět základních oblastí, které s sebou nesou zvýšená rizika nelegitimního ovlivňování, a u nichž bychom měli chtít usilovat o jejich zvýšenou ochranu před tímto jednáním. Jedná se o:

A. kritické technologie pro ekonomickou bezpečnost EU,
B. vybrané obory výzkumu a vzdělávání,
C. vybraná spolupráce s třetími stranami,
D. technologie a zboží dvojího užití, vojenský materiál a
E. to, co se daná akademická instituce sama rozhodne do této oblasti zařadit.

A. Kritické technologie pro ekonomickou bezpečnost EU

K definování toho, co přesně chceme v této oblasti chránit, lze využít dokument Doporučení Evropské komise ze dne 3. 10. 2023 o kritických technologických oblastech pro hospodářskou bezpečnost EU pro další posouzení rizik s členskými státy[14] a jeho přílohu[15]. Za citlivé lze považovat všech deset oblastí technologií, které jsou obsaženy ve výše zmíněném dokumentu a jeho příloze.

14 COMMISSION RECOMMENDATION of 3.10.2023 on critical technology areas for the EU„s economic security for further risk assessment with Member States; C(2023) 6689 final, https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en

15 ANNEX to the Commission Recommendation on critical technology areas for the EU„s economic security for further risk assessment with Member States, C(2023) 6689 final, tamtéž

Jedná se o:

TECHNOLOGICKÁ OBLAST	* Technologie uvedené u každé oblasti představují pravděpodobné klíčové body pro hodnocení rizik, jejich seznam však není vyčerpávající.
1. POKROČILÉ POLOVODIČOVÉ TECHNOLOGIE	• Mikroelektronika včetně procesorů • Fotonika (včetně vysokoenergetických laserů) • Vysokofrekvenční čipy • Zařízení na výrobu polovodičů ve velmi pokročilých velikostech uzlů
2. TECHNOLOGIE UMĚLÉ INTELIGENCE	• Vysokovýkonná výpočetní technika • Cloud a edge computing • Technologie datové analýzy • Počítačové vidění a zpracování jazyka, rozpoznávání objektů
3. KVANTOVÉ TECHNOLOGIE	• Kvantové výpočty • Kvantová kryptografie • Kvantová komunikace • Kvantové snímání a radary
4. BIOTECHNOLOGIE	• Techniky genetické modifikace • Nové genomické techniky • Genový tah • Syntetická biologie
5. POKROČILÁ KONEKTIVITA, NAVIGACE A DIGITÁLNÍ TECHNOLOGIE	• Zabezpečená digitální komunikace a konektivita, jako např. RAN a otevřená RAN (rádiová přístupová síť) a 6G • Technologie pro kybernetickou bezpečnost včetně kybernetického dohledu, bezpečnostních systémů a systémů proti vniknutí, digitální forenzní analýzy • Internet věcí a virtuální realita • Technologie distribuované účetní knihy a digitální identity • Naváděcí, navigační a řídící technologie včetně avioniky a určování polohy na moři
6. POKROČILÉ SNÍMACÍ TECHNOLOGIE	• Elektrooptické, radarové, chemické, biologické, radiační a distribuované snímání • Magnetometry, magnetické gradiometry • Podvodní snímače elektrického pole • Gravimetry a gradiometry

7. VESMÍRNÉ A POHONNÉ TECHNOLOGIE	• Technologie specializující se na vesmír od úrovně jednotlivých součástí po celý systém • Technologie pro sledování vesmíru a pozorování Země • Určování polohy, navigace a času ve vesmíru (PNT) • Zabezpečená komunikace včetně připojení na nízkou oběžnou dráhu Země (LEO) • Pohonné technologie včetně hypersoniky a součástí pro vojenské použití
8. ENERGETICKÉ TECHNOLOGIE	• Technologie jaderné fúze, reaktory a výroba elektrické energie, technologie radiologické přeměny/obohacování/recyklace • Vodíková a nová paliva • Net-zero technologie včetně fotovoltaiky • Inteligentní sítě a uchovávání energie, baterie
9. ROBOTIKA A AUTONOMNÍ SYSTÉMY	• Drony a vozidla (vzdušné, pozemní, povrchové a podvodní) • Roboti a roboticky řízené přesné systémy • Exoskelety • Systémy s podporou AI
10. POKROČILÉ MATERIÁLY, VÝROBNÍ A RECYKLAČNÍ TECHNOLOGIE	• Technologie pro nanomateriály, chytré materiály, pokročilé keramické materiály, stealth materiály, materiály navržené jako bezpečné a udržitelné • Aditivní výroba včetně výroby v terénu (mimo výrobní závod) • Digitálně řízená výroba s mikropřesností a laserové obrábění/svařování v malém měřítku • Technologie pro těžbu, zpracování a recyklaci kritických surovin (včetně hydrometalurgické těžby, biologického loužení, filtrace pomocí nanotechnologie, elektrochemického zpracování a černé hmoty)

B. Vybrané obory výzkumu a vzdělávání

Za vybrané obory výzkumu a vzdělávání, u nichž spatřujeme potřebu je zvýšeně chránit a které s sebou nesou zvýšené riziko nelegitimního ovlivňování, považujeme zejména ty, které se týkají bezpečnostního výzkumu a regionálních studií, pokud se zaměřují na vysoce rizikové státy (článek 7, písm. B), aplikovaného výzkumu, v jehož rámci dochází ke spolupráci s vysoce rizikovými státy, systémy ochrany kritické infrastruktury a další obory, pokud mohou být zneužity k omezování či porušování základních lidských práv a svobod.

C. Vybraná interakce s třetími stranami

Jde zejména o spolupráci v jakékoliv formě[16] spočívající v:

- pracovních cestách do,
- přijímání zejm. pracovních návštěv z,
- navštěvujících a hostujících akademicích z,
- podpisech smluv s právnickými a fyzickými osobami z,
- spolupráci na výzkumných, vzdělávacích, komerčních a dalších projektech a
- dalších formách spolupráce s právnickými a fyzickými osobami pocházejícími z anebo majícími sídlo či státní příslušnost anebo hájícími zájmy

těch zemí, které jsou definovány v článku 7, písm. B tohoto metodického doporučení jako vysoce rizikové.

D. Technologie a zboží dvojího užití a vojenský materiál

Jedná se o všechny oblasti výzkumu či spolupráce, které lze zahrnout pod režim zák. č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálem, anebo pod režim kontroly obchodování se zbožím a technologiemi dvojího užití[17].

Technologie a zboží dvojího užití definuje Nařízení Evropského parlamentu a Rady (EU) 2021/821 ze dne 20. května 2021, kterým se zavádí režim Unie pro kontrolu vývozu, zprostředkování, technické pomoci, tranzitu a přepravy zboží dvojího užití. Zpravidla se jedná o takové druhy zboží, software a technologií, které se používají převážně pro civilní účely, jsou však použitelné i pro vojenské účely[18].

Příklad č.1:

Jen z nedávné minulosti jsou doložitelné informace o zájmu zpravodajských služeb cizí moci o informace z oblasti vývoje a aplikace vznikajících a převratných technologií, domácí a zahraniční politiky, stavby a provozu produktovodů, ale i oblasti start-upů[19] nebo potravinové bezpečnosti[20].

16 Osobně písemně, online, hybridně, ...

17 Zahraniční obchod s uvedeným zbožím a technologiemi je s ohledem na jeho citlivost sledován mezinárodními kontrolními uskupeními, v nichž Česká republika participuje s cílem aktivně a zodpovědně přistupovat k plnění jejich zásad v oblasti mnohostranné výměny zboží; https://www.mpo.cz/cz/zahranicni-obchod/licencni-sprava/mezinarodni-kontrolni-rezimy-zbozi-dvojiho-pouziti/zakladni-informace-oddeleni-mezinarodnich-kontrolnich-rezimu--10749/

18 https://eur-lex.europa.eu/CS/legal-content/summary/dual-use-export-controls.html#:~:text=Na%C5%99%C3%ADzen%C3%AD%20Evropsk%C3%A9ho%20parlamentu%20a%20Rady,%2C%2011.6.2021%2C%20s a https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:02021R0821-20231216

19 https://www.irozhlas.cz/zpravy-svet/rusky-agent-doucovani-cesko-konzulant_2211100912_afo a https://www.tyden.cz/rubriky/zahranici/evropa/rusky-spion-se-vydaval-za-cecha-aby-ziskal-informace-od-francouzskych-inzenyru_559610.html

20 https://jamestown.org/program/mss-wechat-sets-the-tone-for-the-national-security-state/

Příklad č.2:

V řadě zpravidla nedemokratických zemí je na univerzitách, ve výzkumných institucích a think tancích nezanedbatelné množství osob, které mají kontakty na domácí bezpečnostní a zpravodajské složky. Mnoho z nich pravidelně podává zprávy o svých plánovaných kontaktech s cizinci, a to jak doma, tak v zahraničí s uvedením data setkání, programu a jmen zahraničních účastníků. Proto, aby získali důvěru západních kolegů, mívají od domácích bezpečnostních a zpravodajských složek umožněno, aby prezentovali umírněnější nebo podle západních měřítek „přijatelnější" názory. To vše je ale součástí úsilí bezpečnostních a zpravodajských složek těchto nedemokratických zemí s cílem kontrolovat a omezovat svobodu slova a akademická práva a svobody[21].

Příklad č.3

Řada třetích zemí vydává různé strategie či jiné vládní dokumenty, které specifikují, na které vědní obory se zaměřuje jejich hlavní pozornost. I když nelze automaticky konstatovat, že se daná země pokusí všechny nové poznatky v těchto oborech získat pomocí technik nelegitimního ovlivňování, tak lze předpokládat, že se zástupci takové třetí země mohou pokoušet o hledání různých zkratek tak, aby učinili viditelný pokrok za kratší čas a s úsporou vynaložených vlastních finančních prostředků[22].

ČLÁNEK 7 ZÁKLADNÍ DUE DILIGENCE

Základní úroveň due diligence se skládá z pěti jednoduchých kroků:

A. vyhodnocení citlivosti oblasti výzkumu či spolupráce,
B. vyhodnocení rizikovosti státu, ze kterého pochází partner,
C. ověření, zda jsou vůči partnerovi uplatňovány v ČR právně závazné sankce,
D. ověření identifikačních údajů partnera a
E. ověření rizikových požadavků.

A. Citlivost oblasti výzkumu či spolupráce

Do oblastí výzkumu či spolupráce, které jsou považovány za **zvýšeně citlivé**, a tudíž i za oblasti s vysokými riziky jsou zařazeny ty, které jsou definovány v článku 6 tohoto metodického doporučení.

V případě, že posuzovaná oblast výzkumu či spolupráce spadá mezi tyto výše definované oblasti, je nutné provést podrobnou due diligence (článek 8). Všechny ostatní oblasti výzkumu či spolupráce jsou zařazeny mezi **nízce rizikové** a stačí u nich provést základní due diligence.

B. Stát, ze kterého pochází partner

Za stát, ze které pochází partner, považujeme takový stát, jehož je fyzická osoba státním příslušníkem, stát, kde má trvalý či přechodný pobyt anebo stát, pro jehož instituci vykonává činnost (ať

21 https://raport.valisluureamet.ee/2024/en/

22 https://isdp.eu/content/uploads/2018/06/Made-in-China-Backgrounder.pdf a https://julkaisut.valtioneuvosto.fi/handle/10024/163963

již v rámci pracovně právního nebo dodavatelského vztahu). U právnické osoby je tím myšlen stát, v němž má daná právnická osoba své sídlo, případně svojí registrovanou pobočku.

Mezi státy, k nimž se vážou **nízká rizika** a postačí u nich provést jen základní due diligence, patří všechny členské státy Evropské unie, Evropského hospodářského prostoru a Evropského sdružení volného obchodu.

U států, které jsou spojeny **s vysokou mírou rizika**, je třeba provést podrobnou due diligence (článek 8). Jedná se o následující kategorie států:

- státy uvedené jako rizikové v aktuální **Bezpečnostní strategii ČR**,
- státy, proti nimž nebo proti jejichž státním příslušníkům je vydáno platné omezující národní opatření (např. formou usnesení vlády, nařízení vlády, či zákona[23]),
- všechny státy, vůči jejichž představitelům existují platná omezující opatření EU a které jsou zároveň uvedené na **EU Sanctions Map**.

Všechny ostatní státy jsou pak vnímány jako státy se **střední mírou rizika**. V takovém případě je plně dostačující provedení základní due diligence.

Vhodnou pomůckou pro další určení míry rizik nelegitimního ovlivňování u středně rizikových států je **Index akademické svobody**. V něm jsou všechny státy světa seřazeny na základě pěti kritérií (svoboda zkoumat a učit, svoboda akademické spolupráce a šíření informací, institucionální nezávislost, integrita a svoboda akademického a kulturního projevu). Výsledkem je stanovení statusu akademické svobody v daném státě, který může nabývat hodnot od 1 (největší míra akademické svobody) až po 0 (nejmenší míra akademické svobody). U států, které jsou v Indexu akademické svobody zařazeny do rozmezí 0–0,2 se však doporučuje provést podrobnou due diligence.

C. Právně závazné sankce

Mezinárodní sankce jsou souhrn omezujících opatření, jež mezinárodní společenství používá jako nástroj k udržení nebo obnovení mezinárodního míru a bezpečnosti, k ochraně základních lidských práv a k boji proti terorismu.

Co v ČR rozumíme pod pojmem mezinárodní sankce stanoví § 2 zák. č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů. Tyto mezinárodní sankce jsou **právně závazné a vynutitelné**.

Každý, kdo udržuje nebo hodlá navázat jakékoli obchodní, akademické nebo i jiné styky s partnery z rizikových států si proto musí včas ověřit, zda jeho partner není uveden mezi subjekty, na něž se v ČR právně závazné sankce vztahují.[24]

Aktuální seznamy sankcionovaných subjektů jsou k dispozici na webu **Sankční mapa EU**, který slouží jako zdroj k zjištění základních informací. Jeho prostřednictvím se lze dostat i k závaznému znění konkrétních omezujících opatření.

23 např. Nařízení vlády č. 55/2024 Sb., o nepřijatelnosti žádostí občanů třetích zemí o udělení oprávnění k pobytu na území České republiky podávaných na zastupitelských úřadech, ve znění pozdějších předpisů

24 https://fau.gov.cz/mezinarodni-sankce-v-cr

V rámci základní due diligence ověřte informace o partnerovi v těchto dvou zdrojích:

Sankční mapa EU

Seznam národních sankcí ČR[25]

Vedle v ČR právně závazných a vynutitelných mezinárodních sankcí uplatňují některé státy (včetně některých členských států EU) i své národní sankce. Tyto **národní sankce třetích států nejsou v ČR právně závazné ani vynutitelné**. Mohou ale být akademickými institucemi využity při hodnocení rizikovosti partnera. Při spolupráci s partnerem, který je na národním sankčním seznamu nějakého třetího státu, je vždy vhodné zvážit, zda navázáním takovéto spolupráce, její realizací či pokračováním v ní není ohrožována reputace akademické instituce, či spolupráci s partnerem ze třetího státu (včetně např. možnosti čerpat finanční prostředky).

Pro ověření, zda se partner nachází na seznamu národních sankcí některého ze třetích států, využívejte službu **Opensanctions**.

Ověření, zda se partner nachází na seznamu národních sankcí některého ze třetích států, je součástí podrobné due diligence, nicméně je na každé jednotlivé akademické instituci, aby se rozhodla, zda je chce také provádět již jako jeden z kroků obsažených v základní due diligence.

D. Ověření identifikačních údajů partnera

U fyzických osob doporučujeme minimálně ověření, zda je možné k nim dohledat informace pomocí služby **Google**[26], **LinkedIn**, ale i dostupných akademických databází, jako je např. **Web of Science**. Primárním cílem je ověření, zda souhlasí informace, které partner o sobě poskytl. Zjištěné nesoulady v oblasti zaměstnání, vzdělání, zaměření výzkumu, spolupráce s bezpečnostními složkami apod. je potřeba vnímat jako rizikové faktory. V takovém případě dochází k zahájení podrobné due diligence.

U právnických osob doporučujeme minimálně ověření jejich statutárního orgánu, názvu, registračního čísla, sídla, webové stránky apod. K ověření lze využít vždy nejméně webovou službu Google a **Opencorporates**, ale i v dostupné akademické databáze (jako je např. Web of Science). Vždy je vhodné pokusit se vyhledat lokální rejstřík právnických osob a údaje ověřit i v něm.

Za rizikové se považuje zjištění, kdy:

1. nesouhlasí sídlo nebo se sídlo nachází v netypickém prostředí (rodinný dům, virtuální sídlo, ...),
2. partner používá řadu alternativních názvů,
3. webová stránka neodpovídá tomu, jak se partner prezentuje, je vytvořena za pomoci tzv. WYSIWYG[27] editorů, deklaruje, že partner něco dělá/organizuje/pořádá, ale v otevřených zdrojích nelze o těchto aktivitách nalézt žádný záznam,

25 zák. č. 1/2023 Sb., o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích

26 U českých fyzických osob můžete využít i Seznam a u slovenských Zoznam, jako variantu ke službě Google je vhodné použít i nějaký alternativní vyhledávač, např. DuckDuckGo, Bing, DogPile apod., které mnohdy poskytnou některé výsledky, které Google nezobrazil. Tento postup aplikujte kdykoliv, kdy se v tomto dokumentu hovoří o využívání služby Google.

27 WYSIWYG (What You See Is What You Get), je zkratka, jejíž překlad znamená „Co vidíte, to získáte". Používá se k označení nástrojů, které umožňují vidět během práce na webové stránce, jak bude zobrazována v prohlížeči. Pro tvorbu webové stránky není využíván html kód, ale formátování, vytváření a vkládání obsahu probíhá podobně jako např. ve Wordu. Díky tomu tvůrce obsahu hned vidí, jak bude vytvářený příspěvek vypadat.

4. partner používá e-mailové adresy na freemailových službách (např. Gmail, Yahoo, QQ, Taobao, AOL, Mail.com),
5. partner se podílí na potlačování základních lidských práv a svobod či takové jednání otevřeně schvaluje či podporuje anebo
6. partner spolupracuje s armádními, bezpečnostními či zpravodajskými složkami třetích zemí.

Zvýšenou pozornost je potřeba věnovat i partnerům z vysoce rizikových zemí, kteří zároveň deklarují svoji vazbu na různé mezinárodní organizace (např. Organizace pro bezpečnost a spolupráci v Evropě, Mezinárodní agentura pro atomovou energii, Organizace pro zákaz chemických zbraní, Organizace spojených národů a jim podřízené organizace). V takovém případě dochází k zahájení podrobné due diligence, stejně jako když je u partnera identifikován některý z výše uvedených rizikových faktorů.

Při prověřování informací o fyzických i právnických osobách je nezbytné věnovat náležitou pozornost tomu, **aby nedocházelo k záměně fyzických a právnických osob s jinými osobami**, které mají shodné některé identifikační údaje, zpravidla jde o jméno a příjmení u fyzických osob a název u právnických osob.

E. Rizikové požadavky

Rizikové požadavky partnerů jsou takové, které jsou anebo by mohly být:

1. v rozporu se zájmy, etickými a dalšími interními pravidly akademické instituce,
2. protiprávní,
3. politického charakteru,
4. porušením zákonem chráněných základních lidských práv a svobod, či
5. v rozporu se zahraničními a bezpečnostními zájmy ČR.

Typicky se bude jednat např. o požadavky na předávání/zpřístupňování osobních informací, které nejsou vzhledem k povaze spolupráce relevantní, žádosti o zajištění víz, žádosti o provize, politická prohlášení, snahu o omezení rozsahu výuky či výzkumu, zásadní nepoměr mezi tím, co jednotlivé strany spolupráce přináší, nerovnoměrné rozložení rizik mezi partnerskými stranami apod.

ČLÁNEK 8 PODROBNÁ DUE DILIGENCE

Podrobná due diligence je nadstavbou due diligence základní, proto v sobě vždy obsahuje provedení všech jejích pěti kroků (článek 7).

1. Ověřte pomocí služby **Opensanctions**, zda jsou vůči partnerovi uplatňovány národní sankce třetích států nad rámec v ČR právně závazných sankcí nebo zda se nenachází na některém ze seznamů politicky exponovaných osob.
2. Ověřte identifikační údaje partnera v databázi **OCCRP Aleph**.
3. U fyzických osob ověřte identifikační údaje partnera v databázích **Europolu** a **Interpolu**.
4. U právnických osob ověřte identifikační údaje partnera v databázi **ASPI Tracker**.
5. Ověřte, zda partner anebo stát, ze kterého partner pochází, nejsou veřejně známí pro nedodržování demokratických hodnot a principů právního státu.

6. Je možné využít i ověření identifikačních údajů partnera v tzv. **Consolidated Screening List**, který je spravovaný americkým Ministerstvem obchodu a který v sobě sdružuje možnost vyhledávání v celé řadě amerických seznamů sankcionovaných či z jiných důvodů listovaných subjektů.
7. Ověřte všechny rizikové informace získané ať již v průběhu základní anebo podrobné due diligence v otevřených zdrojích[28].

Takto získané informace vyhodnoťte zejména s ohledem na reputační, finanční, operační a další rizika.

ČLÁNEK 9 VYHODNOCENÍ DUE DILIGENCE

Vyhodnocení rizik nelegitimního ovlivňování na základě provedené due diligence by měl vždy provádět někdo jiný než ten, kdo (kumulativně):

- bude na základě tohoto hodnocení rozhodovat o dalším postupu,
- má na spolupráci zájem či spolupráci dojednává.

Jak pro základní, tak i pro podrobnou due diligence platí, že výstup by měl být **písemný**. Dohledané rizikové **informace by měly být ozdrojované** tak, aby bylo usnadněno jejich opětovné dohledání při případné pozdější kontrole[29]. Součástí vyhodnocení due diligence by mělo být i **doporučení k mitigaci rizik** pro management akademické instituce či její samostatné součásti. Ve vyhodnocení by měla být dohledaná rizika nejen shrnuta, ale mělo by být vysvětleno i to, co z nich pro akademickou instituci vyplývá a jaké jí hrozí škody.

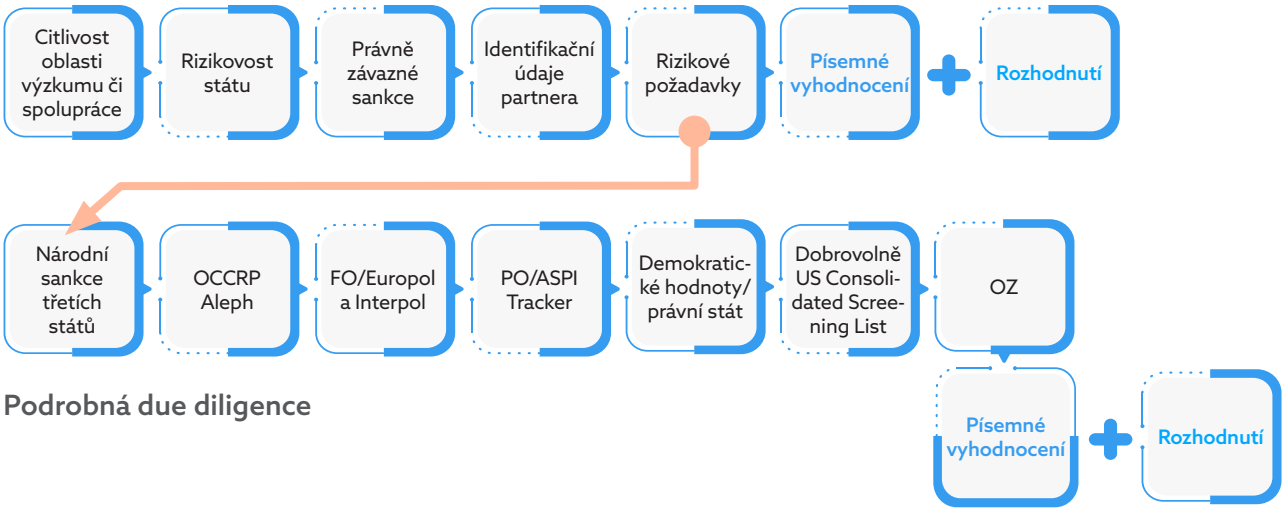
Rizika nelegitimního ovlivňování se mohou také časem vyvíjet a měnit, a proto by se u třetích stran, se kterými vysokoškolské a výzkumné instituce uzavírají dlouhodobá partnerství, měl proces vyhodnocení těchto rizik alespoň jednou za jeden až dva roky opakovat. Dále je vhodné provést novou due diligence také vždy při významné změně podmínek spolupráce a při zjištění nových informací, které by mohly mít dopad na výsledek vyhodnocení těchto rizik.

Při hodnocení rizik nelegitimního ovlivňování platí, že **hlavním cílem je umožnit akademikům spolupracovat s jejich partnery bezpečněji**, a proto by prioritou mělo být hledání cest, jak **rizika řídit, ale zároveň spolupráci uskutečnit**. Návrh zákazu spolupráce s partnerem by měl být vždy až tím nejkrajnějším řešením. Jako nejvhodnější se jeví hledání možností **řízení přístupu** partnera k citlivým informacím ať již fyzicky, anebo např. v kybernetickém prostoru.

28 Primárně za využití vyhledávačů jako jsou Google, DuckDuckGo, Firefox apod.

29 Lze doporučit uložení dohledaných zdrojových informací pro případnou pozdější kontrolu s pomocí internetových archivů, které zdarma umožňují veřejný přístup k archivovaným verzím webových stránek, např. Wayback Machine

Základní due diligence



Podrobná due diligence

FO = fyzická osoba PO = právnická osoba OZ = otevřené zdroje

II. SPOLUPRÁCE SE ZÁSTUPCI TŘETÍCH STRAN

Spolupráce s fyzickými nebo právnickými osobami, včetně těch, se kterými akademické instituce spolupracují dlouhodobě, s sebou může nést i určitá rizika. Může se stát, že spolupráce bude zneužita k neoprávněnému získání informací, znalostí, technologií či jinému druhu podpory nežádoucích zájmů třetí strany. Toto může v konečném důsledku být v neprospěch akademické instituce (ať již jednotlivce, její části či jako celku), ČR jejích partnerů nebo spojenců. Může se jednat o dopad ve sféře ekonomické či bezpečnostní, o ovlivnění tématu prováděného výzkumu nebo jiné činnosti související s odborností jednotlivých akademiků (např. odborný posudek v citlivé oblasti).

Míra zvažovaných rizik, a tudíž nutnost přijetí konkrétních opatření na jejich řízení, se odvíjí od vyhodnocení rizikovosti dané spolupráce v rámci základní anebo podrobné due diligence. Před zahájením konkrétní spolupráce je rovněž vhodné ověřit, jaká jsou akademickou institucí uplatňovaná interní pravidla a postupy pro spolupráci s třetími stranami.

ČLÁNEK 10 PÍSEMNĚ ZAKOTVENÁ SPOLUPRÁCE

Písemné zakotvení vzájemné spolupráce je klíčovým momentem potenciálně zásadně ovlivňujícím její průběh a výsledek, ale i případné širší důsledky. Může se jednat o dopad na smluvní instituci, její širší celek, stát nebo širší mezinárodní společenství, a to i v případě dokumentů, jako je například memorandum o porozumění (MoU). Na jeho základě může druhá smluvní strana požadovat kroky, které mohou mít nepříznivý dopad, popřípadě může samotnou existenci takovéhoto problematického ustanovení medializovat nebo jinak zneužít k poškození např. dobrého jména instituce.

Pokud partner požaduje, aby smluvní dokument obsahoval určité specifické pasáže, je vhodné posoudit, a to i v pohledu do budoucna, zda text:

- není pro takovýto druh dokumentu neobvyklý,
- neodporuje právnímu řádu ČR ani obecně uznávaným a zakotveným hodnotám instituce či širšího organizačního celku,
- má vůbec nějakou souvislost s oblastí vzájemné spolupráce,
- nezasahuje do oblasti působení některého z orgánů veřejné moci (např. MZV).

V takovém případě je dobré se zamyslet, jaký má partner důvod pro to, aby smlouva takový text obsahovala, co tím sleduje.

Následující pravidla a postupy poskytují přehled hlavních oblastí problémů a aspektů, které je třeba při písemném zakotvení spolupráce se třetí stranou zvažovat či aplikovat, a to ve dvou ohledech:

- v kontextu míry rizika dané spolupráce stanovené vyhodnocením due diligence,
- ve vztahu k charakteru smluvního dokumentu (memorandum o porozumění či jiný obecný rámcový dokument anebo konkrétní smlouva o spolupráci na projektu, výzkumu apod).

Vyváženost a reciprocita

Písemné ujednání o spolupráci by mělo, pokud možno vždy, zejména však v případech spolupráce, kdy je prováděna **podrobná due diligence**, obsahovat vyvážené závazky a výhody. Spolupráce by neměla být bezdůvodně výhodná pouze jednostranně. Jedná se zejména o následující otázky:

- prezentace či medializace samotné spolupráce,
- vzájemné sdílení a využívání dat a informací během dané spolupráce,
- prezentace (publikace), medializace, vlastnictví a využívání (včetně komercionalizace) výsledků a výstupů (ochrana duševní vlastnictví včetně know-how, patenty, personální zapojení apod.) spolupráce po jejím ukončení,
- přiměřenost a vyváženost sankcí,
- přiznání autorství.

Obecné právní záruky

Písemné zakotvení konkrétní spolupráce (nejčastěji formou smlouvy) musí **vždy** obsahovat dostatečně podrobný a jasný popis tématu, předmětu či oblastí spolupráce. Lépe se tak předejde situaci, kdy se bude partner v průběhu spolupráce snažit posunout zájem do oblasti, která bude již považována za citlivou či nežádoucí.

Smluvní ujednání by mělo **vždy** obsahovat popis způsobu řešení situace, kdy partner nedostojí svým finančním anebo jiným klíčovým smluvním závazkům v rámci spolupráce anebo při ní dojde ke sporu mezi smluvními partnery. Smluvní dokument by měl **vždy** obsahovat ustanovení uvádějící jaký orgán bude spor řešit a podle jakého práva. Velmi problematické může být např. řešení prostřednictvím arbitrážního orgánu partnerské země, jejíž právní systém se od českého výrazně liší a neposkytuje obvyklé adekvátní záruky na spravedlivé rozhodování. Závazek řídit se v rámci spolupráce právním řádem státu třetí strany může být rovněž velmi problematický.

Závazné smluvní dokumenty, zejména ty, které se týkají spolupráce, u níž je prováděna **podrobná due diligence**, by měly obsahovat ustanovení umožňující Vaší instituci spolupráci bez sankce omezit,

přerušit či eventuálně ukončit v případě, že dojde ze strany partnera k nějaké aktivitě, která bude v rozporu s právním řádem České republiky anebo která bude institucí vyhodnocena jako závažným způsobem poškozující její zájmy či reputaci. Smlouva musí obsahovat jasně definované podmínky, kdy ji lze vypovědět, optimálně bez sankce.

Ochrana před zneužitím spolupráce

Dokumenty smluvně upravující spolupráci, zejména tu, u níž je prováděna **podrobná due diligence,** by měly obsahovat explicitní ustanovení řešící otázku využití jejích výsledků. Jedná se např. o deklaraci odmítající využití výsledků spolupráce pro vojenské účely, k porušování lidských práv nebo etických norem.

Ochrana dobrého jména instituce a širší akademické obce ČR

V případech spolupráce definovaných v článku 6 je vhodné se vždy zamyslet nad tím, zda nemůže být spolupráce s třetí stranou zneužita k politickým účelům. Může také nastat situace, kdy bude takováto spolupráce zneužita např. k nežádoucím politickým prohlášením, jejichž důsledkem může být poškození reputace Vaší instituce. Může také dojít k situaci, kdy ve vztahu k (i zvažované) nějaké spolupráci může být na Vaší instituci vyvíjen nátlak za účelem prosazení cíle nějaké třetí strany (ať již potenciálního partnera dané spolupráce anebo jiného subjektu).

V případech spolupráce s dalšími subjekty (článek 13) je rovněž vhodné do smluvního ujednání zahrnout ustanovení bránící případným nevhodným (zejména obchodním, lobbistickým ale i soukromým či politickým) aktivitám partnera, které by mohly mít za následek poškození dobrého jména instituce.

Rovněž je vhodné zkontrolovat, zda písemné ujednání neobsahuje text, který neadekvátně či na úkor Vaší instituce a neodůvodněně posiluje dobré jméno partnera či další subjekt (např. donora), popřípadě negativně zmiňuje jiný, nezúčastněný, subjekt (např. třetí zemi). Takový text může rovněž poškodit reputaci Vaší instituce.

Ochrana akademických práv a svobod

U spolupráce, kdy je prováděna **podrobná due diligence**, je vhodné do písemného dokumentu včlenit jednoznačné vyjádření vylučující omezování akademické svobody v rámci spolupráce v souladu s příslušnými pravidly a zvyklostmi akademického prostředí ČR.

ČLÁNEK 11 ZAHRANIČNÍ CESTY

Zahraniční cesty, jako běžná součást spolupráce se třetími stranami ve vysokoškolském a výzkumném prostředí, s sebou nesou specifická rizika z hlediska nelegitimního ovlivňování. Jedná se o vědecké konference, workshopy, jazykové kurzy, studentské stáže a studijní pobyty anebo výzkumné (včetně terénního výzkumu), studijní či jiné cesty a návštěvy v partnerské akademické instituci, popř. v jiné organizaci (i soukromé cesty).

Pobyt v cizím či neznámém prostředí a upření pozornosti na cíl cesty a zároveň vnímání dalších podnětů spojených s tímto prostředím vede k větší zranitelnosti. Vytváří se tak pro útočníka příznivější podmínky k tomu, aby snadněji dosáhl svého cíle.

Před každou cestou je nutné, aby její účastník stanovil její rizikovost zejm. s ohledem na danou zemi na základě článku 7, písm. B, ve vztahu k náplni cesty dle článku 6 a rovněž s ohledem na případné sankce dle článku 7. písm. C toho se řídil následujícími doporučeními a pravidly:

A. U zahraniční cesty do státu s nízkým rizikem anebo týkající se oblasti neobsažené v článku 7, písm. B je doporučeno přinejmenším:

- nastudovat/zopakovat si základní informace pro cesty do zahraničí (interní pravidla či směrnice, **Protivlivový manuál pro sektor vysokých škol** apod.),
- zvážit možnost konzultace s odpovědným pracovníkem instituce s ohledem na specifika dané cesty (téma a program, instituce/místo atd.),
- překontrolovat rozsah informací, které lze o účastníku cesty veřejně dohledat na internetu (zejm. sociálních sítích apod.)

B. U zahraniční cesty do státu se středním rizikem je, kromě kroků v bodu A. výše, doporučeno si také ověřit následující informace a řídit se následujícími klíčovými pravidly. U vysoce rizikových států je tento postup považován za nezbytný:

- kontaktovat pracovníka zodpovědného v dané instituci za problematiku nelegitimního ovlivňování (dále jen odpovědný pracovník) a konzultovat s ním možná rizika z pohledu cíle, aktivit, popřípadě logistických aspektů cesty,
- registrovat se do cestovního systému **DROZD** spravovaného Ministerstvem zahraničních věcí ČR,
- zjistit si kulturní a jiná specifika dané země včetně pravidel či zákonných omezení týkajících se cizinců (např. omezení vývozu ze země) či akademických svobod,
- ověřit si, zda nejsou vůči partnerské instituci anebo osobám spolupráce (např. přednášející v případě konferencí či workshopů apod.) uplatněny sankce,
- ověřit si, že se na vyvážené know-how nebo zboží nevztahují omezující opatření vyplývající z mezinárodních sankcí nebo kontrolních režimů (článek 6 písm. D),
- uvědomit si, že v některých státech mohou existovat i specifické právní úpravy mající dopad na „bezpečnost" výstupů Vašich výzkumných či vzdělávacích aktivit v daném státě (možnost monitorovat Vaši online či jinou komunikaci,[30] vyžádání přístupu notebooku apod.),
- ověřit si existenci specifických pravidel pro používání prostředků kybernetické ochrany (např. VPN) v daném státě,
- po návratu z cesty (nechat) zkontrolovat (antivir, antimalware atd.) svá elektronická zařízení kvůli zjištění škodlivého software nebo jiného způsobu napadení.

30 https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/soldatov_presentation_/soldatov_presentation_en.pdf

Klíčové momenty/situace, kdy být na zahraniční cestě obezřetný:

Nezbytné informace

Jaké informace (dokumenty, soubory) si sebou (ne)vzít? Co (ne)říci o své práci?

Účastník cesty by se měl snažit omezit rozsah a dostupnost detailních informací o své osobě, předmětu/tématu zahraniční cesty, pracovních aktivitách, ale i podrobnostech o pobytu (hotel, číslo pokoje apod.). Pokud je to možné, je vhodné se tímto pravidlem řídit i u informací poskytovaných v žádosti o vízum či jiných úředních dokumentech týkajících se vstupu do cizí země.

Je vhodné si připravit pravdivou, ale obecnější, obsahově dostačující, informaci o účelu cesty, kterou lze poskytnout jako odpověď na dotaz příslušníka bezpečnostních složek, pracovníka státního orgánu, či kohokoliv jiného. I při neformálním rozhovoru, např. s kolegou z partnerské instituce, v rámci konference či společenské události může být hovor zaveden na citlivé osobní či pracovní detaily. Na tuto situaci je dobré se také připravit a být schopen téma hovoru změnit nebo jej ukončit.

I informace, které jsou někomu sdělovány při soukromém či telefonickém hovoru, mohou být vyslechnuty či zaznamenány i „nepovolanou osobou" (taxikář, personál hotelu, restaurace apod.).

Neformální a společenské události a volnočasové aktivity

Co je společenská konverzace a co už je nepřijatelný zájem o citlivé detaily mé práce či soukromí?

Častou příležitostí pro získání užitečných informací jsou pro útočníka různé společenské či jiné události a volnočasové aktivity, kdy dochází k neformální konverzaci, přičemž náchylnost k „otevřenosti" může být podpořena např. i konzumací alkoholu. V těchto situacích, ale nejen při nich, může dojít i k přílišné/neobvyklé snaze o navázání přátelství či intimního vztahu (tzv. honey trap) anebo se může hovor stočit k interním či citlivým pracovním či osobním otázkám. Této situace může být rovněž zneužito k „nesmírně lákavé" nabídce ke spolupráci anebo naopak k vydírání a následnému vynucování spolupráce. Pokud k takovéto nabídce dojde, je nutné ji rezolutně odmítnout a ihned informovat odpovědného pracovníka případně jinou relevantní osobu z instituce. Pokud se účastník cesty stane předmětem vydírání nebo jiné formy nátlaku, měl by se snažit spolupráci rovněž odmítnout a ihned o situaci náležitě informovat. Nikdy by se neměl snažit takovéto situace řešit sám.

Elektronická zařízení a datové nosiče

Jaká elektronická zařízení s sebou (ne)vzít na zahraniční cestu a jak je chránit?

V závislosti na vyhodnocení rizika cesty je dobré se nejprve zamyslet, jaká všechna zařízení s sebou účastník cesty nutně potřebuje. Pokud si s sebou hodlá vzít notebook, je vhodné zjistit, zda je v jeho organizaci možné si zapůjčit notebook „na jedno použití", tj. „čistý", kde nejsou nahrány kontakty, e-maily, kalendář, informace, které nejsou nezbytně nutné pro danou cestu, a který bude po návratu pracovníky IT oddělení náležitě prověřen a následně zformátován (u cest do vysoce rizikových států pokud možno vždy - článek 7, písm. B). Obdobně je vhodné postupovat u mobilního telefonu. U vysoce rizikových států a při spolupráci v oblastech s vysokými riziky (viz článek 6) může po vyhodnocení rizik nastat i situace, že se účastník cesty rozhodne si notebook s sebou nebrat vůbec a nahradit jej blokem a tužkou a telefon použít obyčejný, tlačítkový, s předplacenou kartou.

Velmi účinným způsobem, jak proniknout do Vašeho „prostředí" (k Vašim informacím, do sítě Vaší instituce atd.), je prostřednictvím škodlivého software či aplikace, který se do Vašeho zařízení dostane připojením cizího datového nosiče, ať již náhodně nalezeného, anebo získaného např. na konferenci nebo jako dar apod. Pokud účastník získá na pracovní cestě informace na datovém nosiči, které nelze obdržet jiným způsobem (např. emailem) a jsou pro něj důležité, **neměl** by tento **datový nosič rozhodně být připojován k žádným zařízením**, ale po návratu předán pracovníkům IT oddělení ke kontrole.

Pokud s sebou účastník cesty veze informace v elektronických zařízeních (notebook, mobil apod.) anebo na datových nosičích (zejm. flash disk), je vhodné zvážit použití některého ze způsobů šifrování (hardwarové, softwarové). Rovněž není vhodné své datové nosiče anebo elektronická zařízení půjčovat jiným osobám. Vždy je dobré mít s sebou druhý datový nosič pro případ, že bude nutné elektronické informace někomu předat. Tento náhradní nosič bude po návratu rovněž předán pracovníkům IT oddělení k prověření.

Elektronické či jiné prostředky sloužící k umožnění fyzického přístupu do prostor, elektronických či IT systémů a sítí mohou být odcizeny nebo odebrány a okopírovány, aniž si toho jejich držitel povšimne. Je proto vhodné je na zahraniční cestu s sebou nebrat.

Technická opatření

Lze se nějak chránit při práci v kybernetickém prostoru?

Základem je zabezpečení přístupu k zařízení (heslo, PIN atd.), k účtům, sítím atd. Vždy je nutné používat silná hesla, různá hesla pro různé účty a zařízení a, pokud je to možné, i dvoufázové/dvoufaktorové ověření. Bezpečnost pohybu v kyberprostoru (na notebooku, mobilním telefonu) pomůže zvýšit použití „virtuální soukromé sítě" – VPN, která ochraňuje datovou komunikaci mezi zařízením účastníka cesty a cílovým zařízením. Je proto vhodné si zjistit, zda tento bezpečnostní prvek nabízí přímo instituce účastníka cesty, případně se poradit s pracovníky IT oddělení o jiných mož.nostech.

Technické chování

Proč se nepřipojovat k veřejným internetovým sítím a z veřejně přístupných počítačů k interním systémům instituce či soukromým účtům?

Používání přihlašovacích údajů do uzavřených systémů, e-mailů, webových služeb apod. z „cizího" počítače je vysoce rizikové, neboť není možné zajistit, aby nebyly tyto údaje zaznamenány a zneužity.

Stejně tak není bezpečné se přihlašovat k „cizím" Wi-Fi sítím (veřejné sítě – hotely, letiště, kavárny) ale i uzavřeným sítím (např. v partnerské instituci, na konferenci domácí sítě apod.). Pokud je v krajním případě nutné takovéto připojení použít, vždy s využitím VPN. Rovněž je nutné se ujistit, že je na elektronických zařízeních účastníka cesty vypnuta funkce automatického připojování k Wi-Fi a připojování pomocí služby BlueTooth. Rizikem je rovněž použití cizí nabíječky elektronického zařízení, zejména těch, jejichž nabíjecí kabel zároveň může sloužit pro přenos dat.

„Zvědavost„ a chování v rozporu s ‚místními mravy"

Mohou být společenské mimopracovní aktivity rizikové?

Je třeba si uvědomit, že v různých zemích platí různé zákony, psaná pravidla i nepsané společenské zvyklosti a tolerance (konzumace alkoholu a omamných látek, intimní vztahy, dopravní přestupky, způsob jednání s úřady apod.), jejichž porušení může mít za následek zadržení míst-

ními bezpečnostními složkami, někdy i hrozbu vězením. Tato situace může být využita k vydírání a vyvinutí nátlaku k jednání ve prospěch třetí strany, tedy v neprospěch pracoviště, instituce či státu účastníka cesty.

Fyzická/vizuální kontrola osobních věcí

Proč mít svá zavazadla, a především elektronická zařízení, pokud možno stále pod kontrolou?

Elektronická zařízení včetně datových nosičů je nutné mít vždy pod kontrolou. Hotelový trezor není vhodné bezpečné úložiště pro data, která jsou citlivá a která je nutno chránit. Personál hotelu umí hotelový trezor otevřít.

Zpětná kontrola po ukončení zahraniční cesty

Co učinit se svými elektronickými zařízeními po návratu ze zahraniční cesty?

Po návratu ze zahraniční cesty by měla být elektronická zařízení zkontrolována. Je rovněž vhodné si zpětně projít případné rizikové okamžiky cesty. Pokud bude nějaká situace vyhodnocena jako anomálie nebo budící podezření, je třeba neprodleně kontaktovat odpovědného pracovníka instituce anebo pracovníky IT oddělení. I v případě, že k identifikaci žádné problematické situace nedojde, je dobré u cest do států s vysokým rizikem změnit přístupová hesla k významným informačním systémům, do vnitřní sítě apod. U středně rizikových států je vhodné toto zvážit.

Uvědomte si, že řada z výše uvedených pravidel platí již během samotné cesty do zahraničí, tj. již např na letišti či nádraží, ale i během cesty zpět!

Indikátory nestandardní situace na zahraniční cestě:

Během cesty (od jejího samotného počátku) je nutné být všímavý a obezřetný, nikoliv však paranoidní, a používat zdravý rozum. Výše popsaná pravidla se nevztahují jen na zahraniční pracovní cesty, ale v adekvátní míře je dobré se jimi řídit i při soukromých cestách do zahraničí.

Hlavní upozorněním na případnou nežádoucí situaci bude pocit, že **něco je jinak**, než je obvyklé, běžné. Následující indikátory nestandardní situace mohou napomoci si toto uvědomit:

- nestandardní průběh celní/pasové kontroly,
- snaha oddělit majitele od jeho zavazadel,
- snaha odebrat ke kontrole elektronická zařízení,
- požadavek na sdělení bezpečnostních prvků (heslo, gesto, PIN) k Vašemu zařízení,
- požadavek na sdělení přístupových údajů do elektronických systémů,
- znaky nestandardní manipulace s věcmi/jinými předměty v hotelovém pokoji během nepřítomnosti účastníka cesty, jiné anomálie (poškození zařízení, odrolená omítka, jiné nečistoty, poškozený zámek apod.),
- někdo při rozhovoru má soukromé či pracovní informace, které by mít neměl anebo nemá důvod pro to, aby je měl,
- smyšlené obvinění z porušení zákona nebo obecných pravidel s cílem vyvinout nežádoucí nátlak za účelem docílení nějaké formy jednání ve prospěch cizí moci.

Pokud k některé z popsaných situací dojde, je nutné neprodleně kontaktovat odpovědného pracovníka/nadřízeného, popř. zastupitelský úřad.

ČLÁNEK 12 NÁVŠTĚVY ZÁSTUPCŮ TŘETÍ STRANY

Kromě cest do zahraniční představují riziko pro vysokoškolské a výzkumné prostředí i návštěvy zástupců třetí strany – zahraničních partnerů (akademiků, studentů, dalších pracovníků vysokoškolských a výzkumných institucí apod., zahraničních diplomatů/pracovníků zahraniční diplomatické mise v ČR či zástupců zahraničních firem, společností či organizací). V návaznosti na posouzení rizika takovéto návštěvy vycházející z vyhodnocení due diligence lze opatření proti těmto rizikům rozdělit do třech základních oblastí (organizační, fyzické a technické), které je třeba vždy kombinovat a uplatňovat v různém rozsahu.

Při přijímání konkrétních opatření v souvislosti s pobytem zástupců třetí strany ve Vaší instituci je třeba brát vždy v úvahu **délku a typ pobytu** a **počet osob** (typ návštěvy). Tyto proměnné a jejich kombinace budou ovlivňovat podobu, rozsah a intenzitu níže popsaných přijímaných opatření.

Pobyt může mít rozsah krátkodobé (několik dnů) a jednorázové/opakované návštěvy anebo na delší časové období (semestr, rok apod.) – hostování, studijní/výzkumný pobyt, stáž. Návštěva může čítat jednu nebo několik málo osob anebo se může jednat o hromadnou akci (typicky konference).

Opatření:

1. Organizační

V závislosti na typu návštěvy a rizikovosti státu, existenci sankcí a oblasti spolupráce (článek 6, článek 7, písm. B a C) je třeba zajistit náležitou registraci včetně jejího potvrzení (a u **vysoce** popřípadě i **středně rizikových států** anebo spolupráce v **oblasti s vysokými riziky** i prověření) osob, které mají navštívit hostitelskou instituci, jejich přijetí (na recepci či jiných vstupních prostorách) včetně identifikace a ukončení (navrácení elektronických přístupových prostředků, klíčů, deaktivace individuálně přidělených/změna hromadných vstupních PIN kódů, vyhodnocení případných incidentů včetně návazné informace pro odpovědného pracovníka instituce apod.). Po ukončení pobytu návštěvy v instituci nebo jiného stanoveného období je také nezbytné provést deaktivaci všech přístupových uživatelských účtů, práv apod. U návštěv z **vysoce rizikových států** anebo týkajících se spolupráce v **oblasti s vysokými riziky** je vhodné zvážit její neustálý doprovod při pohybu v prostorách instituce.

Zahraniční návštěvy (z **vysoce rizikových států** vždy písemně) by měly být adekvátní formou poučeny o pravidlech instituce týkajících se:

- pořizování audio/videozáznamu a fotografií v prostorách instituce (předměty, dokumenty, jednání, prostory, osoby),
- tisknutí informací z IT systémů instituce, jejich kopírování na datové nosiče či jiné platformy anebo jiné způsoby přenosu dat mimo instituci (např. e-mail),
- připojování externích zařízení (flash disk, externí harddisk, mobilní telefon atd.) do zařízení či sítě instituce.

2. Fyzické

S ohledem na účel a náplň pobytu návštěvy a její typ a rovněž dle úrovně rizika, je třeba stanovit pravidla fyzického pohybu návštěvy včetně omezení jejího vstupu do určitých prostor v rámci budovy/instituce (popřípadě dalších prostor souvisejících s pracovní stránkou pobytu) a zajistit jejich dodržování. Jde o vymezení určeného prostoru, v jehož rámci se návštěva smí oprávněně pohybovat, a uplatňování a kontrolu těchto pravidel (stálý osobní doprovod, elektronické přístupové prostředky, klíče, kamery apod.). Důležité je také návštěvu s těmito pravidly srozumitelně (u **vysoce rizikových států** vždy písemně) seznámit.

S cílem zabránit úniku citlivých informací je doporučeno si pro jednání s návštěvami z vysoce rizikových států (článek 7, písm. B) vymezit zvláštní, „špinavý" prostor. Těmto návštěvám by také nikdy neměl být umožněn vstup do prostor, kde jsou řešeny citlivé informace týkající se vědy a vzdělávání (článek 6) anebo citlivé interní informace.

3. Technické

Technická opatření týkající se spolupráce se zástupci třetí strany spočívají především v přesném definování rozsahu případných přístupů do interních IT systémů vaší instituce (či její širší součásti) pro partnera, přičemž jednou z takovýchto situací je návštěva zástupců přímo ve Vaší instituci. Před zahájením spolupráce, respektive návštěvou ve Vaší instituci, vždy pečlivě zvažujte, na jakou dobu a do jakých částí Vašeho systému, k jakým částem výzkumu, datům, funkcionalitám, neveřejným informacím včetně kontaktů a informací netýkajících se předmětu spolupráce, poskytnete druhé straně přístup. Řiďte se zásadou „need to know" (daný člověk má mít přístup jen k těm informacím, které pro svoji práci nezbytně potřebuje).

Součástí technických opatření jsou rovněž technické prostředky sloužící k omezení fyzického přístupu osob do určitého prostoru anebo ke kontrole takovéhoto přístupu (např. kamery, brány, mříže apod.).

U návštěv z **vysoce rizikových států** anebo týkajících se **oblastí s vysokým rizikem** je vhodné zvážit adekvátní kombinaci všech tří typů opatření (např. neustálý doprovod návštěvy; omezený fyzický přístup do vybraných prostor; velmi omezený uživatelský přístup do systémů a k datům, popř. fyzická separace vybraných kritických dat na oddělená úložiště).

Indikátory problematického chování či jednání zástupce třetí strany:

Určité chování či situace může (avšak nutně být nemusí) být varovným signálem, že zástupce třetí strany představuje pro hostitelskou instituci riziko z hlediska nelegitimního ovlivňování. Následující indikátory se mohou vyskytnout izolovaně či kumulovaně, je však nutné je posuzovat i v širším kontextu dané návštěvy, případné širší spolupráce a dalších informací využitých v rámci procesu due diligence, popřípadě zjištěných nad rámec tohoto procesu.

Jedná se především o:

- snahu o neoprávněný vstup do jiných než určených prostor bez zjevného a opodstatněného důvodu,
- snahu o neoprávněný vstup do sítí, IT systémů či k elektronickým zařízením bez zjevného a opodstatněného důvodu,
- snahu o neoprávněné pořizování audio či video záznamu a fotografií prostor, osob, zařízení apod.,
- snahu/zájem o získání informací či dokumentů (v tištěné anebo elektronické podobě) nesouvisejících účelem či tématem návštěvy,
- neodůvodněné rozesílání nevyžádaných e-mailových či jiných druhů zpráv prostřednictvím počítače nebo mobilního telefonu členům hostitelské instituce nebo osobám s nimi spjatým anebo jiným právnickým subjektům,
- neodůvodněné odmítání spolupráce/vyžadování práce o samotě,
- odesílání velkého množství dat mimo síť instituce bez zjevného a oprávněného důvodu,

- zjevně neodůvodnitelnou aktivitu v prostorách instituce výrazně mimo standardní pracovní dobu,
- neobvyklé či neodůvodnitelné sociální chování (nepřiměřená snaha o navázání užších osobních kontaktů, znalost soukromí dalších osob z instituce apod.),
- podezřelé styky či aktivity mimo pracovní rámec návštěvy – např. neodůvodněné kontakty s pracovníky své diplomatické mise nebo dalších (mimo obor vlastního akademického působení) vysokoškolských a výzkumných institucí, soukromých firem či orgánů veřejné správy nebo bezpečnostních složek.

V případě, že se zástupce třetí strany bude v rámci pracovního programu návštěvy pohybovat i v prostorách jiné instituce, je třeba, zejména u návštěv z vysoce rizikových zemí (článek 7, písm. B) anebo při spolupráci v **oblasti s vysokými riziky** (článek 6), prodiskutovat potřebná opatření s odpovědným pracovníkem této instituce.

Rovněž je vhodné mít na paměti, že k nelegitimnímu ovlivňování ze strany zástupce třetí strany může dojít i během případných mimopracovních kontaktů (společenských, sportovních, soukromých apod.). V těchto situacích je dobré se řídit některými z pravidel uvedených v článku 11 „Zahraniční cesty" – obezřetné poskytování a sdělování informací, kontrola elektronických zařízení, nepřipojování k Wi-Fi sítím, „zdrženlivé" chování a rovněž případná konzultace s odpovědným pracovníkem.

U každé návštěvy je důležité určit/připomenout, kdo je za ni zodpovědný z hlediska realizace a kontroly dodržování nastavených pravidel a přijatých opatření.

ČLÁNEK 13 DALŠÍ SUBJEKTY A SITUACE

Z hlediska možných rizik a z nich vyplývajících pravidel spolupráce lze obdobně pohlížet i na subjekty jiného typu, jako jsou právnické či fyzické osoby sídlící v ČR (mající státní příslušnost ČR) anebo v jiném členském státě EU, které nespadají do definice „třetí strana" a které mohou být rovněž aktéry nelegitimního ovlivňování a ve prospěch třetí strany působit.

Mezi formy nelegitimního ovlivňování může v tomto smyslu také patřit např. i snaha využití záštity/jména/prostoru Vaší instituce pro komerční/soukromou/společenskou/politickou či jinou akci, která bude nějakým způsobem šíře vnímána jako kontroverzní a která Vás může poškodit reputačně, ekonomicky, popř. odborně.

ČLÁNEK 14 FINANCOVÁNÍ, DARY A POZORNOSTI

V rámci mezinárodní spolupráce není neobvyklé, že třetí strana nabídne finanční prostředky na nějaký projekt, studijní obor, zakoupení nějakého zařízení či služby, financování zahraniční cesty, sponzorský dar, grant apod. Jedná se o velmi častý způsob, kterým se třetí strana může snažit nelegitimně prosadit své zájmy, vliv anebo alespoň posílit svoji reputaci. Taková situace může být v neprospěch přijímající instituce. Vždy je proto nutné se řídit interními pravidly pro příjem darů a mimorozpočtových finančních prostředků.

Při kontaktech s třetími stranami (ale i dalšími subjekty zmíněnými v článku 13), může nastat situace, kdy protistrana bude chtít poskytnout nějaký dar (věcný, peněžní, službu či pozornost). K takové situaci může dojít jak při cestě do zahraničí, tak v rámci návštěvy protistrany ve vaší instituci, a to včetně společenského/sportovního/soukromého setkání mimo Vaše či jiné prostory související s účelem návštěvy.

Na takovou situaci je třeba být vždy připraven a dokázat správně zareagovat, jak s vědomím všech relevantních pravidel Vaší instituce, tak i kulturních specifik a zvyklostí země či kultury partnera. V některých zemích či kulturních okruzích může být odmítnutí daru nebo nějaké pozornosti považováno i za urážku. Je dobré mít na paměti, že i zdánlivě nevinné dary či upomínkové předměty (propisovací tužka, flash disk, zapalovač atd.) mohou také obsahovat elektronické zařízení pořizující audio nebo audio-vizuální záznam a případně jej odesílat někomu cizímu. Přijetí daru může být protistranou také využito k nějakému požadavku netýkajícímu se předmětu spolupráce – podrobněji viz článek 7, písm. E.

V situaci, kdy je dar či pozornost vyhodnocena jako potenciálně problematická, avšak není možné ji odmítnout, je nutné o této záležitosti co nejdříve informovat odpovědného pracovníka instituce. Takto by mělo být postupováno i v případě, že byl takovýto dar či pozornost úspěšně odmítnuta. Popsání okolností situace a způsob jejího úspěšného řešení zefektivní proces mapování incidentů nelegitimního ovlivňování a sdílení této zkušenosti pomůže se na takovéto situace lépe připravit či jim čelit i dalším kolegům (nejen) z akademické obce.

ČLÁNEK 15 INFORMOVÁNÍ O NELEGITIMNÍM OVLIVŇOVÁNÍ PŘI SPOLUPRÁCI S TŘETÍ STRANOU

Pokud je v rámci spolupráce s třetími stranami zaznamenána situace, kdy dochází k nelegitimnímu ovlivňování nebo dojde k vybavení si takové situace anebo podezření na ni zpětně, je nezbytné se neprodleně obrátit na odpovědného pracovníka instituce.

U spolupráce s nízkým rizikem (stát, oblast) v případě pouhého podezření či nejistoty je možné nejprve záležitost prodiskutovat s kolegy, kteří mají se spoluprací s daným partnerem/obdobnou spoluprací či situací výrazně větší, popřípadě nedávné zkušenosti.

Zajištění spolupráce se třetími stranami, která bude pro instituci přínosná a zároveň bezpečná, závisí na připravenosti rizikům nelegitimního ovlivňování v této oblasti čelit. K budování této odolnosti významnou mírou přispívá shromažďování, analýza a vyhodnocování (prokázaných či potenciálních) incidentů nelegitimního ovlivňování. Tento proces umožní nastavování či upravování vhodných opatření v rámci Vaší instituce a v rámci spolupráce v oblasti čelení nelegitimnímu ovlivňování v českém vysokoškolském a výzkumném sektoru i výměnu klíčových poznatků.