Srovnávací analýza vybraných modelů technických řešení sázkových her provozovaných prostřednictvím technických zařízení a návrh organizačního řešení státního dozoru nad sázkovými hrami a loteriemi

Ministerstvo financí

Březen 2013

Ernst & Young

Obsah

1. Shrnutí

1.1. Zadání projektu

Předloženou zprávu zpracovala společnost **Ernst & Young**, s.r.o. v rámci veřejné zakázky „**Srovnávací analýza vybraných modelů technických řešení sázkových her provozovaných prostřednictvím technických zařízení a návrh organizačního řešení státního dozoru nad sázkovými hrami a loteriemi**“ (dále také Projekt, srovnávací analýza dále také Zpráva) pro **Ministerstvo financí** (dále „MF“). Projekt byl zpracován v období leden – březen 2013.

Předmětem této veřejné zakázky byla (i) realizace **srovnání vybraných evropských zemí z hlediska technického řešení výkonu státního dozoru** nad trhem on-line gamblingu a následně (ii) navržení **nového modelu státního dozoru** v České republice včetně stanovení rámcových nároků tohoto modelu na zdroje.

1.2. Shrnutí hlavních závěrů

Hlavní závěry srovnávací analýzy

Při zpracování srovnávací analýzy jsme analyzovali šest hlavních parametrů. Ve většině srovnávaných parametrů je situace ve srovnávaných zemích velmi obdobná, výjimku představuje „specifikace technického řešení systému provozování a monitoringu online sázkových her“. V rámci tohoto parametru se **situace v jednotlivých zemích nejvýrazněji odlišuje zejména v oblasti využívání informačních systémů pro monitoring trhu on-line herního průmyslu ze strany národního regulátora**. V rámci naší analýzy jsme identifikovali tři hlavní modely výkonu státního dozoru v oblasti on-line herního průmyslu:

1. Model státního dozoru využívající centralizovaný informační systém pro monitoring založený na **on-line architektuře**.
2. Model státního dozoru využívající centralizovaný informační systém pro monitoring založený na **off-line architektuře**.
3. Model státního dozoru nevyužívající **žádný centralizovaný informační systém** pro monitoring.

Roli a funkce **regulátora a státního dozoru** nad sázkovými hrami a loteriemi **vykonává ve většině analyzovaných zemí samostatný úřad**. Výjimkou je Španělsko, kde vedle samostatného úřadu vykonává státní dozor také útvar v rámci Ministerstva financí a veřejné správy.

Návrh nového modelu výkonu státního dozoru

Hlavním **cílem** MF by mělo být nastavení takového způsobu výkonu státního dozoru, který mu umožní **efektivní nepřetržitou kontrolu nad děním na trhu on-line herního průmyslu**. Výkon státního dozoru by současně neměl klást enormně vysoké administrativní nároky na operátory (provozovatele platforem), ani na hráče. České regulatorní prostředí by mělo být pro operátory nastaveno takovým způsobem, aby tito operátoři měli zájem stát se součástí českého trhu a respektovat přitom český právní řád.

Z hlediska tří identifikovaných modelů výkonu státního dozoru byl v rámci projektu pro účely dosažení požadovaných cílů fungování státního dozoru **jako nejvhodnější označen model využívající centralizovaný informační systém pro monitoring založený na on-line platformě**. Tento systém umožní MF monitorovat všechny licencované operátory, resp. všechny jejich licencované platformy v reálném čase. Tento monitoring pak bude představovat účinný preventivní nástroj při boji s podvody operátorů a praním špinavých peněz a umožní MF rychle reagovat na aktuální situaci na trhu v případě potřeby.

Z hlediska srovnávaných zemí by se měl tedy český model svým charakterem nejvíce blížit italskému modelu. Centralizovaný informační systém by měl pokrývat, resp. monitorovat, všechny on-line hry povolené českým právním řádem.

Nároky nového modelu výkonu státního modelu na zdroje

V budoucnu by měl dle doporučení Evropské komise[1] i současné praxe ve většině analyzovaných zemích útvar zajišťující výkon státního dozoru disponovat širšími kompetencemi a vyšší mírou nezávislosti, než je tomu nyní. Tyto požadavky je možné zajistit prostřednictvím zřízení organizační složky státu (samostatného regulačního úřadu) formálně oddělené od MF. V případě, že by nebylo reálné zřídit tuto organizační složku státu, je možné rovněž posílit kompetence současného odboru 34 „Státní dozor nad sázkovými hrami a loteriemi" v rámci MF tak, aby tento odbor mohl provozovat nový informační systém a flexibilně reagovat na aktuální situaci na trhu herního průmyslu.

Z námi provedených rámcových odhadů založených na znalostech tvorby obdobných informačních systémů vyplývá, že:

- cena za **vytvoření** centralizovaného informačního systému pro monitoring se může pohybovat **v řádu stovek mil. Kč**, přičemž
- **roční provozní náklady** tohoto systému se mohou pohybovat **v řádu desítek mil. Kč**.

Akční plán

Pro potřeby úspěšné implementace nového technického řešení jsme identifikovali následujících sedm hlavních aktivit:

1. Příprava **nového zákona o provozování sázkových her**.
2. **Přípravné práce k uspořádání soutěže o návrh** informačního systému (IS).
3. Realizace **soutěže o návrh** architektury IS.
4. Příprava **věcného zadání veřejné zakázky** pro dodání IS.
5. Příprava **materiálu do vlády** o přípravě IS a jeho schválení.
6. Příprava a **realizace veřejné zakázky** na vytvoření a dodávku IS.
7. **Analýza a vývoj IS**.

Celkovou dobu trvání přípravy a tvorby nového modelu a technického řešení výkonu státního dozoru indikativně odhadujeme na **přibližně dva roky**. Tato doba může být významným způsobem negativně ovlivněna zejména případnými průtahy při:

- schvalování nového koncepčního uspořádání státního dozoru,
- realizace zadávacích řízení a
- tvorbě informačního systému.

Z akčního plánu nicméně vyplývá, že centralizovaný informační systém je **reálné uvést do provozu až po plánovaném datu začátku účinnosti nového zákona** o provozování sázkových her (1. 1. 2014), a to **i v případě bezproblémové realizace** všech výše uvedených aktivit.

1.3. Okolnosti limitující zpracování Zprávy

- Všechny postupy provedené v rámci projektu byly realizovány v souladu se smlouvou o poskytování poradenských služeb uzavřenou mezi Ministerstvem financí a Ernst & Young, s.r.o. a v souladu s nabídkou Ernst & Young, s.r.o. Postup zpracování Zprávy byl před její realizací i v jejím průběhu konzultován a následně odsouhlasen Ministerstvem financí.
- Při zpracování srovnávací analýzy vybraných modelů technických řešení sázkových her provozovaných prostřednictvím technických zařízení jsme vycházeli zejména z veřejně dostupných informací, informací a dokumentů získaných od regulátorů v jednotlivých zkoumaných zemích a informací poskytnutých Ministerstvem financí.

[1] Zdroj: Sdělení Komise Evropskému parlamentu, Radě a Hospodářskému a sociálnímu výboru a Výboru regionů ze dne 23. 10. 2012: Příprava uceleného evropského rámce pro on-line hazardní hry.

- Při zpracování návrhu modelu státního dozoru nad sázkovými hrami v České republice jsme vycházeli především ze společných diskusí se zástupci Ministerstva financí. Tato Zpráva by neměla být (vzhledem k rozsahu projektu, danému časovému rámci pro jeho zpracování i požadavkům MF) jediným podkladem pro tvorbu samotného systému provozování a monitoringu sázkových her provozovaných pomocí technického zařízení. Zpráva může sloužit jako úvodní „ideový“, koncepční dokument, na který by měly navázat další podrobnější studie a návrhy řešení (vedle samotné detailnější specifikace architektury systému by měly být realizovány také například analýzy nákladů a přínosů apod.).
- Tato Zpráva je určena Ministerstvu financí a měla by být vždy chápána a čtena jako nedílný celek a v kontextu informací a zvolených postupů, jež byly v době její přípravy k dispozici. Ernst & Young, s.r.o. nenesou žádnou zodpovědnost za případné škody vzniklé jakýmkoliv použitím této Zprávy.

2. Porovnání přístupů k výkonu státního dozoru v jednotlivých zemích

V této kapitole uvádíme následující informace:

- **Způsob zpracování srovnávací analýzy**, ve kterém popisujeme náš přístup k vytvoření srovnávací analýzy.
- **Shrnutí porovnání jednotlivých zemí** obsahující hlavní informace o jednotlivých zemích ve všech zkoumaných parametrech.
- **Porovnání analyzovaných parametrů v jednotlivých zemích**, ve kterém srovnáváme jednotlivé zkoumané parametry v analyzovaných zemích.
- **Charakteristiku jednotlivých zemí** obsahující popis jednotlivých zemí z hlediska všech zkoumaných parametrů.

2.1. Způsob zpracování srovnávací analýzy

Při zpracování srovnávací analýzy jsme postupovali v souladu s postupem předloženým v naší nabídce. Tento postup se skládal ze tří hlavních kroků, kterými byly:

- Potvrzení postupu a analyzovaných parametrů.
- Sběr informací a dat.
- Zpracování srovnávací analýzy.

2.1.1. Potvrzení postupu a analyzovaných parametrů

Na úvod tohoto projektu jsme se zástupci MF prodiskutovali postup navržený v naší nabídce. Nejdříve jsme si s MF na úvodní schůzce potvrdili vzorek zkoumaných zemí pro srovnávací analýzu. Těmito zeměmi byly **Dánsko, Francie, Velká Británie, Španělsko, Itálie a Malta**. V rámci projektu byla dle zadání MF srovnávána zejména technická řešení provozování sázkových her v těchto zemích.

Dále jsme si s MF rovněž na úvodní schůzce **odsouhlasili tzv. matici parametrů** (viz příloha č. 1), která byla základním nástrojem pro realizaci srovnávací analýzy, resp. pro sběr dat a informací.

2.1.2. Sběr dat a informací

Tento krok byl **klíčovým pro úspěšnost celého Projektu**. Bylo třeba získat značné množství potřebných informací a dat a **náročnost jejich získání byla vysoká**. Při získávání informací a dat jsme postupovali následujícím způsobem:

1. **Od MF jsme získali část informací, dokumentů a dat** ke srovnávaným zemím.
2. **Oslovili jsme kanceláře Ernst & Young v příslušných zemích** s žádostí o získání potřebných informací a asistence s vyplněním matice parametrů. Kolegové nám zaslali některé potřebné údaje a v některých případech navázali kontakt přímo s národními regulátory a provozovateli technických zařízení.
3. **Průběžně jsme realizovali průzkum**, ve kterém jsme se zaměřili na mapování a analyzování veřejně dostupných důvěryhodných zdrojů na internetu. Zejména se jednalo o webové stránky národních regulátorů a dalších státních institucí.
4. V dalším kroku **zaslalo MF námi připravené dopisy na národní regulátory** se žádostí o poskytnutí potřebných dokumentů, dat a informací.

Během sběru dat a informací se potvrdila naše původní domněnka, že sběr dat a informací bude časově velmi náročný. Relativně krátký termín pro zpracování srovnávací analýzy a obtížná dostupnost některých dat neumožnily získání všech nezbytných dat a informací, zejména z oblasti technického řešení centralizovaných informačních systémů pro monitoring.

2.1.3. Zpracování srovnávací analýzy

Základním nástrojem při zpracování srovnávací analýzy byla tzv. **matice parametrů**. Matice obsahovala přehled **základních parametrů** a s nimi spojených **klíčových otázek**, na které jsme hledali v rámci realizace srovnávací analýzy odpovědi.

Základní zkoumané parametry odpovídaly jak požadavkům MF, tak obecnému modelu provozování a monitoringu online hazardních her, do kterého musí být zapojeni **tři klíčoví aktéři** (státní dozor, operátor a samotní hráči) a který musí **zajistit základní funkce** (zejména ověření identifikace hráčů, boj s praním špinavých peněz a kontrolu celého systému). V rámci analýzy jsme se tedy zaměřili na následující oblasti (parametry):

- **Specifikace technického řešení systému provozování a monitoringu online sázkových her.**

  V tomto parametru jsme zkoumali zejména **základní charakteristiky systému** (tvůrce, uživatel a provozovatel systému, výše nákladů spojených se systémem, maximální počet operátorů připojených k systému apod.), **funkční specifikace systému** (funkcionality systému, data zaznamenávaná systémem, využití nástrojů „business intelligence“ apod.) a **technické specifikace systému** (charakter architektury systému, zajištění fyzické, logické, datové bezpečnosti apod.)

- **Technické požadavky na provozovatele sázkových her.**

  V tomto parametru jsme zkoumali zejména **funkční a technické požadavky na platformy operátorů** (popis minimálních technických a funkčních požadavků na operátory ze strany regulátora), **průběh kontroly hraní a sázení** (způsob sledování transakcí v reálném čase, způsob vyhodnocování získaných dat) a **způsob regulace** finančních transakcí).

- **Technické zabezpečení kontroly technických zařízení ze strany státního dozoru.**

  V tomto parametru jsme zkoumali zejména způsob využívání a charakter IT auditů, způsob plnění funkčních požadavků regulátora ze strany operátora a způsob zajištění, nastavení a realizace kontroly platforem a transakcí.

- **Metody ověření identifikace hráčů.**

  V tomto parametru jsme zkoumali zejména výčet požadovaných identifikačních dat uživatelů, způsob verifikace požadovaných identifikačních dat uživatelů, způsob ochrany identifikačních dat uživatelů a existenci a charakter seznamu blokovaných uživatelů.

- **Způsoby boje s praním špinavých peněz.**

  V tomto parametru jsme zkoumali zejména hlavní způsoby boje s praním špinavých peněz, existenci monitoringu účastníků s politickým profilem, způsob reportování podezření na praní špinavých peněz místním úřadům a způsob uchovávání dat o transakcích.

- **Monitorování podvodů při sázení a hraní.**

  V tomto parametru jsme zkoumali zejména způsob sledování a odhalování podvodů a data využívaná pro účely sledování a odhalování podvodů.

V prvním kroku jsme shromáždili **obsáhlejší relevantní data** do našich **pracovních textových dokumentů** (pro každou zemi), které byly strukturovány stejným způsobem jako matice parametrů (tzn. dle jednotlivých parametrů a otázek, na které jsme hledali odpovědi).

Ve druhém kroku jsme pak **vyplnili matice parametrů** pro každou zemi prostřednictvím **popisu stávajícího stavu** (sloupec „Popis stavu“). Matice parametrů zpracované pro jednotlivé země jsou uvedeny v příloze č. 2.

Ve třetím kroku jsme připravili **textovou srovnávací analýzu**, v rámci které jsme:

- charakterizovali jednotlivé země prostřednictvím popisu současného stavu zkoumaných oblastí (parametrů),
- provedli detailnější srovnání zemí v jednotlivých oblastech (parametrech),
- provedli srovnání jednotlivých zemí z hlediska technického řešení provozování sázkových her včetně uvedení silných a slabých stránek identifikovaných modelů státního dozoru.

2.2. Shrnutí porovnání jednotlivých zemí

V tomto shrnutí uvádíme stručný popis jednotlivých analyzovaných zemí ve všech zkoumaných parametrech a rovněž uvádíme hlavní výhody a nevýhody modelů výkonu státního dozoru v analyzovaných zemích.

V **Dánsku** je národním regulátorem využíván centralizovaný informační systém (IS) pro monitoring založený na off-line architektuře. Prostřednictvím tohoto systém regulátor pravidelně sbírá a vyhodnocuje data od operátorů. Cílem regulátora je rovněž dohled nad plněním předpisů ze strany operátorů. Národní regulátor v tomto ohledu využívá přístup, kdy po operátorech požaduje, aby mu pravidelně zasílali potvrzení o tom, že plní jím stanovené požadavky. Regulátor dále pravidelně kontroluje data ukládaná operátory do speciálně zřízeného úložiště. Operátoři mají rovněž povinnost podstupovat povinné audity ze strany regulátorem certifikovaných auditorů a zasílat výsledky těchto auditů regulátorovi. Technické platformy operátorů musí být v souladu s technickými a funkčními požadavky regulátora stanovenými právním předpisem a regulátor může kdykoliv realizovat IT audity těchto platforem, a to i s využitím třetích stran. Operátoři mají povinnost ověřovat registrující se hráče se svými interními i externími národními databázemi a registry, a mají povinnost implementovat opatření v boji proti podvodům a praní špinavých peněz.

V **Itálii** využívá národní regulátor tzv. „na míru vytvořený" komplexní centralizovaný informační systém pro monitoring dění na trhu hraní a sázení („Totallizatore"), který je provozován státem vlastněnou firmou, a je založený na on-line architektuře. Systém regulátorovi umožňuje analyzovat a vyhodnocovat data z trhu v reálném čase a díky tomu podnikat případná opatření, pokud detekuje podvody nebo praní špinavých peněz. Systém operátorovi rovněž umožňuje sledovat daňové příjmy generované herním průmyslem. Cílem operátora je tak zejména neustálý monitoring dění na trhu on-line sázení a hraní a dohled nad tímto děním. Technické platformy operátorů musí být v souladu s technickými a funkčními požadavky regulátora stanovenými v rámci veřejné výzvy k získání licence vyhlášené regulátorem. Regulátor může kdykoliv realizovat IT audity těchto platforem, a to i s využitím třetích stran. Operátoři mají povinnost ověřovat registrující se hráče a implementovat opatření v boji proti podvodům a praní špinavých peněz.

Ve **Francii** je ze strany národního regulátora využíván centralizovaný informační systém pro monitoring dění na trhu hraní a sázení založený na off-line architektuře. Operátoři mají povinnost pravidelně zasílat regulátorem stanovená data do tohoto systému, který tato data následně ex-post analyzuje a vyhodnocuje. Cílem operátora je zejména pravidelný monitoring dění na trhu on-line sázení a hraní a dohled nad tímto děním. Technické platformy operátorů musí být v souladu s technickými a funkčními požadavky regulátora stanovenými právním předpisem a regulátor může kdykoliv realizovat IT audity těchto platforem, a to i s využitím třetích stran. Operátoři mají povinnost ověřovat registrující se hráče zejména s registrem osob se zákazem hraní, který je vedený regulátorem. Operátoři mají dále povinnost implementovat opatření v boji proti podvodům a praní špinavých peněz.

Regulátor na **Maltě** využívá centralizovaný informační systém pro monitoring dění na trhu hraní a sázení založený na on-line architektuře („The Remote Gambling Monitoring System"). Tento systém disponuje pouze omezenými funkcemi a využívá veřejně dostupnou standardizovanou platformu. Cílem operátora je zejména neustálý monitoring dění na trhu on-line sázení a hraní a dohled nad tímto děním. Technické platformy operátorů musí být v souladu s technickými a funkčními požadavky regulátora stanovenými právním předpisem a regulátor může kdykoliv realizovat IT audity těchto platforem, stejně jako tzv. compliance audity, a to i s využitím třetích stran. Operátoři mají povinnost ověřovat registrující se hráče zejména se svou interní databází identifikačních údajů registrovaných hráčů. Operátoři mají dále povinnost implementovat opatření v boji proti podvodům a praní špinavých peněz.

Ve **Španělsku** využívá národní regulátor centralizovaný informační systém pro monitoring dění na trhu hraní a sázení založený na on-line architektuře. Prostřednictvím tohoto systému může regulátor ověřovat správnost fungování platforem operátorů. Cílem operátora je zejména neustálý monitoring dění na trhu on-line sázení a hraní a dohled nad tímto děním. Technické platformy operátorů musí být v souladu s technickými a funkčními požadavky regulátora stanovenými právním předpisem, zejména musí zahrnovat centrální herní jednotku a interní kontrolní systém. Regulátor může kdykoliv realizovat IT audity těchto platforem, a to i s využitím třetích stran. Operátoři mají povinnost ověřovat registrující se hráče zejména se svou interní databází identifikačních údajů registrovaných hráčů a s registrem osob se zákazem hraní vedeným regulátorem. Operátoři mají dále povinnost implementovat opatření v boji proti podvodům a praní špinavých peněz.

Regulátor ve **Velké Británii** nevyužívá žádný centralizovaný informační systém pro monitoring dění na trhu hraní a sázení. Obdobně jako v Dánsku regulátor po operátorech požaduje, aby mu pravidelně zasílali potvrzení o tom, že plní požadavky stanovené regulátorem. Cílem operátora je zejména dohlížet na plnění předpisů ze strany operátorů. Operátoři mají povinnost podstupovat povinné audity ze strany regulátorem certifikovaných auditorů a zasílat výsledky těchto auditů regulátorovi. Technické platformy operátorů musí být v souladu s technickými a funkčními požadavky regulátora stanovenými právním předpisem a regulátor může kdykoliv realizovat IT audity těchto platforem, a to i s využitím třetích stran. Operátoři mají povinnost ověřovat registrující se hráče se svými interními i externími národními databázemi a registry, a mají povinnost implementovat opatření v boji proti podvodům a praní špinavých peněz.

Souhrnná tabulka porovnávající vybrané parametry v jednotlivých zemích

Parametr / analyzovaná země	Dánsko	Itálie	Francie	Malta	Španělsko	Velká Británie
Typ centralizovaného informačního systému	Off-line	On-line	Off-line	On-line	On-line	Neexistuje
Postavení regulátora	Samostatný úřad	Samostatný úřad	Samostatný úřad	Samostatný úřad	Samostatný úřad / Útvar v rámci ministerstva	Samostatný úřad
Provozovatel centralizovaného informačního systému	Regulátor	Státem vlastněná firma SOGEI	n / a[2]	Regulátor	n / a	Irelevantní – IS neexistuje
Způsob stanovení funkčních a technických požadavků	Jednotně	Jednotně	Jednotně	Jednotně	Specificky v rámci výzvy	Jednotně
Musí být servery platforem umístěny v dané zemi?	NE	n / a	ANO	n / a	NE	ANO
Jsou povoleny hotovostní transakce?	NE	NE	NE	n / a	n / a	ANO
Jak je ID hráče ověřována?	Interní a externí databáze	n / a	Interní a externí databáze	Interní databáze	Interní a externí databáze	Interní a externí databáze

Z porovnání jednotlivých parametrů vyplývá, že situace se v jednotlivých zemích nejvýrazněji odlišuje zejména v oblasti využívání centralizovaných informačních systémů pro monitoring. V rámci naší analýzy jsme identifikovali tři hlavní modely výkonu státního dozoru úzce související s touto oblastí:

1. Model státního dozoru využívající centralizovaný informační systém pro monitoring založený na on-line architektuře.
2. Model státního dozoru využívající centralizovaný informační systém pro monitoring založený na off-line architektuře.
3. Model státního dozoru nevyužívající žádný centralizovaný informační systém pro monitoring.

U těchto modelů jsme definovali hlavní výhody a nevýhody, které dále uvádíme v souhrnné tabulce na následující straně. Pro účely definování těchto výhod a nevýhod jsme srovnávali následující kategorie:

- Možnost regulátora **rychle reagovat na situaci na trhu** díky využití business inteligence (BI) nástrojů (detekce podvodů, praní špinavých peněz, kalkulace daní apod.) využívajících data z trhu herního průmyslu v rámci modelu.
- Efektivita modelu v oblasti **prevence** podvodů a praní špinavých peněz.

[2] „N / a“ v tomto kontextu znamená, že jsme v rámci projektu neměli k dispozici potřebná data.

- Náročnost modelu na **zdroje** (finanční, personální).
- Náročnost modelu (resp. centralizovaného informačního systému) na **technickou infrastrukturu** systému a na **bezpečnost a spolehlivost** (zálohování, přenos dat, výpadky systému).
- Nároky modelu na **aktivitu operátora** (zejména vyhodnocování dat) v rámci modelu.

Hlavní výhody a nevýhody jednotlivých modelů výkonu státního dozoru

Model / zhodnocení	Hlavní výhody	Hlavní nevýhody
Centralizovaný on-line IS **Itálie, Malta, Španělsko**	▶ Regulátor má možnost využívat business intelligence (BI) nástroje v reálném čase. Díky BI nástrojům má možnost velmi rychle reagovat na případně identifikované podvody, praní špinavých peněz apod. ▶ Systém představuje efektivní nástroj pro prevenci podvodů a praní špinavých peněz.	▶ Velmi vysoké nároky na technickou infrastrukturu systému. ▶ Vysoké nároky na bezpečnost a spolehlivost systému. ▶ Náročnější a pomalejší implementace a nasazení systému ve srovnání s off-line systémem. ▶ Vysoké nároky na finanční (investiční i provozní) i personální zdroje v případě komplexního IS s mnoha funkcionalitami. ▶ Relativně vysoké nároky na aktivitu regulátora.
Centralizovaný off-line IS **Dánsko, Francie**	▶ Nižší nároky na technickou infrastrukturu systému ve srovnání s on-line systémem. ▶ Nižší nároky na bezpečnost a spolehlivost systému ve srovnání s on-line systémem. ▶ Rychlejší a méně finančně náročnější implementace a nasazení systému ve srovnání s on-line systémem. ▶ Nižší nároky na aktivitu regulátora ve srovnání s on-line systémem.	▶ Regulátor využívá BI nástroje pouze se zpožděním - nemá možnost vyhodnotit data z trhu v reálném čase a následně dostatečně rychle reagovat na případné podvody a praní špinavých peněz. ▶ Systém není tak efektivním nástrojem v prevenci podvodů a praní špinavých peněz jako on-line IS vzhledem k tomu, že regulátor nemá možnost reagovat dostatečně rychle na aktuální situaci na trhu (má k dispozici pouze zpožděná data).
Neexistence centralizovaného IS **Velká Británie**	▶ Pro regulátora se jedná o nejjednodušší model regulace - jsou kladeny relativně nízké nároky na aktivitu regulátora. ▶ Ve srovnání s modely využívajícími IS jsou kladeny nižší nároky na zdroje (finanční, personální).	▶ Regulátor nemá k dispozici aktuální data z trhu herního průmyslu – nemá možnost průběžně vyhodnocovat aktuální situaci na trhu a rychle na ní reagovat. ▶ Regulátor nemá k dispozici nástroj pro prevenci podvodů a praní špinavých peněz v podobě IS.

2.3. Porovnání analyzovaných parametrů v jednotlivých zemích

Tato kapitola vrcholově porovnává hlavní analyzované parametry v jednotlivých zemích (detailně specifikované v kapitole 2.1.3).

2.3.1. Specifikace technického řešení systému provozování a monitoringu online sázkových her

V rámci srovnání modelů technického řešení je možné provést základní rozdělení na země:

1. Využívající centralizovaný informační systém (IS) pro monitoring založený na on-line architektuře.
2. Využívající centralizovaný informační systém (IS) pro monitoring založený na off-line architektuře.
3. Nevyužívající žádný centralizovaný informační systém pro monitoring.

Charakteristika těchto tří základních modelů je uvedena dále.

1. **Model státního dozoru využívající centralizovaný informační systém pro monitoring založený na on-line architektuře**

- Do první skupiny patří **Itálie**, **Malta** a **Španělsko**. Definičním znakem centralizovaného informačního systému založeného na on-line architektuře je monitoring platforem operátorů a vyhodnocování dat získaných z těchto platforem v reálném čase. **Nejvíce propracovaným systémem** (a současně na zdroje nejnáročnějším) z těchto zemí disponuje Itálie. Tento systém nazvaný „**Totallizatore**“ je vybaven řadou funkcionalit, které umožňují například automatickou detekci podvodů a praní špinavých peněz nebo výpočet daňových příjmů generovaných on-line herním průmyslem. Protikladem Itálie je Malta využívající pro svůj systém nazvaný „**The Remote Gambling Monitoring System**“ tzv. freewarovou (nezpoplatněnou) platformu. Tento systém zvládá pouze velmi omezené množství funkcí a **nenabízí takové možnosti státního dozoru** jako italský Totallizatore, avšak je poměrně nenáročný na zdroje (je obsluhován pouze jedním IT administrátorem).
- V rámci centralizovaných informačních systémů založených na on-line platformě jsme identifikovali dvě kategorie:
  - **Systém založený na tzv. „na míru vytvořeném“ řešení**, tzv. systém postavený výhradně za účelem monitoringu on-line trhu hraní a sázení. Tímto systémem je italské Totallizatore. Za předpokladu odpovídající investice je možné tento systém vytvořit tak, aby splňoval zcela specifické požadavky regulátora a umožnil mu skutečně efektivní a propracovaný výkon státního dozoru.
  - **Systém založený na standardizovaném řešení**, kdy je využita veřejně dostupná platforma.
  - Tímto systémem je maltský “RGMS”. Využití tohoto systému neposkytuje tak efektivní možnosti výkonu státního dozoru vzhledem k tomu, že úpravy v rámci takového systému jsou limitované možnostmi platformy, na které je založen.
- Mezi jednotlivými centralizovanými informačními systémy založenými na on-line platformě jsou **značné rozdíly**, které jsou způsobeny rozdílnou komplexností a vybaveností jednotlivých systémů funkcionalitami. Srovnávané systémy se rovněž **liší** tím, jaká **data** na trhu herního průmyslu **monitorují a zaznamenávají**, a jakým způsobem je **vyhodnocují** (zda upozorňují na potenciální rizika, podvody, praní špinavých peněz, apod.).
- Pokud jsou vybaveny vhodnými funkcionalitami, představují tyto systémy **preventivní opatření** před podvody a praním špinavých peněz. Možnosti regulátora tyto případy jsou totiž veřejně známé a mohou potenciální pachatele podvodů a praní špinavých peněz od jejich jednání odradit.
- V této souvislosti uvádíme, že v průběhu realizace projektu jsme neměli k dispozici detailnější data týkající se technického řešení systému ve Španělsku.

2. **Model státního dozoru využívající centralizovaný informační systém pro monitoring založený na off-line architektuře**

- Do druhé skupiny patří ze srovnávaných zemí **Dánsko** a **Francie**. Systém provozovaný dánským regulátorem si pravidelně stahuje data ukládaná operátory do speciálně zřízených úložišť. Tato data jsou následně analyzovaná pro účely výkonu státního dozoru. Systém využívaný francouzským regulátorem pouze pasivně přijímá data zasílaná operátory (identita hráčů, informace o hráčských účtech, informace o realizovaných transakcích), kteří mají povinnost zasílat tato data v regulátorem předepsaném formátu na pravidelné bázi (obvykle každý den). Systém tato data ex-post analyzuje a vyhodnocuje, což regulátorovi umožňuje cílený výkon státního dozoru založený na zjištěních vyplývajících z těchto analýz.
- Tento druh centralizovaných informačních systémů může být (stejně jako systémy založené na off-line architektuře) rovněž vybaven nástroji k analyzování a vyhodnocování dat, nicméně tyto výsledky má regulátor k dispozici vždy se zpožděním oproti vývoji na trhu. To regulátorovi neumožňuje např. okamžitý zásah v případě identifikování podvodu nebo praní špinavých peněz.
- V této souvislosti uvádíme, že v průběhu realizace projektu jsme neměli k dispozici detailnější data týkající se technického řešení systému ve Francii.

3. **Model státního dozoru nevyužívající žádný centralizovaný informační systém pro monitoring**

- Do třetí skupiny patří **Velká Británie**. Lokální regulátor využívá namísto centralizovaného informačního systému pro monitoring odlišný přístup. Cílem regulátora je zejména ověřování, zda operátoři plní požadavky stanovené regulátorem. Na operátory jsou kladeny vysoké regulatorní nároky. Operátoři musí regulátorovi aktivně a pravidelně prokazovat, že splňují jím stanovené předpisy. Toto prokazování spočívá v testování platforem operátorů ze strany regulátorem certifikovaných auditorů třetích stran a následné zaslání výsledků testování regulátorovi.
- Z hlediska regulátora je toto zřejmě nejjednodušší model výkonu státního dozoru vzhledem k tomu, že jeho role je v tomto modelu spíše pasivní a vyčkávací.

Jednotlivé centralizované informační systémy (založené na on-line i off-line architektuře) se kromě jiného **liší i náročností jejich implementace a nasazení**. Náročnost implementace a nasazení těchto systémů se odvíjí zejména od **rozsahu funkcionalit a komplexnosti** konkrétního systému. Tato komplexnost závisí jednak na **potřebách regulátora**, a dále pak rovněž na **typu platforem** (hry, sázky, on-line kasina apod.) povolených v dané zemi a majících povinnost být k systému připojeny.

Roli a funkce **regulátora a státního dozoru** nad sázkovými hrami a loteriemi **vykonává ve většině analyzovaných zemí samostatný úřad**. Výjimkou je Španělsko, kde vedle samostatného úřadu vykonává státní dozor také útvar v rámci Ministerstva financí a veřejné správy. Níže uvádíme tabulku shrnující základní informace o regulátorech a provozovatelích centralizovaných informačních systémů pro monitoring on-line herního trhu.

Parametr / analyzovaná země	Dánsko	Itálie	Francie	Malta	Španělsko	Velká Británie
Regulátor	Dánský úřad pro hraní a sázení	Samostatný úřad pro státní monopoly	Francouzský úřad pro hraní a sázení	Úřad pro loterie, hraní a sázení	Národní komise pro hraní a sázení / Ministerstvo financí a veřejné správy	Komise pro hraní a sázení
Postavení regulátora	Samostatný úřad	Samostatný úřad	Samostatný úřad	Samostatný úřad	Samostatný úřad / Útvar v rámci ministerstva	Samostatný úřad
Provozovatel IS	Regulátor	Společnost SOGEI	Regulátor	Regulátor	Regulátor	Irelevantní – neexistuje IS

2.3.2. Technické požadavky na provozovatele sázkových her

Ve všech analyzovaných zemích jsou ze strany regulátorů stanoveny minimální funkční a technické požadavky na platformy operátorů, které se mezi jednotlivými zeměmi odlišují jak rozsahem, tak charakterem. Tyto předpisy jsou ve všech analyzovaných zemích stanoveny obecně platným právním předpisem s výjimkou Itálie, kde jsou stanoveny specificky v rámci každé veřejné výzvy k získání licence vyhlášené regulátorem.

Po operátorech se ve všech zemích požaduje, aby **monitorovali chování hráčů**, a aby zálohovali zejména data o transakcích (hraní, sázení, finanční převody). Obvykle se rovněž vyžaduje, aby byla platforma vybavena určitými funkcionalitami, zejména pro účely ochrany a informování hráčů.

V některých zemích je ze strany národního regulátora kladen větší důraz na **funkční charakteristiky** platforem operátorů (Velká Británie), v některých spíše na **technické charakteristiky** (Španělsko)

Některé země vyžadují, aby byly **servery operátorů, na kterých jsou provozovány platformy, umístěny** přímo v dané zemi (Francie, Velká Británie), v některých zemích tento požadavek stanoven není (Dánsko, Španělsko). Nicméně pokud tento požadavek stanoven není, je nařízeno, že národní regulátor musí mít zajištěn neomezený vzdálený přístup do těchto serverů. Požadavek kladený na operátory ze strany regulátora spočívající v povinnosti umístit server v dané zemi vyplývá zejména z obavy regulátora z toho, že by regulátor mohl jen obtížně kontrolovat server, pokud by byl umístěn v jiné (např. velmi vzdálené) zemi.

Ve většině zemí je zakázáno využívání **hotovostních transakcí**, výjimku představuje Velká Británie, kde jsou hotovostní transakce povoleny za určitých podmínek. Národní regulátor obvykle rovněž stanoví povolené způsoby **zasílání finančních prostředků na hráčský účet**.

2.3.3. Technické zabezpečení kontroly technických zařízení ze strany státního dozoru

Ve všech zemích realizují národní regulátoři **IT audity** zaměřené na kontrolu stavu technických zařízení operátorů. A to buď prostřednictvím vlastních kapacit, nebo s využitím externích kapacit. Ve všech zemích jsou pro tyto účely rovněž využívány **externí kapacity – certifikovaní auditoři**. Charakter těchto auditů se však v jednotlivých zemích liší. Například ve Španělsku jsou operátoři povinni na žádost regulátora představit zástupcům regulátora svá technická zařízení, a to buď přímo ve svých provozovnách, nebo v místě stanoveném regulátorem. Ve Francii pak musí operátoři regulátorovi na základě jím realizovaného IT auditu předložit tzv. akční plán, ve kterém popisují, jakým způsobem odstraní nedostatky zjištěné regulátorem v rámci auditu.

IT audity jsou dále ve všech zemích s výjimkou Velké Británie realizovány jak prostřednictvím **vzdáleného přístupu**, tak prostřednictvím **fyzické kontroly na místě**. Dle informací, které jsme měli v rámci přípravy srovnávací analýzy, nevyužívá regulátor ve Velké Británii systém vzdáleného přístupu pro účely kontroly operátorů.

2.3.4. Metody ověření identifikace hráčů

Ve všech zemích mají operátoři **povinnost ověřovat identifikační údaje poskytnuté hráčem**. Tato povinnost souvisí zejména s prevencí praní špinavých peněz a vyplývá ze směrnice Evropské unie o boji proti praní špinavých peněz (která se aktuálně vztahuje pouze na kasina, nicméně bude novelizována tak, aby se vztahovala na všechny hry).

Ve všech zemích jsou právními předpisy stanoveny rovněž **minimální identifikační údaje**, které musí hráč při registraci do platformy poskytnout. Tyto údaje se však v jednotlivých zemích liší. Například v Dánsku a Španělsku mají hráči povinnost poskytnout kromě dalších údajů i své daňové číslo.

Konkrétní způsob ověřování údajů poskytnutých hráčem se v jednotlivých zemích liší. Ve většině zemí (Dánsko, Francie, Španělsko, Velká Británie) mají operátoři povinnost ověřit tyto údaje jak s interními databázemi (obsahujícími zejména identifikační údaje poskytnuté hráči v rámci procesu registrace a seznam hráčů vyloučených z hraní), tak s i externími databázemi (jedná se například o registry hráčů vyloučených z hraní na vlastní žádost, registry sociální správy apod.), v jedné zemi mají operátoři povinnost ověřit tyto údaje pouze s interními databázemi (Malta). K Itálii jsme v této oblasti neměli k dispozici potřebné informace.

2.3.5. Způsoby boje s praním špinavých peněz

Formy boje s praním špinavých peněz jsou ve všech srovnávaných zemích **velmi obdobné**, což je způsobeno zejména tím, že všechny tyto země měly povinnost do svých právních řádů implementovat směrnici Evropské unie o boji proti praní špinavých peněz. Tato směrnice členským státům Evropské unie ukládá povinnost implementovat opatření v boji proti praní špinavých peněz. Operátoři ve všech zemích tak mají především tyto povinnosti:

- Prověřovat všechny hráče a hodnotit rizika související s praním špinavých peněz (realizovat tzv. „due dilligence“).
- Uplatňovat zvláštní režim pro osoby s politickým profilem (tzv. „zesílené due dilligence“).
- Informovat lokální úřady, pokud identifikují podezřelé transakce.
- Uchovávat data související s transakcemi a informacemi o hráčích a jejich hráčských účtech.
- Realizovat vlastní interní kontroly funkčnosti platforem.
- Pověřit vybraného zaměstnance, který bude zodpovědný za realizaci opatření pro boj s praním špinavých peněz v rámci operátora. Současně představuje tento zaměstnanec „styčný bod“ pro komunikaci s místními úřady zodpovědnými za řešení případů souvisejících s praním špinavých peněz. Pověřený zaměstnanec musí těmto úřadům zejména hlásit všechny podezřelé transakce, které by mohly souviset s praním špinavých peněz.

Centralizované informační systémy pro monitoring plní v této souvislosti zejména následující úlohy:

- Zaznamenávají, ukládají a vyhodnocují data především o uskutečněných transakcích a otevřených hráčských účtech.
- Ověřují správnost a úplnost dat poskytnutých operátory.
- Ověřují identitu hráčů (due dilligence).
- Pro účely regulátora generují automatické varovné reporty signalizující podezřelé chování hráčů a praní špinavých peněz.

Na základě informací generovaných systémem indikující podezření na aktivity spojené s praním špinavých peněz může regulátor podniknout kroky k eliminaci těchto aktivit. Centralizované informační systémy pro monitoring tak mohou pro regulátora znamenat **představovat významný nástroj** pro včasný a efektivní zásah v případě odhalení praní špinavých peněz.

Tyto systémy rovněž představující významný **preventivní nástroj praní špinavých peněz**. A to zejména s ohledem na to, že hráči jsou si vědomi toho, že regulátor má k dispozici nástroje pro detekci těchto aktivit.

2.3.6. Monitorování podvodů při sázení a hraní

Ve všech zemích (s výjimkou **Itálie**, kde jsme **neměli k dispozici relevantní data**) mají operátoři **povinnost předcházet podvodům**. Pro tyto účely jsou využívána obdobná data jako pro účely prevence a detekce praní špinavých peněz.

V tomto ohledu plní **centralizované informační systémy pro monitoring** totožné úlohy, jako v případě monitorování praní špinavých peněz, tzn. zejména:

- Zaznamenávají, ukládají a vyhodnocují data především o uskutečněných transakcích a otevřených hráčských účtech.
- Ověřují správnost a úplnost dat poskytnutých operátory.
- Ověřují identitu hráčů (due dilligence).
- Pro účely regulátora generují automatické varovné reporty signalizující podezřelé chování hráčů a praní špinavých peněz.

Stejně jako v případě praní špinavých peněz mohou regulátorovi centralizované informační systémy pro monitoring umožnit včasné odhalení podvodů realizovaných v rámci trhu herního průmyslu.

2.4. Charakteristika jednotlivých zemí

V této kapitole uvádíme popis jednotlivých zemí v členění dle parametrů, které jsme v rámci naší analýzy zkoumali (tyto parametry jsou detailně popsány v kapitole 2.1.3).

U každého parametru **popisujeme hlavní charakteristiky pro danou zemi**. Struktura tohoto popisu (popisovaná témata) se **u jednotlivých zemí vzájemně odlišuje** vzhledem k tomu, že jsme v rámci sběru dat pro srovnávací analýzu **neměli ve všech případech k dispozici zcela srovnatelná data**.

2.4.1. Dánsko

1. Specifikace technického řešení systému provozování a monitoringu online sázkových her

V Dánsku je dle našich informací využíván centralizovaný informační systém pro monitoring trhu online hraní a sázení založený na off-line architektuře. Tento systém je provozován regulátorem a je založen na základě pravidelného stahování si dat z úložišť operátorů, kam mají operátoři povinnost pravidelně ukládat data. Detailnější informace o fungování tohoto systému jsme v rámci projektu neměli k dispozici. Informační systém je provozován regulátorem, kterým je samostatný „Dánský úřad pro hraní a sázení".

2. Technické požadavky na provozovatele sázkových her

V Dánsku jsou stanoveny technické i funkční požadavky na platformy operátorů jednotně. Po operátorech se požaduje, aby platforma zajistila zejména následující:

- Monitoring podezřelých situací v reálném čase, který upozorní na potenciální podvody nebo praní špinavých peněz a bude automaticky generovat reporty popisující tyto situace.
- Silnou kontrolu přístupu do platformy zahrnující mimo jiné automatické odhlášení hráče po určité době nečinnosti nebo zabezpečení hráčského účtu prostřednictvím digitálního podpisu hráče.
- Povolení hraní jen osobám starším 18 let.
- Ochranu platformy před hackerskými útoky, využívání firewallu, využívání dalších opatření pro ochranu platformy a dat v rámci platformy (uložených i přenášených).
- Zálohování všech důležitých dat a jejich spolehlivé vygenerování v případě potřeby.

Mezi další požadavky na operátory platforem patří např.: „fair play prostředí" platformy, povinné prvky vizualizace hráčského prostředí platformy, transparentní komunikace výsledků hraní směrem k hráči apod. Platforma rovněž musí aktivně kontrolovat průběh hraní a sázení.

Servery, na kterých jsou platformy operátorů provozovány, nemusí být umístěny přímo v Dánsku, pokud jsou umístěny v zemi, se kterou má Dánsko uzavřenou dohodu o vzájemné výměně informací.

Hotovostní transakce nejsou povoleny, přičemž hráč může na svůj účet zaslat finanční prostředky pouze z bankovního účtu finanční instituce, která svou činnost legálně provozuje v Dánsku. Tento účet přitom musí být před akceptací zaslaných finančních prostředků ověřen ze strany operátora. O každé finanční transakci musí být vedeny a ukládány detailní záznamy.

3. Technické zabezpečení kontroly technických zařízení ze strany státního dozoru

V Dánsku jsou realizovány zejména tyto typy kontrol:

- Povinná IT certifikace platformy ze strany regulátorem akreditovaných společností. Audity související s touto certifikací jsou nezbytné pro udělení licence, a jsou zaměřeny na zhodnocení funkčních a technických parametrů platforem – například zda jsou implementovány nástroje pro detekci podvodů a praní špinavých peněz, nebo jaká je úroveň bezpečnosti platformy. Využíváno je pro tyto účely mj. penetrační testování.
- Testování dat zálohovaných operátorem ze strany regulátora. Regulátor může provádět kontroly a testování prostřednictvím vzdáleného přístupu do tzv. datového úložiště SAFE, které musí povinně zřídit a využívat každý operátor. V tomto úložišti musí operátor povinně zálohovat data v předepsaném formátu, a regulátor odsud může stahovat data pro účely kontrol. Regulátor pro tyto účely rovněž provozuje tzv. Tamper Token systém, který je bezpečnostním systémem využívaným pro generování identifikačních kódů nezbytných pro bezpečné uložení dat ze strany operátora do úložiště SAFE a validaci správnosti uložených dat. Tato data jsou následně pravidelně stahována regulátorem za účelem kontroly a výkonu státního dozoru.

- Testování ostatních dat neuložených v systému SAFE. Na žádost regulátora o poskytnutí dat musí operátor regulátorovi tato data poskytnout do 5 pracovních dnů.
- Platformy musí procházet každé 3 měsíce tzv. „testy křehkosti“. Tyto testy se provádějí u všech rozhraní, která ukládají, zpracovávají a přenášejí herní a finanční data. Výsledky testů jsou zasílány regulátorovi.
- Platformy musí každý rok procházet tzv. „ingresní testy“. Tyto testy se provádějí u všech rozhraní, která ukládají, zpracovávají a přenášejí herní a finanční data. Výsledky testů jsou zasílány regulátorovi.

Ze strany operátora by mělo být rovněž realizováno interní testování platforem zahrnující tyto aktivity:

- Ustanovit zaměstnance zodpovědného za interní testování platforem a kontrolu kvality a bezpečnosti platforem.
- Denní inspekce technických zařízení ze strany personálu operátora.
- Periodický interní audit zaměřený na testování náhodných vzorků.
- Zaslání hlášení regulátorovi, pokud interní kontrola odhalí nesoulad s požadavky operátora.
- Zpracovávání a archivace výsledků interních kontrol.

4. Metody ověření identifikace hráčů

Operátor nesmí umožnit vedení anonymních hráčských účtů nebo účtů vedených na fiktivní jméno. Identita hráče musí být vždy ověřena.

V rámci procesu registrace musí hráč uvést alespoň následující údaje:

- Jméno.
- Adresu.
- ID číslo / CPR-číslo (národní dánský identifikátor).
- Zemi pobytu.
- Zamýšlený účel sázení / hraní.

Identifikační údaje uvedené hráčem musí být ověřeny (zejména zda je hráči 18 let), a to prostřednictvím porovnání údajů s:

- Registrem (vedeným regulátorem) z hraní na vlastní žádost vyloučených osob,
- Národním registrem sociální správy,
- Národním digitálním identifikačním systémem a
- interním registrem z hraní a sázení vyloučených osob.

Pokud jsou údaje v pořádku, systém musí zaregistrovat a archivovat všechny informace spojené s hráčovou registrací.

Zabezpečení hráčových údajů v platformě je zajištěno tím, že přístup na hráčský účet musí být autorizován prostřednictvím digitálního podpisu. Platforma pak musí při přenosech dat využívat kódování.

Regulátor vede a spravuje registr z hraní a sázení na vlastní žádost vyloučených osob. Operátoři pak vedou interní registry z hraní a sázení vyloučených osob, kdy u každé takové osoby musí evidovat důvod vyloučení.

5. Způsoby boje s praním špinavých peněz

Operátor má povinnost provádět hodnocení rizik spojených s praním špinavých peněz, a to u každého hráče. Cílem je stanovit rizikový profil hráče a v závislosti na tom realizovat adekvátní opatření (standardní prověřování hráče – tzv. „due dilligence“ nebo zesílené prověřování hráče – „enhanced due dilligence“).

Zesílené prověřování hráče by mělo být realizováno rovněž u osob s politickým profilem.

Regulátor musí pověřit svého zaměstnance, který bude zodpovědný za informování regulátora o podezření na praní špinavých peněz. V této souvislosti musí operátor nastavit a využívat interní systém reportingu, jehož účelem je, aby se informace o podezření na praní špinavých peněz vždy dostala k zaměstnanci zodpovědnému za hlášení této informace regulátorovi.

Dalšími opatřením pro boj s praním špinavých peněz jsou zejména:

- Zálohování dat o transakcích hráčů (např. hráčovi identifikační údaje, celkových sázkách a výhrách daného hráče, důvody ukončení hraní nebo sázení apod.).
- Zákaz vedení fiktivních nebo anonymních účtů.
- Automatické generování upozornění na velmi vysoký vklad ze strany hráče (více než 20.000 DKK).
- Realizace interních kontrol operátora.

6. Monitorování podvodů při sázení a hraní

Platformy operátorů musí být vybaveny nástroji k detekci podezřelých transakcí, které by mohly indikovat podvod. Platformy rovněž musí být vybaveny nástroji schopnými tyto podezřelé transakce analyzovat a generovat automatická upozornění na potenciální podvod.

Pro tyto účely jsou zejména sledována tato data:

- Velmi vysoké výhry (hranice je interně stanovena operátorem).
- Velmi vysoké transfery finančních prostředků.

2.4.2. Itálie

1. Specifikace technického řešení systému provozování a monitoringu online sázkových her

V Itálii je využíván centralizovaný informační systém s názvem „Totalizzatore“, jehož provozovatelem a technickým správcem je státem vlastněná firma SOGEI. Uživatelem tohoto systému je jak národní regulátor – Samostatný úřad pro státní monopoly (systém mu umožňuje řídit a monitorovat autorizované operátory), tak autorizovaní operátoři – provozovatelé sázkových a jiných hazardních her (kterým systém umožňuje provozovat hazardní hry).

Systém je založen na tzv. on-line architektuře. K Totalizzatore musí být připojeny všechny licencované platformy operátorů, přičemž kapacita připojení platforem je neomezená. Legislativa vyžaduje, aby každá vypsaná sázka byla zaznamenána v kontrolních a ověřovacích systémech ještě předtím, než se sázkaři mohou sázení zúčastnit. Totalizzatore potvrzuje přijetí sázek prostřednictvím registrace sázek přijatých sázkovými kancelářemi, a to v reálném čase. Systém Totalizzatore je připojen k síti licencovaných operátorů a umožňuje identifikovat vítězné „tikety“ – sázky, a to ihned po skončení příslušné (sportovní, sázkové) události. Většinou tak tento systém umožní okamžité vyplacení výhry.

Efektivita komplexní IT architektury Totalizzatore spočívá v udržování silné kontroly všech jednotlivých fází celého procesu – od udělení státní licence přes implementaci příslušné herní platformy po průběžnou kontrolu a monitoring.

Systém disponuje zejména následujícími funkcionalitami:

- Kontrola daňových příjmů pro účely daňové správy (generovaných celým herním průmyslem).
- Kontrola podvodů a praní špinavých peněz prostřednictvím odhalování podezřelých transakcí nebo chování hráčů.
- Kontrola správnosti fungování platforem operátorů (např. odpovídající pravděpodobnost výhry, počet transakcí).
- Kontrola identity hráčů prostřednictvím napojení na externí databáze.

Pro zajištění bezpečnosti systém průběžně ověřuje integritu a kvalitu přenášených dat. Systém rovněž provádí křížovou kontrolu mezi informacemi v systému a v platformách operátorů.

2. **Technické požadavky na provozovatele sázkových her**

V Itálii jsou technické i funkční požadavky na platformy operátorů stanoveny vždy specificky v rámci veřejné výzvy k získání licence vyhlášené regulátorem (Samostatný úřad pro státní monopoly). Tyto požadavky se týkají zejména:

- Technické úrovně platformy.
- Zabezpečení platformy.
- Vybavení platformy z hlediska funkcionalit.

Platforma musí ukládat všechny realizované sázky a transakce (každé musí být přiřazeno unikátní identifikační číslo). Dále musí platforma umožnit provedení křížové kontroly ze strany operátora, resp. operátorova systému pro monitoring Totalizzatore.

Hotovostní transakce nejsou povoleny.

3. **Technické zabezpečení kontroly technických zařízení ze strany státního dozoru**

- Italský regulátor může kdykoliv realizovat IT audity, a to prostřednictvím:
- Vzdáleného přístupu s využitím dat získaných z platforem operátorů.
- Kontroly na místě v provozovnách operátorů.

4. **Metody ověření identifikace hráčů**

V této oblasti nebyla v rámci sběru dat pro Itálii dostupná data.

5. **Způsoby boje s praním špinavých peněz**

V této oblasti nebyla v rámci sběru dat pro Itálii dostupná data. Nicméně vzhledem k tomu, že Itálie implementovala směrnici Evropské unie o boji proti praní špinavých peněz, mají operátoři zejména následující povinnosti:

- Prověřovat všechny hráče (realizovat due dilligence).
- Uplatňovat zvláštní režim pro osoby s politickým profilem (zesílené due dilligence).
- Informovat lokální úřady, pokud identifikují podezřelé transakce.
- Uchovávat data související s transakcemi a informacemi o hráčích a jejich hráčských účtech.
- Realizovat vlastní interní kontroly.

6. **Monitorování podvodů při sázení a hraní**

V této oblasti nebyla v rámci sběru dat pro Itálii dostupná data.

2.4.3. Francie

1. **Specifikace technického řešení systému provozování a monitoringu online sázkových her**

Francie, konkrétně národní regulátor (samostatný Francouzský úřad pro hraní a sázení), využívá tzv. centralizovaný informační systém založený na tzv. off-line architektuře. Operátoři mají povinnost zasílat do off-line systému data ve formátu stanoveném regulátorem. Jedná se o následující data:

- Identitu a kontaktní adresu každého hráče.
- Informace o účtu každého hráče včetně data zřízení účtu a informace o platební metodě, kterou hráč využívá.
- Transakce realizované v rámci hráčova účtu.

Frekvence zasílání dat ze strany operátorů je obvykle denní. Systém tato data následně ověřuje a analyzuje.

2. **Technické požadavky na provozovatele sázkových her**

Ve Francii jsou stanoveny technické i funkční požadavky na platformy operátorů jednotně. Platforma musí obsahovat tzv. „front-end systém“, který sbírá a archivuje data vyměněná mezi operátorem a hráčem. Tento „front-end systém“ musí být umístěn na technickém zařízení ve Francii.

Po operátorech se požaduje, aby platforma zajistila zejména následující:

- Zálohování, ověřování správnosti a zajištění bezpečnosti uložených dat.
- Výhradní využití webových stránek s koncovkou „fr“.
- Spolehlivý generátor čísel fungující v souladu se statistickou pravděpodobností.
- Umožnit regulátorovi získání dat uložených v rámci platformy prostřednictvím vzdáleného přístupu (pro účely kontroly).

V rámci každé hry musí operátor informovat hráče, zda data, která má hráč k dispozici, jsou zpožděná nebo v reálném čase.

Hotovostní transakce, stejně jako hra na dluh, nejsou povoleny. Hráč může zaslat finanční prostředky na svůj hráčský účet pouze z bankovního účtu finanční instituce provozované v členské zemi Evropské unie, která má s Francií uzavřenou dohodu o spolupráci v boji proti podvodům a vyhýbání se daňovým povinnostem.

3. Technické zabezpečení kontroly technických zařízení ze strany státního dozoru

Francouzský regulátor (Francouzský úřad pro hraní) může kdykoliv realizovat IT audity u operátorů (zaměřené na posouzení bezpečnosti a fungování platforem), a to prostřednictvím:

- Vzdáleného přístupu s využitím dat získaných z platforem operátorů.
- Kontroly na místě v provozovnách operátorů.

Výsledkem těchto auditů jsou doporučení technicko-organizační povahy, která jsou sdělena operátorům, aby mohli odstranit zjištěné nedostatky. Operátoři musí následně připravit a regulátorovi prezentovat akční plán k odstranění těchto nedostatků.

Při realizaci IT auditů může regulátor využít certifikované auditory třetích stran.

Operátoři musí regulátorovi každoročně zasílat přehled kroků (a jejich finanční náročnost), které provedli v oblasti propagace bezpečného hraní a boji proti patologickému hráčství. Dále musí regulátorovi zasílat výsledky bezpečnostních auditů realizovaných třetími stranami.

Operátoři musí zástupcům regulátora kdykoliv umožnit kontrolu svých technických zařízení.

Zástupci regulátora mohou provádět kontrolu fyzické bezpečnosti zařízení, testy zařízení apod.

Zástupci regulátora mohou pro své účely rovněž stáhnout jakákoliv data ze serveru využívaného pro provoz platformy.

Operátor musí zástupcům regulátora poskytnout nezbytnou součinnost prostřednictvím vysvětlení technických a funkčních aspektů svých zařízení.

4. Metody ověření identifikace hráčů

V rámci procesu registrace musí hráč uvést alespoň následující údaje:

- Jméno.
- Věk.
- Adresu a e-mailovou adresu.
- Číslo účtu, ze kterého posílá vklady na hráčský účet.

Předtím, než je hráč zaregistrován a je mu umožněno hrát nebo sázet, musí být ověřena jeho e-mailová adresa, zda již není uvedena v interní databázi operátora u jiného hráče.

Po tomto ověření musí operátor dále ověřit, zda hráč není uveden v registru hráčů se zákazem hraní vedeném regulátorem. Toto ověření musí operátor provádět každý měsíc. Pokud operátor zjistí, že hráč v tomto registru uveden je, je operátor povinen zablokovat hráčův účet.

Proces otevření hráčského účtu je rozdělen do dvou kroků:

- Otevření dočasného účtu.
- Otevření permanentního účtu po provedení kontroly ze strany operátora.

Po tom, co si hráč otevře dočasný účet, má povinnost operátorovi doložit:

- Kopii platného průkazu totožnosti.
- Dokument potvrzující, že jím nahlášený bankovní účet skutečně patří jemu.

Teprve poté může být hráči zřízen permanentní účet a hráč si může vybírat své výhry.

Data hráčů musí být bezpečně uložena. Pokud jsou tato data přenášena, pak musí být přenosový kanál autentizován.

5. Způsoby boje s praním špinavých peněz

Operátor je povinen regulátorovi garantovat, že implementuje opatření pro boj s praním špinavých peněz. Ve výročních zprávách má operátor povinnost uvést a popsat opatření přijatá v boji s praním špinavých peněz.

Platformy musí být vybaveny automatickými nástroji upozorňujícími na podezřelé transakce, resp. na potenciální praní špinavých peněz a podvody.

Kromě toho musí operátor, jak je rovněž uvedeno v předchozím bodě, každý měsíc aktivně ověřovat, zda je hráč s otevřeným hráčským účtem evidovaný v registru hráčů se zákazem hraní vedeném regulátorem.

Pro účely boje s praním špinavých peněz jsou ukládány a archivovány zejména tyto informace:

- Data o hráčském účtu (identifikační údaje hráče, datum otevření účtu, nastavení osobních finančních limitů apod.).
- Data o finančních transakcích.
- Data o sázkách (umístění sázek, výhry / prohry).

Dále má operátor povinnost zejména:

- Prověřovat všechny hráče (realizovat due dilligence).
- Uplatňovat zvláštní režim pro osoby s politickým profilem (zesílené due dilligence).
- Informovat lokální úřady, pokud identifikuje podezřelé transakce.
- Realizovat vlastní interní kontroly.

6. Monitorování podvodů při sázení a hraní

Jak je uvedeno výše v předchozím bodě, platformy operátorů musí být vybaveny automatickými nástroji upozorňujícími na podezřelé transakce, resp. na potenciální praní špinavých peněz a podvodů. Pro tyto účely jsou využívána totožná data jako pro boj s praním špinavých peněz, tzn.:

- Data o hráčském účtu (identifikační údaje hráče, otevření účtu, nastavení osobních finančních limitů apod.).
- Data o finančních transakcích.
- Data o sázkách (umístění sázek, výhry / prohry).

2.4.4. Malta

1. Specifikace technického řešení systému provozování a monitoringu online sázkových her

Centralizovaný informační systém využívaný na Maltě se nazývá „**The Remote Gambling Monitoring System**“ (dále rovněž „RGMS“). Je využíván výhradně národním regulátorem, kterým je samostatný Úřad pro loterie, hraní a sázení, a je založen na tzv. on-line architektuře.

RGMS je systémem provozovaným na tzv. freeware platformě soukromé softwarové společnosti Nagios Enterprise a slouží k základnímu monitorování dění na on-line tru hraní a sázení. K RGMS musí být připojeny všechny licencované platformy operátorů, přičemž kapacita připojení platforem je neomezená.

Z hlediska nákladů se jedná o velmi úsporný systém, který však poskytuje regulátorovi velmi omezené možnosti výkonu státního dohledu. Vzhledem k využití freewarové verze regulátor za používání systému neplatí žádné poplatky. Obsluhu systému zajišťuje pouze jeden IT administrátor. Systém je v rámci údržby pravidelně modernizován.

Systém není vybaven pokročilými funkcionalitami a lze ho charakterizovat následujícím způsobem:

- Není napojen na žádné externí databáze.
- Nemonitoruje daňové příjmy, ani není napojen na informační systém sloužící daňové správě.
- Není vybaven žádnými business inteligence nástroji (např. pro odhalování podvodů či praní špinavých peněz).
- Neověřuje správnost monitorovaných dat.
- Zaznamenává pouze status připojení hráčů k platformě (připojen / nepřipojen).

V současné době zvažuje Úřad pro loterie a hraní přechod na pokročilejší centralizovaný informační systém, který by oproti současnému systému disponoval business inteligence nástroji a umožnil tak regulátorovi kvalitnější výkon státního dohledu.

2. Technické požadavky na provozovatele sázkových her

Na Maltě jsou stanoveny technické i funkční požadavky na platformy operátorů jednotně. Po operátorech se požaduje, aby platforma zajistila zejména následující:

- Spolehlivý generátor čísel fungující v souladu se statistickou pravděpodobností.
- Systémovou bezpečnost využívající kryptování uložených dat.
- Bezpečnost hráčského účtu zahrnující řízení hesel, automatické odhlašování z účtu, blokování simultánního přihlášení na účet apod.
- Zálohování a uchovávání dat vyžadovaných regulátorem (týkajících se např. sázek, vkladů, času hráče stráveného hraním, zůstatku na hráčském účtu apod.)

Platformy musí dále splňovat zejména následující požadavky: uchovávat informace o identitě, registraci a transakcích hráčů, počítat daňové odvody v rámci platformy, automaticky generovat reporty obsahující agregované informace o transakcích, zajistit implementaci opatření pro boj s praním špinavých peněz, zajistit povinné prvky vizualizace hráčského prostředí platformy apod.

Součástí platformy musí být povinně zejména tzv. kontrolní systém, který musí být umístěn na serveru na Maltě.

Právními předpisy jsou povoleny následující způsoby zasílání finančních prostředků na hráčský účet:

- Kreditní a debetní karty.
- Elektronické převody.
- Šeky.

Hotovostní transakce nejsou povoleny.

3. Technické zabezpečení kontroly technických zařízení ze strany státního dozoru

Maltský regulátor může operátorovi žádajícímu o licenci nebo již licencovanému kdykoliv nařídit, aby podstoupil audit kontrolního systému své platformy ze strany auditora certifikovaného regulátorem.

Regulátor může realizovat „audity shody“ zaměřené na ověření dodržování požadavků regulátora ze strany operátora. Tyto audity se mohou zaměřit na tyto aspekty:

- Technické.
- Obchodní.
- Finanční.
- Právní.

Kontrolovány jsou zejména následující oblasti: kontrolní systém platformy, dokumentace operátora, bezpečnostní politika operátora, organizační bezpečnost, kontrola a klasifikace aktiv, školení personálu, fyzická bezpečnost, dodržování právních předpisů apod.

4. Metody ověření identifikace hráčů

V rámci procesu registrace musí hráč uvést alespoň následující údaje:

- Jméno.
- Věk.
- Místo bydliště.
- Platnou e-mailovou adresu.

Předtím, než je hráč zaregistrován a je mu umožněno hrát nebo sázet, musí být ověřena jeho e-mailová adresa, zda již není uvedena v interní databázi operátora u jiného hráče. Dále by měly být ověřeny další identifikační údaje, zda již nefigurují v interní databázi operátora. V případě že ano, regulátor má povinnost nepovolit registraci hráče.

Data hráčů musí být chráněna např. pomocí bezpečného uložení, šifrování v případě jejich transferu, uložení hráčských hesel v jednosměrném kryptografickém formátu apod.

5. Způsoby boje s praním špinavých peněz

Pro účely boje s praním špinavých peněz regulátor od operátora vyžaduje zejména následující:

- Platformy musí být vybaveny nástroji schopnými detekovat podezřelé transakce, resp. identifikovat potenciální praní špinavých peněz.
- Platformy musí generovat automatická upozornění, pokud výběr finančních prostředků dosáhne určité hranice.
- Hráči musí využívat pouze jeden bankovní účet pro vklady finančních prostředků i jejich výběry.
- Operátor musí realizovat přístup založený na posouzení rizika spočívající v prověřování hráče (due dilligence).
- Operátor musí disponovat pověřenými a vyškolenými zaměstnanci pro boj s praním špinavých peněz.
- Platformy musí ukládat a archivovat data týkající se hráčských údajů, transakcí, finančních převodů apod.

Dále má operátor povinnost zejména:

- Uplatňovat zvláštní režim pro osoby s politickým profilem (zesílené due dilligence).
- Informovat lokální úřady (konkrétně tzv. „Financial Intelligence Analysis Unit"), pokud identifikuje transakce podezřelé z praní špinavých peněz.
- Realizovat vlastní interní kontroly.

6. Monitorování podvodů při sázení a hraní

Platformy musí být pro účely detekce podvodů vybaveny nástroji pro automatickou identifikaci podezřelých transakcí. Pro tyto účely jsou využívána obdobná data jako pro účely boje s praním špinavých peněz, tzn. zejména data týkající se hráčských údajů, transakcí, finančních převodů apod.

Platformy musí monitorovat zejména:

- Koluzní chování hráčů (podvodné dohody hráčů).
- Tzv. „chip-dumping" chování hráčů při pokeru. Jedná se o zakázané úmyslné ztrácení žetonů jedním hráčem ve prospěch jiného hráče.

2.4.5. Španělsko

1. Specifikace technického řešení systému provozování a monitoringu online sázkových her

Všechny licencované platformy operátorů musí být připojeny k centralizovanému informačnímu systému provozovanému národním regulátorem, který je dle našich informací založen na tzv. on-line architektuře. Španělský regulátor (Národní komise pro hraní) může prostřednictvím tohoto systému ověřovat správnost fungování platforem operátorů. Některé aktivity v rámci výkonu státního dozoru v oblasti monitoringu on-line herního trhu vykonává vedle Komise pro hraní a sázení rovněž Ministerstvo financí a veřejné správy, resp. útvar tohoto ministerstva s názvem Generální ředitelství pro hraní a sázení.

2. Technické požadavky na provozovatele sázkových her

Ve Španělsku jsou stanoveny technické i funkční požadavky na platformy operátorů jednotně. Platforma musí povinně obsahovat dvě součásti:

- Centrální herní jednotku.
- Interní kontrolní systém.

Centrální herní jednotka musí zajistit následující:

- Zálohování a uchovávání všech transakcí realizovaných v rámci platformy.
- Správný průběh hráčských aktivit.
- Možnost neustálé kontroly všech transakcí v rámci platformy, chování hráčů a jejich výsledků, a následně v případě potřeby rekonstrukci všech těchto aktivit.

Servery, na kterých jsou platformy operátorů provozovány, nemusí být umístěny přímo ve Španělsku. Nicméně jak centrální herní jednotka, tak i její záloha, musí být připojeny k centralizovanému informačnímu systému regulátora pro monitoring. Regulátor může operátorovi nařídit, aby vytvořil zrcadlovou kopii centrální herní jednotky (sekundární jednotku) na území Španělska.

Po operátorech se požaduje, aby platforma zajistila zejména následující:

- Spolehlivý generátor čísel fungující v souladu se statistickou pravděpodobností.
- Spolehlivé autentizační mechanismy.
- Výhradní využití webových stránek s koncovkou „es“.

Operátoři musí při žádosti o udělení licence detailně specifikovat především: procesy podporované platformou, způsob registrace hráčů, zálohovaná data, hráčský účet, platební mechanismy apod.

3. Technické zabezpečení kontroly technických zařízení ze strany státního dozoru

Španělský regulátor může kdykoliv realizovat IT audity, a to prostřednictvím:

- Vzdáleného přístupu s využitím dat získaných z platforem operátorů.
- Kontroly na místě v provozovnách operátorů.

IT audity může regulátor realizovat buď s využitím vlastních kapacit, nebo s využitím třetích stran. Operátor musí regulátorovi poskytnout všechna relevantní data, zpřístupnit mu své provozovny a technická zařízení, záznamy, dokumenty apod.

Platformy operátorů by měly být kontrolovány každé dva roky. Pokud tento audit není realizován ze strany regulátora, musí operátor na své náklady zajistit audit své platformy ze strany certifikovaného auditora třetí strany. Operátoři jsou na žádost regulátora povinni představit zástupcům regulátora svá technická zařízení, a to buď přímo ve svých provozovnách, nebo v místě stanoveném regulátorem.

Dále regulátor realizuje audity inspekce zaměřené na dodržování právních předpisů ze strany operátorů.

4. Metody ověření identifikace hráčů

V rámci procesu registrace musí hráč uvést kromě základních identifikačních údajů (zejména jména) své daňové identifikační číslo a místo trvalého pobytu.

Operátor má povinnost následně ověřit, zda identifikační údaje uvedené hráčem nejsou duplicitní s jinými údaji uvedenými v operátorově interní databázi. Není povoleno, aby měl jeden hráč více hráčských účtů. Kromě porovnání hráčem poskytnutých identifikačních údajů s interní databází má operátor povinnost ověřit tyto údaje s národním registrem hráčů se zákazem hraní a sázení. Tento registr je veden regulátorem.

Operátor má dále povinnost implementovat opatření, která zajistí fyzickou a logickou bezpečnost dat uložených v platformě tak, aby k nim neměl přístup nikdo nepovolaný.

5. Způsoby boje s praním špinavých peněz

Národní institucí, která se zabývá bojem s praním špinavých peněz je „Komise pro prevenci a boj s praním špinavých peněz a přestupky v měnové oblasti“ (dále „Komise“).

Operátoři mají v oblasti boje s praním špinavých peněz zejména následující povinnosti:

- Identifikovat hráče disponujícího neobvykle vysokými finančními prostředky pro účely hraní a sázení.
- Prošetřit každou podezřelou transakci potenciálně související s praním špinavých peněz.
- Archivovat údaje související s realizovanými transakcemi po dobu 5 let od ukončení aktivního hraní či sázení daného hráče.
- Informovat Komisi o každé podezřelé transakci potenciálně související s praním špinavých peněz.
- Implementovat interní pravidla pro předcházení praní špinavých peněz.

Operátor musí provádět hodnocení rizik spojených s praním špinavých peněz, a to u každého hráče. Cílem je stanovit rizikový profil hráče a v závislosti na tom realizovat adekvátní opatření (standardní prověřování hráče - due dilligence nebo zesílené prověřování hráče - enhanced due dilligence).

Zesílené prověřování hráče by mělo být realizováno zejména u osob s politickým profilem. V této souvislosti jsou realizována především tato opatření:

- Osobám s politickým profilem může povolit účast na hraní a sázení na konkrétní platformě jen vrcholné vedení společnosti operátora provozujícího tuto platformu.
- Operátor musí vyvinout maximální úsilí, aby prověřil zdroj příjmů, které jsou využity při hraní a sázení.
- Operátor musí po celou dobu aktivní účasti osoby s politickým profilem na hraní a sázení realizovat zvýšený monitoring aktivit této osoby.

6. Monitorování podvodů při sázení a hraní

Operátor má povinnost implementovat opatření pro předcházení podvodům při hraní a sázení.

2.4.6. Velká Británie

1. Specifikace technického řešení systému provozování a monitoringu online sázkových her

Ve Velké Británii není využíván žádný centralizovaný informační systém pro monitoring trhu online hraní a sázení. Regulátorem je samostatný úřad Komise pro hraní a sázení.

2. Technické požadavky na provozovatele sázkových her

Ve Velké Británii jsou stanoveny technické i funkční požadavky na platformy operátorů jednotně. Od operátorů se vyžaduje, aby platforma zajistila zejména následující:

- Spolehlivý generátor čísel fungující v souladu se statistickou pravděpodobností.
- Zobrazení informací pro hráče na hráčském účtu (zůstatek na účtu, uskutečněné sázky, finanční transakce, měnu pro hraní apod.)
- Informování hráče o pravidlech her, popisu her a pravděpodobnosti vítězství
- Nastavení finančních limitů ze strany hráče

Platformy musí dále splňovat zejména následující požadavky: zajistit povinné prvky vizualizace hráčského prostředí platformy, zajistit tzv. zodpovědnou konstrukci hry nepodporující závislost hráčů, zajistit implementaci opatření k odhalování podvodů nebo praní špinavých peněz apod.

Servery, na kterých jsou platformy operátorů provozovány, musí být umístěny na území Velké Británie.

Dále jsou ze strany regulátora (Komise pro hraní a sázení) stanoveny rozsáhlé standardy v oblasti bezpečnosti provozování platforem.

Právními předpisy jsou povoleny následující způsoby zasílání finančních prostředků na hráčský účet:

- Hotovost.
- Debetní karty.
- Šek.

Hotovostní transakce jsou povoleny ve specifikovaných případech. Využití kreditních karet není povoleno.

3. Technické zabezpečení kontroly technických zařízení ze strany státního dozoru

Ve Velké Británii využívá národní regulátor (Komise pro hraní a sázení) přístupu založeného na hodnocení rizika (tzv. risk-based approach). Tento přístup hodnotí rizika neplnění požadavků regulátora ze strany operátorů ze dvou pohledů:

- „Viditelnosti“ neplnění požadavků.
- Dopadu neplnění požadavků na hráče.

Rizika následně kategorizuje do třech skupin:

- Skupina rizik vyžadující nejvýznamnější dohled (u této skupiny je vyžadováno každoroční testování rizik třetími stranami a zaslání výsledku testování regulátorovi).
- Skupina rizik vyžadující střední dohled (u této skupiny je operátor povinen doložit regulátorovi, že plní jeho požadavky).
- Skupina rizik vyžadující zmírněný dohled (tato skupina rizik je monitorována regulátorem).

Každoroční testování rizik třetími stranami a zaslání výsledku testování regulátorovi se vyžaduje například pro tyto oblasti:

- Generátor náhodných čísel.
- Zdrojový kód, na kterém je platforma založena.
- Nástroje pro detekci podvodů.
- Shoda skutečných her pro peníze s hrami „nanečisto“.

Povinnost každoročního testování rizik třetími stranami se nevztahuje na operátory, u kterých činí roční objem vkladů od hráčů méně než 250.000 liber.

Regulátor při ověřování plnění požadavků ze strany operátorů využívá následující nástroje:

- Compliance audity.
- Kontrolu webových stránek operátora.
- Kontrolu výsledků testování platforem.
- Kontrola výsledků každoročního testování.
- Informace od třetích stran apod.

Operátoři mají dále povinnost zasílat regulátorovi informace týkající se:

- Pravidelného čtvrtletního sběru dat ze strany regulátora.
- Významných změn ve vedení organizace operátora.
- Tzv. klíčových událostí (např. insolvence operátora, soudní rozhodnutí týkající se operátora apod.).
- Dalších záležitostí, o kterých si regulátor informace vyžádá.

4. Metody ověření identifikace hráčů

V rámci procesu registrace musí hráč uvést alespoň následující údaje:

- Základní identifikační údaje (jméno).
- Místo trvalého pobytu.
- E-mailovou adresu.
- Bankovní účet vedený na hráčovo jméno.
- Dodatečné údaje v případě osob s rizikovým profilem: povolání, zdroj finančních prostředků pro hraní a sázení, obchodní zájmy apod.

Operátor musí realizovat prověřování hráče (due dilligence), tzn. musí zejména ověřovat jeho identifikační údaje. Regulátor pro tyto účely vytvořil manuál, ve kterém popisuje možné způsoby verifikace identity hráče. Mezi hlavní způsoby ověření identity hráče patří:

- Externí elektronické databáze.
- Využití znalostí soukromých agentur shromažďujících potřebné údaje.
- Veřejně dostupné registry (dlužníků, osob páchajících přestupky, zesnulých osob apod.).
- Způsoby zabezpečení údajů poskytnutých hráčem a celé platformy jsou specifikovány v technických standardech vydaných regulátorem.

5. Způsoby boje s praním špinavých peněz

Národní institucí zabývající se bojem s praním špinavých peněz je „Agentura pro boj se závažným organizovaným zločinem“ (dále „Agentura“).

Operátoři mají v oblasti boje s praním špinavých peněz zejména následující povinnosti:

- Implementovat interní pravidla pro předcházení praní špinavých peněz.
- Realizovat přístup založený na hodnocení rizika a důslednému prověřování hráčů a identifikovat rizika související s praním špinavých peněz.
- Monitorovat všechny transakce a neustále zlepšovat opatření pro boj s praním špinavých peněz.
- Zaznamenávat, co a z jakého důvodu v této oblasti realizovali.
- Pověřit vybraného zaměstnance (tzv. „nominated officer“) shromažďováním všech údajů souvisejících s praním špinavých peněz a informováním Agentury o jakýchkoliv podezřelých transakcích (elektronicky s využitím agenturního rozhraní nebo v papírové podobě stanovené Agenturou).
- Realizovat vlastní interní kontroly.
- Zaznamenávat a uchovávat data využitelná pro boj s praním špinavých peněz. Zejména se jedná o: zprávy zaměstnance pověřeného bojem proti praní špinavých peněz zaslané vrcholnému vedení operátora, záznamy o identifikaci hráče a ověření této identifikace, záznamy o školení zaměstnance pověřeného bojem proti praní špinavých peněz, všechny podezřelé transakce a ze strany regulátora v této souvislosti realizované kroky apod.

Zesílené prověřování hráče by mělo být realizováno zejména u osob s politickým profilem. V této souvislosti jsou realizována především tato opatření:

- Osobám s politickým profilem může povolit účast na hraní a sázení na konkrétní platformě jen vrcholné vedení společnosti provozující tuto platformu.
- Operátor musí vyvinout maximální úsilí, aby prověřil zdroj příjmů, které jsou využity při hraní a sázení.
- Operátor musí po celou dobu aktivní účasti osoby s politickým profilem na hraní a sázení realizovat zvýšený monitoring aktivit této osoby.

6. Monitorování podvodů při sázení a hraní

Operátor má povinnost předcházet podvodům a detekovat snahy o podvody. Zejména má povinnost monitorovat chování hráčů a detekovat podezřelé chování a transakce. Operátor dále musí prověřit všechna upozornění hráčů na podvody ostatních hráčů.

3. Návrh nového modelu státního dozoru

V úvodu této kapitoly popisujeme způsob, jak jsme přistoupili k přípravě **návrhu nového modelu státního dozoru nad on-line trhem herního průmyslu** (dále jen „státní dozor“). Dále uvádíme charakteristiku tohoto modelu v členění dle jednotlivých zkoumaných parametrů, rámcové požadavky na zdroje potřebné pro realizaci modelu a v závěru kapitoly pak předkládáme návrh akčního plánu k realizaci modelu.

3.1. Způsob přípravy návrhu nového modelu státního dozoru

V první fázi projektu jsme realizovali **srovnávací analýzu**, jejímž předmětem bylo srovnání šesti evropských zemí z hlediska technického řešení regulace on-line gamblingu. Na základě této analýzy jsme identifikovali tyto **tři základní modely** výkonu státního dozoru („modely“):

1. Model využívající centralizovaný informační systém pro monitoring založený na **on-line architektuře**.
2. Model využívající centralizovaný informační systém pro monitoring založený na **off-line architektuře**.
3. Model nevyužívající **žádný centralizovaný informační systém** pro monitoring.

Následně bylo naším úkolem jeden z těchto modelů označit jako nejvhodnější pro výkon státního dozoru v České republice.

Kromě těchto modelů byl výsledkem analýzy popis zemí v jednotlivých zkoumaných parametrech, kterými byly:

- Specifikace technického řešení systému provozování a monitoringu online sázkových her.
- Technické požadavky na provozovatele sázkových her.
- Technické zabezpečení kontroly technických zařízení ze strany státního dozoru.
- Metody ověření identifikace hráčů.
- Způsoby boje s praním špinavých peněz.
- Monitorování podvodů při sázení a hraní.

Po zpracování srovnávací analýzy jsme v rámci společného jednání (diskusního workshopu) s Ministerstvem financí zejména:

- představili námi zpracované popisy **tří základních modelů** a jejich základní charakteristiky,
- diskutovali **výhody a nevýhody** jednotlivých modelů a srovnávali tyto modely mezi sebou,
- představili základní **srovnání jednotlivých zemí** v členění dle jednotlivých zkoumaných parametrů,
- diskutovali **cíle** státního dozoru v České republice a základní **omezení** z hlediska zdrojů,
- stanovili **žádoucí charakteristiky výkonu státního dozoru** v České republice v rámci jednotlivých zkoumaných parametrů a diskutovali vhodnost jednotlivých modelů.

Závěry tohoto jednání (diskusního workshopu) následně tvořily základ pro zpracování návrhu nového modelu státního dozoru, který jsme rovněž zpracovali pro oblasti pokrývající všech šest analyzovaných parametrů. Výsledkem jednání byla rovněž definice cílů státního dozoru. Hlavním **cílem** MF jako regulátora by mělo být nastavení takového způsobu výkonu státního dozoru, který mu umožní **efektivní nepřetržitou kontrolu nad děním na trhu on-line herního průmyslu**. Výkon státního dozoru by současně neměl klást enormně vysoké administrativní nároky na operátory (provozovatele platforem), ani na hráče. **České regulatorní prostředí** by mělo být pro operátory nastaveno takovým způsobem, aby tito operátoři by měli zájem stát se součástí tohoto trhu a respektovat přitom český právní řád.

3.2. Charakteristika návrhu nového modelu státního dozoru

3.2.1. Specifikace technického řešení systému provozování a monitoringu

Vhodný model výkonu státního dozoru

Z hlediska tří identifikovaných modelů byl v rámci projektu pro účely dosažení požadovaných cílů fungování státního dozoru jako nejvhodnější označen model využívající centralizovaný informační systém pro monitoring založený na on-line platformě. Tento systém umožní Ministerstvu financí monitorovat všechny licencované operátory, resp. všechny jejich licencované platformy v reálném čase. Tento monitoring pak bude představovat účinný preventivní nástroj při boji s podvody operátorů a praním špinavých peněz a umožní MF rychle reagovat na aktuální situaci na trhu v případě potřeby. Hlavní výhody a nevýhody tohoto modelu jsou uvedeny v kapitole 2.2 této Zprávy.

Z hlediska srovnávaných zemí by se měl tedy český model svým charakterem **nejvíce blížit italskému modelu** využívajícímu centralizovaný informační systém Totalizzatore. Centralizovaný informační systém by měl pokrývat, respektive monitorovat **všechny on-line hry povolené českým právním řádem**.

Centralizovaný informační systém by měl disponovat zejména následujícími funkcionalitami:

- Detekce podezření na podvody ze strany operátorů (generování automatických výstražných upozornění, tzv. „red flags“).
- Detekce podezření na praní špinavých peněz (generování automatických výstražných upozornění, tzv. „red flags“).
- Sledování daňových příjmů generovaných operátory (generování daňových reportů za každého operátora a v této souvislosti úzká spolupráce s daňovou správou)
- Verifikace identifikačních údajů poskytnutých hráči a následné povolování jejich registrace. Pro tyto účely by mohl být využit zejména tzv. Informační systém základních registrů.
- Vedení registrů osob se zákazem hraní (zákazem nařízeným ze strany regulátora – Ministerstva financí – nebo na vlastní žádost hráče).
- Verifikace správnosti dat poskytovaných operátory.
- Možnost variantního nastavení generování automatických reportů (obsahujících např. počet denně realizovaných transakcí, počet vsazených peněz apod.).

Centralizovaný informační systém pro monitoring bude vzhledem k jeho unikátnosti zřejmě vhodné vytvořit tzv. „na míru“ dle specifických potřeb MF.

3.2.2. Technické požadavky na provozovatele sázkových her

Způsob stanovení technických požadavků na operátory

Technické a funkční požadavky na operátory by měly být **stanoveny centrálně prostřednictvím právního předpisu spíše obecnějšího charakteru**, aby nebylo třeba jej příliš často aktualizovat v souvislosti s rychle postupujícím technickým rozvojem na trhu. Základními **principem bude požadavek na konektivitu platforem operátorů** ve vztahu k centralizovanému informačnímu systému pro monitoring.

Detailní specifikace požadavků by pak měla být stanovena (a pravidelně aktualizována) prostřednictvím **podzákonných předpisů (technických norem)**.

Charakter funkčních a technických požadavků

Tyto požadavky by měly zejména zajistit, aby byly platformy operátorů bezpečné pro hráče (např. aby měl hráč maximální přehled o svých aktivitách v rámci platformy, aby platformy nepodporovaly vytvoření závislosti hráče a neumožnily hraní hráčům pod 18 let, aby umožnily nebo dokonce vyžadovaly nastavení určitých limitů pro hraní apod.) bezpečné z hlediska uchovávání a přenosů dat, a aby měl operátor kdykoliv možnost získat z těchto platforem spolehlivá data potřebná pro výkon státního dozoru.

Požadavky na umístění serverů operátorů

Požadavky na umístění serverů, na kterých jsou provozovány platformy, by měly být ze strany Ministerstva financí formulovány tak, aby na operátory nekladly takové nároky, které by mohly případně vést k růstu nelegálního trhu s on-line hrami v České republice.

Nicméně pro efektivní výkon státního dozoru je zcela nezbytné, aby mělo **MF kdykoliv možnost získat potřebná data** uložená v platformách operátorů, a to prostřednictvím vzdáleného přístupu i návštěvy v provozovně operátora. Vhodným řešením tak může být stanovení povinnosti pro operátory, aby na území České republiky povinně umístili alespoň své archivační servery pro účely kontrol na místě. Rovněž by měla být ze strany MF stanovena povinnost, která data by na těchto serverech měla být operátory archivována.

Způsoby zasílání finančních prostředků na hráčský účet

Povolené způsoby zasílání finančních prostředků na hráčský účet by měly být stanoveny právním předpisem. Povolenými způsoby by měly být zejména:

- Bankovní převod.
- Využití debetní karty.

Mezi **zakázané způsoby** zasílání finančních prostředků na hráčský účet by mělo patřit zejména využití:

- Kreditní karty.
- Šeku.

Kreditní karty i šeky by neměly být povoleny z toho důvodu, že umožňují hru na dluh, která je z hlediska sociálních dopadů nežádoucí.

Omezení zahraničních bankovních účtů

Pro účely zaslání finančních prostředků na hráčský účet by mělo být povoleno pouze využití českých bankovních účtů, aby bylo případně možné využít čísla těchto účtů pro účely verifikace identifikačních údajů poskytnutých ze strany uchazečů o registraci.

3.2.3. Technické zabezpečení kontroly technických zařízení ze strany státního dozoru

Cíl auditů ze strany MF

Mezi **hlavní cíle** auditů realizovaných ze strany MF by mělo patřit zejména ověření toho, zda operátoři plní požadavky stanovené MF. Prostřednictvím těchto auditů by mělo být ověřováno zejména plnění aspektů charakteru:

- **Technického** (správné fungování technických zařízení operátorů – např. fungování generátorů náhodných čísel).
- **Právního** (všeobecné dodržování právních předpisů souvisejících s jejich podnikáním).
- **Organizačního** (vnitřní uspořádání organizace operátora – např. zda jsou dostatečně nastaveny procesy pro účely boje s praním špinavých peněz apod.).

Způsob realizace auditů ze strany MF

MF musí mít možnost realizovat své audity jak prostřednictvím **vzdáleného přístupu**, tak prostřednictvím **výkonu kontroly na místě**. V rámci těchto auditů musí mít operátor povinnost poskytnout MF všechna relevantní požadovaná data, informace a dokumenty, které budou využity pro účely auditu.

Audity lze rozdělit do dvou hlavních fází:

- **V rámci procesu udělování licence.**

  V této fázi bude mít audit charakter správního řízení a bude se řídit správním řádem (zákon č. 500/2004 Sb.). Cílem tohoto auditu je ověření, zda operátor splňuje všechny podmínky k udělení licence.

- **V rámci výkonu kontroly již licencovaných operátorů.**

  Výkon kontroly v této fázi by měl Ministerstvu financí poskytnout určitou míru ujištění o tom, že jsou ze strany operátorů dodržovány podmínky, za kterých jim byla udělena licence k provozování platforem.

Pro účely auditu by mělo Ministerstvo financí využívat jak svých **interních kapacit**, tak i ze strany MF licencovaných **auditorů třetích stran** (zejména pro účely odborného posouzení technické oblasti). MF by pro tyto účely nemělo zaměstnávat celou řadu IT odborníků, ale tyto odborníky zajistit externě. Lze totiž předpokládat, že audity budou vyžadovat celou řadu různých specializací, a proto bude pro MF výhodnější tyto odborníky najímat ad hoc v případě potřeby.

Role centralizovaného informačního systému při realizaci auditů MF

Centralizovaný informační systém by měl při výkonu auditů zejména:

- umožňovat vzdálený přístup k datům operátora,
- automaticky ukládat a analyzovat data operátora a
- detekovat nesprávné fungování platforem (mající vliv na bezpečnost hráčů a správnost dat poskytovaných MF).

3.2.4. Metody ověření identifikace hráčů

Identifikační údaje poskytované hráči

Ze strany MF by měly být stanoveny **minimální požadavky na identifikační údaje**, které by měl hráč ucházející se o registraci operátorovi poskytnout. Minimálními identifikačními údaji by pak měly být zejména:

- Jméno a příjmení.
- Datum narození.
- Adresa trvalého pobytu.
- E-mailová adresa.
- Číslo bankovního účtu.

Způsob ověření identifikačních údajů hráčů

Způsob ověření identifikačních údajů poskytnutých hráčem by měl klást **minimální administrativní požadavky** jak na hráče (uchazeče o registraci v rámci určité platformy), tak na operátory. Cílem je, aby byla tato verifikace **maximálně automatizovaná**, a aby na hráče ani operátory nekladla příliš vysoké nároky.

Role centralizovaného informačního systému při ověření identifikačních údajů hráčů

Centralizovaný informační systém (CIS) by měl při ověření identifikačních údajů hráčů (např. prostřednictvím napojení na Základní registry veřejné správy, Centrální registr dlužníků, Registr pojištěnců veřejného zdravotního pojištění, Registr pojištěnců ČSSZ apod.) fungovat jako místo pro ověření identifikačních údajů poskytnutých každým uchazečem o registraci. Operátor by prostřednictvím automatizovaného nástroje zaslal identifikační údaje do CIS a ten by následně rozhodl, zda hráč může být registrován, nebo že registrován být nesmí (současně by operátor v rámci své interní databáze ověřil, výskyt poskytnutých identifikační údajů z pohledu duplicity).

Pro tyto účely by jednou z databází obsaženou v CIS měl být rovněž **registr hráčů se zákazem hraní** (zákazem nařízeným ze strany regulátora – Ministerstva financí – nebo na vlastní žádost hráče).

3.2.5. Způsoby boje s praním špinavých peněz

Povinnosti operátorů v oblasti boje s praním špinavých peněz

Povinnosti pro operátory jsou stanoveny ve směrnici Evropské komise k boji proti praní špinavých peněz, která stanoví, že operátoři musí zejména:

- Prověřovat všechny hráče a hodnotit rizika související s praním špinavých peněz (realizovat tzv. „due dilligence“).
- Uplatňovat zvláštní režim pro osoby s politickým profilem (tzv. „zesílené due dilligence“).
- Informovat příslušný úřad, pokud identifikují podezřelé transakce.
- Uchovávat data související s transakcemi a informacemi o hráčích a jejich hráčských účtech.
- Realizovat vlastní interní kontroly funkčnosti platforem.
- Pověřit vybraného zaměstnance výkonem boje proti praní špinavých peněz?

Tato opatření by se měla týkat všech povolených her, aby bylo dosaženo maximálního efektu boje s praním špinavých peněz.

Role centralizovaného informačního systému v oblasti boje s praním špinavých peněz

Centralizovaný informační systém by měl v oblasti boje proti praní špinavých peněz plnit zejména následující úlohy:

- Zaznamenávat, ukládat a vyhodnocovat data o uskutečněných transakcích a otevřených hráčských účtech.
- Ověřovat identifikační údaje poskytnuté uchazeči o registraci.
- Generovat automatické „alerty“ upozorňující na podezřelé chování hráčů a praní špinavých peněz.

3.2.6. Monitorování podvodů při sázení a hraní

Povinnosti operátorů v oblasti boje proti podvodům

Operátoři by měli realizovat opatření pro prevenci a detekci podvodů ze strany hráčů zejména ze své vlastní iniciativy. Tato opatření by měla spočívat zejména v následujících aktivitách:

- Detekce pokusů o podvody prostřednictvím automatických nástrojů v rámci platforem.
- Zablokování účtů hráčů podezřelých z podvodů.

Role centralizovaného informačního systému v oblasti boji s podvody operátorů

Centralizovaný informační systém by měl v oblasti boje proti podvodům plnit zejména následující úlohy:

- Zaznamenávat, ukládat a vyhodnocovat data o uskutečněných transakcích a provádět křížové kontroly těchto dat s daty poskytovanými operátory.
- Generovat automatické reporty signalizující podezřelé podvody operátorů.

3.3. Rámcové požadavky na zdroje pro realizaci modelu státního dozoru

3.3.1. Organizační uspořádání státního dozoru

V současné době je výkon státního dozoru realizován prostřednictvím **odboru 34 „Státní dozor nad sázkovými hrami a loteriemi“** Ministerstva financí, ve kterém pracuje 30 zaměstnanců. Tento odbor se skládá z Oddělení správního řízení a Oddělení právního a metodického.

Oddělení správního řízení aktuálně vykonává zejména činnosti spojené s povolováním provozování sázkových her a loterií. Oddělení právní a metodické aktuálně vykonává zejména koncepční činnost, monitoruje vývoj v právní oblasti na úrovni Evropské unie a rovněž vykonává dohledovou činnost nad trhem herního průmyslu[3].

[3] Zdroj informací: Webové stránky MF - http://www.mfcr.cz/cps/rde/xchg/mfcr/xsl/orgstru_59231.html.

Na výkonu státního dozoru se dle informací MF kromě výše uvedeného odboru podílí rovněž vybraní **zaměstnanci finančních úřadů** (v České republice se dle informací MF jedná o stovky zaměstnanců), kteří vykonávají fyzické kontroly zařízení operátorů na místě.

V budoucnu by měl dle doporučení Evropské komise[4] i současné praxe ve většině analyzovaných zemích útvar zajišťující výkon státního dozoru disponovat širšími kompetencemi a vyšší mírou nezávislosti, než je tomu nyní. Tento útvar by měl provozovat centralizovaný informační systém pro monitoring on-line herního průmyslu a rychle reagovat na zjištění získaná prostřednictvím tohoto systému. Pro tyto účely by byla žádoucí rovněž dostatečná flexibilita interních procesů tohoto útvaru.

Současně bude pro úspěšné zavedení nového modelu státního dozoru nezbytné, aby byl tento útvar schopen realizovat audity operátorů zejména prostřednictvím vzdáleného přístupu, k čemuž využije centralizovaný informační systém. Tyto požadavky je možné zajistit prostřednictvím dvou variant uvedených dále. U obou variant popisujeme jejich hlavní výhody a nevýhody v těchto oblastech:

- Význam postavení útvaru státního dozoru z hlediska vnímání ze strany operátorů.
- Míra závislosti útvaru státního dozoru na ostatních útvarech MF a s tím spojená flexibilita interních procesů v rámci útvaru státního dozoru.
- Dodatečné náklady a případná negativní publicita spojená se změnou uspořádání útvaru státního dozoru.

Níže uvádíme obě varianty možného uspořádání státního dozoru zajišťující výkon nového modelu státního dozoru.

- Tyto požadavky je možné zajistit prostřednictvím **zřízení organizační složky státu** formálně oddělené od MF (fakticky zřízením samostatného regulačního úřadu). Hlavními výhodami této varianty mohou být transparentnost a relativně silnější postavení samostatného regulačního úřadu z hlediska vnímání ze strany operátorů a relativní nezávislost na ostatních útvarech MF, která s sebou nese rovněž vyšší flexibilitu interních procesů. Zároveň toto řešení respektuje aktuální trendy v ostatních zemích (viz výsledky srovnávací analýzy) a je v souladu také s doporučením Evropské komise. Důležitou výhodou je také možnost přímé, flexibilní a efektivní spolupráce v rámci sítě evropských národních regulátorů / orgánů státního dozoru nad sázkovými hrami a loteriemi. Hlavní nevýhodou jsou dodatečné náklady a negativní publicita spojená se zřízením „nového úřadu“ v době, kdy je záměrem státu úřady spíše rušit a slučovat.

  V případě zřízení organizační složky státu (samostatného regulačního úřadu) by mohly být dodatečné náklady na její zřízení vykompenzovány přínosy této změny (např. vyšším počtem realizovaných transakcí v rámci legálně provozovaných platforem, efektivnější kontrolou nad daňovými odvody apod.).

- V případě, že by nebylo reálné zřídit tuto organizační složku státu, je možné rovněž **posílit kompetence současného odboru 34** „Státní dozor nad sázkovými hrami a loteriemi“ v rámci MF. Hlavní výhodou této varianty je potřeba nižších nákladů na zavedení nového modelu ve srovnání s možností zřízení nového úřadu a neexistence negativní publicity spojené se zřizováním nového úřadu. Hlavními nevýhodami jsou nižší legitimita postavení odboru ve srovnání se samostatným regulačním úřadem, vyšší závislost na ostatních útvarech MF a s tím spojená nižší flexibilita interních procesů, a rovněž relativně slabší postavení útvaru státního dozoru z hlediska vnímání ze strany operátorů.

3.3.2. Finanční požadavky

Předpoklady pro formulování finančních požadavků na technické řešení

Ze závěrů společného jednání s MF vyplynulo, že vhodný centralizovaný informační systém pro monitoring by měl svou robustností rámcově odpovídat italskému systému Totalizzatore a umožnit neustálé monitorování trhu (mít k dispozici data z trhu v reálném čase) pomocí jednotného rozhraní

[4] Zdroj: Sdělení Komise Evropskému parlamentu, Radě a Hospodářskému a sociálnímu výboru a Výboru regionů ze dne 23. 10. 2012: Příprava uceleného evropského rámce pro on-line hazardní hry.

s informačními systémy (platformami) operátorů. Systém by měl být přitom vybaven funkcionalitami uvedenými v kapitole 3.2.1. „Specifikace technického řešení systému provozování a monitoringu“.

Systém bude klást vysoké nároky především na **bezpečnost informací** v něm uložených a jím přenášených a na **stabilitu** z hlediska minimalizace výpadků provozu tohoto systému. Z pohledu funkcionality se systém nejvíce blíží řešení **business intelligence** s využitím již získaných dat ve vlastním datovém skladu nebo příležitostně přímo ze systémů operátorů (vzdáleně přístupných). Vedle toho bude od systému vyžadován **přenos dat v reálném čase a jejich ověřování** oproti externím či vlastním databázím a registrům (např. v průběhu registrace hráčů).

Další předpoklady:

- Systém bude komunikovat se stovkami až tisíci operátorů.
- Systém bude ověřovat data miliónů uživatelů.
- Systém bude monitorovat a vyhodnocovat milióny transakcí denně.

Rámcový odhad finančních nároků technického řešení

Tyto finanční nároky jsme rozdělili na investiční (jednorázové) náklady a provozní (opakované) náklady. Investiční náklady jsme dále odhadli pro dvě možné alternativy - systém navržený zcela nově a rovněž pro systém vybudovaný prostřednictvím úpravy standardního řešení. Níže uvádíme bližší specifikace v rámci těchto položek (včetně obvyklých cen člověkohodin prací na tvorbě IS, na základě kterých je možné v rámci zadávacího řízení hodnotit jednotlivé nabídky).

- **Investiční náklady na tvorbu systému.**
  - Návrh nového systému.
    - Obvyklá cena obdobně zaměřených projektů se pohybuje v řádu 100 až 250 mil. Kč.
    - Cena člověkohodiny programátora obvyklá na trhu se pohybuje v rozmezí 2 000 až 2 500 Kč.
  - Úprava standardního řešení.
    - Obvyklá cena obdobně zaměřených projektů se pohybuje v řádu 50 až 100 mil. Kč.
    - Cena člověkohodiny programátora obvyklá na trhu se pohybuje v rozmezí 1 000 až 2 000 Kč.
- **Provozní náklady na provoz systému**
  - Náklady na údržbu systému (tzv. maintenance) činí obvykle 15 – 25 % z investičních nákladů.
  - Náklady na licencování systému činí obvykle 12 000 až 24 000 Kč ročně za licenci[5]. Tyto náklady by byly hrazeny v případě, že bylo implementováno standardní řešení. Pokud by byla autorská práva k IS převedena na MF, pak tyto náklady nevzniknou.

V případě návrhu a tvorby nového informačního systému je možné rozdělit potřebné investiční náklady do tří kategorií: i) návrh informačního systému činí 12 -15 % z investičních nákladů; ii) tvorba informačního systému činí 50 % z investičních nákladů; a iii) dodávka hardware pro informační systém činí 35 – 38 % z investičních nákladů.

Z výše uvedených rámcových odhadů vyplývá, že cena za **vytvoření** centralizovaného systému pro monitoring se bude pohybovat **v řádu stovek mil. Kč**, přičemž **roční provozní náklady** se budou pohybovat **v řádu desítek mil. Kč**. Jedná se o velmi hrubý odhad založený na analogii s informačními systémy využívanými v České republice finančním sektorem.

Tyto **odhady finančních nároků a konkretizace architektury a funkcionality systému se budou postupně zpřesňovat** spolu s tím, jak budou postupovat přípravné práce na vytvoření systému (např. realizace soutěže o návrh a příprava věcného zadání veřejné zakázky – podrobnosti o těchto aktivitách

[5] Zdroj: Boris Evelson Forrester, průměrné licenční náklady za populární sady business inteligence.

jsou uvedeny v kapitole 3.4.1.). **Reálné nacenění tvorby a dodání systému lze získat až prostřednictvím realizace veřejné zakázky, kdy uchazeči předloží konkrétní cenové nabídky.**

Příklady v minulosti již zrealizovaných veřejných zakázek na tvorbu a dodání relativně unikátních a rozsáhlých informačních systémů nevylučují možnost vyšších investičních nákladů, než které jsme výše uvedli v našem rámcovém odhadu.

Dosavadní praxe rovněž ukazuje, že u podobných dlouhotrvajících projektů může v průběhu jejich realizace dojít k navýšení jejich rozpočtu o 15 – 25 % z důvodů, které není možné v úvodu těchto projektů předpokládat.

Doporučujeme Ministerstvu financí spolupracovat s Ministerstvem pro místní rozvoj a dalšími institucemi při přípravě nového programového období s cílem zajistit finanční prostředky pro vybudování systému centralizovaného informačního systému pro monitoring ze Strukturálních fondů Evropské unie.

3.3.3. Personální požadavky

Tato kapitola vychází z kapitoly 3.3.1. „Organizační uspořádání státního dozoru“. Implementace technického řešení pro výkon státního dozoru s sebou zřejmě ponese potřebu zřídit nový organizační útvar či jednotku (např. oddělení) zabývající se obsluhou informačního systému a analyzováním a vyhodnocováním informací získaných prostřednictvím tohoto systému. Při odhadovaném rámcovém rozsahu informačního systému a povaze činností, které bude obsluha systému vykonávat, odhadujeme potřebu **2 až 4 dodatečných zaměstnanců** pro zajištění výše uvedených činností.

Kromě obsluhy informačního systému a analyzování a vyhodnocování informací získaných prostřednictvím tohoto systému bude nutné zajistit rovněž zajistit údržbu systému. Pro tyto účely doporučujeme využít jednak služeb externí společnosti, a rovněž interních zaměstnanců. Náročnost této obsluhy odhadujeme na potřebu 1 až 2 zaměstnanců.

- V případě varianty posíleného odboru 34 doporučujeme využít kapacity interního útvaru MF zodpovědného za oblast informačních a komunikačních technologií (ICT).
- V případě varianty zřízení organizační složky státu (samostatného regulačního úřadu) bude třeba, aby si tato složka potřebné zaměstnance zajistila sama.

Centralizovaný informační systém rovněž umožní podstatně zvýšit počet kontrol (auditů) realizovaných prostřednictvím vzdáleného přístupu, což potenciálně může vést k možným úsporám na personálních kapacitách finančních úřadů, jejichž kontroloři v současnosti vykonávají kontroly operátorů na místě.

V konečném důsledku by tak mohlo zavedení nového modelu státního dozoru přinést určité úspory v personální oblasti. Pro potvrzení tohoto pozitivního efektu by však bylo třeba realizovat detailnější studii zaměřenou na toto téma.

3.4. Návrh akčního plánu k realizaci modelu státního dozoru

Akční plán je založen na hlavních aktivitách souvisejících s tvorbou technického řešení pro výkon státního dozoru. Doba trvání jednotlivých aktivit zahrnutých v akčním plánu má indikativní charakter.

3.4.1. Přehled hlavních aktivit

V rámci realizace technického řešení jsme identifikovali následujících sedm hlavních aktivit, které dále specifikujeme:

1. Příprava nového zákona o provozování sázkových her.
2. Přípravné práce k uspořádání soutěže o návrh informačního systému (IS).
3. Realizace soutěže o návrh architektury IS.
4. Příprava věcného zadání veřejné zakázky pro dodání IS.
5. Příprava materiálu do vlády o přípravě IS a jeho schválení.
6. Příprava a realizace veřejné zakázky na vytvoření a dodávku IS.
7. Analýza a vývoj IS.

1. Příprava nového zákona o provozování sázkových her

V době přípravy této Zprávy připravuje MF zcela nový zákon, který by měl nahradit stávající zákon o loteriích a jiných podobných hrách (č.202/1990 Sb.). Návrh tohoto zákona by měl být předložen do vlády do 30. 6. 2013 a měl by nabýt účinnosti nejpozději 1. 1. 2014.

Vzhledem ke stanovenému termínu předložení návrhu zákona na vládu předpokládáme časovou náročnost této aktivity v rozsahu 3 měsíců.

2. Přípravné práce k uspořádání soutěže o návrh architektury IS

V této aktivitě by měly být realizovány všechny přípravné kroky, které následně zajistí úspěšný průběh soutěže o návrh. Bude se jednat zejména o přípravu podmínek a dostatečné specifikace zadání soutěže o návrh. Součástí této aktivity bude rovněž sestavení kvalifikované nezávislé komise složené z expertů, která následně v rámci soutěže o návrh posoudí předložené návrhy.

Předpokládáme časovou náročnost této aktivity v rozsahu 1 až 3 měsíců. Pro účely přípravy akčního plánu jsme tuto náročnost stanovili na 2 měsíce.

3. Realizace soutěže o návrh IS

Základem pro vytvoření a dodávku centralizovaného informačního systému je specifikace funkčních a technických požadavků, která by měla vzejít ze soutěže o návrh informačního systému. Pro MF by bylo velmi obtížné dostatečně konkrétně definovat věcné zadání pro dodávku IS bez detailnější znalosti variantních technických možností. Tyto znalosti může MF získat právě prostřednictvím veřejné zakázky v podobě soutěže o návrh, která MF přinese zejména následující výhody:

- Získání variantních návrhů a různých pohledů na řešení unikátního IS.
- Možnost využít silné stránky jednotlivých návrhů.
- Možnost vyhnout se nevhodným řešením a vyvarovat se určitých rizik spojených s tvorbou nového IS.
- Získání dostatečných podkladů pro vytvoření věcného zadání veřejné zakázky pro vytvoření a dodávku IS.
- Možnost verifikovat dosavadní úvahy.

Výsledkem soutěže o návrh by tak mělo být získání takových podkladů, které umožní připravit kvalitní detailní věcné zadání pro veřejnou zakázku, jejímž předmětem bude dodání centralizovaného informačního systému pro monitoring.

Předpokládáme časovou náročnost této aktivity v rozsahu 2 až 4 měsíců. Pro účely přípravy akčního plánu jsme tuto náročnost stanovili na 3 měsíce.

4. Příprava věcného zadání veřejné zakázky na dodání IS

Věcné zadání by mělo být dostatečně konkrétní a srozumitelně formulované tak, aby mohlo MF v rámci zadávacího řízení získat maximálně porovnatelné nabídky. Pro tyto účely budou využity zejména znalosti a podklady získané v rámci soutěže o návrh centralizovaného informačního systému pro monitoring. Do přípravy tohoto věcného zadání by měl být rovněž zapojen IT útvar MF (aktuálně se jedná o odbor 33 „Řízení ICT resortu“) zejména z toho důvodu, aby byl výsledný informační systém kompatibilní s IT prostředím MF, a aby byl rovněž v souladu s interními koncepčními dokumenty MF pro tuto oblast.

Předpokládáme časovou náročnost této aktivity v rozsahu 1 až 3 měsíce. Pro účely přípravy akčního plánu jsme tuto náročnost stanovili na 2 měsíce.

5. Příprava materiálu do vlády o přípravě IS a jeho schválení

S ohledem na význam a předpokládaný finanční rozsah tohoto zcela nového koncepčního řešení státního dozoru bude nezbytné, aby byl záměr vybudovat nový centralizovaný informační systém projednán a schválen na úrovni vlády. Materiál do vlády by měl vycházet z dostupných podkladů MF (kromě jiného může být využita tato Zpráva), a měl by být připraven až poté, kdy bude hotové věcné zadání veřejné zakázky na vytvoření a dodávku informačního systému. To umožní, aby byly v materiálu do vlády zahrnuty dostatečné informace o předpokládaném rozsahu plánované veřejné zakázky.

Předpokládáme časovou náročnost této aktivity v rozsahu 1 až 3 měsíce. Pro účely přípravy akčního plánu jsme tuto náročnost stanovili na 2 měsíce.

6. Příprava a realizace veřejné zakázky na vytvoření a dodávku IS

Centralizovaný informační systém pro monitoring bude ze strany MF vybrán na základě realizace veřejné zakázky. Vzhledem k odhadované finanční náročnosti všech aktivit souvisejících s vybudováním IS lze předpokládat, že se bude jednat o nadlimitní veřejnou zakázku zadávanou v rámci otevřeného zadávacího řízení. Pro účely této veřejné zakázky doporučujeme zajistit možnost získání finančních prostředků ze strukturálních fondů Evropské unie určených na modernizaci technické infrastruktury veřejné správy (pravděpodobně aktuálně připravovaný Integrovaný regionální operační program).

Zadávací řízení by mělo být připraveno a realizováno ve spolupráci s útvarem MF zodpovědným za metodickou podporu pro oblast veřejných zakázek (aktuálně se jedná o oddělení 2302 – „Zadávání veřejných zakázek“).

Kromě věcného zadání veřejné zakázky bude třeba připravit rovněž ostatní dokumenty k veřejné zakázce, které vyžaduje zákon o veřejných zakázkách. V případě standardního průběhu zadávacího řízení (bez významnějších komplikací) odhadujeme jeho délku na 4 až 6 měsíců. Nicméně v rámci zadávacího řízení mohou nastat zejména následující události, které mohou vést k jeho prodloužení:

- Podání námitek uchazeče proti vyloučení ze zadávacího řízení pro nesplnění požadavků ze strany zadavatele.
- Podání námitek uchazeče proti rozhodnutí zadavatele o výběru nejvhodnější nabídky.
- Odvolání se uchazeče k Úřadu pro ochranu hospodářské soutěže z důvodu vyloučení uchazeče ze zadávacího řízení pro nesplnění požadavků stanovených zadavatelem nebo z důvodu podání námitek proti rozhodnutí zadavatele o výběru nejvhodnější nabídky.

Stávající praxe potvrzuje, že výše uvedené události se vyskytují poměrně často a při plánování je třeba brát v potaz jejich výskyt. Náš níže uvedený odhad časové náročnosti této aktivity je spíše založen na více optimistických předpokladech, kdy nedojde k výraznějším zdržením v rámci realizace veřejné zakázky.

Pokud by předpokládaná hodnota zakázky činila alespoň 300 mil. Kč bez DPH, pak by se jednalo o tzv. „významnou veřejnou zakázku“ dle § 16 zákona o veřejných zakázkách (č. 137/2006 Sb.), kdy by tato zakázka podléhala zvláštnímu režimu. Odůvodnění této veřejné zakázky by musela schválit vláda a v rámci zadávacího řízení by došlo ke značnému prodloužení lhůt.

Předpokládáme časovou náročnost této aktivity v rozsahu 4 až 8 měsíců. Pro účely přípravy akčního plánu jsme tuto náročnost stanovili na 6 měsíců.

7. Analýza a vývoj IS

V této fázi bude vítězný uchazeč vzešlý ze zadávacího řízení zodpovědný zejména za:

- Realizaci předimplementační analýzy.
- Vytvoření zdrojového kódu informačního systému (software).
- Zajištění hardware pro provoz IS (servery apod.).
- Testování a pilotní provoz.
- Náběh nově vytvořeného systému do plného provozu.
- Proškolení uživatelů.
- Finální předání systému do užívání MF.

Je dobrou praxí před nasazením IS do ostrého provozu realizovat testování a pilotní provoz IS. V této fázi již bude možné IS reálně provozovat a umožnit operátorům napojit se na tento IS. Nezbytnou součástí úspěšného nasazení systému bude rovněž dostatečná komunikace směrem k operátorům na trhu herního průmyslu.

Předpokládáme časovou náročnost této aktivity v rozsahu 8 - 12 měsíců. Pro účely přípravy akčního plánu pracujeme s předpokladem, že pilotní provoz IS bude možné zahájit po 6 měsících a následně bude možné do dalších 6 měsíců předat systém do plného užívání. Tuto aktivitu jsme tak v akčním plánu rozdělili na dílčí aktivity 7a (Analýza a vývoj IS) a 7b (Testování a pilotní provoz IS).

3.4.2. Akční plán aktivit v oblasti výkonu státního dozoru

Níže uvedený akční plán znázorňuje indikativní dobu trvání jednotlivých aktivit souvisejících s tvorbou technického řešení pro výkon státního dozoru. Je možné, že reálná doba trvání těchto aktivit se bude lišit. Pro tyto účely jsme odhadli rozsah doby trvání těchto aktivit uvedených v kapitole 3.4.1.

Celkovou dobu trvání přípravy technického řešení pro výkon státního dozoru odhadujeme na 25 měsíců. Tato doba může být významným způsobem negativně ovlivněna zejména případnými průtahy při:

- schvalování nového koncepčního uspořádání státního dozoru,
- realizaci zadávacích řízení a
- tvorbě informačního systému.

Z akčního plánu nicméně vyplývá, že centralizovaný informační systém může být uveden do provozu až po plánovaném datu začátku účinnosti nového zákona o provozování sázkových her, a to i v případě bezproblémové realizace všech uvedených aktivit.

4. Přílohy

4.1. Příloha č. 1 – Matice parametrů

Parametr	Klíčové otázky	Analyzovaná země č. 1			
		Hlavní zjišťované informace	**Popis stavu**	**Hlavní výhody**	**Hlavní nevýhody**
Specifikace technického řešení **systému provozování a monitoringu online sázkových her** (dále "systém")	Jaké jsou základní **charakteristiky systému**?	Tvůrce (dodavatel), vlastník a provozovatel systému. Přehled uživatelů systému (např. státní dozor, finanční úřady, operátoři, policie apod.). Výše investičních a provozních nákladů systému (z hlediska finančního, personálního a časového) a zdroje/způsob financování. Pro které typy online sázkových her (dále "platformy") provozovatelů online sázkových her (dále "operátoři") existuje povinnost se k systému připojit. Maximální počet platforem operátorů, který může být k systému připojen. Počet operátorů a platforem reálně připojených k systému, způsob licencování. Průměrný denní objem transakcí, které systém monitoruje/zpracovává. Systémem zpracovaný průměrný denní počet sázek/finančních převodů (dále "transakce") uskutečněných na platformách operátorů. Délka životního cyklu obnovy systému. Výčet a typ externích registrů/databází napojených na systém. Legislativní požadavky na fungování systému. Podpora kontroly daňových příjmů z herního průmyslu prostřednictvím systému.	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*
	Jaká je **funkční** specifikace systému?	Jaké jsou funkcionality systému. Data sledovaná a zaznamenávaná systémem. Využití nástrojů "business intelligence" pro odhalení podvodů a boj s praním špinavých peněz. Ověřování dat v systému (kompletnost, správnost, aktuálnost).	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*
	Jaká je **technická** specifikace systému?	Charakter provozní, datové, softwarové, hardwarové a technologické architektury systému. Charakter rozhraní a komunikačních protokolů systému. Zajištění fyzické a logické bezpečnosti. Zajištění datové bezpečnosti včetně realizace validačních kontrol. Zajištění komunikační bezpečnosti systému. Způsob připojení platforem operátorů k systému.	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*

Parametr	Klíčové otázky	Analyzovaná země č. 1			
		Hlavní zjišťované informace	**Popis stavu**	**Hlavní výhody**	**Hlavní nevýhody**
Technické požadavky na **provozovatele sázkových her**	Jaké jsou **funkční a technické požadavky** na platformy operátorů?	Popis minimálních technických požadavků na platformy operátorů. Popis požadavků na funkcionality platforem operátorů.	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*
	Jak probíhá **kontrola** hraní a sázení?	Způsob sledování uskutečněných transakcí v reálném čase. Způsob vyhodnocování získaných dat (interim, ex-post).	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*
	Jak jsou regulovány **finanční transakce**?	Způsoby zasílání finančních prostředků na účet hráče/sázejícího (dále "účastník"). Přístup k povolování hotovostních transakcí. Způsob monitoringu zneužití identity účastníka. Způsob omezení využívání kreditních karet/bankovních účtů jiného státu.	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*
Technické zabezpečení **kontroly technických zařízení** ze strany státního dozoru v reálném čase	Jak je technicky zabezpečena **kontrola technických zařízení**?	Způsob využívání a charakter IT auditů (kontrol) platforem operátorů. Způsob kontroly plnění funkčních požadavků na platformy provozovatelů. Způsob zajištění, nastavení a realizace kontroly platforem a transakcí v reálném čase (např. analýza auditních záznamů). Způsob využití preventivních (automatických) nástrojů kontroly (např. monitoring výkonu, počtu přihlášených uživatelů apod.). Způsob nastavení a fungování management reportingu (sestavování zpráv a jejich distribuce), nastavení systému hlášení mimořádných událostí a upozornění (red flags).	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*
Metody **ověření identifikace hráčů**	Jak probíhá proces **registrace** a **ověřování** uživatelů?	Výčet požadovaných identifikačních dat uživatelů a způsob jejich sběru. Způsob verifikace požadovaných identifikačních dat uživatelů. Způsob ochrany identifikačních dat uživatelů. Existence a charakter seznamu blokovaných uživatelů.	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*
Způsoby **boje s praním špinavých peněz**	Jaké jsou hlavní způsoby **boje s praním špinavých peněz**?	Způsob monitorování a vyhodnocování rizik souvisejících s možností praní špinavých peněz. Existence monitoringu účastníků s politickým profilem. Způsob reportování podezření na praní špinavých peněz místním úřadům. Aplikace principu "poznej svého zákazníka", tzn. způsob poznání a prověřování uživatelů a jejich finančních zdrojů. Způsob uchovávání dat o transakcích. Další způsoby boje s praním špinavých peněz.	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*
Ostatní	Jak jsou **monitorovány podvody** při sázení a hraní?	Způsob sledování a odhalování podvodů. Data využívaná pro účely sledování a odhalování podvodů. Postup při odhalení podvodů.	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*	*Bude předmětem Projektu.*

4.2. Příloha č. 2 – Matice parametrů a textové dokumenty pro jednotlivé země

Matice parametrů i textové dokumenty zpracované pro jednotlivé analyzované země jsou přiloženy v samostatném souboru ve formátech MS Excel, resp. MS Word. Tyto dokumenty byly dle dohody se zástupci MF zpracovány v anglickém jazyce.

4.3. Příloha č. 3 – Seznam zdrojů

V této příloze uvádíme seznam významných zdrojů, které jsme využili pro účely zpracování srovnávací analýzy a návrhu nového modelu státního dozoru. Konkrétní zdroje informací jsou pak uvedeny v pracovních textových dokumentech zpracovaných pro jednotlivé země (viz přílohu č. 2).

- Informace získané od kanceláří Ernst & Young v jednotlivých analyzovaných zemích.
- Národní zákony jednotlivých analyzovaných zemí o hraní a sázení.
- Ostatní zákony jednotlivých analyzovaných zemí (např. o boji proti praní špinavých peněz).
- Národní technické standardy jednotlivých analyzovaných zemí.
- Dokumenty a webové stránky národních regulátorů jednotlivých analyzovaných zemí.
- Webové stránky Ministerstva financí.
- Dokumenty Evropské komise.
- Informace poskytnuté ze strany zástupců MF.

Ernst & Young

Audit | Daně | Transakce | Poradenství
www.ey.com