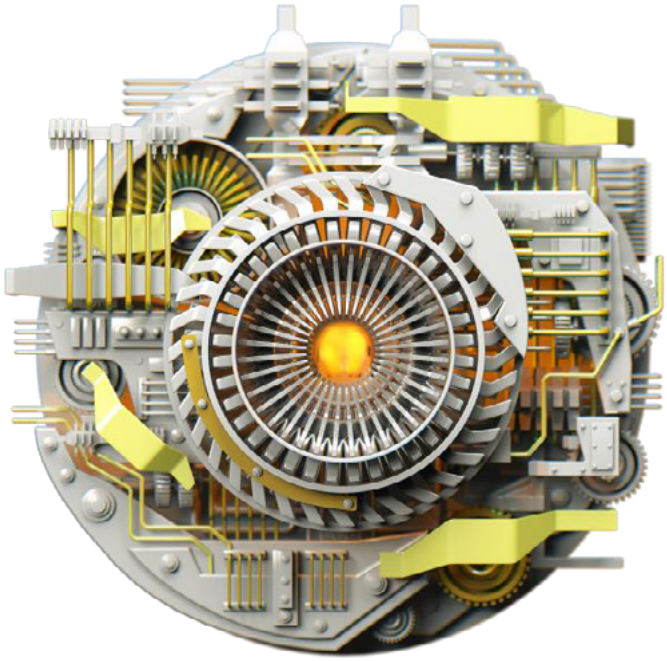
Deloitte.



# Správa dat:

## Proč je to důležité prověřování účinnosti sankcí

### 1. Co je to prověřování sankcí a kdo jej provádí?

V roce 2019 vyústila donucovací opatření a vyšetřování porušování sankcí k pokutám ve výši 8,14 miliard USD (celosvětově) za nedodržení předpisů AML, KYC a sankčních předpisů.[1]

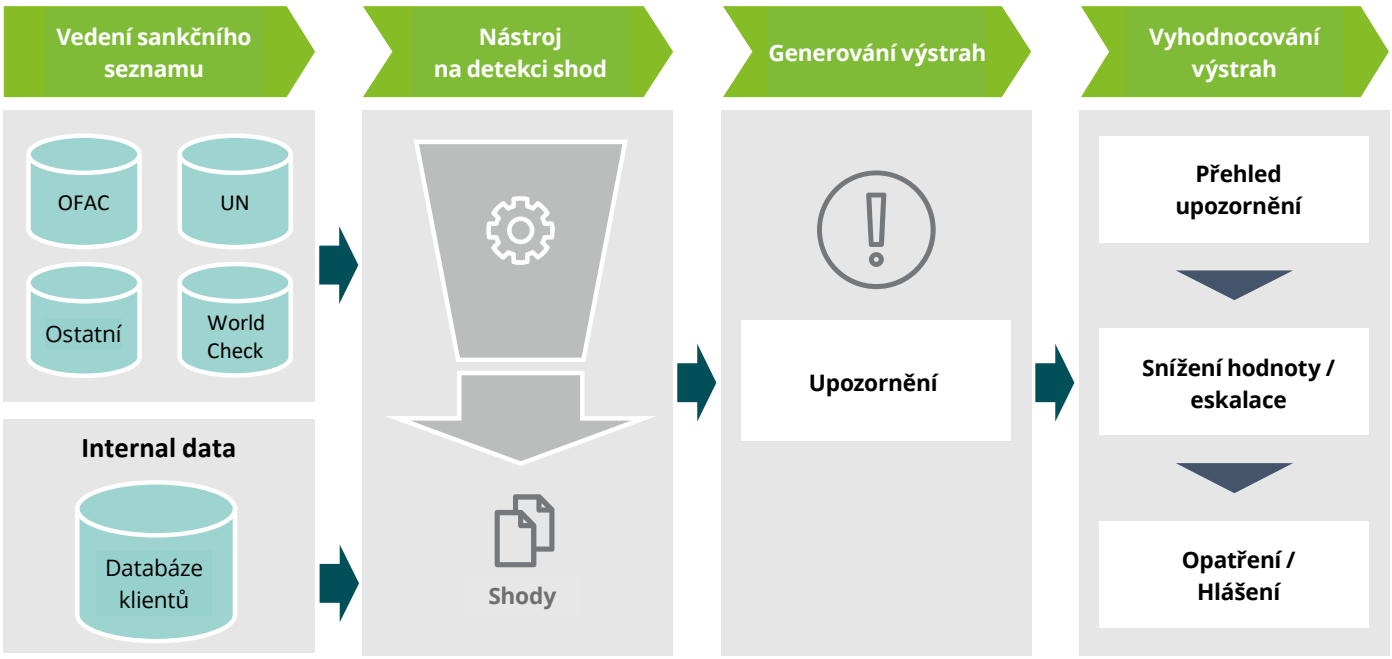
Jedním z příkladů vysokých pokut je např. 8,9 miliardy USD, které BNP Paribas zaplatila v roce 2014 americkým úřadům za porušení obchodních sankcí USA. Další případ je z roku 2020, kdy byla Standard Chartered Bank pokutována částkou 24,9 miliony USD za vážné porušení sankcí poskytnutím úvěrů ve výši přibližně 119,1 milionů USD ruské bance na Ukrajině. A třetí příklad je z roku 2018, kdy Société Générale souhlasila s tím, že americkým úřadům zaplatí 1,3 miliardy USD za urovnání případu zahrnujícího zpracování dolarových transakcí v rozporu s americkými sankcemi.[2,3] Spojení se sankcionovanou osobou, subjektem nebo zemí může vést také k významnému poškození pověsti finanční instituce.

Wolfsbergská doporučení pro prověřování sankcí uvádějí, že finanční instituce by měly „udržovat účinný a efektivní proces prověřování sankcí". Očekává se, že by větší finanční instituce měly k zajištění souladu s předpisy a zvládnutí rostoucí složitosti v oblasti sankcí využívat technologie. Technologie mohou pomoci provést požadovanou analýzu a také nezbytné kontroly. Použití vhodných technologických řešení a automatizace může zvýšit efektivitu. Nedávné technologické trendy nejen usnadnily institucím prohledávání obrovského množství dat, ale také zvýšily očekávání ohledně procesu Due Diligence a standardů v odvětví.

Sankce jsou hlavní součástí celosvětového úsilí proti finanční kriminalitě. Jsou zaměřeny na státy, fyzické nebo právnické osoby, které jsou zapojeny do nezákonných činností či jsou podezřelé z účasti na nich. Vlády a organizace jako OSN, OFAC a EU uvalují sankce a omezení, ale finanční instituce mají za úkol je uplatňovat. Jsou povinny prohledávat své klientské databáze a údaje o transakcích, aby odhalily jakákoli potenciální porušení. Některé z organizací, které vydávají sankční seznam, ovšem nemají pravomoc vymáhat tresty, např. OSN. Pak jsou tu však místní úřady, jako je FINMA ve Švýcarsku, které prosazují platné sankční předpisy. Neexistuje žádný model „jedno pravidlo pro všechny" pro dodržování sankcí, který by byl vhodný pro všechny instituce. Model by měl být navržen tak, aby zohledňoval faktory, jako je povaha podnikání instituce, zahrnuté země a používané měny. Aby instituce zavedly účinný program dodržování sankcí, musí nejprve určit rozsah použitelných sankčních předpisů. Program dodržování sankcí zahrnuje dva typy prověřovací kontroly: prověřování transakcí a prověřování klientů.

Oba typy kontrol jsou závislé na spolehlivém mechanismu založeném na hledání shody. Ten vzájemně porovnává data z interních a externích zdrojů, aby se zjistily podobnosti, které naznačují možnou shodu. Jakmile je identifikována možná shoda, je vygenerováno upozornění. Poté je přesměrován ke kontrolorovi shody, aby posoudil, zda výstraha označuje shodu „skutečnou", nebo „falešnou". Při identifikaci skutečné shody s dostatečnou jistotou musí instituce uplatnit nezbytná opatření, jako je zablokování transakce a hlášení příslušným orgánům.

## Proces prověřování sankcí




Aby byly instituce schopny držet krok s měnícím se prostředím sankcí a aby zůstaly v souladu se svými regulačními povinnostmi, je pro ně efektivní proces správy dat stále důležitější. V tomto kontextu se podíváme na základy správy dat a potenciální přístup k vybudování robustního programu prověřování sankcí.

## 2. Co je to správa dat?

Správa dat zahrnuje shromažďování, údržbu a používání dat bezpečným, účinným a efektivním způsobem. Organizace stále více vnímají data jako klíčové aktivum pro vytváření hodnoty, a proto nabývá na důležitosti robustní strategie správy dat.

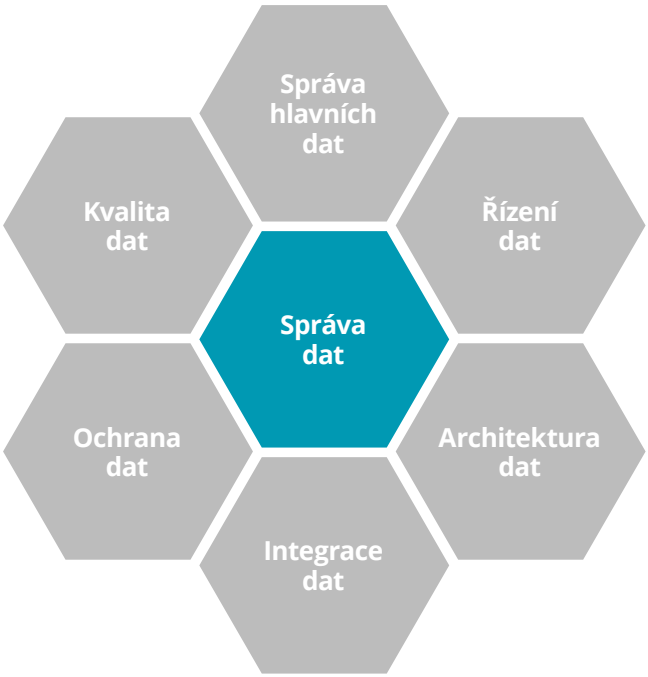
„Cílem správy dat je pomáhat lidem, organizacím a souvisejícím stranám optimalizovat využití dat v mezích předpisů a regulace, aby mohli činit rozhodnutí a přijímat opatření, které maximalizují přínos pro organizaci.“[4]

Dobře udržovaná strategie správy dat může organizacím pomoci získat konkurenční výhodu nad svými obchodními rivaly, protože zlepšuje provozní efektivitu a rozhodování. Organizace, které mají kontrolu nad svými daty, mohou být také agilnější, mohou dříve zaznamenat trendy na trhu a dříve přijmout proaktivní opatření.

„Zacházení s daty jako s aktivem může vést k různým výhodám, které lze zpeněžit, měřit a spravovat.“[5]

## 2. 1. Proces prověřování sankcí

Správa dat se skládá z následujících prvků:




### Řízení dat

Odkazuje na soubor pokynů (plánování, monitorování a prosazování) pro řízení datových aktiv a zajišťuje, aby všichni dodržovali pravidla.[6]

### Architektura dat

Datová architektura je koncepční struktura nebo rámec prostředí správy dat, jeho součástí a interakcí. „Propojuje rámec, lidi, procesy, projektové zásady, technologie a postupy pro správu a používání cenných podnikových informačních aktiv."[4]

### Integrace dat

Integrace dat je proces spojování dat z různých zdrojů/kanálů sběru dat a jejich vkládání do formátu pro zpracování.

### Ochrana dat

Ochrana dat se týká soukromí a citlivosti osobních údajů o klientech a postupů pro zajištění toho, aby osobní údaje byly shromažďovány, sdíleny a používány vhodnými způsoby.

### Kvalita dat

Kvalita dat se týká přesnosti, úplnosti, aktuálnosti a konzistence dat spolu s požadavky a pravidly pro jejich použití. Problémy s kvalitou dat jsou většinou spojené se správou dat. „Bez správy dat se úsilí o kvalitu dat stává nákladným jednorázovým úkonem." Aby byla zajištěna kvalita dat, je nutné porozumět jejímu účelu, činnosti, kontextu a způsobu měření.[4]

### Správa hlavních dat

V obchodním kontextu jsou kmenová data klíčová data v systému. Nemají transakční povahu, i když mohou zahrnovat záznamy o transakcích. Představují nejcennější datová aktiva organizace. Účelem správy kmenových dat je poskytnout procesy pro sběr, agregaci, párování a konsolidaci dat. Kmenová data představují „jediný zdroj pravdy" organizace pro konkrétní soubor dat a zajišťují společné porozumění.

## 3. Význam cyklu správy dat pro účinné prověřování sankcí

Principy skupiny Wolfsberg říkají:

> „Prověřování sankcí se využívá při odhalování, prevenci a narušování finanční kriminality a zejména sankčního rizika. Porovnává data získaná z operací finanční instituce, včetně záznamů o klientech a transakcích ze strukturovaných (KYC) i nestrukturovaných (produktová dokumentace, poznámky klientů) se seznamy sankcionovaných jmen a dalšími ukazateli sankcionovaných stran nebo míst."[7]

Vzhledem k tomu, že finanční instituce denně zpracovávají velké objemy údajů o klientech a transakcích, může být prověřování těchto údajů s relevantními seznamy sankcí náročným úkolem. Finanční instituce jsou podle předpisů povinny zajistit, že nebudou mít vztah s jednotlivci nebo subjekty, které jsou na sankčním seznamu, ani se subjekty, které jsou vlastněny sankcionovanými osobami a subjekty nebo jsou s nimi propojeny. To není snadný úkol, protože mnoho jedinců používá podobná jména, což má za následek velké množství falešných shod ve výsledcích. K určení přesnosti shody lze použít dodatečné informace, jako je geografická poloha, adresy, zaměstnání nebo datum narození – úplnost a kvalita dat zvyšuje možnost potvrzení skutečné shody

Finanční instituce jsou rovněž povinny prověřovat vysoce rizikové transakce procházející prostřednictvím klientských účtů, aby se zajistilo, že klienti nepřevádějí peníze sankcionovaným jednotlivcům, subjektům, jurisdikcím nebo obchodním sektorům či od nich. Každá instituce by se měla rozhodnout, které typy transakcí a které atributy v nich jsou relevantní pro prověřování sankcí. Příjemci a odesílatelé transakcí jsou relevantní pro sankční programy založené na seznamu, zatímco adresy jsou relevantnější pro prověřování proti geografickým sankčním programům.

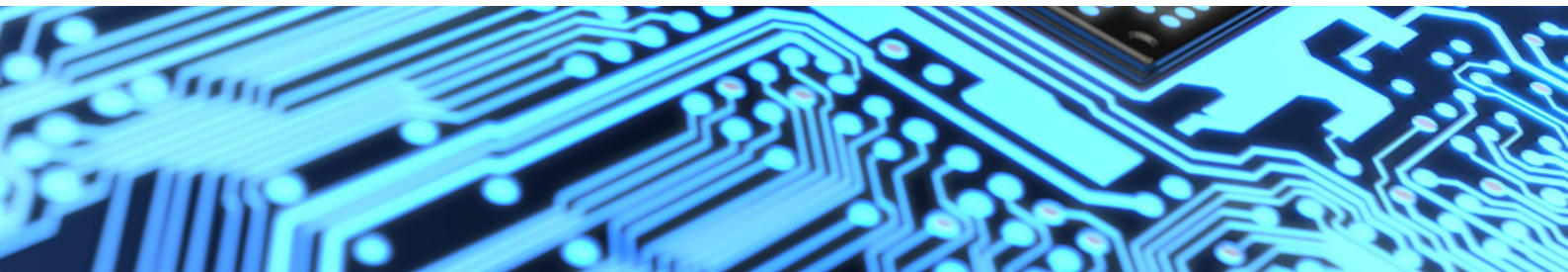
Mezi další běžné transakční atributy používané pro prověřování patří plavidla, agenti, zprostředkovatelé a jiná textová pole, jako jsou referenční informace o platbě nebo stanovený účel platby v poli 70 swiftové zprávy.

.

### 3. 1. Správa dat získaných z prověřování sankcí

Kontroly prověřování spoléhají na interní i externí zdroje dat. Některé z klíčových interních zdrojů dat napříč geografickými lokalitami a obchodními sektory jsou kmenová (klientská) data, transakční data a další klientské informace specifické pro obchodní sektor. Mezi externí zdroje dat patří sankční seznamy a další ukazatele sankcionovaných stran. Pro screening a obohacení zdrojů dat lze také použít další externí zdroje dat, jako jsou veřejné rejstříky, vládní seznamy nebo jiné spolehlivé nezávislé licencované zdroje. Zdroje dat jsou často distribuovány mezi více IT systémy a musí být identifikovány, aby bylo možné posoudit, které prvky dat jsou potřebné pro proces screeningu. Účelem identifikace dat je získat celkový pohled na klientskou základnu instituce.

Je důležité, aby všechny zdroje dat mohly být propojeny a integrovány na co nejpodrobnější úrovni, a měly by mít stejné standardy kvality. Než mohou být klientská, referenční nebo transakční data použita pro screening, musí být extrahována, obohacena, zmapována, transformována a/nebo nahrána do jediné platformy. Pokud dojde během procesu k poškození nebo kompromitaci dat, model prověřování sankcí nebude fungovat tak, jak bylo zamýšleno. „Supervisory Guidance on Model Risk Management", vydaný Office of the Compthroller of the Currency (Úřad měnové kontroly ministerstva financí Spojených států amerických), uvádí: „Proces ověření zahrnuje kontrolu, že interní a externí datové vstupy jsou i nadále přesné, úplné, v souladu s účelem a designem modelu, a v co nejvyšší dostupné kvalitě."[8] Finanční instituce by proto měly zajistit, aby datová kvalita, úplnost a integrita byly pravidelně testovány, dokumentovány a sledovány.



## 3. 2. Správa sankčních seznamů

I když se může zdát, že sankční seznamy jsou jednoduché a přímočaré, v praxi zahrnují velké množství různých údajů, včetně nejen jmen uvedených subjektů a jednotlivců, ale také dalších podrobností, jako jsou známé zkratky, akronymy, aliasy a geografické polohy. Za účelem zavedení efektivního procesu řízení by instituce měly jasně definovat, kdo je odpovědný za doručení a vedení sankčních seznamů. Prvním krokem v procesu správy sankčních seznamů je stanovení priority seznamů považovaných za relevantní pro prověřování. Mohou to být externě získané seznamy od třetích stran, nebo mohou být seznamy získané z webových stránek regulačních orgánů (např. OFAC, OSN, EU) a také interní seznamy jednotlivců, subjektů, regionů, přístavů nebo zakázaného zboží. Výběr seznamů závisí na různých faktorech, jako je typ klientů, nabízené produkty a povaha podnikání.

Za účelem výběru příslušných seznamů by finanční instituce měly provést posouzení založené na riziku a vzít v úvahu příslušné regulační požadavky. Finanční instituce, které využívají externí dodavatele pro získávání a udržování regulačních sankčních seznamů, by měly mít formální proces pro sladění seznamů poskytnutých třetí stranou s regulačními seznamy, aby byla zajištěna úplnost. Na druhé straně finanční instituce, které se spoléhají pouze na sankční seznamy z regulačních webových stránek, musí zajistit, aby jejich proces zahrnoval konsolidaci dat z více zdrojů, které mohou být v různých formátech. Kromě toho budou někteří jednotlivci/subjekty zahrnuti do více než jednoho seznamu, takže je nutné odstranit duplikáty, protože pokud tak neučiníte, může se upozornění vygenerovat dvakrát. V takových případech by finanční instituce měla zvážit realizaci systému správy sankčních seznamů pro čištění, analýzu a formátování dat seznamu, aby se zlepšila přesnost shody a snížil se počet falešně pozitivních výsledků.

## 4. Výzvy při správě dat pro prověřování sankcí

Finanční instituce čelí mnoha problémům se správou dat pro účely prověřování sankcí. Níže uvádíme vybrané příklady:

### Prověřování politicky exponovaných osob (PEP) a osob s vazbou na PEP

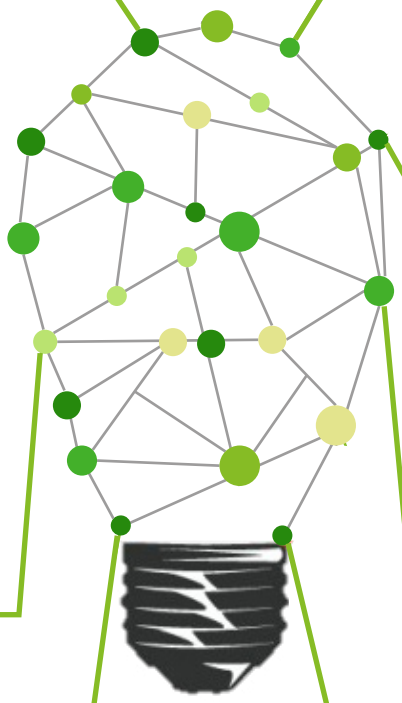
Ačkoli vládní nařízení, jako je čtvrtá směrnice Evropské unie proti praní špinavých peněz nebo doporučení FATF, poskytují detailnější požadavky týkající se PEP, neexistuje jasný způsob, jak identifikovat PEP a jejich společníky na celém světě. Existuje mnoho externích poskytovatelů PEP databází může však být obtížné použít informace, které obsahují, ke správnému přiřazení klienta finanční instituce k PEP. V reakci na dohled, který je na ně aplikován, se PEP snaží najít způsoby, jak se vyhnout odhalení, jako je otevírání účtů jménem korporací v offshore jurisdikcích namísto jejich vlastních jmen nebo jmen členů rodiny.

### Různé systémy psaní a regionální konvence pojmenování

Finanční instituce musí často prověřovat klienty, jejichž jména jsou na seznamech, které nejsou původně napsány latinkou, ale čínštinou, azbukou nebo arabštinou, jako jsou podezřelí teroristé ze zemí Blízkého východu. Mnoho jmen teroristů na seznamu OFAC SDN obsahuje také aliasy. Může být užitečné znát určitá pravidla týkající se jmen. Například mnoho arabských jmen začíná slovem „Abu“, které znamená „otec“. Abu, za kterým následuje podstatné jméno, znamená „svoboda“ nebo „boj“ a používají jej teroristé i legitimní političtí vůdci.

### Izolované systémy

V mnoha případech nejsou systémy finančních institucí po akvizici nebo fúzi integrovány v jejich pobočkách a dceřiných společnostech.



### Sjednocení sankčního seznamu

Finanční instituce by měly zavést účinný proces, který zajistí, že sankční seznamy, které používají v procesu prověřování, poskytují přesný a úplný jednotný seznam pro prověřování.

### Nedostatečná správa dat

Neúplnost, nedostatečná kvalita a integrita údajů jsou hlavními důvody špatné výkonnosti systémů prověřování sankcí. Chybějící nebo nesprávné informace Know Your Customer (KYC) nebo chybějící informace o vlastnících společnosti, skutečných majitelích dodavatelích nebo jiných protistranách mají negativní dopad na účinnost screeningových nástrojů, protože vytvářejí velké množství falešně pozitivních shod nebo znemožňují odhalit sankcionované entity či jednotlivce.

### Manuální zpracování dat

Klientská data jsou často zadávána do bankovního systému ručně během procesu onboardingu, což také zvyšuje pravděpodobnost chyb.

### Objem dat

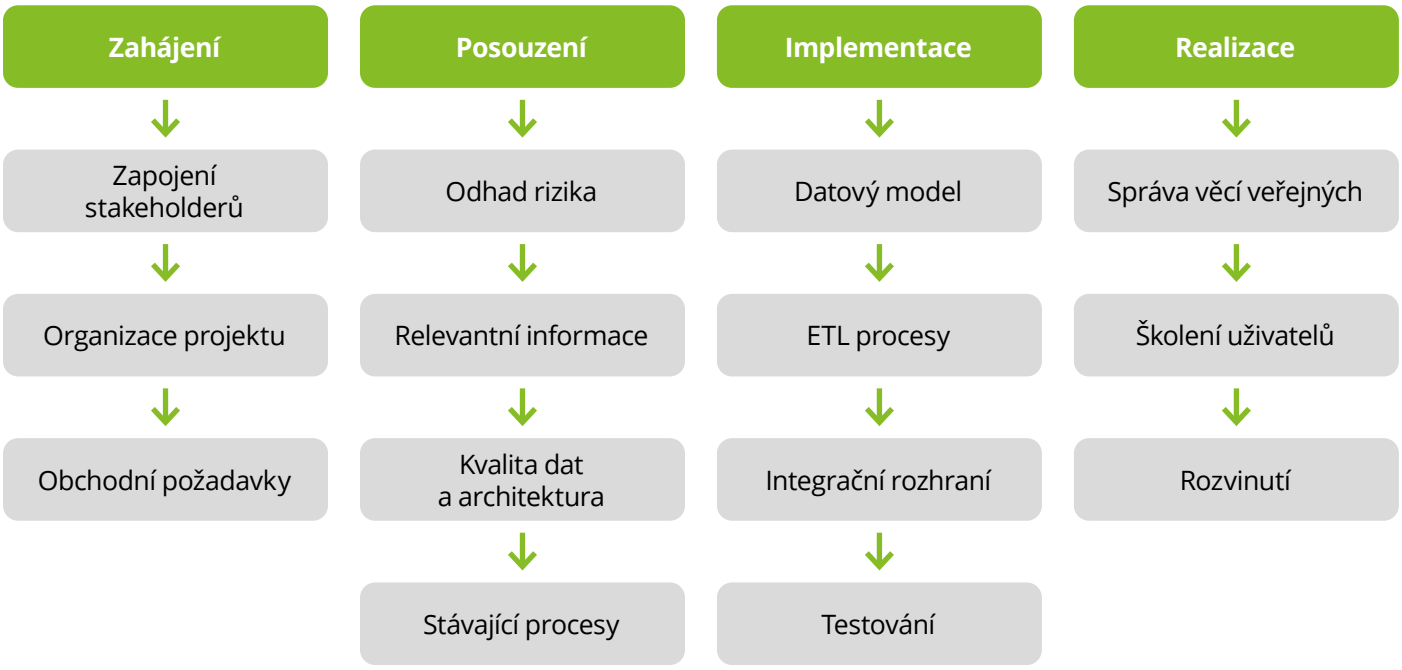
Velký objem dat související s komplexním procesem prověřování sankcí činí provoz systému manuálního zpracování velmi obtížné, ne-li nemožné.

# 5. Možné řešení a jeho přínosy

## 5. 1. Návrh a realizace

Níže uvedený obrázek ilustruje realizaci i a fungování řešení pro finanční instituce při zavádění efektivního procesu prověřování sankcí. Řešení by muselo být částečně automatizované, přizpůsobené konkrétním obchodním potřebám a navrženo s holistickým přístupem založeným na riziku. Řešení obecně probíhá podle definovaného procesu, který se skládá z následujících kroků:

### Proces prověřování sankcí




### Zahájení

Vyžaduje se přístup shora dolů, do kterého jsou od samého počátku zapojeny příslušné zainteresované strany. Pro efektivní proces prověřování sankcí je zapotřebí technologie a přístup založený na datech. Organizace projektu by měla být definována předem, aby bylo možné zapojit příslušné zainteresované strany do všech fází projektu.

### Posouzení

Posouzení je založeno na obchodních požadavcích a zabývá se souvisejícími riziky, kvalitou požadovaných dat a datovou architekturou, jakož i stávajícími procesy, na které má screeningový systém vliv.

### Implementace

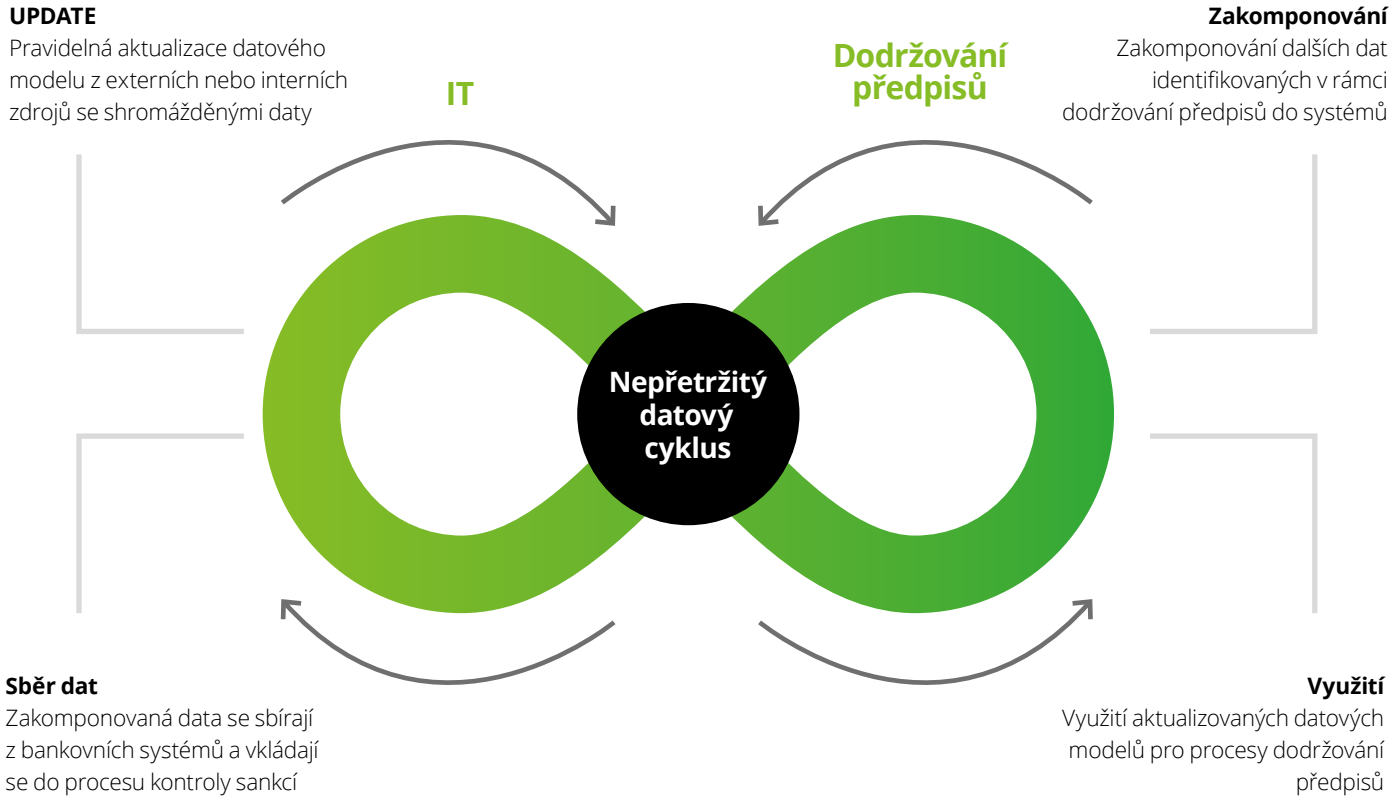
Datový model vytváří technický základ pro potenciální řešení. Měl by být flexibilní a rozšiřitelný. Přizpůsobené procesy „extrakce, transformace, načtení" (ETN) musí zajistit, že budou shromažďována aktuální data a že budou vhodně transformována. Integrační rozhraní umožňují využívat informace relevantními obchodními procesy.

### Realizace

Před uvedením technologického řešení do provozu musí být definováno řízení procesu a uživatelé musí být vyškoleni. Dalším zásadním aspektem je nasazení a údržba řešení, např. verzování řešení v procesu nasazení, aby bylo zajištěno zefektivnění údržby a aby byly nové verze nasazeny správně.

## 5. 2. Návrh a provedení

Jakmile je systém v provozu, měl by zajistit nepřetržitý cyklus dat mezi IT systémy organizace a systémem screeningu compliance oddělení. Data generovaná procesem kontroly sankcí by měla být automaticky aktualizována v odpovídajících IT systémech. Tato data mohou zahrnovat zjištění z interního vyšetřování nebo aktualizace modelů hodnocení rizikovosti klientů. To umožňuje IT systémům extrahovat přesná data pro jejich zahrnutí do screeningového modelu.




Toto schéma ukazuje rámec pro nepřetržitý cyklus správy dat pro účely prověřování sankcí. Interní data z IT systémů organizace proudí do procesu screeningu, kde se obohacují o další informace a poté se vrací zpět do IT systémů. Aby byla zajištěna kontinuita procesu, měla by být jmenována osoba odpovědná za správu dat, která bude vykonávat funkci dohledu. Stručně řečeno, efektivní správa dat a analýzy hrají důležitou roli při odhalování a snižování rizika finanční kriminality. Regulátoři z celého světa zdůrazňují důležitost zavádění nových technologií pro posílení programů prověřování sankcí finančních institucí.

## 6. Trendy v prověřování sankcí

Vzhledem k rostoucímu množství dat a neustále se měnícímu prostředí kontroly sankcí se stává automatizace zpracování a katalogizace dat, spolu s kontrolou sankcí v reálném čase, nutností. V poslední době se ve velkých institucích objevuje trend zavádění komplexnějšího přístupu a většímu využití dostupných dat.

„Sdílení informací je zásadní pro boj proti praní špinavých peněz, financování terorismu a financování šíření zbraní hromadného ničení. Překážky ve sdílení informací mohou negativně ovlivnit účinnost úsilí v oblasti boje proti praní peněz/financování terorismu. To podtrhuje důležitost rychlého, smysluplného a komplexního sdílení informací.“[9]

## 7. Zdroje


[1]"AML, KYC & Sanctions Fines for Global Financial Institutions Top $36 Billion Since Financial Crisis", Fenergo, 2020, https://www.fenergo.com/news/aml-kyc-and-sanctions-fines-for-global-financial-institutions-top-$36-billion-since financial-crisis.html

[2]"Banks adopt AI to manage sanctions and compliance risk", A. Ross, 2020, https://www.ft.com/content/98e82234- 16a8-11ea-b869-0971bffac109

[3]"Standard Chartered fined $24.9M for Ukraine sanctions breaches", N. Hodge, 2020, https://www.complianceweek.com/sanctions/standard-chartered-fined-249m-for-ukraine-sanctionsbreaches/28686.article

[4]"What Is Data Management?", Oracle, 2020, https://www.oracle.com/database/what-is-data-management/

[5]"Data integration: after the teenage years. Recruit Institute of Technology", B. Golshan, A. Halevy, G. Mihalia, W-G. Tan, 2017, https://dl.acm.org/doi/pdf/10.1145/3034786.3056124

[6]"Big data privacy: a technological perspective and review. Journal of Big Data ", P. Jain, M. Gyanchandani, N. Khare, 2016, https://journalofbigdata.springeropen.com/track/pdf/10.1186/s40537-016-0059-y

[7]"Wolfsberg principles on sanctions screening", The Wolfsberg Group, 2019, https://www.wolfsbergprinciples.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

[8]"Supervisory Guidance on Model Risk Management", Office of the Comptroller of the Currency, April 4, 2011, https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf

[9]"FATF Private Sector Information Sharing Guidance", Financial Action Task Force, November 2017, https://www.fatfgafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf


## Kontakty:


**Martin Kubačka**
**Partner | Deloitte Czech Republic**
mkubacka@deloittece.com
+420 776 306 694



**Tomáš Mihóčik**
**Senior Manager| Deloitte Slovakia**
tmihocik@deloittece.com
+421 910 820 005



**Marie Vichrová**
**Specialist Lead | Deloitte Czech Republic**
mvichrova@deloittece.com
+420 735 715 397



Přeloženo z anglického originálu Data management: Why it matters for effective sanctions screening publikovaného na webu Deloitte Switzerland.

Deloitte.