Autor: Institut pro regulaci hazardních her, z.s.

Věc: **Vyhodnocení dopadu vyhlášky MF o způsobu zasílání a oznamování informací a dat provozovateli hazardních her ve vztahu k ochraně soukromí a osobních údajů – navrhované náležitosti**

Zpráva:

Vážení,

Na základě dohody z jednání, které se uskutečnilo dne 4.2. 2019 si Vám dovolujeme zaslat návrh na seznam náležitostí, které by dle názoru IPRH mělo vyhodnocení dopadu reportovací vyhlášky obsahovat.

Obsah

I. ÚVOD **2**

II. PRÁVNÍ TITUL PLNĚNÍ PRÁVNÍ POVINNOSTI **2**

III. NÁLEŽITOSTI VYHODNOCENÍ DOPADU VYHLÁŠKY MF O ZPŮSOBU ZASÍLÁNÍ A OZNAMOVÁNÍ INFORMACÍ A DAT PROVOZOVATELI HAZARDNÍCH HER VE VZTAHU K OCHRANĚ SOUKROMÍ A OSOBNÍCH ÚDAJŮ **3**

1. Vyjasnění, zda má být zpracováno Posouzení vlivu na ochranu osobních údajů či nikoli 3
2. Účel zpracování osobních údajů 5
3. Právní titul zpracování osobních údajů 5
4. Zpracovávaný rozsah a kategorie osobních údajů 6
5. Hodnocení rozsahu a kategorií osobních údajů vzhledem k účelu zpracování (tzv. posouzení nezbytnosti) 6
6. Identifikace, hodnocení a kategorizace rizik zpracování osobních údajů 7
7. Zabezpečení přístupu k datům a organizační opatření – právní pohled 7
8. Technické zabezpečení dat 8
9. Doba uložení 9
10. Způsob informování subjektů osobních údajů 9
11. Zvážení předávání osobních údajů do zahraničí 9

IV. ZÁVĚR **10**

I. Úvod

Pokud nějaký právní předpis členského státu či EU po správci požaduje, aby osobní údaje zpracovával, resp. aby prováděl určitou činnost, pro kterou je zpracování osobních údajů nezbytné, bude se na takové zpracování aplikovat právní titul plnění právní povinnosti. Jedná se legitimní zpracování, nicméně je třeba splnit další náležitosti. Právní povinnost musí být zvláštním právní předpisem **stanovena natolik určitě, aby z ní bylo možné poznat, jaká zpracování na jejím základě budou probíhat. Správce také nesmí mít nepřiměřenou možnost vlastního uvážení v tom, jak povinnost splní. Daný účel nesmí být překročen**.

Právní povinnost musí vyplývat ze zákona, ale upřesněna může být i v podzákonném předpisu. Ustanovení zvláštního právního předpisu, které tuto povinnost obsahuje, se označuje tzv. právní základ. Na právní základ klade nařízení nároky specifikované v čl. 6 odst. 3 GDPR. [1]

Základ musí být stanoven právem ČR nebo EU. **Účel zpracování musí vycházet z tohoto právního základu. Právní základ nebo jeho doprovodné předpisy by měl obsahovat konkrétní ustanovení pro přizpůsobení činnosti správce, typu osobních údajů, které mají být zpracovány, dotčených subjektů osobních údajů, subjektů, kterým lze osobní údaje poskytnout, a účelu tohoto poskytování, účelového omezení, doby uložení a jednotlivých operací zpracování a postupu zpracování, jakož i dalších opatření k zajištění zákonného a spravedlivého zpracování, jako jsou opatření pro jiné zvláštní situace při nichž dochází ke zpracování a musí splňovat cíl veřejného zájmu a být přiměřené sledovanému legitimnímu cíli**.

Je tedy nezbytné, aby výše uvedené otázky vyhodnotil dokument sestavený správcem osobních údajů. V závislosti na naplnění podmínek stanovených ÚOOÚ[2] je třeba vyhodnotit, zda by měly být výše uvedené otázky zodpovězeny v rámci formalizovaného Posouzení vlivu na ochranu osobních údajů nebo jiného dokumentu. K metodice hodnocení vydal ÚOOÚ závazný dokument (více v bodě III. 1 tohoto dokumentu).

II. Právní titul plnění právní povinnosti

Zpracování osobních údajů subjektů primárně vyplývá z ust. § 133 odst. 1, písm. a) zákona č. 186/2016 Sb. Ministerstvo stanoví vyhláškou způsob oznamování a zasílání informací a přenosu dat provozovatelem orgánům vykonávajícím státní správu v oblasti provozování hazardních her podle tohoto zákona, **rozsah přenášených dat** a jiné technické parametry přenosu dat.

Právním základem je v tomto případě § 1 vyhlášky MF o způsobu oznamování a zasílání informací a přenosu dat provozovatelem hazardních her, rozsahu přenášených dat a jiných technických parametrech přenosu dat, který stanovuje, že data jsou poskytována v podobě vzdáleného přístupu, kterým je zabezpečený dálkový přístup k serveru provozovatele poskytujícímu chronologický přehled o herních a finančních datech, denního herního výkaznictví, denního herního zápisu a oznámení nebo zasílání jiných informací orgánům vykonávajícím dozor.

Širším účelem zpracování je dle důvodové zprávy (vypořádání připomínek) dozor nad dodržováním zákona o hazardních hrách a podmínek stanovených v základním povolení a v povolení k umístění herního prostoru. Užším je efektivnější kontrola řádného plnění povinností vyplývajících z daňových a účetních předpisů a dále kontrola sebeomezujících opatření.

[1] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3

[2] K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů. *Https://www.uoou.cz/* [online]. 8.2.2019 [cit. 2019-02-11]

Ve zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů bylo zdůrazněno, že příslušným správním orgánům budou předávány pouze informace a data ve vazbě na jedinečný identifikátor uživatelského účtu, tedy pouze ve formě anonymních údajů. Lze tedy shrnout, že navrhovaná úprava je v souladu s ochranou soukromí a osobních údajů. S tímto tvrzením byl ze strany IPRH vyjádřen nesouhlas, neboť se nejedná o data anonymizovaná, ale pseudonymizovaná. S tímto názorem zaměstnanci MF souhlasili. Proto je třeba posoudit výše uvedené zpracování osobních údajů a vydat a dokument, kterým budou zákazníci provozovatelů o zpracování informováni.

III. Náležitosti vyhodnocení dopadu vyhlášky MF o způsobu zasílání a oznamování informací a dat provozovateli hazardních her ve vztahu k ochraně soukromí a osobních údajů

1. Vyjasnění, zda má být zpracováno Posouzení vlivu na ochranu osobních údajů či nikoli

Nejprve je třeba vyjasnit, jakou by měl mít dokument MF strukturu. Existují dvě varianty – 1. Obecně neurčená struktura vyplývající z čl. 6 odst. 3 GDPR[3], která se použije za předpokladu, že není třeba sestavit Posouzení vlivu (nejsou naplněny podmínky pro jeho sestavení), 2. Formalizované Posouzení vlivu na ochranu osobních údajů. Posouzení vlivu na ochranu osobních údajů je nutné v případech, kdy zpracování osobních údajů má za následek vznik vysokého rizika pro práva a svobody fyzických osob, a to s přihlédnutím k povaze, rozsahu, kontextu, účelům zpracování a využitím nových technologií.

ÚOOÚ k tématu sestavil, a 8.2. 2019 vydal, dokument, ve kterém stanovil 10 podmínek, z nichž pokud jsou 2 a více naplněny kriticky, nebo 1 kriticky a 5 významně, správce osobních údajů musí sestavit Posouzení vlivu na ochranu osobních údajů. Zároveň uvádí zcela zásadní poznámku: „*Při hodnocení rizikovosti nelze brát v úvahu předpokládaná konkrétní řešení (například splnění nějakých technických nebo organizačních opatření typu pseudonymizace údajů) nebo vliv určitých faktorů (například zohlednění hrozeb, které na zpracování působí). Tyto úvahy budou již součástí vlastního posouzení vlivu na ochranu osobních údajů, jehož provedení je až následným krokem (v případech, kdy se na základě provedeného hodnocení rizikovosti dojde k závěru, že v rámci zpracování osobních údajů hrozí vysoká rizika pro práva a svobody subjektů údajů).*“

Samotné podmínky:

- Zpracování zahrnující monitorování subjektů údajů
- Zpracování kritických údajů, údajů umožňujících přímou identifikaci a/nebo údajů vysoce osobní povahy subjektů údajů
- Zpracování osobních údajů, které mohou vystavit subjekty údajů ohrožení z okolního prostředí
- Zpracování osobních údajů velkého rozsahu
- Zpracování zahrnující snímání veřejně přístupových prostor
- Zpracování osobních údajů s omezeným ovlivněním subjekty údajů
- Zpracování osobních údajů veřejně přístupných

[3] Dokument obsahující konkrétní ustanovení pro přizpůsobení správce, typu osobních údajů, které mají být zpracovány, dotčených subjektů osobních údajů, subjektů, kterým lze osobní údaje poskytnout, a účelu tohoto poskytování, účelového omezení, doby uložení a jednotlivých operací zpracování a postupu zpracování, jakož i dalších opatření k zajištění zákonného a spravedlivého zpracování, jako jsou opatření pro jiné zvláštní situace při nichž dochází ke zpracování a musí splňovat cíl veřejného zájmu a být přiměřené sledovanému legitimnímu cíli.

- Zpracování osobních údajů v technologicky složitých nebo pokročilých infrastrukturách nebo platformách
- Zpracování osobních údajů s vazbou na jiné správce nebo zpracovatele
- Zpracování osobních údajů s využitím nových technologických nebo organizačních řešení

Příklad vypořádání s podmínkami:

- Zpracování zahrnující monitorování subjektů údajů
  - Kritické naplnění – Zpracování údajů monitorujících fyzický pohyb nebo pobyt pomocí souřadnic.

- Zpracování kritických údajů, údajů umožňujících přímou identifikaci a/nebo údajů vysoce osobní povahy subjektů údajů
  - Kritické naplnění – Údaje vysoce osobní povahy *[například údaje z logů, historie navštívených stránek, údaje o uskutečněných voláních, údaje elektronické pošty, údaje o zařízeních (např. ICT) používaných subjektem údajů, finanční údaje (zahrnuje údaje o stavu majetku, výši finančních prostředků, dluzích nebo půjčkách, platební morálce) apod.]*.

- Zpracování osobních údajů, které mohou vystavit subjekty údajů ohrožení z okolního prostředí
  - Významné naplnění – s*ituačně daná zranitelnost (subjekty jsou zařaditelné jako členové vymezené skupiny podle toho, zda jde o žadatele vůči veřejné správě, o zaměstnance ve vztahu k zaměstnavateli, o příjemce vůči poskytovatelům zdravotních či sociálních služeb, odběratele léčiv, odběratele erotických pomůcek).*

- Zpracování osobních údajů velkého rozsahu
  - Kritické naplnění – *Při jeho určování je doporučeno (v souladu s pokyny WP243 a WP248) vzít v úvahu především následující faktory: počet dotčených subjektů údajů, objem údajů a/nebo rozsah zpracovávaných údajů, délka nebo trvání činnosti zpracování osobních údajů, zeměpisný rozsah činnosti zpracování údajů; přičemž tyto faktory musí být hodnoceny individuálně.*
    - *od 10001 subjektů údajů nebo více než 1,0 ‰ populace ČR nebo dotčených států,*
    - *a/nebo nad 20 přistupujících osob/zaměstnanců správce,*
    - *a/nebo s více než 20 místy zpracování/pobočkami,*
    - *a zároveň úroveň nejméně státu (NUTS = NUTS1) z hlediska původu/umístění subjektů údajů.*

- Zpracování osobních údajů v technologicky složitých nebo pokročilých infrastrukturách nebo platformách
  - Kritické naplnění – *Systémy sloužící k analýzám, profilování.*

- Zpracování osobních údajů s využitím nových technologických nebo organizačních řešení
  - Kritické naplnění – *Jedná se pro správce o nová řešení, nikde dosud nerealizovaná, se kterými nejsou žádné zkušenosti.*

Výjimka z Posouzení vlivu na ochranu osobních údajů:

Čl. 35 odst. 10 GDPR: Pokud má zpracování podle čl. 6 odst. 1 písm. c) nebo e) právní základ v právu Unie nebo členského státu, které se na správce vztahuje, a toto právo upravuje konkrétní operaci nebo soubor operací zpracování a pokud bylo posouzení vlivu na ochranu osobních údajů již provedeno jakožto součást obecného posouzení dopadů v souvislosti s přijetím uvedeného právního základu, odstavce 1 až 7 se nepoužijí, ledaže by členské státy považovaly provedení tohoto posouzení před činnostmi zpracování za nezbytné.

Příklad hodnocení[4]:

- *Jestliže byly splněny 2 z výše uvedených podmínek, je MF povinno zpracovat Posouzení vlivu na ochranu osobních údajů se všemi jeho náležitostmi.*
- *Výjimka se neuplatní, neboť posouzení nebylo sestaveno v rámci přijetí vyhlášky.*
- *Posouzení vlivu na ochranu osobních údajů musí být sestaveno, jinak dojde k porušení čl. 35 GDPR ze strany MF.*
- *Musí být rozhodnuto o metodice provádění, která bude v obecné podobě vycházet z čl. 35.*
- *Musí být rozhodnuto, zda provést posouzení interně nebo pověřit externího specialistu. V tomto ohledu je nezbytné zvážit zejména teoretický střet zájmů a skutečnost, zda by předmětné posouzení měl provádět ten samý subjekt, který vydal podzákonný právní předpis a který je zároveň správcem osobních údajů.*
- *Musí být rozhodnuto, zda je zpracování v souladu s předpisy EU, a to i s ohledem na bod výše.*

2. Účel zpracování osobních údajů

Stanovení dostatečně určitého účelu zpracování osobních údajů. Je zcela nezbytné pro následné posouzení legitimity rozsahu zpracování osobních údajů. Pokud nevyplývá účel přímo ze zákona, je definujícím momentem pro celé další zpracování stanovení účelu, které musí proběhnout nejpozději při shromažďování osobních údajů. Účel musí být určitý, výslovně vyjádřený a legitimní. Účel musí být stanoven dostatečně určitě na to, aby z něj bylo jasné, jaká zpracování na základě něj budou a nebudou probíhat, a aby mohl být posouzen jeho soulad s GDPR.

Účel musí být zároveň výslovně vyjádřený, to znamená, že musí být sdělen subjektům osobních údajů – zákazníkům provozovatelů. [5]

Příklad hodnocení[6]:

Dozor nad dodržováním zákona o hazardních hrách a podmínek stanovených v základním povolení a v povolení k umístění herního prostoru.

Kontrola řádného plnění povinností vyplývajících z daňových a účetních předpisů a dále kontrola sebeomezujících opatření.

3. Právní titul zpracování osobních údajů

Viz čl. 6 GDPR a bod II. tohoto dokumentu.

Příklad hodnocení*:*

[4] U každého bodu vždy příkladně uvádíme dílčí část možného obsahu dokumentu, pro lepší představu, co se pod daným bodem skrývá. Uváděný příklad nenahlíží na daný bod z celé perspektivy, spíše jen pomáhá zpracovateli Posouzení k tomu, aby si představil konkrétní část konečného obsahu dokumentu v daném bodě.

[5] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3, str. 108

- *Plnění právní povinnosti ve smyslu čl. 6 odst. 1, písm. c).*
- *Zmocnění § 133 odst. 1, písm. a) zákona č. 186/2016.*
- *§ 1 vyhlášky MF o způsobu oznamování a zasílání informací a přenosu dat provozovatelem hazardních her, rozsahu přenášených dat a jiných technických parametrech přenosu dat.*

4. Zpracovávaný rozsah a kategorie osobních údajů

Přesný výčet dat, které se v souvislosti s vyhláškou zpracovávají. Kategorizace dat a jejich seřazení dle citlivosti. Sekundárně zpracovávané osobní údaje. Níže uvedený příklad je jen zcela obecný, neboť kategorie musí být přehledně a jednoznačně explicitně uvedeny v přesné podobě.

Příklad výčtu:

Chronologický přehled o herních a finančních datech, denního herního výkaznictví, denního herního zápisu a oznámení nebo zasílání jiných informací orgánům vykonávajícím dozor. Data jsou vždy vázána k jedinečnému identifikátoru účtu. Jedná se o pseudonymizovanou verzi dat. To znamená, že data lze dešifrovat a) spojením s jinými daty, b) předáním dešifrovacího klíče.

V datovém balíčku se uvede jedinečný identifikátor uživatelského konta, který je na začátku tvořen identifikačním číslem provozovatele, nebo, nebylo-li identifikační číslo provozovateli přiděleno, vlastním číslem provozovatele, jež bylo provozovateli přiděleno v souvislosti s vydáním základního povolení, a dále identifikátorem účastníka hazardní hry. Tyto dvě části jsou od sebe odděleny pomlčkou (znak s dekadickým kódem 45). Každý záznam týkající se shodného uživatelského konta musí obsahovat shodnou jedinečnou hodnotu, která bude zachována ve všech automatizovaných výstupech poskytnutých provozovatelem. V případě, že je účastníku hazardní hry prostřednictvím shodného uživatelského konta umožněna účast na více druzích hazardních her, uvede se vždy shodný jedinečný identifikátor uživatelského konta.

5. Hodnocení rozsahu a kategorií osobních údajů vzhledem k účelu zpracování (tzv. posouzení nezbytnosti)

Účelové omezení je možné považovat za hlavní zásadu zpracování osobních údajů, která funguje jako nejvýznamnější určovatel toho, jak může správce s osobními údaji nakládat. Vymezením účelu (viz bod 2.) si správce určí, z jakého důvodu osobní údaje zpracovává, a následně může zpracovávat osobní údaje, až na výjimky, pouze pod tímto účelem. Toto určení je zcela nezbytné, neboť se od něj následně odvíjejí ostatní zásady činnosti, jako je minimalizace údajů a omezené uložení. Správce totiž může shromažďovat a zpracovávat jen ty osobní údaje, které jsou vzhledem k účelu zpracování relevantní, a pouze v rozsahu, který je nezbytný. To znamená, že jakmile jednou správce stanoví účel zpracování, musí při každé zamýšlené operaci zpracování pečlivě vážit, jestli je tato operace nezbytná k naplnění účelu a jestli využívá pouze relevantní a přiměřené osobní údaje. Uvedené je v případě veřejnoprávních subjektů úzce související se zásadou legality veřejné správy. Každé zpracování reportovaných dat by tak mělo odpovídat a být formálně přiřazeno k účelu vyplývajícímu ze zákona a vyhlášky.

Hodnocení se zároveň odráží v celé řadě dalších principů, mimo jiné záměrné a standardní ochrany osobních údajů, která v tomto případě znamená, že správce při volbě prostředků zpracování (softwarových aplikací, HW prostředků), ale i při zpracování samotném použije opatření, která zajistí dodržená hlavních zásad, mimo jiné minimalizace nebo nezbytnosti.

Jinými slovy, software bude dopředu naprogramovaný tak, aby shromažďoval jen nezbytné údaje, a naopak nepotřebné údaje likvidoval. [7]

Příklad:

Nejedná se o jednu z explicitně vymezených kategorií osobních údajů uvedených ve čl. 9 GDPR, nicméně se zajisté jedná o data, jejichž zpracování může již jejich povahy vážně ohrozit základní právo subjektů údajů na soukromí (naplňuje řadu rizikových faktorů dle metodiky ÚOOÚ k Posouzení vlivu na ochranu osobních údajů). Je zjevné, že pouze samotná informace, zda má subjekt osobních údajů založené herní konto, představuje citlivou osobní informaci. Další herní a finanční data jsou ještě o mnoho citlivější.

Posoudíme-li rozsah zpracovávaných údajů vzhledem k jeho účelu, musíme konstatovat, že legitimní, avšak lze pochybovat o nezbytnosti poskytování dat v pseudonymizované podobě a je otázkou, zda je tento způsob ochrany dostatečný. Účelu by pravděpodobně posloužila i data plně anonymizovaná, případně pseudonymizovaná, ale poskytovaná ve vzorcích, tak jak testuje kvalitu např. ČSÚ. Tato možnost by měla být jednoznačně podrobena výzkumu, neboť se jeví jako výrazně bezpečnější a zároveň odpovídající účelu zpracování.

Naopak jako složitá se jeví anonymizace osobních údajů, neboť z anonymizovaných údajů se kombinací s jinými údaji znovu stávají postupně osobní údaje.

6. Identifikace, hodnocení a kategorizace rizik zpracování osobních údajů

Přesné vymezení největších rizik pro zpracování celého setu údajů, jejich konkrétní a měřitelné hodnocení a následné způsoby ověřování, že rizika nebyla naplněna. Nařízení explicitně uvádí, že je nutné zohlednit rizika náhodného nebo protiprávního zničení osobních údajů, ztráty osobních údajů, pozměnění osobních údajů nebo neoprávněného zpřístupnění třetím osobám.

Při zvážení rizik by měl správce myslet na IT rizika, ale i lidský faktor (pochybení, trestná činnost), fyzické prostředí, hodnověrnost subdodavatelů, obchodních partnerů atp. Popsání opatření za účelem zmírnění rizik, záruk, mechanismů k zajištění ochrany osobních údajů (čl. 25 GDPR, kodexy dle čl. 40 GDPR) by na tento krok mělo navazovat (viz body 7 a 8). Posuzování rizik je otevřený a neukončený proces.

Příklad:

- *Celkem bylo identifikováno 10 rizik-*
  - *Napadnutí systému zvenčí – např. 1- 5*
  - *Napadnutí systému zevnitř – fyzická krádež zaměstnance – např. 1-5.*
- *Návrh případných opatření:*
- *Plán pro incident a obnovu systému:*
- *Přístupová práva:*
- *Kodex chování:*

7. Zabezpečení přístupu k datům a organizační opatření – právní pohled

Přesný výčet situací a explicitní výčet státních orgánů, které budou disponovat možností k „odheslování“ databází tak, aby to bylo přiměřené k účelu. Zároveň je třeba analyzovat

[7] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3, str. 114

možnost propojení databáze s jinými, kterými správce (anebo jiný státní orgán) disponuje a k tomuto přizpůsobit pravidla přístupu k datům atd. K tomuto je nezbytné konstatovat, že není přípustné databázi propojit s databází zpracovanou za jiným účelem, neboť by došlo k porušení zásady účelového omezení zpracování osobních údajů.

V neposlední řadě je třeba vyřešit přístup k datům v rámci jednotlivých oddělení správce, explicitně stanovit osoby nakládající s daty. S daty by i v rámci oddělení měly nakládat jen osoby k tomu určené, přičemž je vhodné, aby žádná osoba nedisponovala všemi daty současně. Vše by mělo být zaznamenáno pro případ řešení úniku dat.

Příklad:

- *Orgány s mající možnost využít data v jiné formě než pseudonymizované (mimo správce):*
  - *Orgány činné v trestním řízení, a to na základě čl. 2 odst. 2, písm. d) GDPR, ale s limity dle směrnice Evropského parlamentu a Rady 680/2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.*

- *Orgány nemající možnost využít data v jiné formě než pseudonymizované:*
  - *Ostatní orgány státní správy, včetně ministerstev, úřadů, správ a nižších územních celků.*

8. Technické zabezpečení dat

Bezpečnost osobních údajů je v poslední době i vzhledem ke známým kauzám velice zásadním tématem. Po hodnocení rizik by se s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování měla přijmout nejen organizační (bod 7), ale i technická opatření.

Nařízení v čl. 32 poskytuje výčet skupin technických a organizačních bezpečnostních opatření, která by měl správce přijmout dle potřeby. Vždy by ale mělo dojí k posouzení uvedených opatření a v případě, že opatření nejsou využita, je třeba dokázat zdůvodnit jejich nevyužití.

Jedním z opatření je i pseudonymizace, která bude zřejmě uplatněna v případě reportovací vyhlášky. Mezi další opatření patří schopnosti zajistit neustálou důvěrnost (kromě pseudonymizace nebo šifrování přispějí k důvěrnosti i metody autentizace a autorizace, pravidla přístupu systémům a úrovní oprávnění), integritu (monitorování přístupu konkrétních osob k osobním údajům a změn, které tyto osoby v osobních údajích provedly, limitování přístupu k osobním údajům pouze na oprávněné osoby), dostupnost (vytváření záložních zdrojů pro případy výpadku) a odolnost systémů a služeb zpracování; schopnosti obnovit dostupnost osobních údajů (organizační a technický opatření k obnově) a přístup k nim včas v případě fyzických či technických incidentů; procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Technické zabezpečení dat by mělo vycházet z Posouzení vlivu na ochranu osobních údajů, resp. Vyhodnocení dopadu vyhlášky.

Příklad:

- *Šifrování na primárním úložišti, externích médiích a zálohách*
  - *Systém HW/SW šifrování*

- *Systém šifrování záloh silnými klíči*
- *Vynucení politik pro použití externích médií*

- *Dostupnost a odolnost systém a služeb*
  - *Next-generation firewall (IPS, Gateway Antivirus, Botnet filter, Geo-IP filter)*
  - *Vizualizační infrastruktura*

- *Důvěrnost a integrita systémů a služeb*
  - *Monitoring administrativních úkonů a přístupu k prostředkům*
  - *Next-generation firewall (application intelligence, SSL Control)*
  - *Slouření Winfows, Max, Linux a Unix pod společnou správu identit a oprávnění*
  - *Správa identit a vícefaktorové ověřování*
  - *SSL certifikáty*

9. Doba uložení

Přesné vymezení, po jakou dobu budou předmětné osobní údaje zpracovávány, a po jaké době se budou likvidovat. Toto posouzení by mělo znovu plně odpovídat účelu zpracování osobních údajů. Všechny osobní údaje by měly být uchovány pouze po dobu, jež je nezbytná pro účely zpracování. Jednu kategorii osobních údajů může zpracovávat správce pro více účelů na základě více právních titulů. Pokud však zpracování některé kategorie nebude nezbytné pro naplnění žádného ze zbývajících účelů, musejí být osobní údaje vymazány, anebo anonymizovány. Subjekty osobních údajů by měly být o době uložení informovány (nebo by to mělo být stanoveno v interním dokumentu). Doba zpracování nesmí být určena jako neurčitá a vždy bude objektivně posuzováno, zda doba uchování nepřekročila dobu nezbytnou k naplnění. Výjimkou z výše uvedeného je jen zpracování pro účely vědeckého a historického bádání.

Příklad:

Dozor nad dodržováním zákona o hazardních hrách a podmínek stanovených v základním povolení a v povolení k umístění herního prostoru – ***x let od doby zpracování.***

Kontrola řádného plnění povinností vyplývajících z daňových a účetních předpisů a dále kontrola sebeomezujících opatření – ***x let od doby zpracování.***

10. Způsob informování subjektů osobních údajů

Rozdělení dat a zvážení, které informace lze vydat veřejně a které odpovídají určitému stupni utajení a nemají být zveřejněny vůbec, případně pouze primárním správcům osobních údajů (provozovatelům hazardních her). S ohledem na čl. 14 odst. 5 písm. c) není třeba plnit informační povinnost, pokud je zpracování výslovně stanoveno právem členského státu, které obsahuje dostatečná opatření k ochraně oprávněných zájmů subjektů osobních údajů. To znovu zdůrazňuje nutnost vyhodnocení a stanovení dostatečných opatření v rámci závazného dokumentu. V rámci transparentnosti činnosti veřejné správy by ale měla být veřejnost informována a důsledcích dopadu reportovací vyhlášky a měly by jí bát zpřístupněny všechny informace, které zpřístupnit lze.

11. Zvážení předávání osobních údajů do zahraničí

Přesné vymezení, zda probíhá či nikoliv. Pokud ano, z jakého titulu, k jakému účelu, a jak je zabezpečeno.

IV. Závěr

- Na základě čl. 6 odst. 3 GDPR by měl každý zákonný nebo podzákonný základ zpracování osobních údajů obsahovat dostatečné posouzení okolností daného zpracování.
- Podle metodiky vydané ÚOOÚ dne 8.2.2019 je nezbytné zvážit naplnění 10 podmínek zpracování osobních údajů, z nichž naplní-li se alespoň 2 podmínky kriticky, anebo 1 kriticky a 5 významně, je obligatorně nutné zpracovat Posouzení vlivu na ochranu osobních údajů, jestliže se neuplatní výjimka stanovená čl. 35 odst. 10. Ta se v tomto případě neuplatní.
- Podle závěrů IPRH je nezbytné provést nejen posouzení okolností zpracování, ale i Posouzení vlivu na ochranu osobních údajů, neboť celá řada podmínek zpracování je naplněna kriticky. IPRH považuje společenský zájem na skutečném Posouzení vlivů zpracování velice citlivých údajů pro subjekty osobních údajů jako velice vysoký.
- Bez provedení Posouzení vlivu na ochranu osobních údajů (nebo posouzení okolností zpracování) může dojít k rozporu reportovací vyhlášky s GDPR. V jeho důsledku může být zahájeno řízení ÚOOÚ s MF, a to na základě podnětu a zjištění ÚOOÚ (ÚOOÚ bylo v připomínkovém řízení sděleno, že data jsou anonymizována), z podnětu subjektů osobních údajů, případně primárních správců osobních údajů – provozovatelů hazardních her. Samostatnou kapitolou může být případné řízení s Evropskou komisí, ke kterému může dojít mimo jiné z podnětu příslušníka jiného státu EU k Úřadu pro ochranu osobních údajů v zemi, kde má bydliště.
- Cílem sestavení tohoto dokumentu bylo vymezení minimálních náležitostí, které by mělo posouzení ze strany MF obsahovat. IPRH znovu konstatuje, že je MF plně k dispozici pro účely jakékoli spolupráce na přípravě předmětného posouzení.