

Smlouva o poskytování poradenských služeb

č. 2018/0367

BDO Advisory s.r.o.

Se sídlem Karolinská 661/4, 186 00 Praha 8

IČ: 272 44 784

zapsaná do obchodního rejstříku vedeného Městským soudem v Praze, spisová značka C 107235, jednající panem Radovanem Haukem, jednatelem

dále jen „**Poradce**”

a

Město Neratovice

Se sídlem Kojetická 1028, 277 11 Neratovice

IČ: 002 37 108

zastoupeno Mgr. Lenkou Mrzílkovou, starostkou

dále jen „**Klient**”

Poradce a Klient (dále společně jen “Smluvní strany”) uzavírají tuto Smlouvu o poradenské činnosti (dále jen “Smlouva”) ve smyslu ustanovení § 1 746 odst. 2. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen “Občanský zákoník”)

Článek I.

Předmět Smlouvy

1. Poradce se zavazuje za podmínek stanovených touto Smlouvou zajistit pro Klienta činnosti v oblastech specifikovaných dále v čl. II. této Smlouvy.
2. Klient se zavazuje zaplatit Poradci za jím provedené činnosti podle této Smlouvy, odměnu stanovenou dále v čl. IV. této Smlouvy a poskytovat Poradci veškerou součinnost potřebnou pro výkon sjednané činnosti podle této smlouvy.
3. Poradce prohlašuje, že je odborně způsobilou osobou k výkonu sjednaných činností podle této smlouvy, má odborné znalosti práva a praxi v oblasti ochrany osobních údajů a je schopen zajistit plnění úkolů konkrétně jmenovaného pověřence pro ochranu osobních údajů.

Článek II.

Poskytované služby

1. Poradce se zavazuje provést pro Klienta služby posouzení shody stavu a způsobu ochrany osobních údajů s nařízením Evropského parlamentu a Rady EU (2016/679) ze dne 27. dubna 2016 o ochraně fyzických osob a v souvislosti se zpracováním osobních

údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES při prováděných činnostech klienta a dále poskytnout Klientovi služby související s implementací a dodržováním nařízením Evropského parlamentu a Rady EU (2016/679) ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále také „GDPR“).

Předmětem závazků Poradce je vypracování:

- a) srovnávací analýzy,
- b) posouzení rizik pro svobody a práva osob,
- c) plánu dosažení souladu s GDPR a
- d) zpracování postupů a dokumentace ochrany osobních údajů

(dále také jen „služby“).

Tyto služby jsou podrobněji vymezeny a popsány v **Příloze č. 1 Technická specifikace**, která je nedílnou součástí této smlouvy

- 2. Smluvní strany se dohodly, že jakékoli rozšíření služeb poskytovaných Poradcem dle této Smlouvy nad rámec stanovený v odst. 1. tohoto článku, bude sjednáno písemným dodatkem k této Smlouvě, v němž bude stanovena další poradenská činnost a odměna, kterou bude Klient hradit.
- 3. Za rozšíření služeb podle této smlouvy se nepovažuje posouzení shody činností klienta s doposud platnými právními předpisy nebo v budoucnu přijatými vnitrostátními právními předpisy nebo předpisy EU upravujícími ochranu osobních údajů a případně schválenými a závaznými kodexy chování dle článku 40 obecného nařízení o ochraně osobních údajů.

Článek III.

Práva a povinnosti Smluvních stran

- 1. Poradce se zavazuje vykonávat poradenskou činnost dle této Smlouvy s veškerou odbornou péčí, chránit obecně a jemu známé zájmy Klienta a informovat Klienta průběžně o plnění předmětu této Smlouvy.
- 2. Klient je povinen poskytovat Poradci veškerou potřebnou součinnost a veškeré informace a podklady potřebné k plnění činností Poradce. Poradce je povinen jednou měsíčně na základě dohody s Klientem tomuto vykázat dosavadní výsledek plnění dle čl. II. a sdělit Klientovi veškeré údaje, které si k dosavadnímu průběhu plnění díla vyžádá.
- 3. Smluvní strany sjednaly, že budou vzájemně spolupracovat a aktivně přistupovat k řešení jednotlivých oblastí činností poskytovaných dle této Smlouvy.
- 4. Poradce je povinen vykonávat činnosti dle této Smlouvy v dohodnutých nebo právními předpisy stanovených termínech.
- 5. Klient je povinen zaplatit Poradci odměnu v dohodnuté výši a termínech v souladu s čl. IV. této Smlouvy.
- 6. Každá ze Smluvních stran určuje kontaktní osobu/osoby, které budou zabezpečovat vzájemné předávání informací a spolupráci, předávání potřebných dokumentů, podkladů a výsledků činnosti dle této Smlouvy. Dojde-li ke změně v osobách pověřených k výkonu komunikace dle tohoto odstavce, je kterákoli ze Smluvních stran

oprávněna pouze písemným oznámením, předaným druhé Smluvní straně, provést změnu či doplnění. Smluvní strany sjednaly, že takové změny a doplnění nejsou považovány za změny této Smlouvy a nebudou prováděny formou dodatku k této Smlouvě.

Kontaktní osobou na straně Poradce je:

Miroslav Kvapil, MSc.

Tel: [REDACTED]

E-mail: miroslav.kvapil@bdo.cz

Kontaktní osobou na straně Klienta je:

Mgr. Petra Kotyzová

Tel: 315 650 335

E-mail: petra.kotyzova@neratovice.cz

Článek IV.

Doba a místo plnění

Poradce je povinen své plnění vymezené v čl. II. výše ve lhůtě 5 měsíců ode dne uzavření smlouvy předat v sídle Klienta. Srovnávací (vstupní) analýzu je Poradce povinen předat Klientovi ve lhůtě 1 měsíce ode dne uzavření smlouvy.

Článek V.

Odměna a náhrada nákladů

1. Klient se zavazuje zaplatit Poradci za služby poskytované dle čl. II této Smlouvy odměnu dle následujícího:

za služby provedené (uskutečněné) dle čl. II., odst. 1. této Smlouvy odměnu v celkové výši 290 000,- Kč bez DPH v zákonné výši na základě faktury Zhotovitele se splatností minimálně 30 kalendářních dní.

2. Odměna stanovená v odst. 1. tohoto článku zahrnuje veškeré náklady Poradce na činnosti vykonávané dle této Smlouvy, a to zejména cestovní náhrady, běžné náklady spojené s poskytnutím (vykonáním) služeb dle této Smlouvy (tj. tel. hovorné, faxovné, poštovné včetně kurýrních poplatků, jazykové překlady, notářské a jiné úřední poplatky, náklady na fotokopírování, technické nosiče, a kancelářské potřeby).
3. Bude-li Klient v prodlení s placením odměny v termínech a výších dle tohoto článku, je povinen uhradit Poradci úroky z prodlení ve výši 0,05 % z dlužné částky za každý den prodlení. Bude-li Klient v prodlení po dobu delší než (30) třicet dnů, je Poradce oprávněn od této Smlouvy odstoupit; předchozí věty neplatí v případě, že nastane situace předvídaná v následujícím odstavci níže tohoto článku.
4. Klient je oprávněn, odmítnout úhradu doručené faktury v případě, že Poradce nesplní svoji povinnost, předat Klientovi plnění uvedené v čl. II. odst. 1 výše včas a řádně, tj.

bez obsahových vad a chybějícího (i částečně) plnění, a to do doby odstranění Klientem vytčených vad a chybějícího plnění.

5. Bude-li Poradce v prodlení se svým (i dílčím) plněním dle článku II, je Klientovi povinen uhradit za každý započatý den prodlení smluvní pokutu ve výši 1.000,-Kč za každé takové (dílčí) plnění uvedené v čl. II. Ustanovením o smluvní pokutě není dotčena povinnost Poradce odevzdat Klientovi to (dílčí) plnění, se kterým je v prodlení.

Článek VI.

Chráněné informace

1. Veškeré informace sdělené kteroukoliv ze Smluvních stran při plnění povinností dle této Smlouvy, jsou považovány za přísně důvěrné a nesmí být zpřístupněny či jakýmkoliv jiným způsobem sděleny třetí osobě, s výjimkou informací, které byly v okamžiku sdělení veřejně známy nebo informací, které Smluvní strany získaly od třetích osob nebo jejichž poskytnutí upravuje platný právní předpis.
2. Poradce je oprávněn poskytovat při nabídce poradenských služeb jako reference údaje o realizovaném projektu, týkající se názvu projektu, názvu a identifikace Klienta, stručného popisu vykonané práce v rozsahu poskytované poradenské činnosti.

Článek VII.

Závěrečná ustanovení

1. Právní vztahy výslovně neupravené touto Smlouvou se řídí ustanoveními Občanského zákoníku v platném znění a platnými právními předpisy upravujícími ochranu osobních údajů.
2. Tato Smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma Smluvními stranami.
3. Poradce je pojištěn na škody v oblasti GDPR do výše 150 mil. Kč. Při podpisu smlouvy předloží klientovi kopii této smlouvy nebo potvrzení pojišťovny o sjednaném pojištění. Poradce je povinen být v uvedeném rozsahu pojištěn po celou dobu trvání smlouvy a na základě výzvy klienta je povinen předložit potvrzení o trvání pojištění.
4. Poradce odpovídá klientovi za škodu, která mu vznikne v důsledku jeho pochybení, nečinnosti nebo jiného vadného plnění a to na základě objektivního principu.
5. Závazek chránit informace dle čl. V. trvá i po skončení (splnění) Smlouvy, resp. zániku Smlouvy jinak než jejím splněním, stejně tak jako odpovědnost poradce za jím doposud poskytnutou činnost.
6. Ustanovení této Smlouvy lze měnit a doplňovat pouze formou písemných dodatků podepsaných oběma Smluvními stranami.
7. Tato Smlouva se sepisuje ve (2) dvou vyhotoveních s platností originálu, přičemž každá ze Smluvních stran obdrží po (1) jednom vyhotovení Smlouvy.
8. Pokud by tato Smlouva trpěla právními vadami, zejména pokud by některé z jejích ustanovení bylo v rozporu s českým právním řádem, v důsledku čehož by mohla být posuzována jako neplatná, považuje se to ustanovení, které není neplatné (netrpí právními vadami) za samostatné a strany vázající, jestliže nejde o ustanovení, které by bylo závislé na ustanovení Smlouvy, jež trpí právními vadami a samo o sobě by bez neplatného ustanovení právně nemohlo strany (či jednu z nich) vázat.

9. Smluvní strany této Smlouvy se zavazují, že v případě sporů o obsah a plnění této Smlouvy vynaloží veškeré úsilí, které lze spravedlivě požadovat k tomu, aby byly tyto spory vyřešeny smírnou cestou, zejména aby byly odstraněny okolnosti vedoucí ke vzniku práva od Smlouvy odstoupit, nebo způsobují neplatnost.
10. Tato smlouva bude zveřejněna v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) a to bez uvedení citlivých údajů (obchodní tajemství, osobní údaje). Zveřejnění smlouvy zajistí Klient.

V Praze, dne 11.6.2018

Ing. Radovan Hauk
jednatel BDO Advisory s.r.o.

BDO Advisory s.r.o.



vlastnoruční podpis

V Neratovicích, dne 4.6.2018

Mgr. Lenka Mrzílková
starostka



vlastnoruční podpis

Příloha č. 1 Technická specifikace

Rámcové stanovení velikosti a počtu subjektů podléhajících poptávce. Městský úřad Neratovice + 8 podřízených organizací

Počet zaměstnanců – Městský úřad Neratovice -118 (včetně veřejné služby, uklízeček a řidičů) + 8 městská knihovna + 18 městská policie + 30 JSDH = 174 + zaměstnanci příspěvkových organizací a společnosti majoritně vlastněné městem

- a) 2 základních škol,
- b) 1 mateřské školy, která má 7 pracovišť
- c) základní umělecké školy,
- e) Domu dětí a mládeže,
- f) domova pro seniory,
- g) Společenského domu Neratovice a
- h) Plaveckého bazénu s.r.o.

Srovnávací analýza

V rámci Srovnávací analýzy bude třeba posoudit úroveň stavu ochrany osobních údajů dle aktuálního rozsahu zpracování těchto údajů v prostředí Městského úřadu Neratovice. Analýza procesů (sestavení Registru zpracování osobních údajů) se zaměří na procesy, v jejichž rámci se osobní údaje zpracovávají. Cílem bude identifikovat konkrétní činnosti a popsat, jakým způsobem se v současné době osobní údaje zpracovávají (například postup při jejich zpracování úřadem, ukládání a dalším jejich zpracování). Současně skutečnosti zjištěné při srovnávací analýze poskytnou Městskému úřadu Neratovice informace o slabínách a nedostacích v zajištění ochrany osobních údajů.

Městský úřad Neratovice požaduje, aby kritéria srovnávací analýzy vycházela zejména z požadavků GDPR a dále z norem řady ISO 27000, podle kterých jako podle dobře vžitě praxe plánuje řídit bezpečnost informací.

Jako součást srovnávací analýzy musí být provedeny úkony vedoucí ke zjištění stavu souladu s požadavky GDPR, kterými budou:

- Zpracování formuláře pro srovnávací analýzu;
- podpora při poskytnutí podpory respondentům u vybraných zpracování a vyhodnocení zpracování osobních údajů (Registr zpracování osobních údajů);
- analýza dokumentace ochrany osobních údajů;
- identifikace procesů organizace zpracovávajících osobní údaje;

- identifikace respondentů pro provedení interview;
- provedení rozhovorů a posouzení stavu na pracovištích zadavatele s důrazem na:
- analýzu zdrojů osobních údajů, právních titulů a účelů k jejich zpracování a způsobu jejich dokumentace;
- doplnění informací ke zpracování osobních údajů k dokončení Registru zpracování osobních údajů,
- analýzu kategorizace typů osobních údajů,
- posouzení opatření fyzické bezpečnosti společnosti s důrazem na prostory kde se ve zvýšené míře manipulují osobní údaje,
- analýzu uživatelských přístupů k osobním údajům v informačním systému,
- prověření ICT infrastruktury v oblasti zpracování a uchovávání osobních údajů: servery a pracovní stanice a další zařízení, na kterých se nacházejí osobní údaje, identifikaci hlavních integrací systémů a komunikačních kanálů, identifikaci a posouzení použitých bezpečnostních mechanismů, identifikace technických možností předání osobních údajů a výmazu osobních údajů z IS;
- posouzení míry outsourcingu a dohod se třetími stranami včetně posouzení smluv o zpracování osobních údajů;
- zpracování záznamu ze srovnávací analýzy popisující míru splnění požadavků GDPR a předání tohoto záznamu zadavateli;
- dokončení Registru zpracování osobních údajů.

Výstupem srovnávací analýzy GDPR by měly být:

Registr zpracování osobních údajů – základní dokument pro zpracování a ochranu osobních údajů obsahující popis jednotlivých zpracování s důrazem na název zpracování, vztah ke zpracování (správce/zpracovatel), zda je pro zpracování využíván jako zpracovatel externí strana, účel zpracování OÚ, kategorie subjektů OÚ, kategorie OÚ, zdroj OÚ, právní titul atd.

Zpráva ze srovnávací analýzy požadavků GDPR – komplexní zpráva o plnění požadavků GDPR zaměřená na typy spravovaných osobních údajů, procesy a opatření pro jejich ochranu. Zpráva by měla obsahovat přehled plnění jednotlivých požadavků GDPR a hodnocení stávajících opatření pro ochranu osobních údajů (bezpečnostní politika, organizace bezpečnosti, řízení aktiv, bezpečnost lidských zdrojů, fyzická bezpečnost a bezpečnost prostředí, řízení komunikací, řízení provozu, řízení přístupu, akvizice, vývoj a údržba informačních systémů, dodavatelské vztahy, zvládání bezpečnostních incidentů, řízení kontinuity činností organizace a řízení souladu s požadavky).

Posouzení rizik pro svobody a práva osob

Posouzení rizik je nezbytné provést pro návrh vhodných organizačních a technických opatření k zajištění plnění požadavků GDPR. Posouzení rizik bude provedeno pro jednotlivá zpracování identifikovaná v rámci Srovnávací analýzy.

Cílem posouzení rizik pro svobody a práva osob je posoudit, jak závažné dopady by měl únik zpracovávaných informací na konkrétní subjekt údajů. Pravděpodobnost a závažnost rizika pro práva a svobody subjektu údajů by měly být určeny na základě povahy, rozsahu, kontextu a účelu zpracování.

Zadavatel požaduje, aby Posouzení rizik pro svobody a práva osob bylo provedeno dle obecně přijímaného postupu pracovní skupiny WP29 uvedeného v dokumentu WP 248 rev.01 „Pokyny pro posouzení vlivu na ochranu údajů a stanovení, v případě, že je pravděpodobné, že zpracování údajů

bude mít za následek vysoké riziko pro účely nařízení 2016/679“ přijaté dne 4. října 2017. Dokument uvádí 9 rizikových faktorů:

- Hodnocení nebo bodování, včetně profilování a předpovídání;
- Automatizované rozhodování, které má právní nebo podobně závažný dopad;
- Systematické monitorování – zpracování, které je používáno k pozorování, monitorování nebo kontrole subjektů údajů;
- Citlivé údaje nebo údaje vysoce osobní povahy;
- Údaje zpracovávané v rozsáhlém měřítku;
- Přirazování nebo slučování datových souborů;
- Údaje týkající se zranitelných subjektů údajů;
- Nové použití nebo využití nových technologických nebo organizačních řešení (např. biometrika);
- Pokud samotné zpracování „brání subjektům údajů v uplatňování některého z jejich práv nebo v používání některé služby či smlouvy.

Posouzení stanoví, zda operace zpracování představují riziko či vysoké riziko a zda je pro posuzované zpracování osobních údajů nutné provést Posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR.

K samotnému vyhodnocení dokument WP248 uvádí:

„Ve většině případů může správce údajů zpracování, které splňuje dvě kritéria, považovat za zpracování, pro něž se vyžaduje posouzení vlivu na ochranu osobních údajů. Pracovní skupina zřízená podle článku 29 se obecně domnívá, že čím více kritérií zpracování splňuje, tím větší je pravděpodobnost, že bude představovat vysoké riziko pro práva a svobody subjektů údajů, a bude proto vyžadovat posouzení vlivu na ochranu osobních údajů, a to bez ohledu na opatření, která hodlá správce přijmout. Avšak v některých případech správce údajů může mít za to, že posouzení vlivu na ochranu osobních údajů vyžaduje i zpracování, které splňuje jen jedno z těchto kritérií. K posouzení rizik pro svobody a práva osob je možné využít následující tabulku:

Výklad jednotlivých kritérií je následující:

1. Hodnocení nebo bodování, včetně profilování a předpovídání, zejména:
 - a. aspektů souvisejících s pracovním výkonem subjektu údajů;
 - b. jeho ekonomickou situací;

- c. zdravotním stavem;
- d. osobními preferencemi nebo zájmy;
- e. spolehlivostí nebo chováním;
- f. místem pobytu či pohybu.

Může se jednat například o:

- a. finanční instituci, která prověřuje svého zákazníka v databázi úvěrových referencí;
 - b. biotechnologickou společnost, která nabízí genetické testování přímo spotřebitelům za účelem posouzení nebo předpovězení rizika nemoci / zdravotních rizik;
 - c. společnost, která vytváří behaviorální nebo marketingové profily na základě používání webových stránek nebo pohybu na nich.
2. Automatizované rozhodování, je: zpracování osobních údajů, jehož cílem je rozhodování o subjektech údajů, jež má:
- a. ve vztahu k fyzickým osobám právní účinky nebo
 - b. má na fyzické osoby podobně závažný dopad.

Může se jednat například o zpracování, které může mít za následek vyloučení nebo diskriminaci jednotlivců.

Na zpracování, které má jen nepatrný nebo žádný dopad na jednotlivce, se toto konkrétní kritérium nevztahuje.

3. Systematické monitorování: zpracování, které je používáno k pozorování, monitorování nebo kontrole subjektů údajů:

- a. včetně údajů shromážděných prostřednictvím sítí nebo
- b. rozsáhlé systematické monitorování veřejně přístupných prostorů.

Při systematickém monitorování by měly být naplněny podmínky:

- a. Osobní údaje mohou být shromažďovány za okolností, za nichž nemusí subjekty údajů vědět, kým jsou jejich údaje shromažďovány a jak budou použity;
- b. Nemusí být v silách jednotlivců zabránit tomu, aby se stali subjektem tohoto zpracování na veřejných (nebo veřejně přístupných) místech.

4. Citlivé údaje nebo údaje vysoce osobní povahy tvoří:

- a. zvláštní kategorie osobních údajů ve smyslu článku 9 GDPR (např. údaje týkající se politických názorů jedince);
- b. osobní údaje týkající se rozsudků v trestních věcech a trestných činů ve smyslu článku 10 GDPR;

Dále se jedná o osobní údaje, které jsou považovány za citlivé (v běžném smyslu toho slova), protože:

- a. mají vazbu na domácnosti a soukromé činnosti (např. elektronická komunikace);
- b. mají dopad na výkon základních práv (např. lokalizační údaje, které mohou znamenat zpochybnění svobody pohybu);
- c. jejich porušení má jednoznačně závažný vliv na každodenní život subjektu údajů (např. finanční údaje, které by mohly vést k podvodům s platbami).

Může se jednat i o osobní dokumenty, e-maily, osobní deníky, elektronická čtecí zařízení vybavená funkcemi poznámek a informace velmi osobní povahy obsažené v aplikacích zaznamenávajících průběh denních aktivit subjektu údajů.

Je důležité, zda subjekt údajů nebo třetí osoby údaje už zveřejnily (mohlo se počítat s dalším využitím údajů).

5. Osobní údaje zpracovávané v rozsáhlém měřítku, přičemž GDPR přesně nevymezuje, co znamená rozsáhlé, WP29 ale doporučuje, aby při určování, zda je zpracování rozsáhlé, byly zvažovány zejména tyto faktory:

- a. počet dotčených subjektů údajů vyjádřený konkrétním číslem, nebo jako podíl příslušné populace;
- b. objem údajů a/nebo rozsah jednotlivých zpracovávaných údajů;
- c. délka nebo trvání činnosti zpracování údajů;
- d. zeměpisný rozsah činnosti zpracování.

6. Přirazování nebo slučování datových souborů, pokud například:

- a. pocházejí ze dvou nebo více operací zpracování údajů prováděných pro různé účely a/nebo;
- b. prováděné různými správci údajů;
- c. prováděné způsobem, který by přesahoval přiměřené očekávání subjektu.

7. Údaje týkající se zranitelných subjektů údajů, se posuzují v případě, že při zpracování osobních údajů existuje nerovnováha moci mezi subjekty údajů a správcem údajů, což znamená, že pro jednotlivce může být nemožné snadno vyslovit souhlas případně nesouhlas se zpracováním svých údajů, nebo vykonávat svá práva.

Mezi zranitelné subjekty mohou patřit:

- a. děti (u nichž lze mít za to, že nejsou schopny vědomě nebo promyšleně vyslovit nesouhlas, popřípadě souhlas se zpracováním svých údajů);
- b. zaměstnanci;
- c. zranitelnější skupiny obyvatelstva, které vyžadují zvláštní ochranu (osoby s duševní chorobou, žadatelé o azyl nebo starší osoby, pacienti atd.) a
- d. všichni ti, v jejichž případech je možné stanovit nerovnováhu ve vztahu mezi postavením subjektu údajů a správcem.

8. Nové použití nebo využití nových technologických nebo organizačních řešení, kdy se jedná například o kombinaci použití otisků prstů a rozpoznávání obličejů pro zlepšení omezení fyzického přístupu atd.

GDPR upřesňuje, že použití nové technologie, definované v souladu s dosaženou úrovní technických znalostí, může zakládat potřebu provést posouzení vlivu na ochranu osobních údajů. Použití této technologie totiž může zahrnovat nové formy

sběru a použití údajů s potenciálně vysokým rizikem pro práva a svobody fyzických osob

Osobní a sociální důsledky zavedení nové technologie mohou být nepředvídatelné. Posouzení vlivu na ochranu osobních údajů pomůže správci údajů porozumět těmto rizikům a řešit je.

9. Zabránění subjektům údajů v uplatňování některého z jejich práv, kdy se jedná o případ, že samotné zpracování osobních údajů „brání subjektům údajů v uplatňování některého z jejich práv nebo v používání některé služby či smlouvy“.

Typicky jde o operace zpracování osobních údajů, které mají za cíl umožnit, změnit nebo zamezit subjektu údajů přístup ke:

- a. službě nebo
- b. uzavření smlouvy.

Jedná se například o banku, která prověřuje svého zákazníka v databázi úvěrových referencí, aby rozhodla, zda mu udělí úvěr, či nikoliv.

Výstupem by měl být:

Dokument popisující rizikovost jednotlivých zpracovatelských operací. Posouzení rizik je možné zaznamenat i v rámci Registru zpracování osobních údajů.

Plán dosažení souladu s GDPR

V návaznosti na Srovnávací analýzu a Posouzení rizik bude zpracován detailní návrh jednotlivých změn, které je třeba provést před nabytím účinnosti GDPR ke dni 25. 5. 2018. Cílem Plánu dosažení souladu s GDPR (dále též „Plánu“) bude podrobné stanovení dílčích úkolů a postupu jejich realizace pro dosažení souladu s GDPR ke stanovenému datu.

Plán zohlední zjištění ze Srovnávací analýzy a bude zaměřen na sestavení postupu k dosažení následujících cílů:

- redukce rozsahu potřebného zpracování údajů a snížit tak náklady na opatření nezbytné na jeho zabezpečení;
- revize bezpečnostní politiky a další bezpečnostní dokumentace, pokrývající oblast osobních údajů;
- úprava procesů spojených s osobními údaji a jejich ochranou;
- přijetí technických opatření pro zlepšení bezpečnosti osobních údajů;
- revize smluv s externími subjekty, kteří vstupují do zpracování osobních údajů, případně se kterými jsou osobní údaje vyměňovány na základě zákonné potřeby;
- provedení školení zaměstnanců zodpovědných za zajištění bezpečnosti osobních údajů.

Výstupem by měl být:

Dokument stanovující plán přijetí potřebných opatření k odstranění nesouladu s požadavky GDPR, jejich vzájemnou návaznost a doporučení pro jejich realizaci. Uvedená opatření budou navrhovat změny v oblastech právních, procesních a ICT.

Plán by měl obsahovat

- popis zadání pro následnou implementaci technických a organizačních opatření;
- odhad náročnosti jednotlivých kroků a doporučení pro postup implementace potřebných opatření.

Zpracování postupů a dokumentace ochrany osobních údajů

V návaznosti na výstupy předcházejících etap by měly být navrženy postupy a následně by měla být zpracována potřebná dokumentace upravující pravidla a postupy ochrany osobních údajů. Dokumentace by měla porývat potřeby zadavatele na řízení zpracování a ochrany osobních údajů v souladu s požadavky GDPR. Lze předpokládat tvorbu dokumentace v následující navrhované podobě.

Výstupem by měl být:

V rámci výstupu uvedené etapy je nutné vypracovat celou řadu řídicích dokumentů včetně pravidel pro případné zajištění nově zaváděné role pověřence (DPO) a pravidel spojených s jeho realizací. V souhrnu je výstupem této etapy soubor pravidel a směrnic:

- Směrnice pro ochranu osobních údajů – dokument, který bude základním řídicím dokumentem pro zpracování a ochranu osobních údajů. Dokument by měl zahrnout i doposud užívané postupy, které nejsou v rozporu s požadavky GDPR uvedené ve stávajících Pravidlech ke zpracování osobních údajů. Pro dokument doporučujeme zvolit následující strukturu:
- Kontaktní údaje správce a pověřence pro ochranu osobních údajů;
- Rozsah ochrany osobních údajů;
- Definice;
- Zásady zpracování osobních údajů;
- Zajištění ochrany osobních údajů;
- Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím;
- Způsob monitorování a prosazování zpracování a ochrany osobních údajů;
- Role a odpovědnosti při zpracování a ochraně osobních údajů;
- Pověřenec pro ochranu osobních údajů.
- Příloha 1 - Přehled vedených registrů a evidencí.
- Příloha 2 - Přehled dokumentace upřesňující zpracování a ochranu osobních údajů.

- Směrnice pro klasifikaci aktiv – dokument upřesňující způsob klasifikace informací k zajištění odpovídající úrovně ochrany informací. Informace, včetně osobních údajů, musí být klasifikovány na

základě jejich potřebnosti a důležitosti pro zabezpečení činností. (Účelem této směrnice je rozpracovat zásady klasifikace a řízení aktiv do postupů pro zacházení s informacemi v dokumentech, počítačových systémech a sítích, mobilních prostředcích ICT, hlasové komunikaci, multimédiích a v poštovním styku. Směrnice by měla být koncipována tak, aby nezahrnovala pouze ochranu osobních údajů, ale pokrývala veškeré údaje, se kterými se zachází. Tato směrnice může být, v případě potřeby, využita pro případný systém řízení bezpečnosti informací.

- Metodika hodnocení rizik zpracování osobních údajů včetně rizik subjektů údajů – dokument stanovující způsob a postupy pro identifikaci a ohodnocení aktiv a výpočet rizik hrozících osobním údajům a subjektům údajů při ztrátě nebo zveřejnění jejich osobních údajů. Metodika by měla pokrývat zejména požadavky GDPR na

- Posouzení rizik pro práva a svobody subjektů údajů.

- Zabezpečení zpracování osobních údajů.

- Posouzení vlivu na ochranu osobních údajů.

- Pravidla pro zvládání porušení ochrany osobních údajů – dokument popisující proces pro vyhodnocení dopadů porušení ochrany osobních údajů, způsob shromáždění důkazů o porušení a postup pro ohlašování a oznamování případů porušení zabezpečení osobních údajů. Metodika by mimo popisu procesu měla obsahovat popis odpovědnosti při výše uvedených činnostech.

- Pravidla pro výkon případné role Pověřence pro ochranu osobních údajů – dokument, který by měl upřesňovat základní pravidla a odpovědnosti Pověřence pro ochranu osobních údajů s následujícím doporučeným obsahem:

- Účel funkce pověřence;

- Podřízenost;

- Vymezení odpovědností;

- Obsah činnosti pověřence z hlediska časového průběhu:

zřízení funkce/role, zavedení agendy včetně dokumentace, pravidelná měsíční agenda s důrazem na monitorování souladu s GDPR, pravidelná roční agenda, nepravidelná agenda s důrazem posudky na prováděná posouzení vlivu na ochranu osobních údajů a činnosti při ohlašování a oznamování případů porušení zabezpečení osobních údajů.

- Evidence – doplňující evidence, které budou shromažďovat údaje o činnostech požadovaných GDPR. Jedná se například o:

- Registr zpracování osobních údajů,

- Registr souhlasů ke zpracování osobních údajů,

- Evidence žádostí o výkon práv subjektu údajů,

- Evidence a řízení porušení zabezpečení osobních údajů (incidentů).

- Návrh vzorů pro zajištění požadavků GDPR:

- vzorová Smlouva pro zpracování osobních údajů (zpracovatelská smlouva),

- vzor Souhlasu se zpracováním osobních údajů,

- vzor Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů.