

Nabídka

VÍME JAK

„Příprava pro GDPR – identifikace účelů a způsobu zpracování osobních údajů“

pro Městský úřad Lipník nad Bečvou

Datum vytvoření nabídky:

28. 7. 2017

Nabídka platná do:

28. 8. 2017

© 2017 AutoCont CZ a.s.

Nabídka a návrh smlouvy vytvořené společností AutoCont CZ a.s. jsou součástí know-how a obchodního tajemství společnosti AutoCont CZ a.s. a nelze je tedy bez předchozího písemného schválení společnosti AutoCont CZ a.s. dále sdělovat třetím stranám či jinak šířit. Příjemce (adresát/příjemce, jemuž je nabídka či návrh smlouvy určen) bere tuto skutečnost převzetím nabídky nebo návrhu smlouvy na vědomí a zároveň se zavazuje zabezpečit ochranu poskytnutého know-how a obchodního tajemství společnosti AutoCont CZ a.s. a zabránit jeho neoprávněnému užití jakoukoli třetí osobou. Všechny ostatní dokumenty poskytované společností AutoCont CZ a.s. (koncepty, studie, analýzy, výstupy auditů atd.) jsou chráněny jako produkt společnosti AutoCont CZ a.s. dle autorského zákona a jejich příjemce je tudíž povinen zabezpečit ochranu poskytnutého produktu společnosti AutoCont CZ a.s. a zabránit jeho neoprávněnému užití jakoukoli třetí osobou.

1 **Obsah**

1	Obsah	2
2	Technické kvalifikační předpoklady - certifikace	3
3	Nabídka	4
3.1	Obecný úvod	4
3.1.1	Co je to GDPR	4
3.1.2	Koncepce přípravy na GDPR, postup zavedení opatření	4
3.2	Obsah nabídky	6
3.2.1	Co je nabídkou řešeno	6
3.2.2	Rozsah nabídky	6
3.2.3	Navazující služby, které nejsou součástí nabídky	7
3.2.4	Služba externího pověřence pro ochranu osobních údajů (externí DPO)	7
3.2.5	Rozfázování	8
3.3	Postup realizace	8
3.3.1	Metodika	8
3.3.2	Požadavky na součinnost	8
3.4	Cenová nabídka	9
3.5	Platební podmínky	9

2 Technické kvalifikační předpoklady - certifikace



3 Nabídka

3.1 Obecný úvod

3.1.1 Co je to GDPR

GDPR neboli General Data Protection Regulation je Nařízení evropského parlamentu a rady (EU), jehož účinnost je dána 25. květnem 2018. GDPR bude přímo závazné pro jednotlivé členské země Evropské unie a nahradí směrnici 95/46/ES, která upravuje ochranu osobních údajů na úrovni Evropské unie. Toto nařízení stanoví mimo jiné i sankce za porušení svých pravidel a to až do výše 20 miliónů Euro nebo 4% celosvětového obrátu organizace.

3.1.2 Koncepce přípravy na GDPR, postup zavedení opatření

Implementace GDPR:

1. **Jedná se o proces, nikoliv jednotlivý projekt.** To znamená, že i po samotném zavedení je nutné počítat s pravidelnými požadavky na zdroje – je nutné pravidelně revidovat opatření, provádět analýzy rizik a s riziky pracovat. Zavedení opatření v roce 2017/2018 je jen první krok.
2. **Je nutná účast nejvyššího managementu na implementaci.** Role nejvyššího managementu je nezastupitelná a klíčová, jen nejvyšší management může zajistit odpovídající podporu realizaci a efektivitu implementace a dále je nutné si uvědomit, že hodnocení některých bezpečnostních parametrů nemůže udělat nikdo jiný, než nejvyšší management.
3. **Je nutné provést organizační změny – případně vytvořit nové role,** vytvořit řídicí struktury v oblasti bezpečnosti.
4. **Požadavky na zdroje (lidé, čas) půjdou napříč organizací, a to včetně non IT oddělení.** Do implementace budou zapojena oddělení napříč organizací, budou nutné organizační změny, bude nutná účast jejich zaměstnanců na jednotlivých částech implementace.

Rizika přípravy na GDPR, postup zavedení opatření:

1. **Požadavky na zdroje - odhad – čas, lidé, technologie.** Je zpracován odhad požadovaných zdrojů, tento odhad je dělán za „ideálních“ podmínek. Nelze vyloučit změny trhu, technologií, zákonů atd.
2. **Součinnost nejvyššího managementu a jednotlivých oddělení napříč organizací.** V okamžiku kdy není poskytována dostatečná (uvažovaná) součinnost, dojde k rozpadu harmonogramu a narušení plánu implementace.

Způsob dosažení cíle:

nasazení organizačních a technických opatření naplňujících požadavky GDPR, splnění požadavků GDPR organizací.

- Detailní plán a harmonogram
 - Požadavky na zdroje, termíny
 - Vytvoření realizačního týmu
 - Plánování analytické fáze – zdroje, termíny, rizika, způsob omezení rizik
- Analytická fáze
 - Identifikace informačních systémů zpracovávajících OÚ
 - Zpracování úvodního auditu – audit shody v nakládání s OÚ dle GDPR
 - Stávající stav vs. požadavky GDPR
 - Přehled požadavků nutných pro implementaci
 - Metodika analýzy rizik
 - Zpracování interní metodiky analýzy rizik
 - Metodika hodnocení rizik (zbytkové riziko, akceptovatelné riziko)
 - Provedení analýzy rizik OÚ
 - Identifikace a ohodnocení aktiv
 - Identifikace a ohodnocení hrozeb
 - Přehled hrozeb (registr hrozeb, registr zranitelností)

- Identifikace a ohodnocení zranitelností
 - Výpočet rizik
 - Plán zvládání rizik
- Přehled opatření nutných pro implementaci GDPR
 - Rizika a opatření (spárování)
 - Organizační opatření (management)
 - Technická opatření (IT oddělení a další technické odb.)
 - Opatření a jejich priority s ohledem na rizika
 - Návrh plánu implementace
- Plán implementační fáze
 - Požadavky na zdroje, termíny
 - Technologie
 - Procesy
 - Organizace
 - Vytvoření realizačního týmu
 - Plánování implementační fáze – zdroje, termíny, rizika, způsob omezení rizik
 - Dlouhodobý plán
 - Plán na rok 2017/2018
- Implementační fáze
 - Implementace jednotlivých opatření dle plánu
 - Organizační opatření
 - Procesy, dokumentace (politiky, směrnice, postupy, metodiky, plány, školení)
 - Technická opatření
 - Implementace technologií (zajištění HW, SW, licence, instalace, konfigurace, školení personálu, testování atd.)
- Start procesů
- Validace stavu
 - Zpracování GAP analýzy
 - Stávající stav vs. požadavky GDPR
 - Přehled požadavků nutných implementovat (které nebyly implementovány, posouzení s ohledem na případné změny zákonů atd.)

3.2 Obsah nabídky

Nabízíme provedení úvodního auditu pro zajištění shody s GDPR.

3.2.1 Co je nabídkou řešeno

Obsahem této nabídky je zpracování první etapy implementace GDPR, tj. **zpracování úvodního auditu – určení shody postupů, procesů a dokumentace s požadavky nařízení GDPR. Rozsah povinností pro službu pověřence pro ochranu osobních údajů.**

Předtím, než začnete zpracovávat osobní údaje (dále jen OÚ), měli byste znát své povinnosti (přinejmenším ty zákonné) a ujistit se, že jsou splněny. Pojmem *zákonost* myslíme dodržování všech povinností, které ukládají zákony a všechny ostatní závazné předpisy a nařízení, a to ve všech fázích životního cyklu OÚ.

Pokud už OÚ zpracováváte a nyní chcete vyřešit shodu s GDPR, budou Vás pro začátek zajímat následující požadavky tohoto nařízení:

- zákonnost, korektnost a transparentnost zpracování
- přiměřenost, relevance a nezbytnost vzhledem ke stanovenému účelu
- podmínky vyjádření souhlasu subjektu OÚ
- kategorie OÚ
- časové omezení
- dokumentovaná odpovídající technická a organizační opatření na ochranu OÚ
- vedení záznamů (vč. porušení zabezpečení ochrany OÚ)
- smluvní vztahy a odpovědnost správce a zpracovatele OÚ
- závazek mlčenlivosti
- jmenování pověřence pro ochranu OÚ

Služby, jejichž využitím identifikujete mezery v naplnění zákonných požadavků a zároveň je můžete odstranit, spočívají zejména v auditní činnosti, pomoci při ustanovení odpovídajících procesů a tvorbě interních předpisů.

- *Audit shody nakládání s OÚ s nařízením EU (GDPR), jehož součástí je audit:*
 - o procesů spojených se správou a zpracováním OÚ,
 - o opatření (organizačních a technických, a jejich dostatečnosti) ke splnění zákonných požadavků,
 - o dokumentace (její úplnosti) nezbytné k ochraně OÚ a prokázání shody s požadavky.

3.2.2 Rozsah nabídky

Nabídka se omezuje na:

- informační systémy organizace
- vlastní správní jednotku a přímo zřizované a vedené organizace
- Výstupem je zpráva obsahující:
 - o Seznam účelů a zpracování OÚ a jejich zákonné požadavky bude ve 3 skupinách:
 - Vlastní zaměstnanci úřadu a jím řízených organizací
 - Občané správního celku
 - Třetí strany – (dodavatelé , vlastníci nemovitostí s věcným břemenem ..)
 - o Seznam způsobů zpracování OÚ, ve kterém budou uvedeni interní vlastníci aktiv, ve kterých jsou OÚ pořizovány. U všech OÚ bude popsán způsob zpracování procesně.
 - o Součástí bude i **Analýza rizik spojených s GDPR**
 - o Seznam doporučených technických a procesních opatření pro zajištění souladu s GDPR
- Zpráva je předána ve formátu MS Office (Word, příp. Excel dokument zprávy)

Nabídka neobsahuje:

- Dodávku HW
- Dodávku SW nebo licencí
- Zpracování BIA
- Provedení penetračního testu nebo bezpečnostního skenu

3.2.3 Navazující služby, které nejsou součástí nabídky

Na realizaci mohou navazovat další služby např.:

- Návrh plánu implementace
- Implementace jednotlivých opatření dle plánu
 - Organizační opatření
 - Procesy, dokumentace (politiky, směrnice, postupy, metodiky, plány, školení)
 - Technická opatření
 - Implementace technologií (zajištění HW, SW, licence, instalace, konfigurace, školení personálu, testování atd.)

3.2.4 Služba externího pověřence pro ochranu osobních údajů (externí DPO)

Pro rozvedení nabídky externího DPO je nutné předem definovat rozsah využití služby napříč příspěvkovými organizacemi (PO) správní jednotky. Pokud bude vyžadována tato služba i pro PO, které jsou svou povahou v režimu služby 24x7 (HZS, Obecní policie apod.), je nezbytné navýšit časovou kapacitu pro činnosti spojené s touto funkcí.

Nabídka se omezuje na:

- Vyhodnocování bezpečnostních incidentů
- Sledování a vyhodnocování souladu nastaveného systému s právním základem
- Monitorování souladu nastavených opatření s koncepcí ochrany osobních údajů
- Poskytování rad a informací ke sporným případům ochrany OÚ
- Školení zaměstnanců
- Tvorba posudků při uplatnění nároků pro sběr a správu OÚ
- Poradenská činnost v oblasti legislativy a správy či zpracování OÚ
- Kontakt se subjekty OÚ a součinnost s dozorovou organizací (ÚOOÚ)

Činnost je založena na měsíční bázi v rozsahu dvou pracovních dnů při režimu 5x8, přičemž není svou povahou možné stanovit přesný rozpis jednotlivých činností. To zvláště ve vztahu k tvorbě posudků nebo řešení incidentů a kontaktu s dozorovým orgánem. V případě bezvýpadkového provozu (MěP, HZS) je nutné zahájit řešení incidentu neprodleně, vzhledem ke lhůtám stanoveným nařízením nebo jinou legislativní úpravou (ZKB). V takových případech bude možné smluvně ošetřit dostupnost DPO při dodatečném jednání.

3.2.5 Rozfázování

Jednotlivé fáze
Analýza rizik s přihlédnutím ke GDPR
Workshop pro sběr dat
Tvorba a revize dokumentace
Zpracování dat a výstupů, směrnice
Audit shody s požadavky GDPR
Audit s jednotlivými subjekty dle analýzy rizik
Předání/akceptace výstupů
prezentace výstupů
záverečné zaškolení pověřených osob

3.3 Postup realizace

3.3.1 Metodika

Provedení auditu, který zmapuje aktuální plnění požadavků GDPR, hodláme realizovat formou účelových interview (metoda Delphi) se správcem IS, uživateli atd.

a) Postup realizace

Samotná realizace má čtyři na sebe navazující fáze/části:

- Přípravná fáze – plánování
- Sběr dat
- Zpracování dat a výstupů
- Připomínkové řízení

Tyto části jsou různě provázané, a proto je jejich souslednost uvedena v rámcovém harmonogramu. Harmonogram bude finalizován v rámci přípravné fáze.

Sběr dat

Interview nebo workshopy a dále shromáždění dostupné dokumentace.

Obsah: vlastní interview nebo workshopy, zajištění a získání písemných podkladů.

Zpracování dat

Obsah: zpracování interview nebo workshopů, písemných podkladů.

- Výstup: draft zprávy

Připomínkové řízení

Samotné připomínkové řízení, kdy jsou auditovaným subjektem předloženy případné připomínky k jednotlivým zjištěním a ty jsou auditorem vypořádány.

- Výstup: Finální podoba výstupu

3.3.2 Požadavky na součinnost

Nejdůležitější částí realizace je sběr informací – výstup je natolik kvalitní a relevantní, nakolik kvalitně se povede získat informace. V rámci sběru informací bude tedy požadována:

- Dokumentace
 - bezpečnostní dokumentace
 - organogramy a procesní mapy

- nařízení a směrnice managementu se vztahem k OÚ, byť nepřímým
- dokumentace systému kvality
- provozní dokumentace a manuály
- schémata
- Účast vytipovaných uživatelů na interview/pracovní schůzky
- Účast vytipovaných správců IS na interview/pracovní schůzky

3.4 Cenová nabídka

Popis	Cena celkem Kč bez DPH
Zpracování Analýzy rizik spojených s GDPR a projektové řízení	54.000,-
Zpracování úvodního auditu, který identifikuje aktuální plnění požadavků GDPR	50.000,-
Služba externího pověřence pro ochranu osobních údajů (eDPO)	21.000,- měsíčně

3.5 Platební podmínky

- Ceny jsou bez DPH včetně dopravy na místo plnění
- Splatnost faktur bude 30 dnů.
- Úhrada dle smluvních podmínek
- Není vyžadována platba zálohou
- Předpokládané ukončení plnění smlouvy listopad 2017
- Místo plnění – sídlo zadavatele