Podpora práce
pověřence pro ochranu osobních údajů
v počátcích jeho působení na Karlově Univerzitě

nabídka služeb od společnosti

PDQM, s.r.o.

verze 1

značka: PDQM-Nabidka UVT UK GDPR 2018-1 v2.docx

Praha, 23.04.2018

Vážený pane řediteli,

V návaznosti na Váš požadavek na oganizačně-konzultační podporu práce pověřence v prvních měsících jeho působení v nově zřízené pozici Vám zasílám nabídku podpory kroků potřebných pro bezproblémové fungování tohoto nového úřadu. Smyslem nabídky je podpořit první realizace procesů v souladu s požadavky nové směrnice i ověření požadované bezpečnosti osobních údajů.

Těším se na spolupráci a jsem s pozdravem,
Mgr. Štěpán P. Nadrchal, PhD.

Ph.D.
Štěpán
Nadrchal

Digitally signed by Ph.D. Štěpán Nadrchal
DN: c=CZ, cn=Ph.D. Štěpán Nadrchal, st=Praha, l=Praha 6, Ve střešovičkách 169/37, 16900, email=nadrchal@pdqm.cz, givenName=Štěpán, sn=Nadrchal, serialNumber=ICA - 638419
Date: 2018.04.23 21:33:48 +02'00'

1 SHRNUTÍ NABÍDKY

Předmětem nabídky je podpora procesů pověřence z informačního hlediska: zajištěním potřebných informací požadovaných v rámci dotazů subjektů údajů případně dozorového úřadu. Druhým výstupem je standardizovat postupy a odpovědi tak, aby jejich budoucí zpracování nevyžadovalo žádnou externí pomoc a mohlo probíhat plně v rámci rektorátu a fakult.

Vzhledem k rozsahu celého úkolu jsou některé oblasti připravené jednoduše a pro bezproblémové a dodržování GDPR pravidel je třeba vypracovat dlouhodobě udržitelné řešení. Proto Vám navrhuji podporu následujících oblastí:

Výstupem úvodní analýzy bude:

- ☞ Kvalitní příprava nových procesů požadovaných GDPR legislativou
- ☞ Dokončení dokumentace zpracování osobních údajů do kvality vhodné i pro prezentaci dozorovým úřadům
- ☞ Zpřesnění přístupu k osobním údajům s ohledem na analyzované potřeby agend
- ☞ Zajištění informační podpory a vzdělávání pracovníků odpovědných za osobní údaje kdekoli v agendách univerzity

Navrhované práce budou realizovány v následujících 6 měsících. Maximální cena prací je 392 000Kč bez DPH.

Předmětem nabídky jsou služby, které PDQM standardně poskytuje klientům. Jejich popis je na našich webových stránkách: http://www.osobni-udaj.cz

Univerzita zvolila vhodný model zajištění splnění požadavků nové legislativy formou užšího týmu a širší skupiny kontaktních osob na univerzitách. Předpokládáme spolupráci v rámci týmu pověřence pro osobní údaje, která zůstane zachována i do dokončení všech naplánovaných úprav v redukované formě i jakožto podpora úřadu DPO.

Obsah dokumentu

2 Základní údaje

2.1 Předkladatel nabídky – PDQM

Předkladatelem nabídky je společnost **PDQM, s.r.o.**
sídlem: Ve Střešovičkách 169/37, Praha 6
zastoupená jednatelem a zástupcem zmocněným v tomto řízení: **Mgr. Štěpán Nadrchal, Ph.D**
(Jednatel jedná za společnost v plném rozsahu samostatně)

Bankovní spojení: ČSOB: 0 - 213719545 / 0300

IČ: 278 70 588; DIČ: **CZ27870588**, společnost je plátcem DPH v ČR.

Telefonní spojení na zmocněného zástupce: **+420 605 203 938**
Kontaktní email: **nadrchal@pdqm.cz**

2.2 Určení nabídky

Nabídka je určena pro: **Ústav výpočetní techniky, Univerzita Karlova v Praze**
sídlem: Petrská 3, Praha 1, 116 36

2.3 Poptávka

Nabídkou reagujeme na poptávku ze strany vedení ÚVT UK, definované v rámci přípravné schůzky.

2.4 Struktura nabídky

Nabídka v následujících kapitolách popisuje jednotlivé oblasti podpory, jak byly uvedeny v úvodním shrnutí nabídky.

3 Podpora procesů požadovaných GDPR legislativou

GDPR legislativa vyžaduje několik nových procesů, které je DPO připraven řešit, ale jejich řešení předpokládá poměrně velké množství manuální práce s mnoha evidencemi v rámci celé UK.

Navrhovaná pomoc by měla zajistit, že bude tato práce výrazně jednodušší a bude možné i rychleji reagovat na dotazy a požadavky subjektů údajů nebo dozorového orgánu.

3.1 Právo subjektu údajů na přístup k osobním údajům

V rámci plnění úkolu připravíme takové informace o agendách a místech uchovávání osobních údajů, aby reakce na požadavek subjektu na přístup k osobním údajům nevyžadovala kontrolu těch úložišť, kde o údaji informace již nejsou nebo nikdy nebyly.

Součástí práva subjektu je i právo na výmaz. Je třeba mít upřesněno, jaké budou důsledky takového požadavku na schopnost univerzity poskytovat informační služby společnosti vůči orgánům státní správy i vůči subjektu samotnému.

3.2 Právo na opravu

Univerzita nemá možnost udržovat informace o bývalých studentech, zaměstnancích aj. osobách aktuálních. Informace je proto třeba vždy chápat jako obraz doby, kdy vznikly. Je třeba ověřit, zda jejich historická povaha nemůže vést ke zkreslování rozhodování o subjektech v aktuálním čase nebo jinak nesprávně daný subjekt ovlivnit.

Univerzita musí zajistit, aby ty subjekty, které jsou s univerzitou v aktivním kontaktu, měli možnost ověřit a požadovat opravu informací o sobě, pokud by byly nesprávné. Většina pracovníků i studentů má možnost nejdůležitější informace o sobě kontrolovat elektronickým přístupem, je ale vhodné ověřit, že je tato možnost dostatečná s ohledem na obecné právo dané GDPR legislativou a je obecně dostupné všem subjektům.

3.3 Právo na výmaz („právo být zapomenut“)

Uplatnění práva na výmaz může negativně ovlivnit povinnosti UK vůči státu a proto je jeho realizaci nutné provést velmi pečlivě právě s ohledem na zákonné povinnosti školy. K tomu by měla vzniknout metodika, jak postupovat.

3.4 Právo na omezení zpracování

Je třeba vypracovat metodiku, jak postupovat v případě tohoto požadavku ze strany subjektu údajů, aby přitom nebyly narušeny obecně platné zákony a předpisy ani nebylo omezena schopnost univerzity poskytovat výuku a spravedlivě hodnotit práci studenta.

3.5 Právo na přenositelnost údajů

Aplikovatelnost práva přenositelnosti je závislá na míře využitelnosti dat univerzity u jiného subjektu. Je třeba posoudit, ve kterých situacích by z tohoto práva mohl mít subjekt prospěch a pro ně navrhnout podporu efektivní s ohledem na potenciální náklady a reálné využití této možnosti v praxi.

3.6 Právo vznést námitku a automatizované individuální rozhodování

V rámci revize míst a způsobů zpracování osobních údajů na univerzitě nebyly identifikovány žádné kroky automatického rozhodování. Práva subjektů související s tímto zpracování proto považujeme v prostředí univerzity za bezpředmětná.

3.7 Ohlašování případů porušení zabezpečení dozorovému úřadu

Povinnost ohlašování vyplývala již ze současné legislativy, ale její interní organizaci je třeba změnit s ohledem na vytvoření nového úřadu pověřence. Je proto vhodné revidovat způsoby, jakým jsou případy porušení ochrany osobních údajů identifikovány a jak se s nimi nakládá v rámci oznamování, korektivních opatření i prevence dalších podobných výskytů.

3.8 Oznamování případů porušení zabezpečení subjektu údajů

Univerzita až dosud neměla potřeby vytvoření mechanismů hromadného oznámení porušení většímu množství subjektů. S ohledem na nařízení GDPR je třeba pro to vytvořit metodiku, aby UK byla připravena na případ, že by k uniku informací o větším počtu subjektů někdy v budoucnu došlo.

3.9 Posouzení vlivu na ochranu osobních údajů

Potřeba posouzení vlivu určitého zpracování na ochranu osobních údajů bude v rámci interních procesů UK výjimečné, ale bude důležité pro práci s osobními údaji v rámci výzkumu a projektů. S ohledem na velký počet projektů a pracovišť, včetně takových, které pracující s citlivými osobními údaji zdravotního nebo sociálního charakteru, je třeba, aby pověřenec i Univerzita samotná byla připravena posouzení dopadů odborně připravit a vysvětlit dopady i pracovníkům–vědcům, jejichž práci může rozhodnutí přímo ovlivnit.

Pověřenec by měl disponovat metodikou, která usnadní posuzování napříč fakultou a poskytne pracovníkům vodítka, jak posuzování dělat a jak rizika a dopady objektivně hodnotit.

4 Dokončení dokumentace zpracování osobních údajů

Efektivní práce pověřence vyžaduje spolehlivý nebo efektivní přístup k dokumentaci dokumentace všech postupů zpracování. Dokumentace je třeba jak pro interní potřebu, tak pro případné prokázání plnění požadavků GDPR nařízení.

Dokumentace musí podporovat řadu z bodů obecného nařízení.

4.1 Zabezpečení zpracování

Byla provedena včasná kontrola zabezpečení údajů, ale i do budoucna je třeba zajistit, že je tato úrovně dostatečná. Nutnou podmínkou pro to je, aby existovaly mechanismy kontroly, že zabezpečení všech míst zpracování zůstává dlouhodobě dostatečné.

4.2 Dokumentace pro spolupráci s dozorovým úřadem

Současná dokumentace byla vypracována zejména s důrazem na prověření ochrany a přiměřenosti zpracovávání osobních údajů. Je třeba připravit dokumentaci i tak, aby bylo ji využít pro prokázání plnění všech povinností v případě výzvy ze strany dozorového úřadu. Dokumentace musí reflektovat i úpravy, které budou realizované v souladu s návrhy v jiných oddílech.

5 Zpřesnění přístupu k osobním údajům

Ochrana osobních ochranu klade požadavky na jejich technické zabezpečení, které je třeba zajistit nezávisle na tom, kdo vyvíjí informační systémy pro jejich zpracování nebo kdo s nimi pracuje. K tomu i s ohledem na požadavky GDPR je třeba věnovat se následujícím oblastem.

5.1 Minimální garantovaná ochrana osobních údajů

Ochrana osobních údajů je v různých evidencích řešena různě a s různou úrovní. Nová interní dokumentace by měla stanovovat závazná nebo doporučující pravidla, jakou úroveň zabezpečení by měly jednotlivé kategorie osobních údajů mít, jak by měla být technicky řešena a jak kontrolována její spolehlivost.

Cílem dokumentace by mělo být dosažené jednotné minimální úrovně zabezpečení osobních údajů na všech pracovištích a fakultách a to bez ohledu na to, jakým prostředkem (typicky informačním systémem) se k nim přistupuje.

5.2 Role Společného správce

Univerzita je jedním z několika společných správců osobních údajů v řadě projektů a pracovišť, které společně založily fakulty s pracovišti Akademie věd, fakultními nemocnicemi, jinými vysokými školami nebo i komerčními organizacemi. Tato společná pracoviště se v současné době řídí metodikou některého ze zapojených pracovišť, ale není pravidlem, aby existovalo ujednání mezi správci.

Pro efektivní správu i koordinaci bude vhodné vytvořit doporučení ujednání a minimální požadavky na ochranu osobních údajů ve všech případech, kdy se univerzita podílí na správě ve sdíleném pracovišti.

5.3 Postavení zpracovatelů

Univerzita má a do budoucna bude vytvářet nové vztahy správce a zpracovatele, ať už sama bude v roli zpracovatele nebo jej bude pověřovat zpracováním spravovaných dat. V současnosti je každý jednotlivý případ řešen individuálně.

S ohledem na zajištění ochrany vlastních informací a minimalizace rizika postihu za nesprávné zpracování dat jiného správce bude důležité pro tyto vztahy stanovit závazná pravidla, aby do budoucna nevytvářely pro UK riziko neplnění požadavků nařízení a s tím spojené riziko postihu.

5.4 Vedení záznamů o zpracování

Univerzita musí vytvořit efektivní způsob dokumentace způsobů zpracování osobních údajů, aby plnila požadavky nařízení bez zásadních dopadů na efektivitu práce a současně byla schopna tuto evidenci využívat.

6 Informační podpora a vzdělávání pracovníků

Prvním z úkolů pověřence pro ochranu osobních údajů dle nařízení GDPR je „poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle tohoto nařízení a dalších předpisů Unie nebo členských států v oblasti ochrany údajů."

Vzhledem k počtu pracovníků UK i počtu pracovišť, kde se s osobními údaji pracuje, není možné, aby byla informační podpora založena výhradně na osobní komunikaci s pověřencem. Pověřenec proto musí disponovat nástroji, jak šířit informace, zlepšovat povědomí o bezpečnosti a pomoci pochopit problematiku bezpečnosti údajů lidem, kteří s informacemi začínají pracovat nově.

Jako minimální základ pro informační potřebu považujeme eLearningové školení přizpůsobené podmínkám univerzity a dostupné všem pracovníkům. Druhým základem jsou doporučení (ať už závazná nebo „best-practices"), která budou zpracovávat většinou častých témat, které musí pracovníci na UK řešit.

7 Nabídka

Předchozí kapitoly podrobněji rozvedly oblasti, které je vhodné zlepšit, aby bylo další zajištění GDPR efektivní. Nejsou přesně popsány formy pomoci, protože přesná součinnost vyplyne nejenom z typu a rozsahu dotazů od subjektů údajů, ale i z kapacit interních členů týmu. Předpokládáme, že formy podpory změn budou podobně podpoře s přípravou na GDPR nařízení:

- Příprava doporučení, jak řešit konkrétní situace, které v činnostech univerzity nastávají
- Vypracování dokumentace o zpracování osobních údajů do dlouhodobě udržitelné formy
- Konzultace a spolupráce s interním GDPR týmem
- Příprava vzdělávacích materiálů

7.1 Cenová nabídka

Odhadovaná náročnost kroků v harmonogramu je základem pro stanovení ceny služby. Na základě posouzení rozsahu prací, které úvodní analýza vyžaduje, odhadujeme pracnost posouzení na 49 dní pracovníků PDQM (8 dní / měsíc po dobu 6 měsíců). Cena služby je kalkulována sazbou 8 000Kč/den bez DPH. **Výsledná maximální cena za je 392 000 Kč bez DPH.**

Uvedená cena zahrnuje veškeré náklady na straně PDQM a případných vyšších nákladů vyplývajících z chybně odhadnutého rozsahu díla. Pokud se v průběhu zpracování ukáže, že některé činnosti nejsou potřebné, nebude jejich časová náročnost započtena a celková cena bude o poměrnou část

ponížena. Cena zahrnuje i náklady na cesty do mimopražských pracovišť univerzity, pokud se ukážou jako nezbytné.

Práce budou fakturovány po dokončení prací.

7.2 Objednávání prací

ÚVT nebo UK může objednat práce dle nabídky písemnou objednávkou s odkazem na tuto nabídku (označení „PDQM-Nabidka UVT UK GDPR 2018-1 v2.docx“). Písemnou formu objednávky stačí předat při osobní schůzce po zahájení prací.

Objednávka musí obsahovat:

- Popis objednávaných prací – odkazem na tuto nabídku případě dalším upřesněním
- Jméno a funkce pracovníka odpovědného zakázku objednat
- Jméno a kontakt pracovníka odpovědného za spolupráci při koordinaci
- Veškeré informace potřebné pro následnou fakturaci (číslo objednávky, identifikaci a sídlo organizace, adresu pro zaslání faktury případně další požadované informace)