



Pražská  
znalecká kancelář

## **Metodika vyplnění dotazníků pro provedení mapování rozsahu a stavu zpracování osobních údajů**

**Zpracoval:** **Pražská znalecká kancelář, s.r.o. (dále též jako „Zpracovatel“)**

Na Bateriích 822/9

162 00 Praha 6 - Střešovice

IČ: 48910660



Obsah:

<b>1</b>	<b>ÚVOD .....</b>	<b>4</b>
<b>2</b>	<b>METODIKA PRO VYPLNĚNÍ FORMULÁŘE Č. 1 .....</b>	<b>5</b>
2.1	Hlavička dotazníku .....	5
2.2	Oblast zpracování osobních údajů .....	5
2.3	Oblast působnosti oblasti či procesu .....	5
2.4	Zpracovávané kategorie osobních údajů .....	5
2.5	Výčet položek osobních údajů .....	6
2.6	Vztah subjektu údajů ke správci či zpracovateli osobních údajů .....	6
2.7	Právní základ zpracování osobních údajů .....	7
2.8	Účel nakládání s osobními údaji .....	7
2.9	Úložiště osobních údajů .....	7
2.10	Specifikace listinného úložiště .....	7
2.11	Specifikace elektronického úložiště .....	7
2.12	Kategorie příjemců včetně příjemců mimo EU .....	7
2.13	Doba zpracování OÚ .....	8
2.14	Doba uložení osobních údajů .....	8
2.15	Využívání spolupráce se zpracovatelem OÚ .....	8
2.16	Způsob kontroly zpracování OÚ .....	8
2.17	Připravenost na uplatňování práv ze strany subjektů OÚ .....	8
2.18	Další požadované dokumenty .....	8
<b>3</b>	<b>METODIKA PRO VYPLNĚNÍ FORMULÁŘE Č. 2 - PŘEHLED POUŽÍVANÝCH APLIKACÍ .....</b>	<b>9</b>
3.1	Název aplikace .....	9
3.2	Výrobce aplikace .....	9
3.3	Seznam zpracovávaných agend .....	9
3.4	Vede evidenci osobních údajů? .....	9
3.5	Výčet položek osobních údajů .....	9
3.6	Vede evidenci zvláštní kategorie osobních údajů? .....	9
3.7	Výčet položek zvláštní kategorie osobních údajů .....	9
3.8	Oblast působnosti .....	10
3.9	Předávání dat .....	10
3.10	Archivace a skartace .....	10
3.11	Připravované realizace .....	10
3.12	Je aplikace ve vlastnictví posuzovaného subjektu nebo je provozována třetí osobou jako služba? .....	10



Pražská  
znalecká kancelář

3.13	Otázky pro správce informačních a komunikačních technologií: .....	10
3.14	Další požadované dokumenty .....	11



## 1 Úvod

Dne 25. května 2018 vstoupí v účinnost nařízení Evropského Parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (dále též „OÚ“) a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), označované jako General Data Protection Regulation (dále jen „GDPR“). GDPR představuje nový právní rámec ochrany OÚ v evropském prostoru s cílem hájit co nejvíce práva občanů EU proti neoprávněnému zacházení s jejich OÚ.

S ohledem na tuto novou legislativu Evropské unie (dále jen „EU“) uzavřelo Ministerstvo vnitra České republiky (dále jen „MVČR“) s Pražskou znaleckou kancelář s.r.o. (dále jen „Dodavatel“) smlouvu č.j. MV-143611-1/LG-2017 ze dne 8.1.2018 na vytvoření systémové analýzy působnosti obcí z hlediska obecného nařízení o ochraně osobních údajů (dále jen „GDPR“). Systémová analýza bude obsahovat dvě části, z nichž první část bude zaměřena na obce s rozšířenou působností a druhá část bude zaměřena na obce se základním rozsahem přenesené působnosti. Každá část systémové analýzy zohlední specifika dané kategorie obcí tak, aby výstup byl pro obce příslušné kategorie do nejvyšší možné míry přiléhavý a využitelný.

Systémová analýza bude provedena na vzorku 11 obcí s rozšířenou působností (z toho jedna městská část) a 6 obcí se základním rozsahem výkonu přenesené působnosti popřípadě s pověřeným obecním úřadem (z toho jedna městská část) vybraných MVČR a bude se vztahovat jak ke všem agendám v přenesené působnosti obcí, tak k základním (všem obcím společným) agendám v samostatné působnosti (se zaměřením na obecný rámec základních činností všech obcí v oblasti výkonu samostatné působnosti - dispozice majetkem, personální agenda, nakládání s osobními údaji o členech zastupitelstva obce a členech iniciačních a poradních orgánů obce, poskytování dotací apod.).

Na základě výše uvedené Smlouvy mezi MVČR a Dodavatelem Vám předkládáme dva dotazníky ve formátu MS Excel k vyplnění. Součástí dotazníků jsou příklady vyplněných dat pro každý dotazník.

V kapitole č. 2 jsou popsány jednotlivé části Formuláře č. 1 a uvedeny příklady pro snadnější vyplnění. Doporučuji metodiku předávat společně s dotazníky, a to odpovědným osobám za vyplnění dotazníků.

Součástí kapitoly č. 2 je požadavek na poskytnutí další dokumentace posuzovaného subjektu. Výčet této dokumentace je uveden pouze v metodice.

V kapitole č. 3 je uveden popis Formuláře č. 2 ohledně přehledu používaných aplikací v rámci Vaší organizace, které zpracovávají osobní údaje. Dále přehledu agend a aplikací, které dané agendy v rámci organizace podporují.

Součástí kapitoly č. 3 je požadavek na poskytnutí další dokumentace posuzovaného subjektu. Výčet této dokumentace je uveden pouze v metodice.

Dotazníky prosím vyplňte jak za vlastní úřad, tak i za všechny podřízené organizace (např. škola, školka, zařízení sociálních služeb, kulturní zařízení, městská policie, technické služby apod.).

## **2 Metodika pro vyplnění Formuláře č. 1**

Dotazníky prosím předat na všechny vedoucí odborů nebo oddělení dle organizační struktury posuzovaného subjektu / úřadu.

### **2.1 Hlavička dotazníku**

**Pracoviště** – Osoba odpovědná za vyplnění dotazníku uvede název odboru nebo oddělení dle organizačního řádu posuzovaného subjektu, kterého se data v dotazníku týkají.

**Kontaktní osoba** – Jméno osoby odpovědné za vyplnění dotazníku

**Datum vyplnění** – Datum vyplnění dotazníku

### **2.2 Oblast zpracování osobních údajů**

Zde uveďte agendu, oblast či proces odpovídající příslušné oblasti působnosti, při níž jsou zpracovávány osobní údaje. Může se jednat o agendy v přenesené působnosti státu (např. stavební povolení, evidence obyvatel, cestovní doklady, rybářské lístky, vedení obecní kroniky atd.), Samostatná působnost (např. Správa bytových fondů, pronájem nebytových prostor, těžba a prodej dřeva), Interní procesy úřadu (např. personalistika, zúčtování mezd, kamerové systémy, GPS lokace vozidel pracovníků). Níže uvedené části dotazníku bude odpovědná osoba vyplňovat pro každou agendu, proces či oblast samostatně.

**Příklady:** Finanční odbor uvede například tyto oblasti či procesy – Vedení účetnictví, Místní poplatky, Potvrzení o bezdlužnosti, Vymáhání daňových pohledávek atd.

Kancelář úřadu (příp. tajemník úřadu) uvede například tyto oblasti či procesy – Jednání rady a zastupitelstva, Poskytování informací dle zákona 106, Stížnosti a petice, Veřejné zakázky, Výběrová řízení, Přijmutí osoby do zaměstnaneckého poměru atd.

Tiskový mluvčí pak oblast publicity – webové stránky, profily na sociálních sítích, dokumentace společenských či kulturních akcích apod.

### **2.3 Oblast působnosti oblasti či procesu**

Odpovědná osoba zde vybere z již předdefinovaných oblastí působnosti, jimiž jsou:

- Přenesená působnost státu (státní správa), jedná se o přenesenou působnost státu dle Hlavy III zákona č. 128/2000 Sb. o obcích;
- Samostatná působnost (samospráva), jedná se o samostatnou působnost dle Hlavy II zákona č. 128/2000 Sb. o obcích;
- Interní procesy úřadu.

### **2.4 Zpracovávané kategorie osobních údajů**

Odpovědná osoba vybere u kategorií osobních údajů, zda je daný proces či oblast zpracovává. Je již předdefinován výběr z možností ANO/NE. Jedná se o následující kategorie:

- Osobní údaje - osobní údaje dle čl. 4 Nařízení Evropského parlamentu a Rady (EU) 2016/679 jsou definovány takto "veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno,

identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.";

- Zvláštní kategorie osobních údajů – zvláštní kategorie osobních údajů je charakterizována článkem č. 9 GDPR takto: "Osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby."
  - Genetické údaje – Nařízení evropského parlamentu a Rady (EU) 2016/679 definuje genetické údaje takto "Osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby";
  - Biometrické údaje – biometrické údaje dle čl. 4 Nařízení evropského parlamentu a Rady (EU) 2016/679 jsou definovány takto "Osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje";

## 2.5 Výčet položek osobních údajů

Pokud jste označili u předchozích kategorií osobních údajů, že jsou v daném procesu zpracovávány zde se uvádí jejich taxativní výčet. U každé kategorie doplnit výčet všech relevantních zpracovávaných osobních údajů.

U kategorie zvláštních osobních údajů, dle článku č. 9 GDPR, se jedná o následující prvky:

- rasový či etnický původ;
- politické názory;
- náboženské vyznání;
- filozofické přesvědčení;
- členství v odborech;
- genetické údaje;
- biometrické údaje za účelem jedinečné identifikace fyzické osoby;
- údaje o zdravotním stavu;
- údaje o sexuálním životě;
- údaje o sexuální orientaci.

**Příklad:** Finanční odbor v rámci procesu Místní poplatky by měl mít uvedeny tyto osobní údaje: Jméno, Příjmení, Titul, Datum narození, Rodné číslo, Trvalé bydliště, Email, Telefon, Datová schránka, Místo pobytu, Státní příslušnost, Podpis. V rámci tohoto procesu se nezpracovávají zvláštní kategorie osobních údajů.

## 2.6 Vztah subjektu údajů ke správci či zpracovateli osobních údajů

Zde se uvádí vztah subjektu údajů ke správci či zpracovateli osobních údajů nebo kategorie subjektů osobních údajů. Jako příklady zde uvádíme následující kategorie:

- Občan – přenesená působnost;
- Občan – samostatná působnost;
- Zaměstnanec;



- Dodavatel;
- Kategorie zvláště zranitelných subjektů údajů – nezletilý.

Výše jsou uvedeny jen příklady, pokud vstupuje do procesu i jiný subjekt údajů prosím o uvedení do dotazníku.

## **2.7 Právní základ zpracování osobních údajů**

Uvede se právní základ zpracování osobních údajů, na základě článku č. 6 GDPR tím může být:

- Oprávněný zájem správce;
- Plnění právní povinnosti;
- Plnění smlouvy nebo jednání o jejím uzavření;
- Souhlas se zpracováním osobních údajů pro jeden či více konkrétních účelů;
- Veřejný zájem, výkon veřejné moci;
- Ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

## **2.8 Účel nakládání s osobními údaji**

Vyplnění účelu nakládání s osobními údaji, tj. popis důvodu, na základě něhož dochází ke zpracování osobních údajů. Uveďte výčet právních předpisů, na jejichž základě dochází ke zpracování osobních údajů. Jedná se o zákony, vyhlášky či případně interní akty řízení.

## **2.9 Úložiště osobních údajů**

Odpovědná osoba vybere z již předdefinovaných možností a to:

- Elektronické úložiště strukturované (databáze, informační systém);
- Elektronické úložiště nestrukturované (lokální disky, email, sdílené disky);
- Listinné úložiště;
- Kombinace výše uvedených úložišť – prosím o upřesnění kombinace úložišť.

## **2.10 Specifikace listinného úložiště**

Vyplnění způsobu vedení listinné evidence v jednotlivých procesech obsahující osobní údaje. V případě že jste nevybrali listinné úložiště či kombinaci úložišť, tak danou položku nevyplňujte.

**Příklad:** Finanční odbor – proces: Místní poplatky – Ukládání listinné evidence do šanonu a uloženo v uzamykatelné skříni na Finančním odboru.

## **2.11 Specifikace elektronického úložiště**

Uvedení názvu informačního systému, který vede evidenci osobních údajů v rámci uvedené oblasti či procesu.

**Příklad:** Finanční odbor – proces: Místní poplatky – IS Spisová služba, Finanční IS, Registr obyvatel, Datová schránka.

## **2.12 Kategorie příjemců včetně příjemců mimo EU**

Dle článku č. 4 je Příjemcem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli.



Uvedení všech kategorií příjemců osobních údajů a to:

- Interní příjemce – uvedení rolí pracovníků úřadu;
- Externí příjemce – uvedení všech možných externích příjemců osobních údajů včetně příjemců mimo EU.

### **2.13 Doba zpracování OÚ**

Osobní údaje mají být uchovány pouze po dobu nutnou k účelu jejich zpracování. Uvedte, zda máte pro posuzovanou oblast zpracování OÚ stanovenou dobu zpracování OÚ (např. kontrola souhlasu k publikaci OÚ v obecním periodiku). Nezaměňujte prosím za dobu uložení OÚ. V případě, že máte stanovenou dobu zpracování uveďte její délku v letech. V případě, že nemáte nebo nevíte, uveďte "NE".

### **2.14 Doba uložení osobních údajů**

Uvedení lhůt pro archivaci záznamů s osobními údaji (pokud je oprávněné osobě známa). Například lze uvést, že se archivuje a skartuje dle schváleného archivačního a skartačního řádu či jiného dokumentu. Nebo uvedení lhůt vyplývajících z legislativy na základě, které se osobní údaje ukládají.

Vyplňte prosím ve tvaru "skartační znak"/"počet let"

Skartační znaky:

- A – označuje dokumenty trvalé hodnoty, navržené k uložení do archivu;
- S – označuje dokumenty, které mohou být po uplynutí skartační lhůty a po vydání skartačního povolení příslušným archivem zničeny;
- V – označuje dokumenty, které budou ve skartačním řízení posouzeny a rozděleny mezi dokumenty se skartačním znakem „A“ nebo mezi dokumenty se skartačním znakem „S“.

### **2.15 Využívání spolupráce se zpracovatelem OÚ**

Odpovězte pouze Ano/Ne. Zpracovatel je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Jedná se zpravidla o třetí stranu, která poskytuje službu úřadu. Jedná se o typický outsourcing. Může se jednat o vedení účetnictví, zpracování mezd apod.

### **2.16 Způsob kontroly zpracování OÚ**

Popište způsob kontroly zpracování OÚ - např. roční audit, kontrola třetí stranou.

### **2.17 Připravenost na uplatňování práv ze strany subjektů OÚ**

Informace o přijatých opatřeních musí být poskytnuta bez zbytečného odkladu a do jednoho měsíce od obdržení žádosti. Činí se tak pouze v odůvodněných případech a bezplatně. Uveďte svoji připravenost na tyto požadavky.

### **2.18 Další požadované dokumenty**

Dále prosím zašlete následující dokumenty, pokud je máte k dispozici a to:



- Organizační struktura posuzovaného subjektu / úřadu;
- Organizační řád;
- Spisový a skartační řád včetně vnitřních předpisů v oblasti archivace listinných dokumentů (Směrnice o archivaci);
- Vnitřní předpisy mající vztah k problematice osobních údajů a k problematice řízení bezpečnosti informací;
- Vzorové smlouvy k problematice zpracování osobních údajů nebo k činnostem, jejichž předmětem je zpracování osobních údajů.

### **3 Metodika pro vyplnění Formuláře č. 2 - Přehled používaných aplikací**

Dotazník prosíme předat na vedoucího odboru/oddělení IT. Níže jsou popsány jednotlivé body dotazníku.

#### **3.1 Název aplikace**

Uvede se název aplikace zpracovávající osobní údaje a její zaměření. Např. IS VERA – Spisová služba.

#### **3.2 Výrobce aplikace**

Uvedení názvu výrobce aplikace.

#### **3.3 Seznam zpracovávaných agend**

V této kolonce uveďte seznam všech agend či procesů, které jsou v dané aplikaci/informačním systému realizovány. Agendy jsou předmětem Formuláře č. 1 (viz předchozí kapitola č. 2). Veškeré agendy, které jsou zpracovávány v aplikacích, musí být v tomto výčtu uvedeny. Je pravděpodobné, že některé agendy budou zpracovávány ve více aplikacích.

#### **3.4 Vede evidenci osobních údajů?**

Výběr z předdefinovaných možností ANO/NE.

#### **3.5 Výčet položek osobních údajů**

Uvedení celého výčtu položek osobních údajů např. Jméno, Příjmení, Rodné číslo, Telefon, Email atd.

#### **3.6 Vede evidenci zvláštní kategorie osobních údajů?**

Výběr z předdefinovaných možností ANO/NE.

#### **3.7 Výčet položek zvláštní kategorie osobních údajů**

U kategorie zvláštních osobních údajů se jedná o následující informace:

- rasový či etnický původ;
- politické názory;

- náboženské vyznání;
- filozofické přesvědčení;
- členství v odborech;
- genetické údaje;
- biometrické údaje za účelem jedinečné identifikace fyzické osoby;
- údaje o zdravotním stavu;
- údaje o sexuální životě;
- údaje o sexuální orientaci.

### **3.8 Oblast působnosti**

Odpovědná osoba zde vybere z již předdefinovaných oblastí působnosti, jimiž jsou:

- Přenesená působnost státu (státní správa);
- Samostatná působnost (samospráva);
- Interní procesy úřadu;
- Kombinace výše uvedených možností – pokud ano prosím o upřesnění jejich kombinace.

### **3.9 Předávání dat**

Výčet aplikací, kterým daná aplikace předává data a jejich popis.

### **3.10 Archivace a skartace**

Popis archivace a výmazu dat z aplikace.

### **3.11 Připravované realizace**

Do dotazníku prosím uveďte ještě připravované realizace aplikací či IS, pokud jsou Vám známi.

### **3.12 Je aplikace ve vlastnictví posuzovaného subjektu nebo je provozována třetí osobou jako služba?**

Odpovědná osoba provede výběr z předdefinovaných možností:

- Ve vlastnictví posuzovaného subjektu;
- Provozováno třetí osobou jako služba;
- Jiný – pokud vyberete jiný je potřeba upřesnit o jaký vztah se jedná.

### **3.13 Otázky pro správce informačních a komunikačních technologií:**

Správce informačních a komunikačních technologií vyplní odpovědi

- Odpovídá zabezpečení aplikace platným bezpečnostním politikám úřadu?
- Máte analýzu rizik pro tuto aplikaci s ohledem na ochranu osobních údajů?
- Provozní vlastník IT infrastruktury aplikace
- Způsob zajištění aplikační podpory
- Využíváte v aplikaci pseudonymizaci OU/ COU?
- Využíváte v aplikaci šifrování OU/COU?
- Přístup k aplikaci pouze přes šifrovaný kanál?



- Má aplikace řízený přístup k OU/COU dle pracovní pozice uživatele?
- Vedete auditní záznamy k aplikaci?
- Používáte dvoufaktorové ověření?
- Je aplikace napojena na SIEM/SOC?
- Řídíte přístup k aplikaci pomocí FW, VLAN, DMZ?
- Je aplikace v HA (redundance, replikace)?
- Provádíte pravidelné zálohy aplikace?
- Máte k aplikaci disaster recovery plan (plán její obnovy)?
- Máte plán zálohování aplikace?
- Provádíte pravidelný test záloh aplikace?
- Provádíte pravidelné vyhodnocování incidentů?
- Provádíte pravidelný test disaster recovery plánu?
- Provádíte pravidelně test zranitelnosti / penetrační testy aplikace?
- Provádí se v aplikaci export dat obsahující OU/COU? Posílají se data z aplikace třetím stranám?
- Je aplikace připravena na přenositelnost OU?

### **3.14 Další požadované dokumenty**

V případě, že máte k dispozici dokumentaci k provozování informačních systémů úřadu dle ISO 2000x a ISO 2700x nebo Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), prosíme o její zaslání.