

**Zpráva reaudit**

o ověření shody s požadavky GDPR

Obecní úřad

Stratov

Středočeský kraj

Návštěva 19. 08. 2019

Datum vyhotovení: 19. 08. 2019



OBSAH

 [1](#_Toc11756646)

[1. Seznam zkratek 3](#_Toc11756647)

[2. Předmět auditu 4](#_Toc11756648)

[3. Základní charakteristika organizace 4](#_Toc11756649)

[4. Manažerské shrnutí zjištění auditu 6](#_Toc11756650)

[5. Podrobný popis zjištění 8](#_Toc11756651)

[6. Přílohy 19](#_Toc11756652)

[Příloha č. 1: Metodika auditu pro ověření shody s požadavky GDPR 19](#_Toc11756653)

1. Seznam zkratek

|  |  |
| --- | --- |
| **Zkratka** | **Vysvětlení zkratky** |
| DPIA | Data Protection Impact Assessment (posouzení vlivu na ochranu osobních údajů) |
| EU | Evropská unie |
| GDPR | General Data Protection Regulation (obecné nařízení o ochraně osobních údajů) |
| ZOZÚ | zákon č. 110/2019 Sb., o zpracování osobních údajů |
| ZOOÚ | zákon č. 101/2000 Sb., o ochraně osobních údajů |

1. Předmět auditu

Na základě dohody a v souvislosti s novým zákonem č. 110/2019 Sb. – o zpracování osobních údajů, který nahradil zákon č. 101/2000 Sb – o ochraně osobních údajů bylo uskutečněno nezávislé ověření shody/reaudit současného nastavení a fungování procesů a bezpečnostních opatření v obci s požadavky stanovenými GDPR.

Byly prověřeny procesy zpracování osobních údajů z následujících hledisek:

* dodržování zásad zpracování osobních údajů,
* vedení dokumentace systému řízení osobních údajů,
* nastavení a fungování organizačních opatření,
* řízení lidských zdrojů z pohledu bezpečnosti osobních údajů,
* nastavení a fungování technických opatření.

Podrobná metodika realizace auditu tvoří Přílohu č. 1 tohoto dokumentu.

1. Základní charakteristika organizace

Stratov je obcí tzv. I. typu, nachází se ve Středočeském kraji, ve správním obvodu obce s rozšířenou působností Lysá nad Labem. Obec je členem dobrovolného sdružení obcí Mikroregion Polabí, jehož cílem je koordinovat práci jednotlivých obcí na rozšiřování povědomí veřejnosti, podnikatelů i turistů o tuto část Polabí. Mikroregion Polabí tvoří obce Lysá nad Labem, Bříství, Jiřice, Ostrá, Kounice, Milovice, Přerov nad Labem, Semice, Stará Lysá, Starý Vestec a Stratov.

* 1. **Identifikované oblasti zpracování osobních údajů**

Obce I. stupně (dle ústavního pořádku ČR) zpracovávají osobní informace zejména v rámci:

* evidence obyvatel,
* zajišťování voleb v obci,
* zabezpečování ochrany veřejného pořádku,
* při jednáních vedení obce/zastupitelů a v návazných zápisech či usneseních,
* sjednávání a uzavírání smluvních ujednání
* správa a výběr správních/místních poplatků
* zajišťování kulturního života obce včetně vítání občánků, evidence jubileí apod.,
* vedení kroniky,
* zdokumentování, informování o životě v obci, a to i za pomoci fotografických a jiných médií případně včetně místního časopisu,
* zajišťování vidimace a legalizace,
* zajištění personálních činností, mezd a vedení účetnictví,
* zřizovatel MŠ,
* bytové hospodářství.
1. Manažerské shrnutí zjištění auditu

Zjištění uvedená v této zprávě jsou kategorizována z hlediska jejich významu dle níže uvedené tabulky.

|  |  |  |
| --- | --- | --- |
| **Významnost zjištění** | **Symbol** | **Popis**  |
| Vysoké riziko |  | Zjištění vysoké významností, jsou zanedbány klíčové požadavky Nařízení GDPR. Existuje vysoké riziko sankcí. |
| Střední riziko |   | Zjištění středné významnosti, některé požadavky Nařízení GDPR nejsou uplatňovány v plném rozsahu.  |
| Nízké riziko |  | Zjištění nízké významnosti, některé požadavky nařízení GDPR nejsou uplatňovány, avšak jedná se o administrativní či jiné nezávažné nedostatky. |

**Souhrn klíčových zjištění auditu**

V tabulce níže jsou shrnuta klíčová zjištění auditu (střední, vysoké riziko). Detailní popis všech zjištění je uveden v kapitole 5.

|  |  |
| --- | --- |
| **Zjištění ke dni:** | **Nález:** |
|  | 24.08.2017 | **19.8.****2019** |
| **1.** |   |  | Evidence / seznam uchovávaných / zpracovávaných osobních údajů včetně umístění |
| **2.** |   |  | **Souhlas se zpracováním osobních údajů součástí smlouvy** |
| **3.** |   |  | **Neplnění informační povinnosti o zpracování (obsahu) osobních údajů** |
| **4.** |   |   | **Uchování osobních údajů poté, co účel zpracování pominul** |
| **5.** |   |  | **Nestanovení skartační lhůty** |
| **6.** |  |  | **Vztah se zpracovatelem osobních údajů** |
| **7.** |   |  | **Pravidla upravujících oblast IT** |
| **8.** |   |  | **Komunikační kanály** |
| **9.** |   |  | **Vnitřní úpravy povinností mlčenlivosti** |
| **10.** |   |  | **Neprovádění analýzy rizik pro práva a svobody subjektů údajů** |
| **11.** |   |  | **Personální bezpečnost a zvyšování bezpečnostního povědomí zaměstnanců** |
| **12.** |   |  | Povinnost jmenovat pověřence pro ochranu osobních údajů |

1. Podrobný popis zjištění

V této kapitole jsou podrobně popsána významná zjištění realizovaného reauditu. U každého zjištění je identifikována jeho závažnost.

|  |  |  |
| --- | --- | --- |
| **1.** |  | Evidence / seznam uchovávaných / zpracovávaných osobních údajů včetně umístění |
| Zjištění: | Obec má zpracovanou evidenci osobních údajů shromažďovaných a zpracovávaných v obci. |

|  |  |  |
| --- | --- | --- |
| **2.** |  | **Souhlas se zpracováním osobních údajů součástí smlouvy** |
| Zjištění: | Osobní údaje jsou zpracovávané pouze na základě některého z platných právních rámců. Pokud jsou zpracovávané na základě Souhlasu, je tento udělen svobodně, informovaně, odděleně od ostatních ujednání. |

|  |  |  |
| --- | --- | --- |
| **3.** |  | **Neplnění informační povinnosti o zpracování (obsahu) osobních údajů** |
| Zjištění: | Obec má zpracovanou a zveřejněnou Informaci o zpracování osobních údajů. |

|  |  |  |
| --- | --- | --- |
| **4.** |   | **Uchování osobních údajů poté, co účel zpracování pominul** |
| Zjištění: | Podle čl. 5 odst. 1 písm. e) musí být osobní údaje uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Obdobnou povinnost stanoví § 5 odst. 1 písm. e). Podle tohoto ustanovení je správce povinen uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování.  |
| Doporučení: | I nadále platí prověřit, zda nejsou dlouhodobě uchovávány listiny, u nichž to není nikterak vyžadováno. Jde například o přílohy žádostí o poskytnutí služeb, různé druhy provozní komunikace a podobně. |

|  |  |  |
| --- | --- | --- |
| **5.** |  | **Nestanovení skartační lhůty** |
| Zjištění: | Ve smyslu zákona č. 499/2004 Sb., o archivnictví a spisové a službě jsou stanovené archivační a skartační lhůty.  |

|  |  |  |
| --- | --- | --- |
| **6.** |  | **Vztah se zpracovatelem osobních údajů** |
| Zjištění: | Obec uzavřela se zpracovateli smlouvu o zpracování osobních údajů, která upravuje v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá.  |

|  |  |  |
| --- | --- | --- |
| **7.** |  | **Pravidla upravujících oblast IT** |
| Zjištění: | Jsou stanovena pravidla pro používání IT. |

|  |  |  |
| --- | --- | --- |
| **8.** |  | **Komunikační kanály** |
| Zjištění: | Jsou stanoveny procesy a pravidla, kdy a za jakých podmínek mají být používány komunikační kanály při předávání osobních údajů. |

|  |  |  |
| --- | --- | --- |
| **9.** |  | **Vnitřní úpravy povinností mlčenlivosti** |
| Zjištění: | Všichni včetně zastupitelů byli poučeni o nutnosti zachovávat mlčenlivost.  |

|  |  |  |
| --- | --- | --- |
| **10.** |  | **Neprovádění analýzy rizik pro práva a svobody subjektů údajů** |
| Zjištění: | Byla zpracována analýza rizik. |

|  |  |  |
| --- | --- | --- |
| **11.** |  | **Personální bezpečnost a zvyšování bezpečnostního povědomí zaměstnanců** |
| Zjištění: | V současné době obec má 5 zaměstnanců – seznámených s problematikou ochrany osobních údajů.  |

|  |  |  |
| --- | --- | --- |
| **12.** |  | Povinnost jmenovat pověřence pro ochranu osobních údajů |
| Zjištění: | Obec s nabytím účinnosti GDPR pověřence pro ochranu osobních údajů zajistila**.** |

1. Přílohy

Příloha č. 1: Metodika auditu pro ověření shody s požadavky GDPR

BDO ve spolupráci s dalšími evropskými pobočkami BDO vyvinulo vlastní metodiku a nástroje, které minimalizují náklady a rizika spojená s problematikou a požadavky GDPR. Compliance audit (ověření shody) je rozdílová analýza, která identifikuje oblasti, které jsou v rozporu s GDPR a související rizika. Společně s identifikací rizik a jejich závažnosti je součástí compliance auditu také návrh optimalizačních opatření.

Audit vychází při compliance auditu z ustanovení GDPR, zákona o ochraně osobních údajů, judikatury a stanovisek orgánů dozoru a standardů řady ISO/IEC řady 27000 upravujících řízení bezpečnosti informací.

Audit zahrnuje:

* prověření vnitřní řídící dokumentace související s ochranou osobních údajů (politiky, směrnice, řády, záznamy, soubory),
* prověření procesů a organizačních a technických opatření souvisejících s ochranou osobních údajů,
* analýzu dat a klasifikaci osobních údajů,
* analýzu zabezpečení dat a přístupových oprávnění,
* prověření dodržování povinností týkajících se ochrany osobních údajů (povinnosti dle GDPR, zákona o ochraně osobních údajů a prováděcích předpisů, kodexů chování a standardů),
* analýzu účelů zpracování osobních údajů a posouzení jeho legitimity ve vazbě na GDPR a
* identifikaci rizik souvisejících s ochranou osobních údajů, včetně klasifikace jejich závažnosti.

**Kritéria auditu**

Jde o nezávislé ověření shody současného nastavení a fungování procesů a bezpečnostních opatření organizace s požadavky stanovenými GDPR.

Bylo prověřeno plnění následujících požadavků požadovaných při zpracování osobních údajů:

* dodržování zásad zpracování osobních údajů,
* vedení dokumentace systému řízení osobních údajů,
* nastavení a fungování organizačních opatření,
* řízení lidských zdrojů z pohledu bezpečnosti osobních údajů,
* nastavení a fungování technických opatření.

Zásady zpracování osobních údajů

GDPR stanoví základní zásady (základní povinnosti), které musí být dodržovány v průběhu zpracování osobních údajů.

***Definice osobních*** údajů

Osobní údaje jsou definovány jako veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě.

Mezi obecné osobní údaje patří jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresa a fotografický záznam. Mezi osobní údaje patří i tzv. organizační údaje (například e-mailová adresa, telefonní číslo či různé identifikační údaje vydané státem).

GDPR definuje také zpracování zvláštních kategorií osobních údajů, citlivých osobních údajů. Těmito údaji jsou údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení. Do kategorie citlivých údajů nařízení nově zahrnuje genetické, biometrické údaje a osobní údaje dětí. Genetickými údaji jsou osobní údaje týkající se zděděných nebo získaných genetických znaků určité fyzické osoby, které vyplývají z analýzy biologického vzorku dotčené fyzické osoby nebo z analýzy jiného prvku, která umožňuje získat rovnocenné informace. Mezi osobní údaje o zdravotním stavu musí být zahrnuty veškeré údaje související se zdravotním /duševním stavem.

Biometrickým údajem jsou osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňují jedinečnou identifikaci. Typickým biometrickým údajem je např. snímek obličeje, otisk prstu, ale podle poslední judikatury i podpis.

Naopak z působnosti GDPR jsou vyloučeny anonymizované údaje, údaje zemřelých osob a údaje získané v rámci činnosti čistě osobní povahy, které nemají obchodní či institucionální charakter.

Transparentnost zpracování osobních údajů

Všechny informace a všechna sdělení týkající se zpracování osobních údajů musí být snadno přístupné, srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků.

Povinnost zpracovávat osobní údaje pouze pro konkrétní a legitimní účely

Osobní údaje mohou být shromažďovány výhradně pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.

Minimalizace osobních údajů

Osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.

Omezení uložení osobních údajů

Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů.

Zákonnost zpracování osobních údajů

Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným způsobem. Zpracovávat osobní údaje je možné pouze tehdy, pokud existuje alespoň jeden z dále uvedených právních titulů (důvodů) pro zpracování osobních údajů:

* subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů,
* zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
* zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,
* zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
* zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, nebo
* zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

Dokumentace systému řízení osobních údajů

V rámci ověření dokumentace systému řízení osobních údajů se audit zabýval, zda jsou procesy zpracování osobních údajů a související procesy řádně dokumentovány. V této souvislosti byla prověřena existenci bezpečnostní politiky nebo jiných pravidel upravujících zásady ochrany osobních údajů. Bylo též prověřeno, zda je zdokumentováno rozdělení pravomocí a odpovědností za řízení a ochranu osobních údajů. Součástí ověření byla také metodika pro identifikaci a hodnocení aktiv a rizik. Ověřena byla také existence plánů zvládání rizik a plánů pro řízení kontinuity. Předmětem auditu byly i smlouvy se zpracovateli osobních údajů a s třetími stranami.

Organizační opatření

Audit se zabýval nastavením organizačních opatření a ověřil, zda jsou zavedena následující organizační opatření:

* nastavení pravomocí a odpovědností,
* identifikace a evidence aktiv,
* řízení rizik,
* zohledňování vlivu změn v rámci a vně organizace na systém řízení osobních údajů,
* řízení dokumentace,
* Identity Management – řízení životního cyklu uživatelů a úrovně jejich přístupu k osobním údajům,
* procesy pro řízení vztahů se zpracovateli a dalšími dodavateli,
* řízení a zvládání bezpečnostních incidentů,
* plány kontinuity,
* procesy pro komunikaci s Úřadem pro ochranu osobních údajů.

Předmětem auditu bylo také ověření monitoringu a hodnocení účinnosti zavedených organizačních opatření.

Řízení lidských zdrojů z pohledu bezpečnosti osobních údajů

Tématem auditu bylo i řízení lidských zdrojů z pohledu bezpečnosti osobních údajů. V této souvislosti bylo ověřeno nastavení a fungování procesů pro řízení lidských zdrojů, včetně získávání a výběru zaměstnanců, uzavírání pracovněprávních smluv, motivace a rozvoje lidských zdrojů a také ukončování pracovněprávních vztahů. Audit se také zabýval zajištěním povinnosti mlčenlivosti ve vztahu k osobním údajům.

Technická opatření

Audit se zabýval fungováním technických opatření a ověřil, zda jsou zavedena následující technická opatření:

* nástroje pro řízení přístupových oprávnění,
* nástroje pro ověřování identity uživatelů,
* klíčové hospodářství,
* prostředky pro zamezení neoprávněného přístupu do prostor či k osobním údajům,
* integrita komunikačních cest (např. ochranou a segmentací sítě, jejího oddělení od vnější sítě a řízením přístupů k síti, bezpečné předávání papírové dokumentace),
* používání nástroje pro ochranu před škodlivým kódem,
* nástroje pro zaznamenávání vykonávaných činností a osobními údaji v informačních systémech,
* nástroje pro sledování a vyhodnocování hrozeb v souvislosti s osobními údaji,
* používání kryptografických prostředků.

**Postup auditu**

Analýza interní dokumentace

V rámci této fáze byly posouzeny vnitřní předpisy, politiky, směrnice, metodiky a další podklady týkající se předmětu auditu. Audit identifikoval procesy zpracování osobních údajů. V rámci posouzení uvedených podkladů byly zhodnoceny nastavení bezpečnostních opatření a rizika pro organizaci i pro subjekty osobních údajů, jak to vyžaduje GDPR.

Ověření procesů a opatření

Audit shromáždil potřebné informace a dokumenty.

Závěr analýzy

Na základě zhodnocených důkazů a informací byla zpracována zpráva, v které byly shrnuty závěry z auditu včetně navržených opatření.

Zdroje informací

Hlavním zdrojem informací byly obdržené písemné podklady a výstupy z rozhovoru s vybranými, zejména vedoucími pracovníky organizace a osobami zodpovědnými za ochranu osobních údajů v organizaci.