V Maršovicích dne: 20.5.2018

 Účinnost od: 25.5.2018

**OBEC MARŠOVICE**

**Ochrana osobních údajů OÚ**

|  |  |  |
| --- | --- | --- |
|  | Jméno a příjmení | Datum |
| Zpracoval | Ing. Zbyněk Vavřina | 20.5.2018 |
| Odsouhlasil | Jiří Ouhrabka | 20.5.2018 |
| Schválil | Jiří Ouhrabka | 20.5.2018 |

Obsah

[1. Všeobecná ustanovení 3](#_Toc512855262)

[2. Úvodní, obecná ustanovení 3](#_Toc512855263)

[3. Definice a pojmy 3](#_Toc512855264)

[4. Odpovědnost Správce, zaměstnance 7](#_Toc512855265)

[5. Zpracovatel 8](#_Toc512855266)

[6. Záznamy zpracování osobních údajů 10](#_Toc512855267)

[7. Zajištění souladu zpracování osobních údajů s obecným nařízením GDPR 10](#_Toc512855268)

[8. Vazba na vnitřní předpisy a procesy 12](#_Toc512855269)

[9. Práva subjektu údajů 12](#_Toc512855270)

[10. Souhlas se zpracováním osobních údajů 14](#_Toc512855271)

[11. Informační povinnost vůči subjektům údajů 15](#_Toc512855272)

[12. Ochrana osobních údajů 17](#_Toc512855273)

[13. Ohlašování porušení ochrany osobních údajů 17](#_Toc512855274)

[14. Školení a zvyšování povědomí 18](#_Toc512855275)

[15. Plán pravidelného ověřování shody s obecným nařízením GDPR 19](#_Toc512855276)

[16. Pověřenec pro ochranu osobních údajů 20](#_Toc512855277)

[17. Podání, evidence a vyřízení žádosti o výkon práv subjektu údajů 21](#_Toc512855278)

[18. Zdroje informací 22](#_Toc512855279)

[19. Kontaktní údaje Správce a Pověřence 23](#_Toc512855280)

[20. Závěrečná ustanovení 23](#_Toc512855281)

[Seznam změn a revizí řízeného dokumentu 23](#_Toc512855282)

# Všeobecná ustanovení

Dne 27.  dubna 2016 došlo k přijetí obecného nařízení GDPR Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a zrušení směrnice 95/46/ES (dále také obecné nařízení GDPR).

1. Tato obecná směrnice stanoví rozsah a způsob uplatňování ochrany osobních údajů fyzických osob v prostředí Obec Maršovice (dále také OÚ), který vystupuje v roli správce a/nebo zpracovatele osobních údajů dle výše uvedeného obecného nařízení GDPR s účinností od 25. května 2018.
2. Tato směrnice je platná pro všechny zaměstnance OÚ, kteří zpracovávají osobní údaje.
3. Obecné nařízení o ochraně osobních údajů je též označováno zkratkou „GDPR“ z anglického originálu General Data Protection Regulation.

# Úvodní, obecná ustanovení

1. Charakteristická pro obecné nařízení GDPR je jeho univerzální použitelnost ve všech státech Evropské unie (a Islandu, Norska a Lichtenštejnska) a tudíž i sjednocující účinek, jelikož jednotná pravidla pro zpracování osobních údajů platí v každém státě EU a třech vyjmenovaných.
2. Obecné nařízení GDPR je založeno na dvou nových přístupech a to na principu odpovědnosti správce a přístupu založeném na riziku v tomto rozsahu:
	1. **Princip odpovědnosti** znamená odpovědnost správce za dodržení zásad zpracování osobních údajů, které jsou v obecném nařízení GDPR uvedeny v článku 5 odst. 1 a zároveň musí správce být schopen tento soulad doložit.
	2. **Princip přístupu založeném na riziku** v širším slova smyslu znamená, že správce již od počátku koncipování zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext a účel zpracování osobních údajů a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu musí přizpůsobit i zabezpečení osobních údajů. V užším slova smyslu jde u přístupu založeném na riziku jako o aplikaci některých povinností pouze v případě, kdy zpracování osobních údajů či porušení ochrany osobních údajů (bezpečnostní incident) představuje riziko či vysoké riziko pro práva a svobody fyzické osoby. V tomto rozsahu princip založený na riziku se uplatňuje zejména u nových povinností: ohlašování, resp. oznamování případu porušení ochrany osobních údajů Úřadu pro ochranu osobních údajů, resp. subjektu údajů, posuzování vlivu zpracování osobních údajů na ochranu osobních údajů a povinné konzultace s Úřadem pro ochranu osobních údajů, jejichž aplikace je vázána na přítomnost rizika či vysokého rizika pro práva a svobody fyzických osob.

# Definice a pojmy

V souvislosti s ochranou osobních údajů dle obecného nařízení GDPR se setkáváme s novými pojmy, ale také s řadou pojmů, které jsou definovány v české právní úpravě. V následujícím výčtu jsou tyto klíčové pojmy z ochrany osobních údajů uvedeny:

**Anonymní údaj –** takový údaj, který buď v původním tvaru, nebo po provedeném zpracování osobních údajů nelze vztáhnout k identifikované nebo identifikovatelné fyzické osobě.

**Automatizované zpracování osobních údajů –** je běžně rozšířenou formou zpracování osobních údajů za použití výpočetní techniky, bez lidského zásahu.

**Biometrický údaj –** osobní údaj technického charakteru zpracování osobních údajů fyzických či fyziologických znaků fyzické osoby, který umožňuje jedinečnou identifikaci. Typickým biometrickým údajem je např. snímek obličeje, otisk prstu, apod.

**Dozorový úřad** **–** Úřad pro ochranu osobních údajů (zkráceně ÚOOÚ) je v České republice nezávislým orgánem, který:

1. Provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů.
2. Přijímá podněty a stížnosti občanů na porušení zákona.
3. Poskytuje konzultace v oblasti ochrany osobních údajů.

**Důvěrnost –** znamená, že k informacím či datům mají přístup pouze oprávněné osoby.

**Integrita –** znamená, informace či data nebyla zpěněna neoprávněnou osobou.

**Identifikovatelná fyzická osoba –** 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.

**OÚ –** Obec Maršovice

**NDA smlouva –** Non-disclosure agreement – Smlouva či dohoda o mlčenlivosti sjednaná v případě, že dvě strany si vzájemně (či jen jedna strana druhé) chtějí zpřístupnit nějaké informace, data či znalosti, u nichž je vhodné omezit jejich využití jen ke sjednanému účelu (např. v rámci pracovního poměru, obchodního jednání, ochrany osobních údajů, apod.).

**Omezení zpracování osobních údajů –** označení uložených osobních údajů za účelem omezení jejich zpracování osobních údajů v budoucnu. Způsoby, jak omezit zpracování osobních údajů, by mohly mimo jiné zahrnovat dočasný přesun vybraných údajů do jiného systému zpracování osobních údajů, znepřístupnění vybraných osobních údajů uživatelům nebo dočasné odstranění zveřejněných údajů z internetových stránek. V systémech automatizovaného zpracování osobních údajů by omezení zpracování osobních údajů mělo být v zásadě zajištěno technickými prostředky tak, aby se na osobní údaje již nevztahovaly žádné další operace zpracování osobních údajů a aby nemohly být změněny. Skutečnost, že zpracování osobních údajů je omezeno, musí být v systému jasně vyznačena.

**Osobní údaj –** veškeré informace o identifikované nebo identifikovatelné fyzické osobě.

**Pověřenec pro ochranu osobních údajů –** neboli DPO (z anglického Data Protection Officer) je nově vytvořenou pracovní pozicí v OÚ podle obecného nařízení GDPR. Hlavním úkolem DPO je monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z obecného nařízení GDPR, provádění interních auditů, školení pracovníků a celkové řízení agendy interní ochrany osobních údajů v OÚ.

**Právní důvody –** oprávnění Správce osobní údaje zpracovávat. Právní důvody jsou nezbytným předpokladem, aby se vůbec dalo mluvit ze strany Správce o legálním zpracování osobních údajů, neboť pokud by Správce nedisponoval řádným právním důvodem ke zpracování osobních údajů, nebyl by schopen doložit plnění svých povinností při ochraně osobních údajů fyzických osob, jelikož by osobní údaje zpracovával nezákonně a musel by osobní údaje zlikvidovat. Výčet právních důvodů:

1. Zpracování osobních údajů je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů.
2. Zpracování osobních údajů je nezbytné pro splnění právní povinnosti, která se na Správce vztahuje.
3. Zpracování osobních údajů je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.
4. Zpracování osobních údajů je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen Správce.
5. Zpracování osobních údajů 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.
6. Subjekt údajů udělil souhlas pro jeden či více konkrétních účelů.

**Profilování –** jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa kde se nachází, nebo pohybu.

**Příjemce (také Třetí strana) –** 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.

Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem ČR, se za příjemce nepovažují. Orgány veřejné moci, kterým jsou osobní údaje sdělovány na základě právní povinnosti pro účely výkonu jejich úředních povinností, jako jsou daňové a celní orgány, finanční vyšetřovací jednotky, nezávislé správní orgány nebo orgány finančního trhu příslušné pro regulaci trhů s cennými papíry a dohled nad nimi, by neměly být považovány za příjemce, pokud obdrží osobní údaje, které jsou nezbytné pro provedení konkrétního šetření v obecném zájmu v souladu s právem EU či ČR. Žádost o sdělení osobních údajů zaslaná orgány veřejné moci by měla být vždy písemná a odůvodněná, měla by se týkat jednotlivého případu a neměla by se vztahovat na celou evidenci ani vést k propojení evidencí. Zpracování osobních údajů těmito orgány veřejné moci by mělo být v souladu s platnými pravidly pro ochranu osobních údajů podle účelů zpracování osobních údajů.

**Pseudonymizace –** je proces skrytí identity, jehož účelem je mít možnost sbírat další údaje týkající se stejné fyzické osoby, aniž by bylo nutné znát její totožnost. Pseudonymizované osobní údaje nejsou anonymizovanými údaji, proto se na ně stále vztahuje regulace obecného nařízení GDPR.

**Souhlas subjektu údajů –** jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.

**Správce –** fyzická osoba, právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů Jsou-li účely a prostředky zpracování osobních údajů určeny právními předpisy EU či České republiky, může toto právo určit dotčeného Správce nebo zvláštní kritéria pro jeho určení.

Pro potřeby této směrnice se Správcem rozumí OBEC MARŠOVICE, zastoupené jeho starostou Jiřím Ouhrabkou .

**Subjekt údajů –** identifikovaná nebo identifikovatelná fyzická osoba. 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.

**Uchovávání osobních údajů –** udržování údajů v takové podobě, která je umožňuje dále zpracovávat.

**Zaměstnanec –** je účastník pracovněprávního vztahu s OÚ, který se zavazuje vykonávat pro OÚ určitou závislou činnost.

**Zásady zpracování osobních údajů** **–** jednotlivé zásady jsou rozvinuty v článku 5 odst. 1 obecného nařízení GDPR. K prokazování souladu se zásadami slouží záznamy o činnostech zpracování osobních údajů. Výčet zásad zpracování osobních údajů:

1. Zákonnost, korektnost, transparentnost – Správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně.
2. Omezení účelu – osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely.
3. Minimalizace údajů – osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány.
4. Přesnost – osobní údaje musí být přesné.
5. Omezení uložení – osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány.
6. Integrita a důvěrnost – technické a organizační ochrana osobních údajů.

**Zpracovatel –** fyzická osoba, právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro Správce.

**Zpracování osobních údajů –** jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Zpracování osobních údajů ve smyslu obecného nařízení GDPR však nelze chápat jako jakékoli nakládání s osobním údajem. Zpracování osobních údajů je nutné považovat již za sofistikovanější činnost, kterou Správce s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky. Pro nakládání s osobními údaji způsobem, který není zpracováním osobních údajů, poskytuje ochranu např. zákon č. 89/2012 Sb., občanský zákoník. Obecným nařízením GDPR se tak jako Správci řídí pouze subjekty, které osobní údaje zpracovávají ve smyslu výše uvedené definice zpracování osobních údajů.

**Zvláštní kategorie osobních údajů –** osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zpracování genetických a biometrických osobních údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

# Odpovědnost Správce, zaměstnance

1. Dle obecného nařízení GDPR je stanovena odpovědnost Správce za jakékoliv zpracování osobních údajů prováděné Správcem nebo pro něj. Správce musí být zejména povinen zavést vhodná a účinná opatření a být schopen doložit, že činnosti zpracování osobních údajů jsou v souladu s tímto obecným nařízením GDPR. Tato opatření by měla zohledňovat povahu, rozsah, kontext a účely zpracování osobních údajů a riziko pro práva a svobody fyzických osob.
2. Správce odpovídá za identifikaci a analýzu různě pravděpodobných a závažných rizik pro práva a svobody fyzických osob, která mohou vyplynout ze zpracování osobních údajů, které by mohlo vést k fyzické, hmotné nebo nehmotné újmě, zejména v případech, kdy by zpracování osobních údajů mohlo vést k diskriminaci, krádeži či zneužití identity, finanční ztrátě, poškození pověsti, ztrátě důvěrnosti osobních údajů nebo jakémukoliv jinému významnému hospodářskému či společenskému znevýhodnění, kdy by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje, kdy jsou zpracovávány osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení nebo členství v odborech, kdy jsou zpracovávány genetické údaje či údaje o zdravotním stavu či sexuálním životě nebo odsouzení v trestních věcech a trestných činů či souvisejících bezpečnostních opatření, kdy jsou za účelem vytvoření či využití osobních profilů vyhodnocovány osobní aspekty, zejména prostřednictvím analýzy nebo odhadu aspektů týkajících se pracovních výsledků, ekonomické situace, zdravotního stavu, osobních preferencí nebo zájmů, spolehlivosti nebo chování, místa pobytu a pohybu, kdy jsou zpracovávány osobní údaje zranitelných osob, především dětí, nebo kdy je zpracováván velký objem osobních údajů a zpracování osobních údajů se dotýká velkého počtu subjektů údajů.
3. Pravděpodobnost a závažnost rizika pro práva a svobody subjektu údajů se určují na základě povahy, rozsahu, kontextu a účelů zpracování osobních údajů. Riziko se hodnotí na základě objektivního posouzení, které stanoví, zda operace zpracování osobních údajů představují riziko či vysoké riziko.
4. V zájmu zachování ochrany osobních údajů a zabránění zpracování osobních údajů, které by bylo v rozporu s tímto obecným nařízením GDPR, odpovídá zaměstnanec za posouzení rizik spojených se zpracováním osobních údajů a přijetí opatření ke zmírnění těchto rizik, například šifrováním dat, heslováním dat, několika úrovňovou ochranou, podepisováním dat kvalifikovaným elektronickým podpisem, používáním bezpečných komunikačních kanálů, ukládáním fyzických dokumentů do uzamykatelných skříní, využíváním PINu u mobilních telefonů, apod. Při posuzování rizik pro ochranu osobních údajů by se měla vzít v úvahu rizika, která zpracování osobních údajů představuje, jako jsou náhodné nebo protiprávní zničení, ztráta, pozměnění, neoprávněné zpřístupnění nebo zpřístupnění předaných, uložených nebo jiným způsobem zpracovaných osobních údajů, které by mohly zejména vést k fyzické, hmotné nebo nehmotné újmě.
5. Zaměstnance je povinen dodržovat zásady zpracování osobních údajů. Výčet zásad je uveden v kapitole 3. Definice a pojmy.
6. Zaměstnanec je povinen zachovávat mlčenlivost o zpracování osobních údajů a přijatých opatřeních k jejich ochraně, o nichž se v souvislosti s výkonem své pracovní činnosti dozvěděl, a to i po skončení pracovního poměru.
7. V případě potřeby se může zaměstnanec obrátit s žádostí o konzultaci na Pověřence.

# Zpracovatel

1. Zpracování osobních údajů zpracovatelem se řídí smlouvou, která zavazuje zpracovatele vůči Správci a v nichž je stanoven předmět a doba trvání zpracování osobních údajů, povaha a účel zpracování osobních údajů, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva Správce. Tato smlouva stanoví, že zpracovatel:
2. Zpracovává osobní údaje pouze na základě doložených pokynů Správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování osobních údajů již neukládá právo EU nebo ČR, které se na Správce vztahuje. V takovém případě zpracovatel Správce informuje o tomto právním požadavku před zpracováním osobních údajů, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu.
3. Zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.
4. Přijme všechna opatření požadovaná podle článku 32 obecného nařízení GDPR.
5. Dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v článku 28 odstavcích 2 a 4 obecného nařízení GDPR.
6. Zohledňuje povahu zpracování osobních údajů, je Správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění Správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených obecným nařízením GDPR.
7. Je Správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36 obecného nařízení GDPR, a to při zohlednění povahy zpracování osobních údajů a informací, jež má zpracovatel k dispozici.
8. V souladu s rozhodnutím Správce všechny osobní údaje buď vymaže, nebo je vrátí Správci po ukončení poskytování služeb spojených se zpracováním osobních údajů, a vymaže existující kopie, pokud právo EU nebo ČR nepožaduje uložení daných osobních údajů.
9. Poskytne Správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené mu Správcem, a umožní audity, včetně inspekcí, prováděných Správcem nebo jiným auditorem, kterého Správce pověřil, a k těmto auditům přispěje.
10. Smlouva nebo jiný obdobný právní akt mezi Správcem a zpracovatelem/zpracovateli musí být vyhotoveny písemně, v to počítaje i elektronickou formu.
11. Smlouva musí minimálně stanovit následující parametry:
12. Předmět zpracování osobních údajů.
13. Dobu zpracování osobních údajů.
14. Povahu zpracování osobních údajů.
15. Účel zpracování osobních údajů.
16. Typ osobních údajů.
17. Kategorii subjektů údajů.
18. Povinnosti a práva Správce.
19. Závazky zpracovatele, který:
20. Zpracovává osobní údaje pouze na základě pokynu Správce.
21. Informuje Správce o předávání do zahraničí, včetně povinnosti předávat na základě požadavků práva EU nebo ČR (pokud to právní předpis nezakazuje z důvodu veřejného zájmu).
22. Přijímá závazek mlčelivosti zaměstnanců zpracovatele.
23. Přijímá vhodná technická a organizační opatření na ochranu osobních údajů.
24. Zapojuje do zpracování osobních údajů další zpracovatele pouze s písemným svolením Správce a informuje Správce o všech zamýšlených změnách týkajících se zpracovatelů.
25. Zajišťuje, že při řetězení zpracovatelů musí každý další první zpracovatelem vybraný zpracovatel přijmout stejné povinnosti jako první zpracovatel.
26. Pokud předává osobní údaje, dochází k němu na základě rozhodnutí Komise nebo jiných nástrojů poskytujících vhodné záruky.
27. Umožní audity prováděné Správcem nebo jiným auditorem, kterého Správce pověřil.
28. Po ukončení zpracování osobní údaje vrátí Správci, nebo je na základě pokynu Správce vymaže (pokud právo EU nebo ČR nestanoví jinak).
29. Je Správci nápomocen při plnění jeho povinnosti reagovat na žádosti o výkon práv subjektů údajů.
30. Je Správci nápomocen při zajišťování ochrany zpracování osobních údajů, ohlašování případů porušení ochrany osobních údajů, posouzení vlivu na ochranu osobních údajů a předchozí konzultace.
31. Zaměstnanec OÚ, který zpracovává osobní údaje, může být v postavení:
32. Správce vs. Zpracovatel – zaměstnanec jako Správce osobních údajů pověří výkonem zpracování osobních údajů jinou fyzickou osobu, právnickou osobu, orgán veřejné moci, agenturu nebo jiný subjekt (např. společnost zajišťující správu informačního systému, právník poskytující externě právní služby, společnost zajišťující externě řízení projektů, apod.).
33. Zpracovatel vs. Správce – zaměstnanec je jinou fyzickou osobu, právnickou osobu, orgánem veřejné moci, agenturou nebo jiným subjektem pověřen pro něj zpracováním osobních údajů.
34. Za dodržování pravidel při zpracování osobních údajů zpracovatelem je odpovědný vždy Správce.

# Záznamy zpracování osobních údajů

1. Povinností Správce je uchovávání záznamů o činnostech zpracování osobních údajů pro doložení shody zpracování osobních údajů s obecným nařízením GDPR dle příslušných zásad.
2. Vést záznamy o činnostech zpracování osobních údajů je v odpovědnosti jmenovaného Pověřence pro ochranu osobních údajů. Pověřenec tyto záznamy nevyhotovuje, Pověřenec je pouze eviduje.
3. Za vyhotovení a předání záznamů o činnostech zpracování osobních údajů v aktuálním stavu Pověřenci odpovídá vždy Správce. Správce je odpovědný za udržování záznamů o činnostech zpracování osobních údajů vždy v aktuálním stavu.
4. Rozsah záznamů o činnostech zpracování osobních údajů je stanoven v Příloze č. 1 této směrnice.

# Zajištění souladu zpracování osobních údajů s obecným nařízením GDPR

1. Soulad nebo též shodu ochrany údajů při jejich zpracování osobních údajů prokazuje na základě principu odpovědnosti Správce nebo zpracovatel.
2. Správce musí být schopen dodržení souladu dokumentovat.
3. Správce musí prověřovat soulad opakovaně s cílem optimalizovat činnosti a jejich ochranu s ohledem na všechna zpracování osobních údajů, která provádí nebo jimi pověřuje své smluvní zpracovatele.
4. Definované oblasti, které jsou posuzovány pro soulad s obecným nařízením GDPR:
5. Jsou dodrženy základní zásady zpracování osobních údajů v souladu s článkem 5 obecného nařízení GDPR.
6. Zpracování osobních údajů je prováděno zákonným způsobem v souladu s články 6 a 9 obecného nařízení GDPR.
7. Podmínky vyjádření souhlasu subjektu údajů jsou v souladu s článkem 7 obecného nařízení GDPR.
8. Osobní údaje ve věci rozsudků v trestných věcech a trestných činů a souvisejících bezpečnostních opatřeních jsou zpracovány za definovaných podmínek v souladu s článkem 10 obecného nařízení GDPR.
9. Je zajištěna požadovaná informovanost subjektu údajů v souladu s články 12 až 14 obecného nařízení GDPR.
10. Jsou zajištěna práva subjektu údajů v souladu s články 15 až 21 obecného nařízení GDPR.
11. Je zajištěno řízení ochrany osobních údajů v souladu s články 24, 25 a 32 obecného nařízení GDPR.
12. Jsou zajištěny podmínky pro zpracování osobních údajů Správcem nebo zpracovatelem se sídlem mimo EU v souladu s článkem 27 obecného nařízení GDPR.
13. Správce provádí zpracování osobních údajů prostřednictvím zpracovatele za požadovaných podmínek v souladu s články 28 a 29 obecného nařízení GDPR.
14. Správce nebo zpracovatel provádí v souladu s článkem 30 obecného nařízení GDPR záznamy o činnostech zpracování osobních údajů.
15. Správce nebo zpracovatel řeší porušení ochrany osobních údajů požadovaným způsobem v souladu s články 33 a 34 obecného nařízení GDPR.
16. Správce provedl v souladu s článkem 35 obecného nařízení GDPR posouzení vlivu na ochranu osobních údajů.
17. Správce zajistil předchozí konzultaci s dozorovým úřadem v souladu s článkem 36 obecného nařízení GDPR.
18. Správce ustanovil v souladu s články 37 až 39 obecného nařízení GDPR Pověřence pro ochranu osobních údajů.
19. Správce zpracovává osobní údaje v souladu s články 40 a 41 obecného nařízení GDPR dle kodexu chování.
20. Správce předává osobní údaje do třetích zemí nebo mezinárodním organizacím v souladu s články 44 až 50 obecného nařízení GDPR.
21. Vhodným způsobem pro opakované ověřování souladu s obecným nařízením GDPR je např. forma interního auditu.

# Vazba na vnitřní předpisy a procesy

1. Zajištění bezpečnosti informací a ochrany osobních údajů v OÚ má přímou vazbu na platné vnitřní předpisy a procesy OÚ. Povinností Správce je udržovat neustále aktualizované vnitřní předpisy a popisy procesů (činností), jejichž obsahem je stanovení povinností zaměstnanců OÚ minimálně v těchto oblastech:
2. Ochrana osobních údajů (tato směrnice).
3. Spisový a skartační řád
4. Organizační řád
5. Provoz informačního systému OÚ
6. Aktualizace vnitřních předpisů probíhá pravidelně 1x ročně.

# Práva subjektu údajů

1. Práva subjektu údajů jsou důležitým prvkem ochrany osobních údajů jako celku, jelikož subjekt údajů je často ve slabším postavení než Správce a tudíž vybalancovávají vztah mezi ním a Správcem.
2. Výčet práv subjektu údajů:
3. **Na přístup k informacím** – se rozumí oprávnění subjektu údajů na základě jeho aktivní žádosti získat od Správce informaci (potvrzení), zda jsou či nejsou jeho osobní údaje zpracovávány a pokud jsou zpracovávány, má subjekt údajů právo tyto osobní údaje získat a zároveň má právo získat následující informace:
4. Účely zpracování osobních údajů.
5. Kategorie dotčených osobních údajů.
6. Příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny.
7. Plánovaná doba, po kterou budou osobní údaje uloženy.
8. Existence práva požadovat od Správce opravu nebo výmaz osobních údajů, právo vznést námitku.
9. Právo podat stížnost u dozorového úřadu.
10. Veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů.
11. Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.
12. **Na opravu respektive doplnění** – subjekt údajů má právo na opravu nepřesných osobních údajů, které se ho týkají. Toto právo vyvěrá ze zásady přesnosti. Neznamená to povinnost Správce aktivně vyhledávat nepřesné údaje (avšak nic mu v tom ani nebrání), ani to neznamená povinnost Správce např. každoročně požadovat po subjektu údajů aktualizaci jeho údajů. Pokud se subjekt údajů domnívá, že Správce zpracovává jeho nepřesné údaje, upozorní jej na to. Je povinností Správce, pokud mu subjekt údajů oznámí, že požaduje opravu jeho osobních údajů, zabývat se jeho žádostí.
13. **Na výmaz údajů („být zapomenut“)** – představuje v obecném nařízení GDPR jinými slovy vyjádřenou povinnost Správce zlikvidovat osobní údaje, pokud je splněna alespoň jedna podmínka:
14. Osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány.
15. Subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování osobních údajů.
16. Subjekt údajů vznese námitky proti zpracování osobních údajů a neexistují žádné převažující oprávněné důvody pro zpracování osobních údajů.
17. Osobní údaje byly zpracovány protiprávně.
18. Osobní údaje musí být vymazány ke splnění právní povinnosti.
19. Osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 obecného nařízení GDPR.

Právo na výmaz se tedy uplatní jen ve vyčtených bodech, tj. když nastane daná okolnost.

Právo na výmaz není absolutní právo, které by subjektu údajů dávalo možnost žádat kdykoli a za jakékoli situace o vymazání osobních údajů. Nelze např. v rámci práva být zapomenut žádat likvidaci všech osobních údajů např. při ukončení zaměstnání či poskytování finančních služeb, jelikož na Správce se vztahují povinnosti o dalším uchování některých osobních údajů.

1. **Na omezení zpracování osobních údajů** – je právo subjektu údajů omezit zpracování osobních údajů Správcem. Smyslem ustanovení je omezit (přerušit) zpracování údajů do doby vyřešení sporné otázky (např. subjekt údajů popírá přesnost údajů; omezení trvá po dobu potřebnou k ověření přesnosti údajů).
2. **Na přenositelnost zpracování osobních údajů** – je právo subjektu údajů, jehož podstatou je možnost za určitých podmínek získat osobní údaje, které se ho týkají a jež Správci poskytl, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému Správci, aniž by tomu původní Správce bránil. Zároveň má subjekt údajů, pokud požádá, i právo na to, aby Správce předal jeho osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu jinému Správci, je-li to technicky proveditelné.

Společné podmínky k aplikaci práva na přenositelnost:

1. Musí jít o zpracování osobních údajů založené na právním důvodu souhlasu či smlouvě.
2. Zpracování osobních údajů se provádí automatizovaně.
3. **Na námitku proti zpracování osobních údajů** – subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které jsou zpracovávány na základě právních důvodů:
4. Zpracování osobních údajů je nezbytné pro plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je Správce pověřen.
5. Zpracování osobních údajů je nezbytné pro účely oprávněných zájmů příslušného Správce či třetí strany.

Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování osobních údajů, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

Námitku lze vznést i proti zpracování osobních údajů pro účely přímého marketingu nebo profilování. Pokud subjekt údajů vznese námitku proti zpracování osobních údajů pro účely přímého marketingu, nebudou již osobní údaje pro tyto účely zpracovávány.

1. **Automatizovanému individuálnímu rozhodování včetně profilování** – toto právo zajišťuje subjektu údajů, že nebude předmětem rozhodnutí založeného výhradně na automatizovaném zpracování osobních údajů, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká. Jinými slovy, jde o zajištění, aby se o právních účincích nerozhodovalo automatizovanými postupy bez lidské ingerence, kromě možných výjimek.

Automatizované rozhodování je přípustné v případě, kdy je nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a Správcem, pokud je povoleno právem EU nebo ČR nebo pokud je založeno na výslovném souhlasu subjektu údajů.

1. Při zpracování osobních údajů je zaměstnanec povinen vždy dodržovat a respektovat práva subjektu údajů definovaní obecným nařízením GDPR.

# Souhlas se zpracováním osobních údajů

1. Udělení souhlasu je jeden z právních důvodů, který lze legálně použít pro sběr a zpracování osobních údajů osobních údajů. Souhlas nesmí být nadužíván, pokud je možné použít jiný právní důvod pro sběr dat, měl by být použit namísto souhlasu. Na základě obecného nařízení DPR může subjekt údajů svůj souhlas odvolat stejně rychle a jednoduše, jako ho udělil a tím tak znemožnit jakýkoliv další zpracování osobních údajů bez jiného právního důvodu.
2. Souhlas musí být vždy specifický, tudíž všeobecný souhlas, který neurčuje přesný účel zpracování osobních údajů, je neplatný.
3. Souhlas musí být informovaný, což znamená, že subjektu údajů musí být poskytnuto dostatečné množství informací o zpracování jeho osobních údajů, které mu umožní pochopit, s čím vlastně souhlas vyslovuje. Povaha zpracování osobních údajů musí být vysvětlena v pochopitelné formě pomocí jasného a srozumitelného jazyka.
4. Souhlas musí mít formu aktivního jednání nebo prohlášení, lze ho tedy poskytnout jakoukoli vhodnou metodou. Například v závislosti na okolnostech může být platný souhlas poskytnut verbálně, písemně, zaškrtnutím políčka na webové stránce, výběrem technických nastavení v aplikaci nebo jakýmkoli jiným prohlášením nebo chováním, které v tomto kontextu jasně dokládá přijetí navrhovaného zpracování osobních údajů tímto subjektem.
5. Mlčení, předem zaškrtnuté políčko, nečinnost nebo pasivní souhlas není považován za platný souhlas.
6. Souhlas musí být možné odvolat.
7. Souhlas musí obsahovat minimálně tyto náležitosti:
8. Jaké osobní údaje subjektu jsou zpracovávány, za jakým účelem (proč) a na základě jakého právního důvodu, popřípadě jak dlouho je budete uchovávat.
9. Budou-li osobní údaje subjektu předávány třetím stranám, pokud ano, tak komu, proč a na jak dlouho.
10. Kde budou osobní údaje subjektu uchovávány a jak budou zabezpečeny.
11. Práva subjektu údajů – taxativně vyjmenovat.
12. Kontakt na Správce osobních údajů, popřípadě na Pověřence.
13. Platí pravidlo, že „mlčení“ neznamená vyjádření souhlasu se zpracováním osobních údajů.

# Informační povinnost vůči subjektům údajů

1. Povinnosti Správce v oblasti poskytování transparentních informací, sdělení a postupů pro výkon práv subjektů údajů jsou detailně upraveny v článcích 12, 13 a 14 obecného nařízení GDPR.
2. Výjimka z povinnosti poskytnout informaci je přípustná pouze v tom případě, že subjekt údajů již těmito informacemi disponuje. Správce však musí být v případě potřeby schopen prokázat, že subjekt údajů byl skutečně informován o všech požadovaných informacích, tj. že došlo ke splnění informační povinnosti dle obecného nařízení GDPR.
3. Do poskytovaných informací subjektu údajů patří:
4. Totožnost a kontaktní údaje Správce.
5. Kontaktní údaje Pověřence pro ochranu osobních údajů.
6. Účely zpracování osobních údajů, pro které jsou osobní údaje určeny, a právní základ pro zpracování osobních údajů.
7. Oprávněné zájmy Správce nebo třetí strany v případě, že je zpracování osobních údajů založeno na čl. 6 odst. 1 písm. f).
8. Případné příjemce nebo kategorie příjemců osobních údajů.
9. Případný úmysl Správce předat osobní údaje do třetí země nebo mezinárodní organizaci.
10. Vedle informací uvedených v předchozím odstavci 3 poskytne Správce subjektu údajů v okamžiku získání osobních údajů tyto další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování osobních údajů:
11. Doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby.
12. Existence práva požadovat od Správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování osobních údajů, a vznést námitku proti zpracování osobních údajů, jakož i práva na přenositelnost údajů.
13. Pokud je zpracování osobních údajů založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování osobních údajů založená na souhlasu uděleném před jeho odvoláním.
14. Existence práva podat stížnost u dozorového úřadu.
15. Skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů.
16. Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4 obecného nařízení GDPR, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování osobních údajů pro subjekt údajů.
17. Pokud Správce hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním osobních údajů informace o tomto jiném účelu a příslušné další informace uvedené v odstavci 2.
18. Odstavce 1, 2 a 3 se nepoužijí, pokud subjekt údajů již uvedené informace má, a do té míry, v níž je má.
19. Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 obecného nařízení GDPR a učinil veškerá sdělení podle článků 15 až 22 a 34 obecného nařízení GDPR o zpracování osobních údajů, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.
20. Pokud se jedná o žádost podle článků 15 až 22 obecného nařízení GDPR, musí být informace o přijatých opatřeních poskytnuta bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit o dva měsíce, o čemž musí být subjekt údajů ze strany Správce informován, včetně důvodů prodloužení.
21. Zásadně platí, že informace podle článků 13 a 14 obecného nařízení GDPR a veškerá sdělení a úkony podle článků 15 až 22 a 34 obecného nařízení GDPR se poskytují a činí bezplatně. Pouze v případě, kdy jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může Správce buď uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost dokládá Správce.

# Ochrana osobních údajů

1. Dle nařízení obecného GDPR je Správce a zpracovatel povinen zavést vhodná technická a organizační opatření, aby zajistil úroveň ochrany odpovídající danému riziku.
2. Při automatizovaném zpracování osobních údajů za pomoci informačního systému obce Maršovice je zaměstnanec povinen vždy dodržovat zásady stanovené směrnicí starosty Provoz IS OÚ.
3. Při papírovém zpracování osobních údajů je zaměstnanec povinen vždy tyto papírové dokumenty uchovávat v trezorech, zamykatelných skříních nebo jinak zabezpečených prostorech, tak aby nemohlo dojít k poručení integrity či důvěrnosti zpracovávaných osobních údajů neoprávněnou osobou. Tato povinnost se vztahuje také na další hmotné nosiče osobních údajů, např. CD, DVD, flashdisk, paměťová karta, přenosný externí disk apod.
4. Správce je povinen v pravidelných intervalech (minimálně 1x za 6 měsíců) provádět kontroly ochrany osobních údajů zpracovávaných OÚ.

# Ohlašování porušení ochrany osobních údajů

1. Správce nebo zpracovatel je povinen řešit porušení ochrany osobních údajů požadovaným způsobem v souladu s články 33 a 34 obecného nařízení GDPR.
2. Za porušení ochrany osobních údajů se považuje porušení ochrany osobních údajů, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Pokud dojde k porušení ochrany osobních údajů, měl by Správce zvážit, zdali nejde o okolnost, kterou je nutné ohlásit dozorovému úřadu, resp. oznámit subjektu údajů. Tyto povinnosti nastanou tehdy, pokud porušení ochrany osobních údajů představuje riziko, resp. vysoké riziko pro práva a svobody fyzických osob.
3. Pokud dojde k porušení ochrany osobních údajů, musí Správce toto porušení bez zbytného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.
4. V případě, že porušení ochrany osobních údajů představuje vysoké riziko pro práva a svobody subjektu údajů, vzniká Správci povinnost zpravit o této události subjekt údajů. Správce tak nemusí činit, pokud použil předběžná opatření, která činí osobní údaje nečitelnými pro všechny neoprávněné osoby (např. šifrování nebo pseudonymizované údaje bez vazby na subjekt údajů) či použil následná opatření, která zajistí, že vysoké riziko se již pravděpodobně neprojeví. Povinnost oznámit porušení ochrany (bezpečnostní incident) subjektu údajů Správci nenastane ani tehdy, pokud by to vyžadovalo nepřiměřené úsilí. V takovém případě však musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení.
5. Pokud nastane porušení ochrany osobních údajů u zpracovatele, hlásí jej bez zbytečného odkladu Správci, pro kterého dotčené osobní údaje zpracovává.
6. Obsah ohlášení dozorovému úřadu:
7. Popis povahy porušení ochrany osobních údajů.
8. Kategorie dotčených subjektů údajů.
9. Počet dotčených subjektů údajů.
10. Množství dotčených záznamů.
11. Identifikace osoby nebo kontaktního místa, které poskytuje bližší informace (jméno, příjmení, adresa, telefon, e-mail apod.).
12. Popis pravděpodobných důsledků porušení ochrany osobních údajů.
13. Popis opatření přijatých s cílem vyřešit porušení bezpečnosti osobních údajů:
14. Uplatněné před porušením ochrany osobních údajů.
15. Uplatněné po porušení ochrany osobních údajů (zejména ke zmírnění možných nepříznivých důsledků).
16. Způsob ohlášení incidentu dozorovému úřadu je definován přímo dozorovým úřadem. K tomuto účelu je k dispozici elektronický formulář a instrukce pro jeho vyplnění na webu dozorového úřadu: [https://www.uoou.cz/oznameni-o-naruseni-bezpecnosti-osobnich-udaju-uradu-pro-ochranu-osobnich-udaju/ds-1573/p1=1573](https://www.uoou.cz/oznameni-o-naruseni-bezpecnosti-osobnich-udaju-uradu-pro-ochranu-osobnich-udaju/ds-1573/p1%3D1573).
17. Způsob oznámení incidentu subjektům údajů je definován přímo dozorovým úřadem. K tomuto účelu jsou instrukce na webu dozorového úřadu: [https://www.uoou.cz/oznameni-o-naruseni-bezpecnosti-osobnich-udaju-subjektum-udaju/ds-1625/p1=1625](https://www.uoou.cz/oznameni-o-naruseni-bezpecnosti-osobnich-udaju-subjektum-udaju/ds-1625/p1%3D1625).
18. Zaměstnanec má povinnost vždy bezodkladně (ihned) a prokazatelně informovat Správce o porušení ochrany osobních údajů.
19. Správce má povinnost vždy bezodkladně (ihned) a prokazatelně informovat Pověřence o porušení ochrany osobních údajů.

# Školení a zvyšování povědomí

1. V souvislosti s obecným nařízením GDPR je povinností Správce a zpracovatele zajištění opakovaného školení zaměstnanců v oblasti ochrany osobních údajů. Jedná se o povinnou součást opatření směřujících k ochraně osobních dat.
2. Školení zaměstnanců o problematice ochrany osobních údajů musí být zdokumentováno a je součástí dokumentace prokazující shodu plnění požadavků na ochranu osobních údajů v OÚ s požadavky obecného nařízení GDPR.
3. Školení zahrnuje všechny kategorie zaměstnanců tj. noví zaměstnanci při jejich nástupu do OÚ v rámci vstupního procesu před tím, než jsou jim zpřístupněny zákaznické a zaměstnanecké osobní údaje; stávající zaměstnance v rámci pravidelného proškolování s ohledem na případné legislativní změny a technologický vývoj.
4. Školení zaměstnanců musí sledovat minimálně následující cíle pro zvyšování povědomí v oblasti ochrany osobních údajů:
5. Zaměstnanci musí chápat obsah problematiky obecného nařízení GDPR – zaměstnanci musí pochopit finanční a reputační rizika plynoucí z obecného nařízení GDPR pro OÚ, včetně rizika možných disciplinárních opatření, nebo dokonce ukončení zaměstnaneckého poměru, pokud jejich přičiněním dojde k narušení ochrany osobních údajů, které poškodí činnost celé či části OÚ.
6. Zaměstnanci musí být schopni rozpoznat porušení ochrany osobních údajů (bezpečnostní incident) – v souladu s povinností hlásit porušení ochrany osobních údajů do 72 hodin od momentu zjištění dozorovému úřadu, včetně distribuce potenciálního oznámení subjektům údajů, které měly své údaje v ohrožení. Tato povinnost je spojena s významným finančním a reputačním rizikem pro celou OÚ. Zaměstnanci musí mít natolik vysoké povědomí o ochraně dat, aby byli schopni rozpoznat, kdy došlo k potenciálnímu porušení, jak a komu takovou událost hlásit.
7. Zaměstnanci se musí poučit z chyb – cílem je seznámení se s poučením z případných předchozích bezpečnostních incidentů, na jejichž základu zřejmě došlo ke změně v některých procesech a postupech OÚ.
8. Školení musí být relevantní – školení musí být specifické pro OÚ s ohledem na interní procesy, postupy a organizační hierarchii. Důraz je kladen na skutečnost, že ochrana osobních údajů úzce souvisí s každodenními pracovními postupy, procesy a návyky v OÚ.
9. Školení musí být minimálně 1x ročně zajistit školení všech zaměstnanců OÚ v oblasti ochrany osobních údajů.
10. Za školení zaměstnanců OÚ v problematice ochrany osobních údajů v souladu s obecným nařízením GDPR je odpovědný Správce.

# Plán pravidelného ověřování shody s obecným nařízením GDPR

1. Za sledování shody tj., zajištění pravidelného ověřování, zda nedochází k případnému nesouladu zpracování osobních údajů s obecným nařízením GDPR je odpovědný Pověřenec pro ochranu osobních údajů a to v souladu s článkem 24 obecného nařízení GDPR, odst. 1.
2. Pro zajištění odpovědnosti Správce dle obecného nařízení GDPR je stanovena touto směrnicí povinnost vypracování plánu pravidelných kontrol shody zpracování osobních údajů (interních auditů) a to minimálně 1x ročně. Za vypracování plánu kontrol odpovídá Pověřenec pro ochranu osobních údajů.
3. Vedení záznamů o interním auditu je prováděno písemně v elektronické podobě.

# Pověřenec pro ochranu osobních údajů

1. Zdroje poskytované pro práci Pověřence – Dle článku 38 odst. 2 obecného nařízení GDPR se OÚ zavazuje, že stanovenému Pověřenci poskytne zdroje nezbytné k plnění jeho úkolů, k přístupu k osobním údajům a operacím zpracování osobních údajů a k udržování jeho odborných znalostí.
2. V závislosti na povaze operací zpracování osobních údajů a na činnostech a velikosti OÚ budou Pověřenci poskytnuty tyto zdroje:
3. Aktivní podpora funkce Pověřence pro ochranu osobních údajů ze strany vedoucích pracovníků.
4. Dostatečný čas na to, aby mohli Pověřenci pro ochranu osobních údajů plnit své povinnosti.
5. Odpovídající podpora z hlediska finančních zdrojů, infrastruktury (prostory, zařízení, vybavení) a případně pracovníků.
6. Oficiální oznámení všem zaměstnancům o jmenování Pověřence pro ochranu osobních údajů.
7. Přístup k dalším službám v rámci OÚ, aby se zajistilo, že Pověřenci pro ochranu osobních údajů mohou od těchto dalších služeb obdržet základní podporu, vstupy nebo informace.
8. Průběžné školení.
9. Pověřenec má ze strany OÚ nárok na záruky pro ochranu osobních údajů umožňující mu jednat nezávislým způsobem, což znamená že:
10. Nedostává pokyny od Správců nebo zpracovatelů týkající se výkonu úkolů Pověřence pro ochranu osobních údajů.
11. Nebude propuštěn nebo sankcionován ze strany Správců nebo zpracovatelů v souvislosti s výkonem úkolů Pověřence pro ochranu osobních údajů.
12. Nedochází ke střetu zájmů s dalšími možnými úkoly a povinnostmi.
13. Úkoly Pověřence jsou stanoveny obecným nařízením GDPR v článku 39 v minimálním rozsahu:
14. Poskytování informací a poradenství Správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování osobních údajů, o jejich povinnostech podle tohoto obecného nařízení GDPR a dalších předpisů EU nebo ČR v oblasti ochrany údajů.
15. Monitorování souladu s tímto obecným nařízením GDPR, dalšími předpisy EU nebo ČR v oblasti ochrany údajů a s koncepcemi Správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování osobních údajů a souvisejících auditů.
16. Poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 obecného nařízení GDPR.
17. Spolupráce s dozorovým úřadem.
18. Působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování osobních údajů, včetně předchozí konzultace podle článku 36 obecného nařízení GDPR, a případně vedení konzultací v jakékoli jiné věci.
19. Pověřenec je povinen brát při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování osobních údajů a současně přihlížet k povaze, rozsahu, kontextu a účelům zpracování osobních údajů.
20. Pověřenec pomáhá v OÚ zavádět základní prvky obecného nařízení GDPR, jako jsou zásady zpracování osobních údajů, práva subjektu údajů, záměrná a standardní ochrana osobních údajů, záznamy o činnostech zpracování osobních údajů, vlastní ochrana osobních údajů a ohlašování a oznamování případů porušení ochrany osobních údajů.
21. Pověřenec může případně vést konzultace s dozorovým úřadem v jakékoli věci a to dle obecného nařízení GDPR v článku 39, odst. 1. písm. e).
22. Pověřenec ochrany osobních údajů je ustanoven starostou.
23. Roli Pověřence je věnováno také „vodítko“ pracovní skupiny WP29 pod evidenčním číslem 243, které obsahuje stanoviska k jeho jmenování, postavení a úkolům.

# Podání, evidence a vyřízení žádosti o výkon práv subjektu údajů

1. Podání žádosti o výkon práv subjektu údajů:
2. Žádosti o výkon práv subjektu údajů jsou podávány vždy prostřednictvím podatelny.
3. Podání žádosti o výkon práv subjektu údajů lze podat písemně, datovou schránkou, e-mailem podepsaný kvalifikovaným elektronickým podpisem nebo jinou technicky proveditelnou formou.
4. Protokol o podání žádosti musí vždy minimálně obsahovat:
5. Kdo žádost podává – např. příjmení a jméno, adresa trvalého pobytu žadatele, datum narození, kontaktní údaje (např. telefon, e-mail, datová schránka, apod.).
6. Předmět žádosti – podrobný popis předmětu žádosti o výkon práv subjektu údajů.
7. Podpis subjektu údajů, který žádost o výkon práv subjektu údajů podává.
8. Každá žádost o výkon práv subjektů je vždy zaevidována pověřeným zaměstnancem obce.
9. Centrální evidence podání žádostí o výkon práv subjektu údajů:
10. Pověřený zaměstnanec vede centrální evidenci všech podaných žádostí o výkon práv subjektu údajů.
11. Subjekt údajů je nutné vždy řádně identifikovat. Pokud se subjekt v žádosti neidentifikuje dostatečně tak, aby jeho identitu bylo možné ověřit, musí si pověřený zaměstnanec od subjektu údajů vyžádat dodatečné údaje k ověření jeho identity
12. Centrální evidence žádostí je vedena samostatně a obsahuje:
13. Číslo jednací přidělené spisovou službou.
14. Datum přijetí žádosti.
15. Datum přijetí do centrální evidence.
16. Příjmení a jméno žadatele, jeho datum narození.
17. Adresa trvalého pobytu žadatele.
18. Kontaktní údaje žadatele (např. telefon, e-mail, datová schránka, apod.).
19. Předmět žádosti o výkon práv subjektů.
20. Datum, kdy byla žádost vyřízena.
21. Vyřízení žádosti o výkon práv subjektu údajů:
22. Pověřený zaměstnanec zajistí vyřízení žádosti o výkon práv subjektu údajů v plném souladu s obecným nařízením GDPR. Vyřízení žádosti musí být provedeno bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit o dva měsíce, o čemž musí být subjekt údajů ze strany pověřeného zaměstnance, včetně důvodů prodloužení. Informaci o prodloužení termínu vyřízení předá pověřený zaměstnanec starostovi OÚ.

# Zdroje informací

1. Doporučené Informační zdroje v oblasti ochrany osobních údajů:

|  |  |  |
| --- | --- | --- |
| Poř. číslo | Název dokumentu | Zdroj dokumentu |
| 1. | Obecné nařízení GDPR Evropského parlamentu a rady (EU) 2016/679 | <http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=EN> |
| 2. | Úřad pro ochranu osobních údajů (dozorový úřad) | <https://www.uoou.cz> |
| 3. | Pokyny pracovní skupiny WP29 | [https://www.uoou.cz/pokyny-pracovni-skupiny-wp29/ds-4728/archiv=0&p1=3938](https://www.uoou.cz/pokyny-pracovni-skupiny-wp29/ds-4728/archiv%3D0%26p1%3D3938) |
| 4. | Osvětový, vzdělávací a poradenský portál k problematice obecného nařízení GDPR | <https://www.gdpr.cz> |

# Kontaktní údaje Správce a Pověřence

1. Na základě obecného nařízení GDPR je Správce povinen sdělit své kontaktní údaje a to včetně Pověřence pro ochranu osobních údajů. Zveřejnit kontaktní údaje Správce a Pověřence pro ochranu osobních údajů na webu OÚ, nebo jiným vhodným způsobem, který bude snadno dostupný pro subjekty údajů. Osobou odpovědnou za sdělení a zveřejnění kontaktních údajů je starosta OÚ.
2. Kontaktní údaje Správce:

|  |  |
| --- | --- |
| Název organizace | Obec Maršovice |
| Sídlo organizace | Maršovice 52 |
| IČ | 00262471 |
| DIČ | CZ 00262471 |
| Statutární zástupce | Jiří Ouhrabka |
| Kontaktní telefon | 483302009 |
| Kontaktní e-mail | ou-marsovice@volny.cz |
| Web | www.obec-marsovice.cz |

1. Kontaktní údaje Pověřence:

|  |  |
| --- | --- |
| Jméno | Zbyněk |
| Příjmení | Vavřina |
| Kontaktní telefon | +420 602 423 675 |
| Kontaktní e-mail | vavrina.gdpr@gmail.com |
| Lokalizace (adresa, kancelář) | nám. Dr. E. Beneše 1, Liberec, kancelář č. 2 |

# Závěrečná ustanovení

1. V případě vzniku škod se postupuje v souladu s interními předpisy OÚ.
2. Směrnice nabývá účinnosti 25. května 2018.

# Seznam změn a revizí řízeného dokumentu

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Verze** | **Datum vydání****/revize/** | **Č. usnesení rady města** | **Účinnost**  | **Popis změny / revize** | **Zpracovatel** |
| 1. | 20. 5. 2018 | --- | 25. 5. 2018 | Implementace GDPR | Ing. Zbyněk Vavřina |
|  |  |  |  |  |  |