

DGPR Předpis č. .../2018
upravující nakládání s osobními údaji

Čl. I.

Předmět úpravy

Stanovení pravidel zpracování osobních údajů ve smyslu "Nařízení Evropského Parlamentu a Rady 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES" v podmínkách Obce Rataje (dále jen „GDPR“).

Čl. II.

Základní pojmy

Pro účely tohoto předpisu se rozumí

- a) osobním údajem –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;,
- b) zvláštní kategorie osobních údajů (citlivé údaje) – zejména etnický původ, náboženství, zdraví, tresty,
- c) pseudonymizovaným údajem – zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu bez použití dodatečných informací, kterými je např. přidělené číslo konkrétnímu subjektu,
- d) anonymizovaným údajem – informace, které nesouvisejí s identifikovanou nebo identifikovatelnou osobou nebo jsou poskytnuty anonymně a nelze pomocí těchto informací subjekt identifikovat,
- e) zpracováním – 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;
- f) Správce osobních údajů – Obec Rataje zastoupená starostou obce, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; účely a prostředky tohoto zpracování jsou určeny právem ČR dle zákona 128/2000 dále jen „Správce“),
- g) Zpracovatel - Obec Rataje zastoupená hospodářkou obce, která zpracovává osobní údaje pro Správce dále jen „Zpracovatel“
- h) 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.

Čl. III.

Zásady zpracování osobních údajů

1. Zákonnosti – nejdůležitější zásada, která vyjadřuje, že Správce může zpracovávat osobní údaje k určitému účelu a pouze tehdy, má-li k takovému zpracování alespoň jeden **právní důvod**:

- a) se zpracováním osobních údajů byl dán souhlas Subjektu,
- b) zpracování osobních údajů je nezbytné pro plnění smlouvy nebo uzavření smlouvy, u níž je Subjekt jednou ze smluvních stran,
- c) zpracování osobních údajů je nezbytné pro plnění právní povinnosti dle jiného právního předpisu,

2. zpracování je nezbytné pro účely legálních zájmů Správce za podmínky, že neporušují práva a svobody Subjektu. Korektnosti – Správce nesmí vůči Subjektu zastírat účel, pro který jsou údaje zpracovávány a současně by měl Subjektu poskytnout informace o tom, jakým způsobem a v jakém rozsahu jsou osobní údaje zpracovávány a komu jsou předávány.

3. Transparentnosti – vyžaduje, aby informace, které Subjekt od Správce dostává či na něž má právo, byly snadno přístupné a srozumitelné, za použití jasných jazykových prostředků.

4. Omezení účelu – znamená, že osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené legitimní účely a nesmějí být zpracovávány způsobem, který je s těmito účely neslučitelný.

5. Minimalizace údajů – úzce souvisí se zásadou omezení účelu a představuje povinnost zpracovávat osobní údaje pouze přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu ke stanovenému účelu. Tato zásada tak brání Správci, aby v souvislosti se stanoveným legitimním účelem požadoval po Subjektu více údajů, než je nezbytně nutné.

6. Přesnosti – osobní údaje musí být zpracovávány v přesné podobě a v případě potřeby aktualizované, protože pouze takové zpracování má význam.

7. Omezení uložení – osobní údaje by měly být uloženy pouze po dobu, která je nezbytná pro účely, pro kterou jsou zpracovávány tzn., že pomine-li účel zpracování má Správce povinnost osobní údaje zlikvidovat.

8. Integrity a důvěrnosti – osobní údaje by měly být dostatečně zabezpečeny, a to prostřednictvím vhodných technických nebo organizačních opatření chránících je před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

Čl. IV.

Právní důvody zpracování osobních údajů

1. Právní důvody zpracování osobních údajů znamenají oprávnění Správce osobní údaje zpracovávat.

2. Právní důvody tak jsou nezbytným předpokladem, aby Správce mohl osobní údaje legálně zpracovávat.

3. **Pokud Správce nedisponuje řádným právním důvodem ke zpracování osobních údajů, je dále nerozhodné, zdali plní ostatní povinnosti, protože osobní údaje by zpracovával nezákonně a musel by osobní údaje zlikvidovat.**

Čl. V. Účel zpracování osobní údajů

1. Účel zpracování osobních údajů musí být vždy legitimní a nesmí být protiprávní. Úzce souvisí se zásadami zpracování a s právními důvody.

2. Správce zpracovává osobní údaje Subjektu pouze za účelem zpracování, které je nezbytné pro splnění právní povinnosti dané zákonem 128/200Sb, která se na správce vztahuje a zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce. Přehled zpracování osobních údajů v zodpovědnostech Zpracovatelů v samostatné příloze

Čl. VI. Zásady zpracování osobních údajů

1. Zpracování osobních údajů musí mít vždy určitý účel a právní důvody musí tento účel pokrývat.

2. Zpracování osobních údajů začíná okamžikem jejich shromažďování.

3. Zpracování osobních údajů spočívá ve

- a) shromažďování,
- b) ukládání,
- c) zaznamenání,
- d) uspořádání,
- e) uložení v archivu,
- f) přizpůsobení nebo pozměnění,
- g) vyhledání,
- h) nahlédnutí,
- i) použití,
- j) šíření nebo jakékoli jiné zpřístupnění,
- k) seřazení či zkombinování,
- l) omezení,
- m) výmaz nebo zničení.

4. Souhlas se zpracováním osobních údajů

- a) je jednoznačným svolením Subjektu ke zpracování osobních údajů,
- b) může být dán písemně, elektronicky, nebo zjevným potvrzením,
- c) obsahuje účel, ke kterému budou data zpracovávána a pokud je účelů více, uděluje se souhlas pro všechny účely,

d) formulace je jednoduchá a jasně odlišitelná od ostatního textu,

e) při zpracování citlivých údajů musí být výslovný souhlas Subjektu s jejich zpracováním.

5. K získání platného souhlasu je potřeba poskytnout Subjektu alespoň tyto informace:

- a) totožnost Správce,
- b) účel každé z operací zpracování, pro které je žádáno o souhlas,
- c) jaké osobní údaje (druhy údajů) budou shromažďovány a používány,
- d) existence práva odvolat souhlas,
- e) jak dlouho budou osobní údaje uchovávány,
- f) komu budou případně sdělovány a v jakém rozsahu,
- g) informace o použití dat v případě automatizovaného zpracování.

6. Informace uvedené v odstavci 5 tohoto předpisu mohou být Subjektu předloženy různými způsoby, jako třeba písemným nebo ústním oznámením např. na zasedání zastupitelstva obce, doručením e-mailem nebo vložení do poštovní schránky apod.

7. Výslovnou povinnost Správce je doložit, že subjekt údajů udělil souhlas.

8. Povinnost prokázat souhlas platí po celou dobu trvání dané zpracovatelské činnosti. Po jejím skončení by důkaz o souhlasu neměl být uchováván déle, než je opravdu nezbytné pro soulad se zákonnými povinnostmi nebo kvůli zjištění, výkonu nebo obhajobě právních nároků.

9. Evidenci získaných souhlasů eviduje Správce v listinné případně elektronické podobě a po dobu jejich uchování jsou uloženy v archivu Správce.

10. Po dosažení účelu zpracování osobních údajů (například naplnění smlouvy) musejí být shromážděné údaje vymazány, anonymizovány nebo předány subjektu, který je ze zákona oprávněn tyto údaje od Správce obdržet.

Čl. VII.

Povinnosti Správce

1. Správce odpovídá

a) za dodržování zásad zpracování dle čl. VI. tohoto předpisu,

b) za dodržování povinností upravených nařízením,

c) za zabezpečení osobních údajů.

2. Před započítím shromažďování osobních údajů Správce poskytne Subjektu informace, jejichž rozsah závisí na tom, zda jsou osobní údaje shromažďovány přímo od Subjektu nebo z jiných zdrojů.

3. O započítí shromažďování osobních údajů a o zdroji jejich získání (pokud nebyly osobní údaje získány přímo od Subjektu) je Subjekt informován písemnou formou.

4. Pokud jsou osobní údaje získávány od Subjektu, poskytne Správce následující informace, kromě případu, kdy je již Subjekt má:

a) totožnost Správce a jeho kontaktní údaje,

b) účely zpracování, pro které jsou osobní údaje určeny a právní základ pro jejich zpracování,

c) oprávněné zájmy Správce nebo třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody Subjektu,

d) případné příjemce nebo kategorie příjemců osobních údajů,

e) doplňující informace jako jsou:

– doba, po kterou budou osobní údaje uloženy,

– existence práva na přístup k osobním údajům, které se Subjektu týkají, a právo na jejich opravu nebo výmaz,

– existence práva kdykoli odvolat souhlas,

– existence práva podat stížnost u dozorového úřadu,

– skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutno uvést do smlouvy a zda má Subjekt povinnost poskytnout osobní údaje.

5. V případě shromažďování osobních údajů z jiných zdrojů než od Subjektu, poskytne Správce v době, kdy provádí zaznamenání osobních údajů nebo pokud se předpokládá sdělení údajů třetí straně, nejpozději v době jejich prvního předání, Subjektu následující informace, kromě případů, kdy je již Subjekt má:

a) totožnost Správce a jeho kontaktní údaje,

f) účely zpracování, pro které jsou osobní údaje určeny a právní základ pro jejich zpracování,

b) kategorie dotčených osobních údajů,

c) případné příjemce nebo kategorie příjemců osobních údajů,

d) doplňující informace jako jsou:

- doba, po kterou budou osobní údaje uloženy,
- existence práva na přístup k osobním údajům, které se Subjektu týkají, a právo na jejich opravu nebo výmaz,
- existence práva kdykoli odvolat souhlas,
- příjemci nebo kategorie příjemců údajů,
- existence práva podat stížnost u dozorového úřadu,
- zdroj, ze kterého osobní údaje pocházejí, případně zda osobní údaje pocházejí z veřejně dostupných zdrojů.

6. Správce poskytne informace uvedené v odstavci 4 a 5

- a) v přiměřené lhůtě, nejpozději do 30 dnů od začátku jejich zpracování,
- b) nejpozději v momentu, kdy poprvé dojde ke komunikaci se Subjektem, mají-li být osobní údaje použity pro účely této komunikace,
- c) nejpozději při prvním zpřístupnění osobních údajů třetí osobě nebo jinému příjemci.

7. Právu Subjektu na přístup k osobním údajům musí být vyhověno ve lhůtě třiceti dnů ode dne podání žádosti Subjektem. Na žádost Subjektu odpovídá Správce písemnou formou. Pokud není právo na přístup k osobním údajům uplatňováno častěji než jedenkrát za šest měsíců, je bezplatné.

8. Povinností Správce je zajistit bezpečnost osobních údajů, tzn. zavést vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, ztrátě, úpravám, neoprávněnému sdělování nebo přístupu, zejména pokud zpracování zahrnuje předávání údajů po síti, jakož i proti jakékoli jiné formě nezákonného zpracování.

9. Povinností Správce je ohlásit případy porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a oznámit případy porušení zabezpečení osobních údajů Subjektu, kterého se týkají.

ČI. VIII.

Zabezpečení osobních údajů

1. Za porušení zabezpečení osobních údajů se považuje porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

2. Povinnosti Správce při zabezpečení osobních údajů

- a) provádět posouzení dopadu na ochranu osobních údajů,
- b) ohlašovat případy narušení bezpečnosti,
- c) analyzovat potenciální hrozby a k tomu přijmout organizačně technická opatření,
- d) jakmile pomine účel zpracování, osobní údaje vedené v písemné a elektronické podobě budou Správce zničeny nebo budou uchovávány pouze pro účely archivnictví,
- e) provádět kontrolu zabezpečení osobních údajů.

3. Správce konstatuje čtyři potenciální hrozby, které zpracování osobních údajů mohou zasáhnout, a k tomu přijímá následující organizačně technická opatření:

I. Zničení nebo zneužití technických prostředků

- a) omezení přístupu k technickým prostředkům (zámky, mříže apod.),
- b) využití pohybových čidel,
- c) a jiné,

II. Přístup neoprávněných osob

- a) řízení přístupu k datům (hesla),
- b) plná kontrola nad daty,

- c) oddělení identifikačních a dalších dat Subjektů, pseudonymizace Subjektů,
- d) programy ochraňující proti neoprávněnému průniku, programy ochraňující proti škodlivým kódům, šifrování dat, využití bezpečnějších komunikačních protokolů apod.,
- e) zálohování dat,
- f) při sdělování osobních dat Subjektu používat e-mail výjimečně; data předávat osobně na nosiči dat; e-mail má riziko úniku dat,
- g) a jiné,

III. Zneužití záznamů oprávněnými osobami

- a) identifikace přistupujících osob do systému (hesla a role),
- b) evidence činnosti při práci s daty (zápis dat, změna dat, kopírování dat, mazání dat),
- c) omezení kopírování dat na přenosná paměťová média, případně omezení zasílání souborů s daty,
- d) oddělení identifikačních a dalších osobních údajů Subjektů,
- e) školení členů výboru a kontrolní komise,
- f) a jiné,

IV. Živelní událost

- a) zabezpečovací zařízení oznamující ohrožení, umístění mimo prostor ohrožených vodou,
- b) zálohování dat,
- c) záložní infrastruktura (hw i napájecí),
- d) a jiné.

4. Ověřování funkčnosti organizačně technických opatření bude zajištěno prováděnou kontrolou oprávněnými osobami Správce, kteří budou ke zjištěnému stavu navrhnout Správci konkrétní opatření k zjištěnému stavu, zejména:

- a) kategorie osobních údajů, které byly porušením zabezpečení dotčeny,
- b) charakter porušení zabezpečení.
- c) počet dotčených Subjektů,
- d) zdali došlo k porušení zabezpečení úmyslně či nedbalostně, přičemž úmyslný čin výrazně zvyšuje riziko takového činu, jelikož osobní údaje byly terčem útoku.

5. Veškeré osobní údaje budou po celou dobu zpracování uchovávány v písemné podobě i v informačním systému Správce a mohou být automatizovaně zpracovávány.

6. K osobním údajům budou mít přístup pouze k tomu oprávněné osoby Správce (členové výboru a v omezeném rozsahu členové kontrolní komise), které budou mít Správce stanoveny podmínky a rozsah zpracování osobních údajů; při automatizovaném zpracování osobních údajů Správce zajistí:

- a) aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,
- b) aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,
- c) pořizování elektronických záznamů, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje a další údaje zaznamenány nebo jinak zpracovány,
- d) zabránění k neoprávněnému přístupu k datovým nosičům,

7. Všechny oprávněné osoby, které zpracovávají osobní údaje nebo kteří se dostanou do styku s osobními údaji Subjektů, jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů a mohou zpracovávat osobní údaje pouze za podmínek a v rozsahu Správce stanoveném; povinnost mlčenlivosti trvá i po skončení funkce ve výboru nebo kontrolní komisi nebo příslušných prací; tím není dotčena povinnost zachovávat mlčenlivost podle jiných právních

předpisů; povinnost zachovávat mlčenlivost se nevztahuje na informační povinnost podle jiných právních předpisů.

8. Pokud dojde k porušení zabezpečení osobních údajů, musí Správce toto porušení bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit dozorovému úřadu (Úřadu pro ochranu osobních údajů), pokud tak není učiněno, musí být uvedeny důvody tohoto zpoždění.

9. Porušení zabezpečení osobních údajů oznámí Správce bez zbytečného odkladu Subjektu, kterého se porušení dotýká, kde popíše povahu porušení zabezpečení, přijatá opatření, pravděpodobné důsledky.

Čl. IX.

Práva Subjektu osobních údajů

1. Právo na přístup k osobním údajům – právo získat potvrzení o zpracovávání osobních údajů od Správce, právo tyto data získat a s nimi následující informace

- a) účely zpracování,
- b) kategorie dotčených osobních údajů,
- c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
- d) plánovaná doba, po kterou budou osobní údaje uloženy,
- e) existence práva požadovat od Správce opravu nebo výmaz osobních údajů, právo vznést námitku,
- f) právo podat stížnost u dozorového úřadu,
- g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
- h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.

2. Právo opravy, resp. doplnění osobních údajů – podnět k opravě či doplnění má právo dát sám Subjekt.

3. Právo na výmaz – povinnost Správce zlikvidovat osobní údaje a předat potvrzení o vymazání Subjektu osobních údajů, pokud je splněna alespoň jedna z následujících podmínek

- a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- b) Subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,
- c) Subjekt údajů vznesl námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
- d) osobní údaje byly zpracovány protiprávně,
- e) osobní údaje musí být vymazány ke splnění právní povinnosti,
- f) souhlas byl udělen na příslušnou dobu.

4. Právo být zapomenut – jde o rozšířené právo na výmaz, Správce provede přiměřené kroky, včetně technických opatření k vymazání veškerých odkazů na osobní údaje Subjektu a jejich kopií.

5. Právo na omezení zpracování - Subjekt údajů má právo na to, aby správce omezil zpracování, v kterémkoli z těchto případů:

- a. subjekt údajů popírá přesnost osobních údajů
- b. zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
- c. správce již osobní údaje nepotřebuje pro účely zpracování
- d. subjekt údajů vznesl námitku proti zpracování

6. Právo na přenositelnost údajů – zcela nové právo Subjektu, 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.

7. Právo vznést námitku – Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami Subjektu, nebo pro určení, výkon nebo obhajobu právních nároků.


8. Právo odvolání souhlasu – Subjekt má právo svůj souhlas kdykoli odvolat. Odvoláním není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním.

Čl. X

Závěrečná ustanovení

Tento předpis nabývá platnosti a účinnosti dnem schválení Představenstvem obce.

V Ratajích dne 20. 5. 2014


Antonín Říkovský
Starosta obce

OBEC RATAJE
okr. Kroměříž