

Metodický pokyn č. 1/2018

ČESKÝ ZAHRÁDKÁŘSKÝ SVAZ, z.s.

vydává

Metodický pokyn č. 1/2018

kteřý stanoví pravidla k nakládání a 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" (GDPR) v podmínkách Českého zahrádkářského svazu, z.s.

Čl. I.

Základní ustanovení

1. Podle citovaného Nařízení Evropského parlamentu a platné právní úpravy v České republice, se nově upravuje systém zpracování a nakládání s osobními údaji, který jsou povinny dodržovat všechny subjekty, které osobní údaje fyzických osob spravují a nakládají s nimi v působnosti Českého zahrádkářského svazu, z.s. (dále jen „svaz“).

2. Nařízení je přímo závaznou evropskou komplexní právní úpravou v oblasti práv a povinností při zpracování osobních údajů směřující ke zvýšení ochrany osobních údajů občanů ode dne jeho účinnosti, tj. dne 25. května 2018. Počítá se s tím, že ke dni účinnosti nařízení bude zrušen zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, který nahradí nový zákon o zpracování osobních údajů, jehož návrh však dosud neprojednala vláda ani Parlament ČR.

3. Tento metodický pokyn (dále jen „pokyn“) doporučuje vhodná organizační a technická opatření pro postup orgánů svazu, organizačních jednotek a dalších svazových institucí (dále jen orgány svazu“) k ochraně osobních údajů jejich členů, zaměstnanců a dalších osob, které jakýmkoliv způsobem spolupracují nebo participují na rozvoji zahrádkářské činnosti (dále jen „subjekt údajů“).

4. Tento pokyn je určen všem osobám, které v rámci své činnosti s osobními údaji nakládají, zejména pro

- funkcionáře orgánů svazu,
- personalistu,

- účetní,
- správce sítí a další IT zaměstnance.

5. Správcem osobních údajů ve svazu jsou orgány svazu (dále jen „správce“), které určují prostředky a účel zpracování osobních údajů, zpracovávají je a odpovídají za dodržování zásad zpracování a pohyb osobních údajů v souladu s platnou právní úpravou.

6. Osobními údaji se rozumí každá informace, která umožňuje identifikovat osobu, již se údaje týkají, zejména jméno, pohlaví, věk, datum narození, rodné číslo, adresa, osobní stav, a dále organizační údaje jako telefonní číslo, e-mail, lokalizační údaje, a zvláště citlivé údaje jako etnický původ, náboženství, zdraví, tresty.

7. Zpracováním osobních údajů se rozumí jakákoliv činnost správce údajů, kterou systematicky za určitým účelem s osobními údaji provádí.

Čl. II.

K obsahu nařízení

1. Nařízení je založeno na stejných základních principech upravujících postup při zpracování osobních údajů jako zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, který nahrazuje. Nová právní úprava je kontinuální v přístupu k ochraně osobních údajů s platnou právní úpravou. Dotčeným subjektům stanoví pouze několik málo nových povinností. Pokud orgány svazu dosud zpracovávají osobní údaje v souladu se zákonem o ochraně osobních údajů, nebude muset své dosavadní postupy příliš měnit.

2. Osobní údaje jsou podle nařízení veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Podrobnější definice osobních údajů i dalších pojmů používaných v nařízení se nacházejí v čl. 4 nařízení.

3. 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.

4. Nadále platí, že osobní údaje musí být shromažďovány a zpracovávány korektně a transparentně, v souladu s právními předpisy a uzavřenými smlouvami, pouze pro legitimní účely a v souladu s účely,

k nimž byly shromážděny. Shromažďovat osobní údaje je možné pouze v rozsahu nezbytném pro naplnění stanoveného účelu. Uchovávat osobní údaje lze pouze po dobu, která je nezbytně nutná pro naplnění stanoveného účelu. Těchto cílů lze dosáhnout zavedením vhodných technických, organizačních a bezpečnostních opatření při práci s osobními údaji a při jejich uchovávání.

5. Ke zpracování osobních údajů na základě zákona k plnění povinností svazu jako zaměstnavatele se nevyžaduje souhlas zaměstnance. Souhlas není třeba ani pro zpracování osobních údajů dětí a manžela zaměstnance pro účely prohlášení poplatníka daně z příjmů (čl. 6 odst. 1 písm. c nařízení).

6. Ke splnění povinností vyplývajících pro orgány svazu z nařízení postačí stručný interní předpis o zpracovávání osobních údajů, dobře vedený archiv a kvalitní zabezpečení počítačové sítě s jasně vymezenými a zabezpečenými přístupovými oprávněními pro úzce vymezený okruh osob.

Čl. III.

Hlavní změny v ochraně osobních údajů vyplývající z nařízení pro orgány svazu

1. Vedení záznamů o činnostech zpracování – oznamovací povinnost vůči Úřadu pro ochranu osobních údajů při zahájení zpracovávání osobních údajů je nahrazena povinností vést záznamy o zpracovávání osobních údajů. Orgány svazu jsou povinny v záznamech uvádět především jak, kdo a za jakým účelem zpracovává jakou kategorii údajů a subjektů a komu budou tyto údaje zpřístupněny. Záznamy by měly být vedeny tak, aby se v nich dalo zpětně orientovat, a Úřad pro ochranu osobních údajů si je může vyžádat k nahlédnutí (čl. 30 nařízení).

2. Ohlašování porušování zabezpečení – porušením zabezpečení osobních údajů je porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů (čl. 4 odst. 12 nařízení). Porušení zabezpečení osobních údajů by měly orgány svazu předcházet vhodnými technickými a organizačními zabezpečeními osobních údajů. Dojde-li k porušení zabezpečení osobních údajů, mají orgány svazu povinnost bez zbytečného odkladu a pokud možno nejpozději do 72 hodin od okamžiku, kdy se o něm dozvěděly, ohlásit tuto skutečnost Úřadu pro ochranu osobních údajů a též bez zbytečného odkladu informovat všechny dotčené subjekty údajů. Povinnost ohlásit tuto skutečnost Úřadu pro ochranu osobních údajů orgán svazu nemá, pokud je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Povinnost informovat dotčené subjekty údajů orgán svazu nemá, pokud je nepravděpodobné, že by toto porušení mělo za následek vysoké riziko pro práva a svobody fyzických osob (čl. 33 a 34 nařízení). Orgánům svazu se doporučuje, aby dokumentovaly též odůvodnění rozhodnutí přijatých v reakci na porušení zabezpečení osobních údajů.

3. Povinnosti orgánů svazu jako správce – orgány svazu zavádí vhodná technická, organizační a bezpečnostní opatření, a to nejen v průběhu samotného zpracování, ale již v době navrhování jeho řešení, aby osobní údaje byly chráněny před neoprávněným zpracováním.

Čl. IV.

Jak postupovat při implementaci nařízení

Do nabytí účinnosti nařízení je třeba provést:

- a. Zpracovat přehled o současném zpracovávání osobních údajů – orgánům svazu se doporučuje zpracovat přehled dosavadních postupů při shromažďování a nakládání s osobními údaji včetně kategorizace těchto osobních údajů. Dále ověřit a uvést, které osoby mají k údajům přístup, kde a v jaké formě se osobní údaje ukládají a jak jsou chráněny před zneužitím, zda je prokazatelný souhlas se zpracováním osobních údajů, k jakému účelu se zpracovávají, po jakou dobu, kde a jak se archivují, pravidla pro likvidaci osobních údajů poté, co pomínul legální účel jejich shromažďování a zpracování, popřípadě, kdy byl odvolán souhlas dotčených osob.
- b. Kontrolu zákonnosti a nezbytnosti zpracovávání – zpracovávat osobní údaje lze jen na základě zákona nebo souhlasu subjektu údajů a v rozsahu a době nezbytných pro naplnění stanoveného účelu. V případě, že zpracování údajů probíhá v rozporu s právními předpisy nebo není potřebné pro činnost orgánu svazu, má orgán svazu povinnost od tohoto zpracování upustit.
- c. Kontrolu smluv – Pokud orgán svazu uzavřel smlouvy, jejichž předmět zahrnuje zpracování osobních údajů, je třeba zkontrolovat soulad těchto smluv se zákonem a nařízením, především dostatečné možnosti omezení či zákazu předávat nabyté informace dál třetím osobám v rozporu se zájmy orgánu svazu či subjektů osobních údajů. Text smluv by měl odpovídat záměru předcházet jakémukoliv nezákonnému zpracování osobních údajů. Průběh plnění smlouvy v souladu s právními předpisy je odpovědností obou smluvních stran. V případě nedostatků je třeba smlouvy změnit, v případě nesouhlasu druhé smluvní strany s takovou změnou smlouvu vypovědět pro rozpor s právními předpisy či ukončit dohodou.
- d. Nastavení vnitřních mechanismů – orgánům svazu se doporučuje přijmout vnitřní předpis, který nastaví pravidla pro nakládání s jednotlivými druhy osobních údajů včetně postupu pro jejich likvidaci, způsobu uchovávání a výčtu osob pověřených shromažďováním a zpracováváním osobních údajů. Výsledkem by mělo být vytvoření funkčního systému ochrany osobních údajů s jasným vymezením oprávnění pro přístup k nim a pro přehlednou archivaci dříve proběhlých úkonů, která umožní orgánům svazu doložit, že zpracování probíhá v souladu s právními předpisy.

Čl. V.

Zásady zpracování osobních údajů

1. Osobní údaje mohou být zpracovávány pouze při dodržení zásad pro jejich zpracování, především zásady zákonnosti, která vyjadřuje, že Správce může zpracovávat osobní údaje k určitému účelu a pouze tehdy, má-li k takovému zpracování alespoň jeden právní důvod, tj. zpracovává-li je na základě zákonného oprávnění, plnění zákonných povinností či je-li to nutné k plnění smlouvy s fyzickými osobami.
2. Zákonným oprávněním a zákonnými povinnostmi se vedle oprávnění a povinností vyplývajících z jiných právních předpisů rozumí i oprávnění a povinnosti orgánů svazu vyplývající ze stanov svazu a ostatních vnitrosvazových předpisů republikového i lokálního charakteru (jednací a volební řád, svazové instrukce, organizační a osadní řády apod.)
3. Správce je povinen subjektu, jehož osobní údaje zpracovává, poskytnout informace k jakému účelu, jakým způsobem a v jakém rozsahu jsou údaje zpracovávány a komu budou poskytovány.
4. Účel zpracování osobních údajů musí být vždy legitimní a nesmí být protiprávní. Úzce souvisí se zásadami zpracování a s právními důvody.
5. Správce je oprávněn zpracovávat osobní údaje pouze tehdy, má-li k tomu právní důvody nebo ke zpracování osobních údajů dal subjekt, jehož osobní údaje se zpracovávají, ke zpracování výslovný souhlas. Tento souhlas může příslušný subjekt kdykoliv odvolat a za takové situace je zpracování osobních údajů vyloučeno a musí být ukončeno. Poskytnutí informací správce podle odstavce 2 a souhlas subjektu ke zpracování osobních údajů musí být prokazatelný při archivaci po celou dobu zpracování.
6. Zpracované osobní údaje musí být uloženy u oprávněných osob stanoveným způsobem tak, aby nemohlo dojít k jejich úniku a seznámení se neoprávněnými osobami, příp. k jejich zneužití či užití k jinému než sjednanému účelu. Zpracované osobní údaje mohou být uloženy jen na nezbytně nutnou dobu, pomine-li účel jejich zpracování či uložení, je správce povinen shromážděné údaje vymazat nebo anonymizovat.

Čl. VI.

Povinnosti správce osobních údajů

1. Správce odpovídá

- a. za dodržování zásad podle čl. V. tohoto pokynu,
- b. za dodržování povinností upravených nařízením,
- c. za zabezpečení osobních údajů.

2. Před započítím zpracování osobních údajů je správce povinen poskytnout subjektu, jehož osobní údaje mají být zpracovány informace o účelu a způsobu zpracování podle čl. V. tohoto pokynu.

3. Osobní údaje je správce povinen zpracovávat výlučně k účelu, se kterým byl subjekt, jehož se údaje týkají, seznámen a v rozsahu, který je pro dosažení účelu nezbytný.

4. Povinností správce je zajistit bezpečnost zpracovaných osobních údajů, tj. zavést vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, ztrátě, úpravám a přístupu neoprávněných osob k osobním údajům.

Čl. VII.

Opatření k zajištění ochrany osobních údajů

1. Kontrolu plnění tohoto metodického pokynu a všech opatření k ochraně osobních údajů provádějí správci a všechny kontrolní orgány svazu v rámci své místní a věcné působnosti.

2. Všechny zjištěné nedostatky a porušení zásad ochrany osobních údajů oznamují kontrolní orgány a správci dotčeným subjektům, příslušným nejvyšším orgánům svazu a organizačních jednotek, které odpovídají za oznámení příslušným dozorovým orgánům Úřadu pro ochranu osobních údajů a za odstranění zjištěných nedostatků, event. za plnění opatření nařízených dozorovými orgány.

3. Za seznámení s tímto pokynem odpovídají v rámci své místní a věcné působnosti funkcionáři orgánů svazu všech stupňů.

4. V příloze k tomuto metodickému pokynu je vzor předpisu upravující nakládání s osobními údaji pro základní organizaci, jež mohou využít s příslušnými úpravami všechny orgány svazu.

Schváleno Republikovou radou ČZS v Praze dne 24. 3. 2018