SMĚRNICE Č. 5/2018, O OCHRANĚ OSOBNÍCH ÚDAJŮ

ORGANIZACE

Obec Radostín nad Oslavou 223, 594 44 Radostín nad Oslavou, IČ: 00295248

Čl 1 ÚČEL SMĚRNICE

1.1 Účelem této směrnice je stanovit základní pravidla zpracování osobních údajů v obecním úřadu.

1.2 Tato směrnice je jedním z organizačních opatření ochrany osobních údajů ve smyslu článku 32 GDPR.

1.3 Tato směrnice dále upravuje procesy realizace práva subjektu údajů na přístup k osobním údajům ve smyslu článku 15 GDPR a ohlašování případů porušení zabezpečení osobních údajů ve smyslu článku 33 a 34 GDPR.

1.4 Účelem této Směrnice je zároveň stanovit základní pravidla zpracování osobních údajů k ochraně osobních údajů a jejich zabezpečení a řešení porušení zabezpečení.

Čl 1 DEFINICE VE SMĚRNICI UŽITÉ

1.1 Za DPO je považován pověřenec pro ochranu osobních údajů (Data Protection Officer) ve smyslu čl. 37 GDPR.

1.2 Za Dozorový úřad je považován Úřad pro ochranu osobních údajů.

1.3 Za GDPR se považuje Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

1.4 Za Osobní údaj se považuje jakákoliv informace o identifikované nebo identifikovatelné fyzické osobě; 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.

1.5 Za Pracovníka se považuje každá osoba, včetně právnických osob, která pro Organizaci vykonává jakoukoliv činnost, zejména zaměstnanec, externí spolupracovník, dodavatel apod.

1.6 Za Subjekt údajů se považuje každá fyzická osoba, včetně osob samostatně výdělečně činných.

1.7 Za Zpracování osobních údajů se považuje 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.

1.8 Za Příslušnou osobu se považuje Zaměstnanec Organizace uvedený v příloze č. 1 této Směrnice, odpovědný za příslušnou agendu v Organizaci.

1.9 Další pojmy touto Směrnicí neurčené mají význam ve smyslu GDPR.

Čl 2 ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

2.1 Organizace určuje účel a prostředky zpracování Osobních údajů pro každou evidenci v Organizaci, včetně doby zpracování, nebo kritéria na základě kterých bude tato doba určena, pokud tyto nevyplývají z právního předpisu.

2.2 Osobní údaje jsou zpracovávány po dobu určenou v bodu 2.1. v souladu s právními předpisy nebo po dobu trvání licence ke zpracovávání osobních údajů správcem.

2.3 Evidence o Zpracování osobních údajů je vedena v záznamech o činnostech zpracování vedených dle čl. 30 GDPR.

2.4 Pracovníci jsou povinni zpracovávat Osobní údaje ve vztahu k subjektu údajů korektně a zákonně.

2.5 Každý pracovník smí zpracovávat osobní údaje pouze za Organizaci určeným účelem, a to pouze Organizací určenými prostředky.

2.6 Pracovníci jsou oprávněni zpracovávat Osobní údaje pouze v souladu s pokyny Organizace. Pracovníci smí zpracovávat pouze Osobní údaje nezbytné pro plnění svých povinností vůči Organizaci.

2.7 Organizace za účelem Zpracování dle bodu 2.6. zřizuje Pracovníkům přístup pouze k nezbytně nutným evidencím osobních údajů.

2.8 Má-li Pracovník podezření, nebo dozví-li se, že jsou Osobní údaje jakéhokoliv subjektu údajů nepřesné, neúplné či zastaralé, ohlásí to Příslušné osobě.

2.9 Má-li pracovník podezření, nebo dozví-li se, že jsou Osobní údaje zpracovávány déle, než je nezbytné pro účely, pro které jsou zpracovávány, ohlásí to Příslušné osobě.

2.10 Tato směrnice se vztahuje na každého Pracovníka Společnosti, když zpracovává osobní údaje nebo plní jinou činnost, která je upravena v GDPR.

2.11 Každý Pracovník, jehož se tato směrnice dotýká bude proškolen na ochranu osobních údajů dle této směrnice a proškolení své osoby stvrdí podpisem.

2.12 Ukládá-li tato směrnice povinnost osobě oznámit jakoukoliv informaci druhé osobě, provede první osoba oznámení v písemné podobě. Za tuto písemnou podobu se považuje listinný dopis nebo e-mail.

Čl 3 ZÁSADY BEZPEČNOSTI

3.1 Pracovník, případně další spolupracující osoby jsou povinny nakládat s Osobními údaji s řádnou péčí, tak aby nedocházelo k únikům Osobních údajů nebo ke zpřístupnění Osobních údajů osobám, které nemají oprávnění.

3.2 Ochrana elektronických dokumentů (evidence) a ochrana před neoprávněným přístupem do sítě je zabezpečena přístupovým heslem, data jsou šifrována, společnost má HW firewall. Přístupová hesla jsou měněna každý 3. měsíc.

3.3 Ochrana před neoprávněným přístupem do prostor Společnosti je zabezpečena uzamykáním vchodových dveří

3.4 Ochrana analogových dokumentů (evidence) před neoprávněným kopírováním a užitím je zabezpečena uložením v uzamčené skříni. Každý analogový dokument podléhá dokumentaci.

3.5 Osobní mobilní zařízení a osobní počítače mohou být využívány k přístupu do systémů Organizace pouze se souhlasem Příslušné osoby.

3.6 Tato směrnice se vztahuje na každého Pracovníka Organizace, když zpracovává osobní údaje nebo plní jinou činnost, která je upravena v GDPR.

3.7 Každý Pracovník, jehož se tato směrnice dotýká bude proškolen na ochranu osobních údajů dle této směrnice a proškolení své osoby stvrdí podpisem.

Čl 4 DPO

4.1 Organizace bude mít nepřetržitě jmenovaného DPO počínaje dnem 25.5.2018.

4.2 DPO je jmenován Organizací.

4.3 Organizace zajistí, aby DPO nedostával žádné pokyny týkající se výkonu jeho úkolů.

4.4 V případě změny DPO pověří nový DPO vhodné pracovníky Organizace, aby dle požadavků GDPR informovali Subjekty údajů, jejichž Osobní údaje Organizace zpracovává, o nové osobě DPO a kontaktních údajích na sebe.

4.5 DPO vykonává alespoň tyto úkoly ve smyslu čl. 39 GDPR:

i) poskytování informací a poradenství pracovníkům Organizace kteří provádějí zpracování osobních údajů, o jejich povinnostech podle GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany osobních údajů;

ii) monitorování souladu Organizace prováděného zpracování s GDPR, dalšími předpisy Unie nebo členských států v oblasti ochrany osobních údajů a s koncepcemi Organizace v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;

iii) poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 GDPR;

iv) spolupráce s dozorovým úřadem a působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování osobních údajů, včetně předchozí konzultace podle čl. 36 GDPR, a případně vedení konzultací v jakékoli jiné věci.

Čl 5 PŘÍSLUŠNÉ OSOBY

5.1 Agenda Příslušných osob se skládá zejména z prevencí incidentů, zabezpečením zpracování osobních údajů, řešením stížností a žádostí, správou systémů a dalšími činnostmi.

5.2 Příslušné osoby jsou uvedeny v příloze č. 1 této Směrnice a obsahuje seznam osob s uvedením rolí.

Čl 6 ZPRÁVA O POSOUZENÍ VLIVŮ

6.1 Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody subjektů údajů, provede Organizace před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.

6.2 Zpráva o posouzení vlivů se zpracovává dle čl. 35 a násl. GDPR. Pro soubor podobných operací zpracování, které představují podobné riziko stačí jedno posouzení.

6.3 Posouzení vlivu se zpracuje vždy pro:

i) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;

ii) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10 GDPR; nebo

iii) rozsáhlé systematické monitorování veřejně přístupných prostorů.

6.4 Posouzení obsahuje alespoň:

i) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů Organizace;

ii) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;

iii) posouzení rizik pro práva a svobody subjektů údajů; a

iv) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu.

6.5 Organizace si vždy vyžádá posudek DPO ke zprávě o posouzení vlivů.

6.6 Pokud ze zprávy o posouzení vlivů vyplývá, že by předmětné zpracování osobních údajů mělo za následek vysoké riziko pro práva a svobody subjektů údajů v případě, že by Správce nepřijal opatření ke zmírnění tohoto rizika, Organizace konzultuje zprávu o posouzení vlivů s Dozorovým úřadem.

Čl 7 KOMUNIKACE SE SUBJEKTY ÚDAJŮ

7.1 Pracovník, který obdržel v jakékoliv formě jakoukoliv žádost či stížnost fyzické osoby, která se týká nebo by se mohla týkat ochrany osobních údajů, zejména žádosti ve smyslu čl. 15–22 GDPR, oznámí tuto skutečnost Příslušné osobě.

7.2 Pokud se osobní údaje týkající se subjektu údajů získávají od subjektu údajů, poskytne pověřená osoba v okamžiku získání osobních údajů subjektu údajů informace dle čl. 13 GDPR, v případě, že osobní údaje nebyly získány od subjektu údajů, poskytne pověřená osoba tyto informace v souladu s čl. 14 odst. 3 GDPR.

7.3 Povinnost poskytnout uvedené informace lze splnit odkazem na zásady ochrany osobních údajů Organizace dostupné na internetové adrese Organizace (www.radostinnadoslavou).

7.4 Příslušná osoba vyřizuje požadavky subjektů údajů v souladu s obecnými pokyny Organizace, bez zbytečného odkladu, nejdéle však do 1 měsíce, a aby mu byly k vyřízení jeho žádosti poskytnuty veškeré informace a v případě, že žádosti nebylo vyhověno, aby byly sděleny důvody tohoto rozhodnutí.

7.5 Pokud není možné dodržet lhůtu, Příslušná osoba tuto skutečnost okamžitě oznámí nadřízenému zaměstnanci nebo DPO, včetně uvedení důvodu, proč není možné lhůtu dodržet, a vyžádá si konzultace, jak správně postupovat dále.

7.6 Neexistuje-li obecný pokyn Organizace k řešení konkrétního požadavku, vyžádá si příslušná pověřená osoba pokyn od DPO.

7.7 Ověřování identity subjektu údajů bude prováděno vždy přiměřeným způsobem, který zaručí dostatečnou identifikaci subjektu údajů s ohledem na formu podání, využitý komunikační prostředek a obsah žádosti subjektu údajů.

7.8 V případě žádosti subjektu údajů o přístup k osobním údajům poskytne příslušná pověřená osoba subjektu údajů nejméně informaci, zda osobní údaje, které se subjektu údajů týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, poskytne mu osobní údaje subjektu údajů a informace o:

i) účelu jejich zpracování;
ii) kategoriích dotčených osobních údajů;
iii) příjemcích nebo kategoriích příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemcích ve třetích zemích nebo v mezinárodních organizacích;
iv) plánované době, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritériích použitých ke stanovení této doby;
v) existenci práva požadovat od společnosti opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování;
vi) právu podat stížnost u dozorového úřadu;
vii) veškerých dostupných informacích o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;
viii) skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

7.9 Informace podle tohoto článku poskytuje Organizace subjektu údajů ve stejné formě, v jaké o informace subjekt údajů požádal.

7.10 V případě opakovaných žádostí subjektu údajů je subjektu údajů účtováno 500,- Kč za každou opakovanou žádost.

Čl 8 OZNAMOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ A POSTUP PRO ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ

8.1 Jakékoli porušení zabezpečení osobních údajů dle ustanovení čl. 4 odst. 12 GDPR společnost bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděla, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.

8.2 Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

8.3 Ohlášení dozorovému úřadu se děje prostřednictvím aplikace datové schránky.

8.4 Veškeré případy porušení zabezpečení osobních údajů společnost oznámí a konzultuje s DPO.

8.5 Ohlášení dozorovému úřadu podle tohoto článku musí přinejmenším obsahovat:

i) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

ii) jméno a kontaktní údaje DPO nebo jiného kontaktního místa, které může poskytnout bližší informace;

iii) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

iv) popis opatření, která Organizace přijala nebo navrhla k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

8.6 Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí Organizace toto porušení bez zbytečného odkladu subjektu údajů.

8.7 Pracovníci hlásí případy porušení zabezpečení Příslušným osobám.

8.8 Organizace přijme opatření k zabránění opakovaného porušení zabezpečení osobních údajů obdobného charakteru.

Čl 9 KONTROLA DODRŽOVÁNÍ SMĚRNICE

9.1 Dohled nad dodržováním této směrnice a závazných právních předpisů vykonává Organizace.

9.2 V případě jakýchkoli pochybností o výkladu této Směrnice či rozsahu a obsahu zákonných povinností poskytuje Organizace závazný výklad, kterým jsou povinni se řídit.

Čl 10 PŘÍLOHY

Nedílnou součástí této směrnice je 1 příloha.

V Radostíně nad Oslavou dne 24.5.2018

…….

Obec Radostín nad Oslavou

PŘÍLOHA Č. 1 O PŘÍSLUŠNÝCH OSOBÁCH KE SMĚRNICI Č. 5/2018

Jméno a příjmení	Zařazení v Organizaci	Agenda Příslušné osoby
Antonín Váša	Starosta	Kontaktní osoba